Draft Telecommunications Security Code of Practice

Contents

Structure of the draft code of practice

This draft code of practice[1] contains three sections:

- Section 1 contains introductory and background information on the code of practice, including its legal status within the new telecoms security framework, how it applies to public telecoms providers, and its oversight by public authorities.
- Section 2 explains the key concepts that need to be understood by all providers when applying the specific security measures contained within the draft Electronic Communications (Security Measures) Regulations 2022 (hereafter referred to as 'the regulations') and by providers when applying the technical guidance measures within Section 3 of the code of practice, in accordance with the tiering system outlined in paragraphs 1.11-1.16 below.
- Section 3 contains the technical guidance measures and maps each individual guidance measure to the relevant security measures in the regulations. It also sets out the implementation timeframes for the technical guidance measures, which certain providers are expected to follow.

[1] Henceforth, any mention of the 'code of practice' or 'code' will be in reference to the 'draft code of practice'.

Section 1: Introduction and background

Introduction

1.1 The government's UK Telecoms Supply Chain Review Report, published in July 2019, highlighted the security risks as well as the economic opportunities associated with the next generation of telecommunications networks, particularly 5G and full fibre networks.[2] The Review concluded that a new, robust security framework was needed for the UK telecoms sector, marking a significant shift from the previous model.

1.2 Since the review was published, the government has been working to put this recommendation into action, developing a new security framework for providers of public electronic communications networks and services (PECN / PECS)[3] through the Telecommunications Security Act 2021 ('the TSA'). This new security framework, set out in the TSA, regulations and this code of Practice, has been drafted in compliance with the UK's international commitments (such as those included in free trade agreements) and relevant exceptions to those commitments.

1.3 This framework is established through the TSA and comprises three layers:

1. **Strengthened overarching security duties on public telecoms providers**. These are set out in new sections 105A and 105C of the Communications Act 2003 ("the Act") as amended by the TSA.

2. **Specific security measures** (hereafter referred to as 'requirements')**.** These are set out in the Electronic Communications (Security Measures) Regulations 2022 ('the regulations') and detail the specified measures to be taken in addition to the overarching duties in the Act.

3. **Technical guidance.** This code of practice provides detailed guidelines to large and medium-sized providers of PECN and PECS (hereafter referred to as 'public telecoms providers') on the government's preferred approach to demonstrating compliance with the duties in the Act and the requirements within the regulations.

Technical Analysis

1.4 The technical content of this code of practice is based on draft guidance developed by experts in the National Cyber Security Centre (NCSC). That guidance was produced following an extensive and detailed analysis of the security of the telecoms sector. It contained a set of technical and procedural measures designed to ensure that security risks are appropriately managed by the providers of PECN and PECS.[4]

[2] *UK Telecoms Supply Chain Review Report* (DCMS, 2019)
[3] As defined in section 151 of the Communications Act 2003
[4] The NCSC published a summary of its security analysis for the telecoms sector in January 2020

Roles and responsibilities of public authorities

1.5 *Government:* The government is responsible for setting and overseeing national policy on telecoms security and resilience. The government will keep the effectiveness of the telecoms security framework under review, and develop it further as new threats emerge. In doing so, it will be supported by Ofcom through its regular reporting on security to the Secretary of State under section 105Z of the Act, as amended by the TSA.

1.6 *Ofcom*: Ofcom will regulate the new framework in accordance with its general duty in section 105M of the Act to seek to ensure that public telecoms providers comply with their security duties. This gives Ofcom a clear remit within the new framework to work with public telecoms providers to improve the security of their networks and services and monitor their compliance.

1.7 The Act (as amended by the TSA) gives Ofcom the ability to monitor and enforce industry compliance with its new legal obligations in the telecoms security framework. It also gives Ofcom new powers to request information from providers in order to carry out its functions.

1.8 *The National Cyber Security Centre (NCSC):* As the UK's national technical authority for cyber security, the NCSC will be able to provide expert and impartial advice when requested by Ofcom. The NCSC and Ofcom have consistently worked closely on security matters and they have agreed a Memorandum of Understanding.[5] This Memorandum contains information on the roles of the respective organisations and how they will work together and share information with each other as part of the new security framework.

