Draft Telecoms Security Resilience Guidance

Guidance for telecoms providers on resilience-related security duties under the Telecommunications (Jersey) Law 2002

Document No: JCRA 25/21 Publication date: 8 August 2025

Jersey Competition Regulatory Authority
2nd Floor Salisbury House, 1-9 Union Street, St Helier, Jersey, JE2 3RF
Tel 01534 514990

Web: www.jcra.je

Document history

Release date	Changes from previous version
08/08/2025	N/A

Contents

1 Overview: Resilience Guidance

Islanders and local organisations depend on reliable communications networks and services to help organise, operate and manage their lives, activities and businesses. More than ever, being able to connect with people, other organisations, applications and relevant information is considered highly important – and even critical – to everyday modern life.

At the same time, telecommunications systems are becoming more complex in their design and operation, which may lead to an increased likelihood of communication network or service failure. The world is also becoming increasingly fragmented, unpredictable and even threatening, with communications networks and services presenting a potential target for malicious actors seeking to disrupt, exploit or harm individuals, organisations and even national economies.

Jersey is not immune from such challenges, which are likely to continue growing and evolving. Recognising this, the Government of Jersey developed a comprehensive telecoms security framework designed to increase the security and reliability of the Island's telecommunications networks and services. The approach and structure of this framework, which aligns closely with that operating in the UK, includes a range of legally defined security measures and guidance on how to achieve compliance. It also supports adherence to licence conditions relating to networks and services resilience and reliability under licences issued to telecoms providers operating a telecommunications system.

The local telecoms security framework gives the Jersey Competition Regulatory Authority (the **Authority**) legal powers and duties to oversee the telecoms security framework's operation and to work with telecoms providers to ensure its effectiveness. Given the Government of Jersey's decision to align its telecoms security framework closely with that of the UK, the Authority has chosen an approach to its telecoms security functions that aligns closely with that of UK communications regulator Ofcom, while also considering the local context where appropriate. This approach supplements the Authority's existing powers under licences issued to telecoms providers.

Among legal requirements is for telecoms providers to reduce the risk of anything occurring that compromises the availability, performance or functionality of their networks and services. This means designing and operating communications systems that are inherently reliable, for the benefit of Islanders and local organisations.

This document contains guidance for telecoms providers which are legally required to design and operate inherently reliable communications systems. The information it contains is not legally binding and telecoms providers may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in this document.

However, should the Authority need to investigate any telecoms security incidents or licence condition contraventions relating to reliability and resilience, then it may use the guidance provided in this document as the basis for examining a telecoms provider's decision-making and actions. In this case, telecoms providers may need to explain why they have chosen a different approach.

This guidance is intended to be read alongside, and serves as a complement to, two other closely related documents within the telecoms security framework:

(1) **Telecoms Security Code of Practice**: deals primarily with the measures providers should adopt to protect networks and service from cyber attacks.

(2) **Telecoms Security Procedural Guidance**: explains the processes operated by the Authority to deliver its telecoms security functions.

The Authority will keep all its telecoms security functions under review and may amend and reissue this guidance from time-to-time. In this case it will consult on any proposed changes and take reasonable steps to ensure telecoms providers are aware of them.

2 Introduction and background

Jersey's telecoms security framework

2.1 The Telecommunications Law (Jersey) Amending Regulations 2024 (the **Amending Regulations**) amended the Telecommunications (Jersey) Law 2002 (the **Law**) with the aim of increasing the security and reliability of Jersey's vital telecoms sector through creating a new telecoms security framework. Providers of public electronic communication networks and services (**Providers**) must comply with the requirements of this telecoms security framework, which relates to both cyber incidents and resilience incidents. This document contains guidance (the **Resilience Guidance**) issued by the Authority under the Law to ensure the reliability and resilience of communication networks and services used by Islanders and local organisations. This section introduces the Resilience Guidance and includes the following content:

- About public telecoms providers
- The legislative framework
- The Authority's role in the telecoms security framework
- About this guidance
- Further sources of information

About public telecoms providers

PECNs and PECSs

2.2 Before amending, the Law only applied to Providers running a telecommunications system, through conditions set out in licences issued by the Authority. The Amending Regulations create a new telecoms security framework which introduce a range of telecoms security duties that apply to both providers of public electronic communications networks (**PECNs**) (which includes Providers running a telecommunications system) and public electronic communications services (**PECSs**).

2.3 These are defined by Article 24A of the Law as being:

> "public electronic communications network" (PECN) means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.
>
> "public electronic communications service" (PECS) means an electronic communications service that is provided so as to be available for use by members of the public.

Providers of both PECNs and PECSs should be aware of their duties under the Law as amended by the Amending Regulations and, where applicable, licence conditions.

Publicly available service

2.4 For clarity, the Authority considers that "Public Electronic Communications Service" means any electronic communications service that is generally available for use by any and all members of the public who are both willing to pay for it and to accept the associated terms and conditions. A publicly available service is distinguishable from a bespoke service restricted to a limited group of individual and identifiable customers.

2.5 Furthermore, the term *members of the public* is not limited to residential or small business customers but also corporate or commercial customers including wholesale network connectivity or services provided to other Providers or businesses.

The legislative framework

The overarching duties set out in the Law

2.6 The Amending Regulations strengthened the Law by imposing additional security duties for all Providers of public telecoms networks and services in Jersey. Article 24K of the Law 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.

2.7 Article 24M of the Law sets out further overarching duties requiring Providers to take appropriate and proportionate measures to stop a security compromise causing adverse effects, and if this happens, to take appropriate and proportionate measures to remedy or mitigate that effect. Article 24S of the Law establishes a duty to report the risk of security compromise to the Authority and to inform users, and Article 24T establishes a duty to report occurrence of security compromises.

Security compromise includes resilience incidents

2.8 Among other things, Article 24K(2) of the Law defines a security compromise as:

(a) anything that compromises the availability, performance or functionality of the network or service;

and

(b) anything that causes signals conveyed by means of the network or service to be lost.

2.9 Based on this definition, a security compromise includes both "cyber security type" compromises such as those caused by malicious actors and resilience related compromises reflecting a broad range of other factors that impact on the availability of PECNs and PECSs. These include impacts caused by external factors, such as floods, cable cuts or power cuts, or internal factors, such as hardware failures, operational process errors or network design flaws.

2.10 Impacts of the type mentioned in Paragraph 2.9 above are mostly associated with threats to network and service availability, reliability and resilience. The protective measures Providers can take to minimise the risk of these factors impacting on availability include increasing resilience through redundancy and capacity planning, hardware and software maintenance, hardening and change management capabilities.

2.11 This Resilience Guidance applies to the category of security compromises and contraventions of licence conditions (see Paragraph 2.19 below) relating to the reliability and resilience of communications networks and services, in terms of their availability, performance or functionality, termed from this point forward as "**Resilience Incidents**".

Duties to take specific measures imposed by the Minister by regulations

2.12 Under the Law, the Minister for Sustainable Economic Development (the **Minister**) has powers to make an order requiring certain Providers to take specified security measures or measures of a specified description. Exercising these powers, the Minister issued the Telecommunications (Security Measures) (Jersey) Order(202x) (the **Security Measures Order**), which came into force on (Day, Month, Year).[1]

2.13 These Security Measures also apply in respect of Resilience Incidents, supplementing the duties imposed on Providers by Articles 24K and 24M of the Law. They require Providers to take specified security measures including in relation to:

- Network architecture
- The protection of data and network functions
- Preparing for remediation and recovery
- Governance
- Reviews

[1] This paragraph to be fully completed following passing of the Security Measures Order.

- Protection of certain tools enabling monitoring or analysis, monitoring and analysis
- The supply chain
- The prevention of unauthorised access or interference
- Patches and updates
- Competency
- Testing
- Assistance

2.14 The Security Measures Order also identifies those Providers to which the Security Measures apply.

Guidance given by the Minister in codes of practice

2.15 The Amending Regulations give the Minister power to issue codes of practice which give guidance to Providers on the Security Measures to be taken under Articles 24K-24N of the Law. Under this power, the Minister issued the [Draft] Code of Practice (the **Code of Practice**), which gives guidance on Security Measures which mainly relate to cyber type security incidents such as those caused by malicious actors.[2]

2.16 It should be noted that the guidance provided in this Resilience Guidance is relevant to all Providers, regardless whether the Security Measures apply to them or not.

Further requirements for Providers to run resilient communication networks and services

2.17 Alongside the security duties imposed under the Amending Regulations, the Law requires both the Authority and Providers to comply with other reliability requirements.