1.9 The NCSC will also continue to offer technical advice to telecoms providers. However, the NCSC will not report providers to the regulator in cases of non-compliance or advise providers on whether the measures they are taking amount to regulatory compliance.

Scope of the code of practice

1.10 This code of practice provides guidance for large and medium-sized public telecoms providers whose security is most crucial to the effective functioning of the UK's telecoms critical national infrastructure (CNI). However, other telecoms providers could choose to adopt any aspects of the guidance that they consider would be appropriate to secure their networks and services.

[5] *Joint statement from Ofcom and the National Cyber Security Centre* (Ofcom and NCSC, 2021)

The tiering system

1.11 To ensure security risks are mitigated proportionately, the code of practice includes a tiering system which sets out the different expectations on public telecoms providers.

1.12 The tiering system places public telecoms providers in one of three tiers, based on their commercial scale:

- **Tier 1** - public telecoms providers with relevant turnover in the relevant period of £1bn or more;
- **Tier 2** - public telecoms providers with relevant turnover in the relevant period of more than or equal to £50m but less than £1bn;
- **Tier 3** - public telecoms providers whose relevant turnover in the relevant period is less than £50m.

Application of the tiering system

1.13 The guidance set out in this code of practice is intended to apply to public telecoms providers in the following way:

- The measures in the code of practice apply to the largest national-scale **(Tier 1)** public telecoms providers, whose availability and security is critical to people and businesses across the UK. We intend these providers to implement measures to the timeframes set out in Section 3.
- The measures in the code of practice also apply to medium-sized **(Tier 2)** public telecoms providers, who will have more time to implement the security measures set out in the code of practice than the Tier 1 providers.
- The smaller **(Tier 3)** public telecoms providers are not expected to follow the measures in the code of practice. However, they may choose to adopt the measures included within the code of practice where these are appropriate and proportionate to their networks and services.

1.14 Whilst the measures are intended to address security risks to public electronic communications networks and services, providers of private networks may wish to adopt the measures included within the code of practice where applicable.

Explanation of terms

Relevant turnover: “Relevant turnover” for the purposes of the tiering system is defined as meaning turnover made from any “relevant activity” carried out wholly or partly in the UK after the deduction of sales rebates, value added tax and other taxes directly related to turnover. Relevant activity means any of the following:

- the provision of electronic communications services to third parties;
- the provision of electronic communications networks, electronic communications services and network access to communications providers; or
- the making available of associated facilities to communications providers.

This is the same as the definition used in the setting of Ofcom's administrative fees, which is clarified in Ofcom's guidance.[6]

Relevant period: It is necessary to consider the relevant turnover of a provider to determine their tier in any given reporting cycle. We intend that the 'relevant period' will be the twelve-month period commencing on 1 January in the previous year. So, for example, if a stakeholder submits data to Ofcom in September 2022, the relevant period would be from 1 January 2021 to 31 December 2021. Relevant turnover from this relevant period would then be used to determine tiers in the 2022/23 reporting cycle. This approach aligns with Ofcom's approach to the collection of equivalent data for administrative fees, which should reduce the burden on stakeholders.

Providers moving Tiers

1.15 For the purposes of applying guidance set out in the code of practice, an existing tier designation will apply to a provider until either of the following criteria are met:
- The provider has been outside of their existing tier's range for at least two years; or,
- The provider is above or below their existing tier's range by more than £10 million.

1.16 This approach will ensure that changing tiers will reflect a true change in the growth or reduction of a provider's business operations, rather than seasonal or other short-term changes in relevant turnover.

Legal status of the code of practice

1.17 The code of practice provides detailed technical guidance to public telecoms providers on the measures to be taken under sections 105A to105D of the Act. The processes for issuing, revising and withdrawing codes of practice are set out in new sections 105F and 105G of the Act and the legal effects of codes of practice are detailed in section 105H.