2.18 For the Authority, this means having regard to Article 7(3)(a) of the Law, which requires consideration whether communication networks and services are provided, both within Jersey and between Jersey and the rest of the world, that are high quality and reliable.[3]

2.19 For Providers, this means complying with licence conditions relating to operating networks and services that are resilient and reliable particularly in relation to the provision of public emergency call services.

The Authority's role in the telecoms security framework

General policy on ensuring compliance with resilience-related security duties

2.20 The Authority has issued Procedural Guidance[4] under the Law explaining how it will carry out its functions to ensure compliance with security duties including providers' reliability and

[2] This paragraph to be fully completed following passing of the Security Measures Order.
[3] States Assembly: Telecommunications (Jersey) Law 2002 – see here for more information.
[4] Jersey Competition Regulatory Authority: Draft Procedural Guidance – see here for more information.

resilience-related security duties, both in the context of compliance monitoring and enforcement. These functions include:

- Information gathering powers under Article 24ZC of the Law;
- Powers to direct Providers to explain any failure to act in accordance with the Code of Practice under Article 24R of the Law;
- Assessment powers under Schedule 2, Part 2 of the Law; and.
- Enforcement powers under Schedule 2, Part 2 of the Law.

Receiving and assessing risk and occurrence of Resilience Incidents

2.21 Article 24S of the Law requires Providers to take reasonable and proportionate steps to inform end-users who may be adversely affected by any significant risk of security compromise of a PECN or PECS.

2.22 Article 24K of the Law requires Providers to inform the Authority 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 requirement includes the occurrence of a Resilience Incident.

2.23 Section 4 of the Procedural Guidance explains the Authority's expectations of Providers in relation to reporting the risk and occurrence of security compromises including those relating to any Resilience Incident. This includes which security compromises to report, when to report and the information required.

2.24 In analysing any reported Resilience Incident, the Authority will seek evidence to understand:

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

Enforcement actions following a Resilience Incident

2.25 The Authority has a general duty under Article 24V of the Law to ensure compliance with security duties. Where Resilience Incidents are not resolved to its satisfaction through engagement with Providers, the Authority may consider the use of enforcement powers. When

assessing whether to open a formal enforcement investigation, the Authority will consider the specific circumstances of the case to decide on the appropriate course of action.

2.26 Section 5 of the Procedural Guidance explains the Authority's approach to enforcement under the telecoms security framework.

The purpose of this Resilience Guidance

2.27 This document contains guidance to Providers required by the Law to comply with expectations and responsibilities established through the telecoms security framework and in licence conditions so that robust and resilient communication networks and services are available for use by Islanders and local organisations.

2.28 It describes a range of good practice approaches in the architecture, design and operational models that underpin robust and resilient communication networks and services. These models are drawn from local experience and guidance provided elsewhere, including in the UK and by the European Union, suitably adapted where proportionate and appropriate for the Jersey context. They should be flexible enough to apply to all Providers while allowing for continued technology evolution and innovation.

2.29 It also sets out the Authority's key expectations on how Providers should adopt these good practice models while also informing the approach taken to assessing and potentially investigating the risk and occurrence of Resilience Incidents reported to the Authority under its security compromise reporting function.[5]

2.30 This Resilience Guidance is produced under Article 24Y and Article 58 of the Law to set out the measures the Authority expects Providers to take in relation to the availability, performance and functionality (or resilience) of their telecommunication networks and services under security duties imposed by the Law. This includes duties imposed under the Security Measures Order and those contained in licence conditions relating to the resilience and reliability of networks and services, and where applicable, in the Code of Practice.

2.31 The Authority will use this Resilience Guidance as a practical reference both:

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

2.32 This Resilience Guidance supersedes and replaces any previous guidance given by the Authority on general network and service resilience and reliability.

[5] Jersey Competition Regulatory Authority: Draft Procedural Guidance – see here for more information.

2.33 The Code of Practice focuses primarily on measures to address cyber security aspects of the security duties imposed by or under the Law, while this Resilience Guidance focuses on other aspects of network and service reliability and resilience. In relation to those Providers to which the Code of Practice applies, this document is intended to be read in conjunction with the Code of Practice, which the Authority will refer to where appropriate.

2.34 The guidance in this document is not the only way for Providers to comply with their resilience-related security duties under the Law. A Provider may choose to comply with their resilience-related security duties by adopting different technical solutions or approaches to those specified in this document. What is appropriate and proportionate will depend on the particular circumstances of the Provider. However, this Resilience Guidance is intended to set out the general approach the Authority would normally expect to take in investigating compliance with resilience-related security duties under the Law or a licence condition as appropriate. Where a Provider has taken a different approach to that set out in this guidance, the Authority would expect them to be able to explain their reasons for doing so.

Further sources of information

2.35 In addition to the guidance contained in this document, Providers can gain related information from a range of other relevant sources, including:

ENISA's Technical Guidance on Security Measures[6]	Gives guidance in relation to appropriate risk assessment, ongoing risk management, operations and business continuity management.
ENISA's Enabling and Managing End-to-End Resilience[7]	Provides a broad and comprehensive introduction to both technical and organisational requirements for developing and maintaining resilient communication networks and services.
EC-RRG Resilience Guidelines[8]	Includes further technology updates to the above ENISA guidance for areas such as All IP Networking, Virtualisation and 5G.
NPSA Guidance on Protecting Buildings and Infrastructure[9]	The National Protective Security Authority has published online guidance on protecting buildings and infrastructure.

[6] ENISA: Guideline on Security Measures under the ECC – see here for more information.
[7] ENISA: Enabling and managing end-to-end resilience – see here for more information.
[8] EC-RRG: Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure – see here for more information.
[9] NPSA: Building & Infrastructure – see here for more information.

3 Key concepts and drivers related to resilience and reliability

Introduction

3.1 The concept of resilience applies to a wide range of settings and scenarios. In this section, the Authority outlines its core position on resilience as it relates to Jersey's communication networks and services. It also highlights a range of relevant risks to resilience that Providers should be aware of and address. Its contents include:

- The breadth of resilience concerning Providers
- Background factors relating to network resilience and reliability
- Relevant risks to network and service resilience

The breadth of resilience concerning Providers

3.2 Achieving an overall aim of ensuring resilient and reliable communication networks and services requires Providers to consider several related factors:

- **Infrastructure**: How reliable and well-connected are the physical components and transmission media comprising and underpinning communication networks and services?;
- **Processes**: How robust are the processes in place to support the full lifecycle of networks and services from inception, through delivery, in-life to decommissioning?; and
- **Availability**: Hower well-engineered is the infrastructure and processes to deliver the appropriate levels for the availability for network and services?

Background factors driving an emphasis on network resilience and reliability

Technology and service evolution

3.3 The technology associated with communication networks and services has continually evolved, often at a rapid rate. Recent years have seen numerous important and influential developments including rollout of Fibre to the Premises (FTTP), Internet of Things (IoT), 5G and Low Earth Orbit (LEO) satellite constellations. Digitisation within the telecoms sector has continued at a pace, allowing the adoption and rollout of Internal Protocol (IP) services, while virtualisation using cloud-based computing has revolutionised network infrastructure.

3.4 Jersey's Providers have responded to and embraced these trends where it has been appropriate and practical in the Island context. Islanders and local organisations have benefitted as a result, with little discernible disadvantage in choice and timeliness compared with communication networks and services available in comparable or larger jurisdictions. It is reasonable to expect that this situation will continue into the future.

3.5 Technology developments have the potential to improve the reliability and resilience of communications networks and services, through advancements including easier deployment of redundant systems, automated fault detection and self-healing networks, and real-time threat intelligence. However, technology and service evolution can also create new risks, such as those associated with power-loss on all IP-networks, technology immaturity and complex dependencies, and the consolidation of services and high reliance on third parties.

Impact of climate change

3.6 There is overwhelming scientific evidence that climate change is happening throughout the world and impacting on communities everywhere, including in Britain and the Channel Islands. One result can be storms causing widespread damage or severe flooding leaving premises uninhabitable or unusable. Jersey experienced Storm Ciarán in 2023, which saw high winds lash the Island and a tornado causing unprecedented destruction across a swathe of the Island.[10] In that same year, major flooding following heavy rains led to the Government of Jersey declaring a major incident after water entered numerous properties in the Grands Vaux area.[11]

3.7 Jersey benefits from having the distribution of its telecoms cable networks delivered mostly through underground ducts rather than having to rely on potentially more vulnerable overhead infrastructure. However, the electricity supply may be disrupted by strong winds through loss of overhead power distribution following a storm, and flooding along with freak weather conditions may affect end-user premises or sites housing electricity grid infrastructure and telecoms network infrastructure. Extreme weather also presents a risk to mobile networks which rely on both physical switching and external infrastructure.