Non-compliance with the guidance measures in the code of practice

1.18 The guidance set out in this code of practice is not the only way for those providers to comply with the new security duties and specific security requirements that have been placed into law.

1.19 A public telecoms provider may choose to comply with those new security duties and specific security requirements by adopting different technical solutions or approaches to those specified in the code of practice. When they do so, Ofcom may require the provider to explain the reasons why they are not acting in accordance with the provisions of the code of practice in order to assess whether they are still meeting

[6] *The definition of "relevant activity" for the purposes of administrative charging* (Ofcom)

their legal obligations under the security framework. Providers are obliged to explain those reasons to Ofcom under section 105I of the Act.

1.20 In determining any question arising in connection with the carrying out by Ofcom of a relevant function, Ofcom must also take into account the provisions in the code of practice where they are relevant and in force at the time in which the question relates to.

1.21 In determining any question arising in legal proceedings, courts and tribunals must take the provisions in the code of practice into account where they are relevant and in force at the time in which the question relates to.

Non-compliance with the new security duties in the Act and/or requirements in the regulations

1.22 In cases of non-compliance with the new security duties and/or specific security requirements, Ofcom will be able to issue a notification of contravention to providers setting out that they have not complied, and any remedial action to be taken. Ofcom also has the ability to direct telecoms providers to take interim steps to address security gaps during the enforcement process.

1.23 In addition, in cases of non-compliance, including where a provider has not complied with a notification of contravention, Ofcom can issue financial penalties. The size of the financial penalties that Ofcom can impose in those instances has been updated through the TSA.

1.24 Further information on how Ofcom will use its powers and regulate the framework will be contained within its procedural guidance.[7]

Implementation timeframes

1.25 Whilst the overarching security duties that form the new telecoms security framework will come into force on 1 October 2022, it would not be proportionate to expect public telecoms providers to be in a position to meet all their obligations by that date. Instead, specific recommended compliance timeframes for individual measures are contained within this code of practice. These are the timelines by which providers would be expected to have taken relevant measures set out in the code of practice, whilst recognising that due to the existing threat environment, the quicker providers are able to implement measures the better.

1.26 It would not be appropriate, proportionate, or technically feasible, to expect providers to implement all measures at the same time. The timeframes within this document reflect which guidance measures are most important and/or most straightforward to implement first, and which guidance measures may require more time to implement.

[7] Ofcom will consult on an update to its existing guidance to account for its enforcement of the new security framework and publish a statement of policy under section 105Y.

Implementation timeframes and the tiering system

1.27 Tier 2 providers will be expected to follow the actions in the code of practice no more than two years later than providers in Tier 1, giving them more time to implement the various measures. This recognises that smaller providers with fewer resources will need more time to implement measures.

1.28 Tier 3 providers must continue to take appropriate and proportionate measures to comply with their new duties under the Act and the regulations. The regulations do not apply to micro businesses. Tier 3 providers may choose to adopt the measures in the code of practice where these are relevant to their networks and services. The government may choose to issue specific guidance for Tier 3 providers in the future.

Providers changing tiers or entering the market

1.29 There may be occasions when public telecoms providers either change tiers, or new public telecoms providers enter the market. Subject to the conditions set out in paragraph 1.15 for existing providers, providers will be expected to follow the same timeframes as existing providers in their tier, irrespective of how recently they joined that tier.

Updating the code of practice

1.30 The government intends to review and update the code of practice periodically as new threats emerge and technologies evolve. Proposed updates will most likely be informed by three broad categories of information:

- security advice provided to the government by the NCSC that sets out where these new threats and vulnerabilities lie, based on its analysis and intelligence;
- evidence from public telecoms providers of new vulnerabilities uncovered by continued and expanded security testing, as well as new incident reporting on security compromises; and
- security reports prepared by Ofcom after the end of each reporting period, containing information and advice that will assist the government with forming policy. The first reporting period for Ofcom is two years following commencement of section 11 of the Telecommunications (Security) Act, with subsequent reporting periods taking place 12 months thereafter. The security report will include information about the extent to which providers have acted in accordance with the code of practice. Access to this information will enable the government to determine how well the new framework is working and help identify where changes to the code of practice need to be made.