3.8 Taking climate change into account means assuming more instances of extreme weather events affecting Jersey in the future. As a result, it could become increasingly likely that the Island could experience significant communications outages that may threaten human life. In these cases, the resilience of Jersey's communications networks to maintain services, particularly access to the emergency services, is made more important.

Societal dependence on telecoms

3.9 The way people use communications networks and services has changed considerably in recent years as the global development of technology and devices permitted new and enhanced applications and interactions. Jersey is as much a part of this trend as elsewhere, with Islanders of all ages becoming increasingly dependent on the ability to access communications and information to help run their lives and organisations.

[10] BBC: Battered Jersey Deals with Storm Ciarán aftermath – see here for more information.
[11] BBC: Jersey households still in hotels after major Grands Vaux flooding – see here for more information.

3.10 This indispensable nature strongly highlights a level of societal dependence on communications – a factor likely to increase as emerging services made possible by technology developments increase interaction, automation, remote monitoring and enable safety critical functions.

3.11 Communications networks and services further remain essential for the general safety and security of Islanders and visitors to Jersey through providing assured access to the local emergency services through calling 999 or 112.

Economic dependency

3.12 Jersey's role as an international finance centre and its reputation for providing high-quality finance services is strongly dependent on the availability, reliability, resilience and security of both on- and off-island communications networks and services. Any significant telecommunications disruption could disproportionally impact on the Island's economy, should organisations or individuals perceive a risk of or experience outages for even short periods of time.

3.13 While other Island industries may be less dominant than finance, all will require communications to operate successfully, with the reliance on communication networks and services only likely to increase as automation and artificial intelligence play an increasing role.

3.14 The Government of Jersey seeks to encourage new industries to the Island, with emphasis on digitally-focused organisations and individuals. Access to world-class communications infrastructure is likely to be a prerequisite for many prospective incoming entities as well as home-grown talent.

Reliance on critical national infrastructure

3.15 Governments globally are recognising the critical need to protect nationally important infrastructure from external threats and to increase resilience and recoverability capabilities. Among infrastructure in this category are power generation and distribution, health provision, transport networks and water supplies.

3.16 Recognising the need for local focus and expertise, the Government of Jersey established a function in 2021 focused on driving up cyber resilience, which evolved subsequently to become the Jersey Cyber Security Centre (**JCSC**).[12] The JCSC's stated role is to promote and improve the Island's cyber resilience using a team of experts to support critical national infrastructure, business communities and citizens to prepare, defend and respond to cyber attacks in Jersey.[13]

[12] The Government of Jersey: Cyber resilience team established – see here for more information.
[13] JCSC: About Jersey Cyber Security Centre – see here for more information.

3.17 The Government of Jersey took further steps to improve the resilience of local critical national infrastructure with the development of a Cyber Security Law in 2024.[14] This law's focus is on developing best practice cyber defence among Operators of Essential Services (**OES**) and establishing the independent objectives and functions of the JCSC.

3.18 A source of support for local OES (including telecoms providers) is information and advice issued by the UK National Infrastructure Commission (NIC).[15] It published a report in 2020 called 'Anticipate, React and Recover' that presents a framework featuring six aspects of reliability and resilience, which together capture the range of possible actions to take to deliver resilient infrastructure systems:[16]

(1) **Anticipate:** actions to prepare in advance to respond to shocks and stresses, such as collecting data on the condition of assets.

(2) **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.

(3) **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.

(4) **Recover**: actions that help quickly restore expected levels of service following an event, such as procedures to restart services following a nationwide loss of power.

(5) **Adapt**: actions that modify the system to enable it to continue to deliver services in the face of changes.

(6) **Transform**: actions that regenerate and improve infrastructure systems.

3.19 While the NIC guidance is relevant for all CNI providers, the six aspects or resilience shown in Paragraph 3.18 above provides useful guidance to Providers required by Article 24K of the Law to take appropriate and proportionate measures to identify and reduce the risks of, and prepare for, security compromises (including network or service outages) occurring. This aligns with anticipate, resist, and absorb stages of the NIC framework.

3.20 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 NIC framework's recover stage. These principles should be backed by longer term adaptations and transformations to be better prepared and recover quicker when future shocks occur.

---

[14] The Government of Jersey: work began in 2024 to develop the Cyber Security Law, which is expected to be enacted in late 2025 or early 2026 – see here for more information.
[15] National Infrastructure Commission – see here for more information.
[16] National Infrastructure Commission: Anticipate, React, Recover, Resilient Infrastructure Systems (May 2020) – see here for more information.

Relevant risks to network and service resilience

3.21 In view of the background factors explained in this section, the Authority expects Providers to carry out systematic and wide-ranging assessments to identify potential risks to network and service resilience and reliability before deciding on the appropriate and proportionate measures that need taking to meet relevant duties under the Law. Among risk areas to consider are:

External physical threat/shocks

3.22 External 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 accidents, vandalism, internal sabotage and terrorism

Human risks

3.23 Human risks 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

Technology, physical and cyber security vulnerabilities

3.24 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)

- Electromagnetic Interference (EMI) such as Electromagnetic Pulses (EMP), malicious electronic interference, geomagnetic induced currents and other space weather phenomenon
- 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"

Loss of key dependencies

3.25 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 telecoms and associated infrastructure

Architecture/design vulnerabilities and failings

3.26 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.

3.27 Many physical and logical component functions of networks can exist as multiple instances in networks for the purpose of reliability and 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.

3.28 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 a shared fate on the single site or duct. If the site or duct fails, they all fail.

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

Software failures

3.30 Communications 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.

3.31 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.

Critical third parties (managed service partners and wholesale network/service providers)

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

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

4 Scope of Provider network and services resilience

Introduction

4.1 This section examines and explains the Authority's approach to the scope of Provider network and services reliability and resilience and related concepts and considerations. Its contents include:

- PECN and PECS network and services scope
- Resilience in the context of Providers
- Infrastructure – network domains overview

PECN and PECS network and services scope

4.2 This Resilience Guidance applies to all Providers of both PECNs and PECSs in the context of their security duties under the Law, and under conditions in licences issued under the Law.

4.3 Each 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 Provider, including as part of managed service arrangements.

4.4 This Resilience 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 Provider, meaning Providers' communications networks and services. This also includes interconnections from the 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-IP) or to the demarcation (peering/interconnect) interfaces with content providers, application providers, Content Delivery Networks (CDNs), internet transit providers or other communications providers.

4.5 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-users.

Resilience in the context of Providers

4.6 As explained above, the guidance set out in this document applies to the sub-category of security compromises relating to the resilience of communications networks and services, in terms of their availability, performance or functionality, which the Authority refers to as Resilience Incidents.

4.7 The Authority interprets 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.

4.8 The Authority notes that the UK's EC-RRG Group[17] provides resilience guidelines for providers of critical national telecommunications infrastructure[18], which explains that resilience can be seen to include:

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

4.9 The Authority expects all 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. 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 Code of Practice, the Authority would expect that 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)

4.10 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

[17] 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). See here for more information.

[18] EC-RRG, 2018: EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure – see here for more information.

cycle.[19] Section 5 of this Resilience Guidance takes key parts pertinent to the processes supporting the availability of communication services.

4.11 In some cases, Providers might not operate all component parts of the network or service that they provide. For example, a 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 procure underlying network services or infrastructure from other Providers. In such cases, the overall resilience of the Provider's services inherently depends on these other parties.

4.12 However, as stated in Paragraph 4.3 above, overall responsibility remains with the Provider to take appropriate and proportionate measures to ensure the security and resilience of the communication networks and services they are providing, where they are providing a PECN or a PECS.

4.13 Providers may seek service level agreements and contractual arrangements to meet their overall reliability and resilience requirements. But it is potentially more effective to ensure that all such external suppliers take a similar and complementary approach to resilience management.

4.14 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

Infrastructure – network domains overview

4.15 The following sub-section provides a high-level overview of the key network domains that typically form part of a Provider's network. Section 5 of this Resilience Guidance then provides technical guidance for each of these domains.

Network infrastructure domains

[19] 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)?. See here for more information.

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

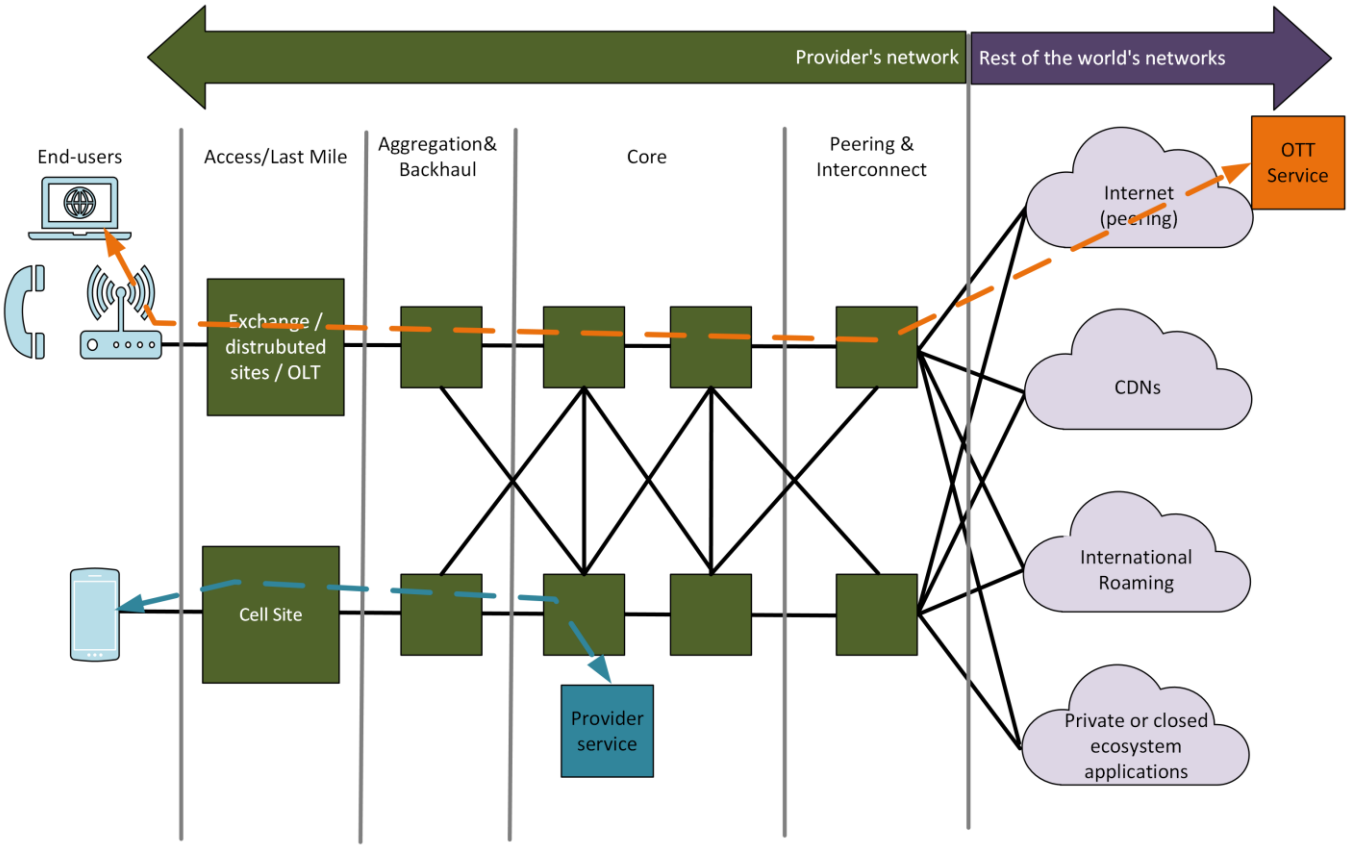
- Access/last mile: wireless/mobile air interface and fixed access
- Aggregation/backhaul: mobile backhaul and fixed aggregation
- Core: small number of sites containing critical network functions or having critical importance
- Peering and interconnect

4.17 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)

4.18 Figure 1 below illustrates a high-level representation of the typical network domains within an end-to-end communications network, and their relative scale for a national UK network. This diagram is not intended to indicate that all networks' topologies or domain hierarchies must align exactly to this.

Figure 1: Typical provider network infrastructure domains



4.19 It is expected that some sites used by multiple Providers may be treated as part of different areas or domains in each case. For example, a wholesale fixed access provider may use the term “core” for some of their sites. However, other Providers using the wholesale providers network may consider these sites to be “access” and “aggregation” rather than “core”.

4.20 Additionally, not all of the domain/site types will be present in all networks. Some Providers may collapse different domain tiers together. For example, some Providers may use co-location data centre sites (aka “tele-hotels”) for both “core” and “peering and interconnect” purposes. This approach may provide a cost effective way to achieve appropriate resilience along with other architectural and interconnection synergies.

4.21 In these various topological cases, the specific resilience approaches and designs may vary, while still being appropriately resilient. Because there are many different possible topology variations, it is not feasible to attempt to capture them all in this Resilience Guidance.

4.22 When using this Resilience Guidance, the Authority will take into account these potential variations and the topology of the network in question.

Access/Last mile

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

- 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, Hybrid Fibre Coax (HFC), FTTP (Active Ethernet), FTTP (xPON) to the end-user premises
- Non-3GPP wireless access – Fixed Wireless Access and non-terrestrial networks such as Low Earth Orbit satellites[20,21]

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

4.25 The biggest reliability and 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.

[20] Fixed-Wireless-Access networks typically have similar network topology domains as Fixed or Mobile networks as shown in Figure 1. As such, this guidance will apply to FWA networks.

[21] Non-Terrestrial-Network topologies can vary from the topology in Figure 1 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 communication networks and services to maintain the overall objectives.

4.26 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
- Cost/investment and associated risk
- Spectrum availability, propagation conditions and cost (for wireless technologies)
- Regulatory environment
- Competition landscape
- Planning permissions limitations

4.27 Some of these factors are not within a Provider's direct control, nor under the Authority's current regulatory remit.

Aggregation/backhaul

4.28 Aggregation/backhaul networks are different to the core and "last mile" domains for a variety of reasons. The number of sites and geographical spread of the aggregation/backhaul domain are typically far greater than the core domain though notably in smaller jurisdictions such as Jersey the requirement to implement a significant number of these sites distinct to core sites is reduced. In this domain the level of physical connectivity resilience may be less than the core domain. Nonetheless aggregation/backhaul sites are expected to be built with an appropriate degree of physical resilience regarding equipment, physically separate/diverse connectivity and power backup.

4.29 The two most typical variants of this domain, based on volume of deployment are:

- Fixed aggregation network – This includes connectivity between customer premises, any remote distribution facilities 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 as required.
- 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.

4.30 In these sub-domains, locations like mobile base stations are often connected to a single "parent" aggregation site without resilient connectivity. But in cases where greater resilience has been deemed necessary by the Provider, mobile base stations may be equipped with resilient connectivity to the mobile core via additional separate connectivity. Similarly for fixed

access networks, it may be appropriate for some fixed access network sites to have resilient aggregation/backhaul connectivity.[22]

4.31 Providers (at all levels of the supply chain) make architectural topology choices about how many end locations/nodes (and users) to aggregate to intermediate aggregation sites, and if those aggregation sites have onward resilient connectivity 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.

4.32 See Section 5 for specific guidance on this domain.

Core

4.33 The core domain is typically made up of a small number of sites which contain the bulk of the key network control plane functions and Providers' own services and applications. For example, this will often include the mobile core functions, SIP/IMS[23] voice platforms, subscriber authentication databases, policy control functions, DNS resolvers and on-net content caching. In other words, the core sites contain a Provider's most critical network and service functions, and are typically built to the highest levels of resilience practically and economically possible.

4.34 Sites in the core domain 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.

4.35 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 a Provider's level of quality of experience (service reliability) is heavily dependent on a Provider's ability to forecast capacity demands on the network.

4.36 See Section 5 for specific guidance on this domain.

Internet peering and non-internet interconnection

4.37 Providers typically have connections from their networks to other networks for "internet" traffic or content, as well as "non-internet" traffic or content.

[22] A CP may deem greater resilience is necessary for a variety of reasons. In addition to the number of customers/premises served by the site, other potential factors might include things like providing connectivity to hospitals, transport hubs such as airports, shipping ports, or a range of other commercial contracts.
[23] Session Initiation Protocol (SIP) is used for registration and signalling of IP-based voice sessions and calls. 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. IMS makes use of SIP.