1.31 Where changes to the code of practice are proposed, the government will consult affected public telecoms providers, Ofcom and any other relevant parties. All proposed changes, regardless of their source, will be discussed with the NCSC before being incorporated into this code of practice. Where a code of practice is

revised (and issued as a revised document), the Secretary of State will lay a draft copy of it before Parliament for scrutiny.

1.32 This current published version of the code of practice therefore provides guidance as to the measures to be taken by relevant public telecoms providers under sections 105A to 105D of the Act, unless revised or withdrawn by the government.

Further information

1.33 There are various documents that can be used to further understand the wider telecoms security framework and policy background of the code of practice. These include:

- NCSC security analysis for the UK telecoms sector
- The Telecommunications (Security) Act 2021
- The Electronic Communications (Security Measures) Regulations 2022

Section 2: Key concepts

1. Overarching key concepts

1.1 There are certain key concepts that are relevant to the guidance measures set out in this code of practice and specific security requirements contained in the regulations. It is important that all public telecoms providers fully understand these key concepts as it will enable them to properly apply the intent of the security requirements. This chapter covers the concepts of security critical functions and network oversight functions, as well as the overarching scope of the code of practice.

1.2 In a number of places within Section 2 of the code of practice there are cross-references to external NCSC and third party publications which provide further advice and information on the topics covered by this code of practice. While the advice set out in such publications is relevant to security more generally, these documents do not themselves form part of the guidance provided by this code of practice.

Explanation of terms

Where the term **'reduce'** is used in the regulations, it is expected that the provider will reduce the risk as far as possible.

The terms **'shall'**, '**should'** and '**may'** have been defined in relation to the guidance given in Section 2. This is to distinguish between where the government believes there is likely to be only one acceptable way of implementing the specific measure, and those which have potential alternatives.

Shall: The use of the word 'shall' in Section 2 indicates where government guidance is that there is likely to only be one viable technical solution to secure the network or service in line with the regulations. We would not expect these technical solutions to vary as a result of different network configurations or business structures.

Should: Where the word 'should' is used within the guidance in Section 2, the government views the solution provided as being the best way to implement the measures in the majority of cases. However, there are known alternatives that providers could possibly deploy, depending on their network or service configurations and business structures, which could attain a satisfactory security outcome.

May: The use of the word 'may' in the guidance within Section 2 indicates that providers are likely to have multiple options, all of which could deliver a satisfactory solution and there are likely to be differences between providers in their implementation.

Scope of measures within code of practice

1.3 Measures contained within Section 3 of the code of practice apply to public electronic communications networks and services, as defined in the Act[8]. This includes, but is not limited to the following elements where they are part of such networks and services:

- the systems and services involved in providing public telecommunications services to customers;
- proof of concepts or trials on the operational network;
- the use of data from the operational network for testing purposes;
- interconnection of development, test and operational systems - although this is an activity which is inappropriate in all scenarios;
- parts of the operational network operated by third parties on behalf of the provider, including as part of managed service arrangements;
- parts of the operational UK network hosted outside the UK; and
- networks supporting the operation of the live network, where these supporting networks can have a material impact on the proper functioning of the operational network.

Security critical functions

1.4 A “security critical function” in relation to a public electronic communications network or service, “means any function of the network or service whose operation is likely to have a material impact on the proper operation of the entire network or service or a material part of it” (Regulation 2).

1.5 Security critical functions will therefore make up different proportions of networks or services, the specific details being dependent on the unique operating mode of each individual network. However, security critical functions will include a broad range of essential functions within the network, and not simply those whose primary function is security. The guidance in this code of practice sets out specific protections targeted at different functions of networks and services that may be considered critical. It does not seek to exhaustively define components as critical.

1.6 When deciding which functions of the network or service could not be considered as security critical, providers should be able to demonstrate that individual functions do not have a material impact on the proper operation of the entire network or service, or a material part of it.