4.38 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.

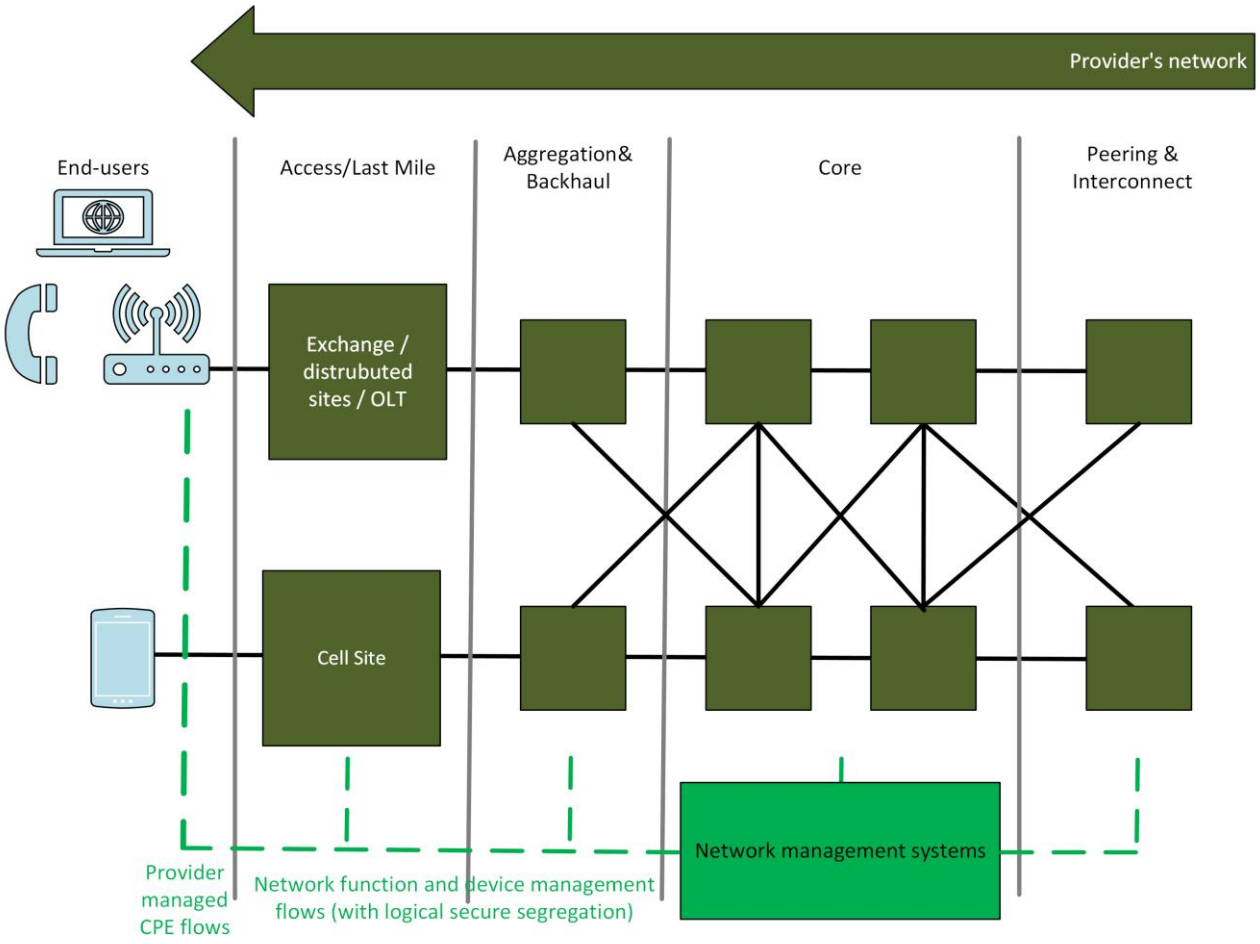
4.39 Non-internet interconnections include use cases such as voice telephony interconnects and international carriage, international mobile roaming and other private connectivity. The scale and the approach to resilience between these different cases can vary significantly. Therefore, the Authority distinguishes between internet-related connectivity (including peering) and non-internet-related interconnection types.

4.40 See Section 5 for specific guidance on this domain.

Network management

4.41 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 2 below provides a pictorial representation of this cross-cutting aspect.

Figure 2: Network management "logical domain"



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

4.43 Figure 2 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 Code of Practice.

4.44 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.

4.45 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 Management Plane Resilience sub-section in Section 5 below for specific guidance on this topic.

4.46 Providers should also refer to the 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 2).

5 Network and service Implementation Resilience Guidance

Introduction

5.1 In this section, the Authority sets out its guidance on the expected measures to be taken by Providers for network and service architecture, design, and implementation under Articles 24K to 24N of the Law. It also reflects the measures expected to be taken to enable a licensee to comply with the relevant licence conditions. Its contents include:

- Basic principles and approach of the Resilience Guidance
- Network infrastructure general physical guidance
- Network infrastructure domains guidance
- Control plane resilience
- Management plane resilience

Basic principles and approach of the Resilience Guidance

5.2 As stated previously, the main objective of this Resilience Guidance is to achieve a good level of resilience and reliability of communication networks and services in Jersey by promoting good practice to be adopted by all types and sizes of Providers.

5.3 This Resilience Guidance has been written with flexibility in mind, in order to be applicable to all Providers and to allow for continued technology evolution. The Authority has set out its expectations in terms of "outcome-based principles" alongside more specific measures including examples where they are needed based on evidence. These examples may be further updated from time to time to include risks and incidents reported under Articles 24S and 24T of the Law.

5.4 As already discussed, the Amending Regulations changed the Law to impose overarching obligations on Providers related to network and service reliability and resilience. Article 3 of the Security Measures Order requires 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.

5.5 The Authority provides guidance below on measures to be taken relating to network architecture, design, and implementation.

Network infrastructure general physical guidance

5.6 The Authority expects Providers to take measures to ensure the general resilience of physical aspects of public electronic communications networks, including giving appropriate

consideration to good practices which apply to the resilience of network infrastructure, and incorporate such good practices into their networks where appropriate.

5.7 The UK's EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure capture a wide range of considerations and good practices in the design and operation of networks. Regarding physical infrastructure in particular, see the section of the UK EC-RRG Resilience Guidelines on design recommendations related to generic physical aspects of communications network resilience.[24]

5.8 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, Providers should refer to the Code of Practice.

5.9 The Authority also expects 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 Guidelines.

5.10 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.

5.11 The Authority lists elsewhere in this Resilience Guidance more specific expectations on the measures which Providers should take regarding loss of power in the following infrastructure domains sections.

Network infrastructure domains guidance

Access/last mile

5.12 As described in the Aggregation/Backhaul sub-section of this Section, 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 (Active Ethernet), FTTP (xPON) to the customer premises

5.13 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.

5.14 All these factors (and more) combine to result in varying levels of user disruption when there is a network or services failure. Therefore, when considering network architecture, design, and

[24] EC-RRG: EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure. See here for more information.

operational models, Providers should put in place measures which specifically consider all these factors.

5.15 Given the scale and geographical reach of network assets within access networks, it can become costly to create highly resilient access networks. The Authority is aware that this domain is likely to have single points of failure, but also understands that the customer concentration should be significantly lower in comparison to the core of networks.

5.16 Access network equipment or locations such as mobile base stations are often connected to a single "parent" aggregation/backhaul site without resilient connectivity.

5.17 However, in order to provide appropriate resilience to core site failures, the Authority would expect Providers to take measures to ensure that network equipment within the access sites supports mechanisms to automatically fail over between core sites, and services should be maintained or re-established automatically. This capability needs to be supported by the aggregation or backhaul network connectivity between the access and core network domains, as covered in the next section.

5.18 In cases where enhanced resilience for a given access network site is deemed appropriate based on the service level requirements (see Paragraph 6.6), Providers should equip mobile base-stations or fixed-access locations with resilient connectivity towards the core network, potentially via an additional aggregation/backhaul site.

5.19 There are multiple design options and approaches for connecting access sites to core sites, with varying degrees of resilience. What is appropriate and proportionate in any given case will depend on the consideration of many factors, such as the number of customers that would be impacted by a given failure, geographical size of the coverage area impacted by a given failure, the service level requirements and criticality of the services being provided, and whether the degree of connectivity resilience is appropriate for the customers being served by that site.

5.20 It may be appropriate to consider the "user-hours-lost" concept (as described in a following sub-section) in conjunction with other considerations regarding the type of services provided and the customers involved.

5.21 On access sites and equipment where a significant 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 Paragraph 3.25 above). Where possible, Providers should seek to mitigate the impact of 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 contact the emergency services. For multiple types of networks, over-reliance on a single source (or path) of network timing/synchronisation is a weakness.

Power backup in fixed access network remote distribution facilities

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

5.23 In the case of new fixed access network deployments, the Authority expects powered "active" components in any remote distribution facilities supporting the provision of infrastructure to customers to have a power backup solution installed.

5.24 When assessing power backup requirements, providers should consider relevant local factors. This includes reviewing published data on the frequency and impact of power outages in Jersey, as well as the availability and prevalence of end-user battery backup solutions.

5.25 Based its assessment of local factors, the Authority considers power backup of approximately four hours to be good practice for active fixed access equipment at the point of installation.

5.26 Should there be an area that is at higher risk of longer or more frequent power outages, the Authority would expect Providers to take this into account and increase the duration of power backup as appropriate.

5.27 As the number or criticality of users served by a site increases, the Authority 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.

Power backup in mobile RAN sites

5.28 In the case of mobile cell sites, in order to meet their duties, Providers should take at least some measures to mitigate against the risks of power outages and support continued operation of their communications services during power outages and surges which might reasonably be expected to occur.

Aggregation/backhaul

5.29 As described in the Aggregation/backhaul sub-section of Section 4, there are two main variants of this domain:

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

5.30 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 end-users and/or premises to aggregate onto a given aggregation site and what reliability and resilience measures to include at the aggregation site. This significantly affects the number of aggregation sites and their geographical distribution.

Aggregating a higher number of customers/premises per aggregation site results in an increased risk of impacting more end-users when failures occur.

5.31 When architecting and designing a network, the Authority would expect Providers to take measures to address such risks, including those explained below.

5.32 Single points of failure are very important in network architecture/design decisions in relation to the number of end-users impacted, the likelihood of failures, the duration of typical impacts (including the typical time to repair), and the criticality of the services being carried by the network. Generally, the Authority would expect Providers to architect and operate their networks to minimise single points of failure that could lead to a significant impact on network service.

5.33 When making architecture, design and operational decisions, Providers should consider the concept of "user-hours lost" as mentioned in the reporting thresholds for security compromises (including Resilience Incidents) in the Authority's Procedural Guidance.[25] Box 1 below provides more information on the concept of user-hours lost.

Box 1: The hours lost concept

The "user-hours lost" figure for any particular incident is calculated by multiplying the number of end-users affected by a service impact and the duration of the service impact.

The Authority considers a service impact to be significant where the user-hours lost figure is equivalent to or above the numerical threshold set out in the tables for fixed and mobile in the Procedural Guidance corresponding to the relevant network/service type. This user-hours lost threshold for incident reporting is calculated by multiplying the minimum number of end-users affected and the minimum duration of service loss or major disruption for the voice or data service/network offered to retail customers.

For example, an interruption to a fixed voice or data service network offered to retail customers, which results in 800 user-hours lost, meets the Authority's threshold for significant disruption. This is based on 100 end-users being affected for eight hours. It is also met by any other combination that results in 800 user hours lost. This would cover larger numbers of end-users disrupted for a shorter period (e.g., 400 customers for two hours). In addition, for a Provider with a smaller customer base, where end-users impacted exceeds 25% of the total number of end-users for an extended period (e.g., 50 end-users for 16 hours).

While the threshold for significant disruption is one criterion for when a security compromise should be reported to the Authority, it is also useful as an architecture/design/operational target to stay below in relation to this Resilience Guidance.

[25] [Link to the Procedural Guidance (jcra.je)]

The Authority expects Providers to consider user-hours lost calculations when making decisions about where to prioritise reliability and resilience measures, including the interplay between the number of end-users affected and the duration.

This Resilience Guidance on how to identify significant service disruption based on user-hours lost does not impact on any aspects of the incident reporting process itself.

5.34 As the number of aggregated end-users/premises increases at an aggregation point in a network, the Authority would expect 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.

5.35 In many cases, it will be expected that onward traffic flows from aggregation sites toward the core will be protected through appropriate resilience mechanisms including fully automatic failover between core sites – making use of separate resilient transmission links – dual parenting to separate core sites, resilient rings, and any other mechanisms that are appropriate.

5.36 Some Providers may adopt quite different approaches in the aggregation/backhaul domain which allow an access site to connect to the core via separate aggregation/backhaul networks, suppliers or disparate technologies.

5.37 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, including battery back-up and electricity generators.

5.38 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.

Core

5.39 Bearing in mind that the most critical network functions reside in the core network domain as stated in the Core sub-section of Section 4, Providers are expected to take measures to ensure the resilience of the core network domain, including the measures set out below.

- Core 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 significant resilient connectivity to other core sites using separate and diverse transmission. This could mean resilient connections to multiple other core sites.
- 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 the Control plane resilience sub-section of this Section, and the management plane.
- 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 site with minimal impact to overall network reliability while maintaining appropriate service levels as per the service level management sub-section of Section 6 (See the Resilience Mechanisms and Approaches sub-section of Section 5 for further discussion on resilience mechanism approaches).
- Core site locations should be selected considering geographical connection diversity and separation, geological hazards like floodplains, extreme weather vulnerability and a range of other potential hazards (as considered in the Relevant Risks to Network and Service Resilience sub-section of Section 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: battery backup and fuel-powered electricity generators. These sites are expected to be able to survive power loss for a minimum of five days, with permanent electricity generators on site which can be refuelled while in operation.

Internet peering and non-internet interconnection

5.40 As previously stated in Paragraph 3.3.4., the Authority distinguishes between internet-related peering and non-internet-related interconnection types.

5.41 The Authority expects 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.

5.42 This means that 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 Providers' networks.

5.43 As part of this, Providers should consider physical and logical routes connecting beyond the Jersey landmass, including subsea cables.

5.44 It is understood that 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.

5.45 Additionally, the wider internet and other interconnects are vectors for unsolicited, abnormal and malicious traffic. Providers should monitor internet peerings and other network interconnections, and perform appropriate traffic management to preserve the integrity and security of the network, of services provided via that network, and of the terminal equipment of end-users (note that network monitoring is covered in further detail in the Processes related to Service Operation sub-section of Section 6).

5.46 Regarding non-internet-related interconnects, Providers are expected to also make use of resilient network elements when connecting to their interconnect partners – as captured in the Control Plane Scaling and Overload Resilience sub-section of Section 5 for example. Furthermore, as per GSMA IR.77[26] Binding Security Requirements and NICC ND1643[27], voice/VoIP/IMS interconnection between networks should be separate from the internet. Providers should also have an appropriately robust operational model to ensure timely fault detection and restoration. These principles are to ensure appropriate service reliability as these voice interconnects are likely to carry emergency service calls and other essential calls.

Control plane resilience

5.47 Networks typically have several different categories of logical and physical planes including user planes, control planes and management planes.[28] This section focuses on the measures the Authority would expect 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 customer sessions and data are 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.

[26] GSMA: IR.77 InterOperator IP Backbone Security Req. For Service and Inter-operator IP backbone Providers v5.0 - Security. See here for more information.
[27] NICC: ND1643V5.1.1 Guidelines on the Minimum Security Controls for Interconnecting Communication Providers. See here for more information.
[28] The user plane is sometimes also known as data plane or forwarding plane.

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

5.49 The guidance contained in this sub-section is not exhaustive in covering every existing or future control plane function or associated protocol. The Authority expects Providers to take resilience and reliability into account for any control plane function or associated protocol that is part of their networks.

5.50 Note that control plane monitoring is covered in the Network Control Plane Monitoring sub-section of Section 6.

Control plane scaling and overload resilience

5.51 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

5.52 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. 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.

5.53 The Authority would expect Providers to take appropriate and proportionate measures to eliminate service impacts if instances of these special control plane functions were to fail, malfunction, respond with unexpected errors or become overloaded.

5.54 Measures the Authority would expect Providers to consider include:

- Network functions which play a part in attaching or authenticating user devices on to the network should be configured with appropriate controls to prevent overload and cascading of overload conditions to other network functions. This should be performed as near to the customer-facing edge of the network as practical.