Network oversight functions

Scope

1.7 Network oversight functions are the components of the network that oversee and control the security critical functions, which make them vitally important in overall network security. They are essential for the network provider to understand the network, secure

[8] See *Telecommunications (Security) Bill: Explanatory Notes*, *Annex A: Scope* (DCMS, 2020)

the network, or to recover the network. Scope will differ from provider to provider depending on the type of network and how those networks are architected.

1.8 Given their importance in allowing the provider to maintain control of the network, network oversight functions are more likely to be targeted for a security attack and the impact of their compromise is greater.

1.9 Network oversight functions include, but are not limited to:

- element managers;
- virtualisation orchestrators;
- management systems (e.g. jump boxes);
- security functions (e.g. firewalls at the edge of a security zone);
- root authentication services (e.g. active directories - ADs);
- multi-factor authentication services;
- security gateways (e.g. supporting the management plane);
- audit and monitoring systems (including network quality monitoring of speech and data); and
- operational support systems.

Guidance

1.10 Best security practices should be implemented for network oversight functions. This includes rapid patching on release of a security update. It also includes rigorously controlling and minimising the attack surface of the function. This could include limiting the accessible interfaces, removing access to third parties, or reducing the number of users with administrative access.

1.11 Wherever possible, more modern security practices should first be implemented in network oversight functions as they are likely to benefit most from these enhanced protections. Specific recommended compliance timeframes for individual measures are contained within Section 3 of this document.

The principle of 'assumed compromise'

1.12 Providers should establish the principle of 'assumed compromise'. This means that providers should normally assume network oversight functions to be subject to high-end attacks, which may not have been detected by the provider, and implement business practices which, by their nature, make it difficult for an attacker to maintain covert access to these functions. This can be achieved through establishing secure platforms which implement trusted boot, and periodically rebuilding the functions to an up-to-date known-good state.

Management functions for network oversight functions

1.13 In addition, given that security compromises affecting network oversight functions are likely to have a significant impact on the proper operation of the network, the management functions used to manage network oversight functions should have

enhanced protections, including using dedicated management functions, a segregated management plane and an enhanced control set.

Approach to monitoring and analysis

1.14 Under Regulation 6, providers must take such measures as are appropriate and proportionate to monitor and analyse both access to security critical functions and their operation, and investigate any anomalous activity. Given the essential role of network oversight functions, the use of these functions and the systems that manage them should be subject to an enhanced level of monitoring, including real-time monitoring of changes to network oversight functions and monitoring for signs of exploitation.

1.15 In addition, when providers start performing security analysis to establish the 'normal behaviour' of their networks in order to be able to identify and investigate any anomalous activity, they should prioritise the analysis of the behaviour of network oversight functions.

Example of how network oversight functions work with security critical functions

1.16 An example of how network oversight functions and security critical functions can work together in the context of virtualisation workloads is set out below[9].

1.17 Typically, when building out the infrastructure to enable the running of virtualised workloads a provider will require:

- the hypervisor – the operating system installed on the physical servers to enable them to run virtual machines (the combination of many hypervisors/physical servers/physical networking that links it all together is usually referred to as the 'virtualisation fabric');
- physical servers to run the hypervisor;
- the virtual workloads themselves; and
- the virtualisation orchestration software that tells the virtual workloads on which servers to run.

1.18 If the virtual workload is a function whose operation has a material impact on the operation of the network, then the following would be security critical functions:

- the virtual workload itself;
- orchestration software that establishes the virtual workload;
- the hypervisor;
- the physical servers on which the virtual workload runs.

In this case, the orchestration tooling would be the network oversight function.

1.19 Because of their importance to overall network security, all network oversight functions should normally be expected to fall within the definition of "security critical functions" set out in the regulations. However, not all security critical functions can be considered as

[9] More information on virtualisation and containerisation can be found in paragraphs 2.26-2.64

network oversight functions as many do not control or oversee other security critical functions.