Ensuring multiple geographically separate control plane aggregation function instances – e.g. Diameter Routing Agents – 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 network function instances can handle overload conditions if one or more instances fails, malfunctions or responds with errors.
- Ensuring all aspects of the network function 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 (e.g. Diameter, SIGTRAN, SIP) to untrusted domains including third parties, the Authority expects Providers to implement security and reliability mechanisms as per the 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; e.g. Diameter Edge Agents, SIP Session Border Gateways, etc.
- 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 organising 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.

5.55 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 standards below.

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

5.56 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 communication 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

5.57 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 Providers

5.58 The Code of Practice contains additional cyber security guidance on measures for incoming and outgoing signalling and control plane protocols which Providers should consider.

CPE/device signalling overload avoidance

5.59 The Authority expects Providers to take measures to avoid customer premise equipment (**CPE**)/device signalling overload[29] where CPE/devices form part of a PECN or PECS, including where CPE/devices are under the control of the Provider.[30] In particular, CPE and other user equipment devices which are attached to Providers' networks should be configured to prevent mass synchronisation of connection/reconnection attempts to the 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 control messages can also be sent to client devices after connection or registration establishment to adjust their subsequent behaviour.

5.60 The Code of Practice contains additional cyber security guidance and measures for customer premise equipment which Providers should consider.

Real-time charging resilience

5.61 It is common practice that mobile networks use real-time charging for their complete mobile subscriber base – both pre-paid and post-paid subscriptions. One of the results of this approach 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, the Authority would expect 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.

5.62 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.

Policy control resilience

5.63 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 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 to, and correct and timely responses from, the Policy Control Function in order for end-user service to function, the Authority expects Providers to take measures to ensure that resilience

[29] Where CPE or user-devices are a potential source of signalling overload to the network, communications providers should also implement overload protection measures on network functions as described in other sections of this guidance.

[30] Where communications providers engineer customer premise equipment (CPE) to contain the provider's embedded services (such as voice clients, TV/video clients, etc), those devices become the edge of the communications provider's network in terms of service endpoints and associated control-plane and user-plane. Such CPEs would be managed by the communications provider as per Figure 2.

and reliability are included in the designs and testing of all aspects of the policy control solution and connectivity.

5.64 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.

Network authentication/authorisation resilience

5.65 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.

5.66 The Authority would therefore expect 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.

Domain Name System (DNS) resilience

5.67 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 use cases for implementation within 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 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.

5.68 A number of control plane protocols and network infrastructure and service solutions have become dependent on "infrastructure DNS" residing within internal private portions of 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 infrastructure DNS is effectively subsumed into the control planes, and as a result, the availability and performance of the infrastructure DNS becomes as critical as the rest of the control planes. Therefore, the Authority would expect Providers to take measures to ensure that infrastructure DNS should take resilience and reliability into account in their designs, testing and operational model.

5.69 Regarding customer facing DNS, including for the purposes of resolving internet destination IP addresses, the Authority also expects Providers to take reliability and resilience into account in their designs, testing, and operational model.

5.70 In order to prevent cascading failures between customer facing DNS and infrastructure DNS instances, the Authority expects 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. This separation is achievable in traditional physical implementation approaches as well as in virtualised or cloud-native implementations.[31]

Management plane resilience

5.71 As per the Network Management sub-section of Section 4, 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" physically separate from the primary network carrying the user and signalling planes.

5.72 While in-band management is typically more cost effective, the Authority would expect 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 nor have an impact on the production traffic. As a minimum, The Authority expects this to include logical separation of management traffic into different sub-networks (e.g. VLANs/VPNs/VRFs) for different network platforms or functions (e.g. types and/or vendors) to limit the potential for problems in one management sub-network to impact another. Refer to the Code of Practice for additional details on measures related to management plane segregation.

5.73 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

[31] Anti-affinity rules are a standard approach in virtualised and cloud-native implementations to ensure that specified virtual machines (VMs), virtual network functions (VNFs), or other specific workloads do not share common hardware resources or interfaces so that failure or overload of one does not affect another. This capability is part of the standardised ETSI NFV-MANO model and is also supported in Kubernetes container-based solutions. See here and here for further information.

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 Provider needed to have field engineers travel to a number of geographically distributed sites simultaneously to restore operation and connectivity of network equipment, this could take a number of days. When architecting, designing and operating communication networks and services, Providers should also consider the measures set out in the 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.

Out-of-band (OOB) management

5.74 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.

5.75 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.

5.76 The Authority would expect 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:

(a) **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.

(b) **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 travelling to large numbers of sites simultaneously to restore correct operation.

(c) **Security**: An OOB management network provides a secure path for network management traffic and reduces the risk of malicious attacks or unauthorised access to the main network.

(d) **Isolation**: An OOB management network provides a separate network for management traffic, which can help to minimise 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.

(e) **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.

5.77 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.

"CP-managed" services – enhancing reliability

5.78 Based on the service level requirements, as covered in the processes related to Network and Service Design sub-section of Section 6, 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 referred to as CP-managed services in this Resilience Guidance and should not be confused with outsourcing service hosting or operation to third parties.

5.79 Some of these CP-managed services may be consumed by end customers – e.g. VoLTE or a digital landline.

5.80 Other CP-managed services may be internally consumed by other functions within the Provider's network. For example, the authentication/authorisation and control plane aggregation/distribution functions used in fixed, mobile and SIP/IMS voice networks can be seen as critical internal network-related services.

5.81 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.

5.82 In addition to the security duties under the Law, Providers may have obligations to ensure the reliable operation of some specific services consumed by users under other statutory or regulatory requirements; for example specific licence conditions. Voice services are a key example as they are used for accessing the emergency services, with licences issued by the Authority containing obligations on Providers to ensure access to this service.

5.83 While this Resilience Guidance sets out measures Providers should take to meet their security duties, the Authority would expect Providers to consider more broadly what measures might be required to meet these wider statutory and regulatory obligations. While the Authority does

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 the Authority considers may be relevant to compliance with these obligations are listed below.

Service implementation independent of the wider internet

5.84 Customer applications or services accessing the internet and the Provider's own services – e.g. digital landline telephony – often use elements of common infrastructure across several parts of the network.

5.85 In cases of critical services, in order to maintain robust and secure service, Providers are advised to design, host and operate these services in a manner that means they are securely separated 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 prioritised and managed end-to-end to ensure that the appropriate level of service reliability is maintained. The recommended approach to maintain reliable service is to host and operate these services entirely within a Provider's own infrastructure to ensure design and operational control of the end-to-end solution.

5.86 For mobile services, 3GPP and GSMA[32] standards dictate separation and differentiation between internet and voice services which allows for respective traffic priority and service reliability to be provided for voice.

5.87 In the case of digital landlines, which inherently use 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 and operational approaches that should be used to provide prioritisation and separation from internet traffic to enable consistent quality of experience, protection of the voice service from DDoS and other malicious attacks, and timely service restoration following a Resilience Incident. [33,34,35]

[32] GSMA IR.92 IMS Profile for Voice and SMS and NG.114 IMS Profile for Voice, Video and Messaging over 5GS.
[33] This assumes that any necessary equipment at the customer's premise has power available in addition to any connectivity required to support voice service. 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.
[34] Distributed Denial of Service – distributed volumetric attacks against a person, a service, a communications provider, or even a collection of communications providers.
[35] "VoIP" is an umbrella term for any approach to Voice over 'Internet Protocol'. It often relates to an 'un-managed' application based on the wider internet; e.g. an 'Over-The-Top' (OTT) application such as WhatsApp. An OTT VoIP delivery model is unlikely to be appropriate for voice services supplied to essential public service providers; such as Local Authorities or health care providers who may need to contact vulnerable people in an emergency, etc.

5.88 As part of a Provider's duty to prepare for the occurrence of compromises on their PECN/PECS (including anything that might affect the resilience of the network or service in terms of their availability, performance, or functionality), the Authority expects Providers to assess their end-users use of the PECN/PECS provided and, where appropriate, to provide users with information about the availability, reliability and potential risks associated with the design and operational model of the PECN/PECS that they provide to their end-users considering the end-to-end path between the end-user equipment and the service hosting point. The Authority would not generally expect end-users of a Provider to understand the technical or operational limitations or risks of a Provider's chosen architecture, design or operational model for their PECN/PECS unless they are made aware of these limitations. Providing such information in appropriate circumstances will allow end-users to make more informed choices and thus help prevent adverse effects arising from any compromise on the PECN/PECS.

5.89 Furthermore, as stated in the Internet Peering and non-Internet Interconnection sub-section of Section 4, voice/VoIP/IMS interconnects between networks are likely to carry emergency calls and other essential calls. In order to maintain appropriate service level reliability, these interconnects should be separate from the internet.

Quality of service and prioritisation mechanisms

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

Resilience mechanisms and approaches

5.91 When architecting, building and operating communication networks and services, Providers should assess the criticality and service level requirements of the services running on/over the network; as per the Network and Service Design sub-section of Section 6. 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 telecoms services, such as CP-managed-voice services (e.g. VoLTE or digital landlines), 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". 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[36], and fully understood by the relevant technical staff.

5.92 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 end-users for a given service or application:

(a) Not externally visible – "zero service impact" – typically having increased complexity and requiring more system resources, therefore limiting scalability

(b) Limited external visibility with automatic failover – network-initiated or application-initiated session re-establishment – end-users may be aware of an impact to service, typically for up to a few seconds, but do not need to take any action

(c) Extensive external visibility – end-user-initiated session/call re-establishment – end-users are very aware of the impact and need to take action to re-establish the service

5.93 The Authority recognises that there are complexity, scalability and cost implications to the different failover approaches above and understands that it is unlikely to be technically feasible or cost effective to support option (a) for all services or traffic types. Aspects relating to how a service recovers from a failure should also be considered.[37] Providers must make choices that align with their service design requirements and obligations.

Network slicing and Telco Cloud

5.94 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.

5.95 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

[36] The relevant technical criteria or parameters for 'load' can vary significantly for each different network device, function, or type of function within a network. Examples of relevant 'load' metrics might include: subscriber numbers, routing or forwarding table sizes, connections-per-second, messages-per-second, traffic mix (e.g. packet size distribution or distribution of QoS markings), throughput, memory usage, CPU usage, etc. This is not an exhaustive list.

[37] 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.

further steps forward that allow significant differences in the build of logical network topologies over common underlying network infrastructure.

5.96 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.

5.97 In most cases, for the reasons listed above, 5G slices are expected to be used for services other than standard consumer end-user internet-related services.

5.98 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.

5.99 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. Providers should take this into account when considering the implementation of network slicing.[38]

5.100 Additionally, at the time of writing this Resilience 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 challenges as well.

5.101 There are multiple different approaches to the infrastructure and operational model including: private cloud (run by the Provider), public cloud (run by a third party), and hybrid or multi-cloud (where multiple different options are used in combination).[39] In addition, there are also multiple 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. For the reasons above, it is not currently

[38] GSMA: NG.127 E2E Network Slicing Architecture. See here for more information.

[39] 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.

possible to provide mature guidance on the resilience aspects of cloud-native Telco Cloud implementations.[40]

5.102 However, the Authority is aware that 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 Resilience Guidance.

5.103 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.

5.104 The Authority expects 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-users. This includes any use of cloud infrastructure or supply chain model used.

[40] The 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.

6 Processes, tools and training

Introduction

6.1 In this section, the Authority sets out its guidance as to the measures to be taken under Articles 24K to 24N of the Law by Providers on processes, tools and training. Its contents include:

- General approach
- Network and service design
- Network and service transition
- Service operation
- Skills competency and training
- Network automation

General approach

6.2 The Authority focuses 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 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.

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

6.4 Where process measures are implemented, in particular, the Authority expects 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.

Network and service design

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

Processes related to network and service design

Service level management

6.6 The service level management process sets the service level requirements for the services that a Provider operates and ensures the designs of each service can meet them. In implementing

any service level management processes, the Authority would expect that Providers should consider the operational support impacts, as well as any use of third-party services consumed as part of the service provision.

Capacity management

6.7 Capacity management considers all resources required to deliver the service, and plans for short, medium and long-term requirements. The Authority would expect 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 a typical 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.[41]

Availability management

6.8 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. The Authority would expect 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.

6.9 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.

[41] The Authority accept that in some networks, the loss of a core site may result in reattachment of a potentially large number of user-devices, and that the control-plane overload controls for network functions and 4.3.2 for CPEs/user-devices, as outlined in the Control Plan Scaling and Overload Resilience sub-section of Section 5, may result in phased reattachment to the network with some impact on users' service. However, applying these controls will minimise overall network and service impacts.

Continuity management

6.10 Continuity management (also often referred to as Business Continuity Management (BCM)) relates to how risks of serious impact to service are mitigated and managed. The Authority would expect 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.

6.11 In relation to this, the Authority would expect Providers to regularly create offline backups of network functions and systems and be able to use the offline backups to recover systems to resume services in a timely manner. The processes of backup and restoration should be routinely tested as appropriate to ensure that the restoration will work when it is critically needed. Further guidance on backup and recovery is contained in the Code of Practice.

6.12 Additionally, Providers should be prepared for the loss of their Network or Service Operations Centre (as described in the Operations Centres and Help Desks sub-section of Section 5) by having back-up operational capabilities to maintain continuous monitoring of network infrastructure and service performance, functionality and availability.

Supplier selection, management and spares

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

6.14 The Authority would expect 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 the following where appropriate for the network device or function:

- 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)

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

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

Tools related to network and service design

6.17 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

Network and service transition

Change management

Processes related to network and service transition

6.18 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. The Authority would expect Providers to take the measures described below to ensure appropriate network and service transition.

Asset and configuration management

6.19 As a part of maintaining network and service resilience, the Authority would expect 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.

6.20 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 Provider to clearly understand which services may be impacted when a given asset fails or is changed.

6.21 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.

6.22 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 of impacts to key services.

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

6.24 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.

Testing and validation management

6.25 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, the Authority 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 that 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.

Knowledge management

6.26 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

Tools related to service transition

6.27 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

Service operation

6.28 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.

6.29 The Authority would expect 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 the Processes Related to Network and Service Design sub-section of Section 6. This includes network monitoring and management in order to ensure that the network and service design requirements and planning rules are being met.

6.30 As a reminder, outsourcing aspects of network or service operation carries risk, and the operational responsibilities remain with the Provider. Refer to Critical Third parties, Managed Service Partners and Wholesale Network/Service Providers sub-section and Technology, Physical and Cyber Security Vulnerabilities sub-section of Section 3. Furthermore, oversight of third-parties is covered in the Code of Practice.

Processes related to service operation

Network control plane monitoring

6.31 The Authority would expect Providers to take measures to ensure appropriate processes are implemented in relation to network control plane monitoring.

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

6.33 Additionally, 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.

6.34 The network control plane aggregation function instances described in Control Plane Scaling and Overload Resilience sub-section of Section 5 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 responsible for network operations.

6.35 Providers should use data analytics to correlate network, service and subscriber/device information related to the network and service health. This should allow a Provider to quickly and pro-actively identify service degradation and relatively 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 the Authority.

6.36 In a mobile network for example, mobile network operators 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.

Network user plane monitoring

6.37 The user plane is also sometimes called the data plane. The Authority would expect 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.

Event management

6.38 The Authority would expect 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.

Incident management

6.39 The Authority would expect 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.

Problem management

6.40 The Authority would expect 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.

Operations centres and help desks

6.41 Providers are expected to take measures to establish operations centres, or similar functions proportionate to their business operations supporting the continuous monitoring of network infrastructure and service performance, functionality and availability.

6.42 As per Article 15 of the Security Measures Order, where it appears to the Provider that a network or service incident may cause an incident to another Provider's network or service, the Provider must, so far as is appropriate and proportionate, provide assistance and information to the other Provider

6.43 Providers are expected to provide their users with the means to contact them to inform users about network and service faults and performance; typically referred to as a help desk.

Tools related to service operation

6.44 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

Skills competency and training

6.45 The Authority would expect 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 Provider to perform their duties.

6.46 Therefore, the Authority expects 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.

6.47 This includes any managed service providers or partners as described in the critical third parties (Managed Service Partners and Wholesale Network/Service Providers) sub-section of Section 3.

6.48 This is consistent with Article 13 of the Security Measures Order which requires 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.

Network automation

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

6.50 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.

6.51 Network automation can span both Service Transition and Service Operation (see previous sections).

6.52 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.

6.53 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.

6.54 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 (ML) to analyse network and/or service performance data and then make automated network changes. This collection of capabilities is sometimes referred to as "AI Operations", making use of artificial intelligence or machine learning in some form.

6.55 This has the potential to prevent network issues and/or restore network services more quickly. However, it can also 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. In cases of AI/ML-related failures, there is a need for explainability in order to ensure that measures are put in place so that future AI/ML-based decisions are less likely to result in repeat failures under the same conditions.

6.56 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, the Authority would expect Providers to take measures to ensure that they apply an appropriate level of diligence when implementing network automation.