Chapter crossovers

1.20 The information in this chapter is useful in understanding the following concepts described in subsequent chapters of this code of practice:

- Network architecture (Chapter 2)
- Protection of data and network functions (Chapter 3)
- Monitoring and analysis (Chapter 5)
- Supply chain (Chapter 6)
- Prevention of unauthorised access or interference (Chapter 7)
- Remediation and recovery (Chapter 8)
- Governance (Chapter 9)
- Reviews (Chapter 10)
- Competency (Chapter 12)
- Testing (Chapter 13)

2. Network Architecture

2.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 3 to design, construct (or where relevant, redesign and develop) and maintain networks securely.

2.2 Regulation 3 is set out below.

> 3.—(1) A network provider must take such measures as are appropriate and proportionate to ensure—
>
> (a) except in relation to an existing part of the public electronic communications network, that the network is designed and constructed in a manner which reduces the risks of security compromises occurring,
>
> (b) in relation to an existing part of the public electronic communications network, that the part is redesigned and developed in a manner which reduces the risks of security compromises occurring, and
>
> (c) that the public electronic communications network is maintained in a manner which reduces the risks of security compromises occurring.
>
> (2) For the purposes of paragraph (1), an existing part of a public electronic communications network is a part that was brought into operation before the coming into force of these Regulations.
>
> (3) The duty in paragraph (1) includes in particular a duty—
>
> (a) to identify and reduce the risks of security compromises to which the entire network and each particular function, or type of function, of the network may be exposed, having appropriate regard to the following—
>
> (i) whether the function contains sensitive data,
>
> (ii) whether the function is a security critical function,
>
> (iii) the location of the equipment performing the function or storing data related to the function, and
>
> (iv) the exposure of the function to incoming signals,
>
> (b) to make a written record, at least once in any period of 12 months, of the risks identified under paragraph (a),
>
> (c) to identify and record the extent to which the network is exposed to incoming signals,
>
> (d) to design and construct the network in such a way as to ensure that security critical functions are appropriately protected and that the equipment performing those functions is appropriately located,
>
> (e) to take appropriate measures in the procurement, configuration, management and testing of equipment to ensure the security of the equipment and functions carried out on the equipment,

(f) to ensure that the network provider is able, without reliance on persons, equipment or stored data located outside the United Kingdom, to identify the risks of security compromises occurring,

(g) to ensure that the network provider is able to identify any risk that it may become necessary to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom, and

(h) to ensure that, if it should become necessary to do so, the network provider would be able to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom.

(4) A network provider must retain any record made under paragraph (3)(b) or (c) for at least 3 years.

(5) A network provider or service provider must ensure, so far as appropriate, that the public electronic communications network or public electronic communications service is designed in such a way that the occurrence of a security compromise in relation to part of the network or service does not affect other parts of the network or service.

Key concepts for understanding the requirements

2.3 The architectural and design decisions which are made when creating and modifying a provider's network or supporting systems are critical to the security of that network. This security architecture determines how difficult it will be to compromise or disrupt the system, the scale of any associated impact, and whether the provider is likely to detect and recover from any compromise.

2.4 As an example, the security architecture determines the network's attack surface from an attacker's perspective. Specifically, the attack surface is the equipment and interfaces that the attacker can target from a given logical location. A mature security architecture will consider attackers to be located both externally and internally, and configure the network into security zones which limit the attack surface appropriately based on risk.

2.5 Whilst a technical discipline in its own right, the security architecture is also fundamental to every other security measure described within this document. It determines the risk to equipment, and hence the necessary controls and protections.

The management plane

2.6 The management plane of a networking system or device is the part of a system that configures, monitors and provides management, monitoring and configuration services to all layers of the network stack, and other parts of the system.

Scope

2.7 The scope will differ from provider to provider but this guidance applies to management access to equipment within operational telecommunications networks, and to management access to equipment that supports the operation of telecommunications networks. Also in scope are the networks of third parties where those third parties perform management on the provider's behalf, and any automated management systems, such as orchestrators and Operational Support Systems (OSS).

Background

2.8 The management plane is the most powerful part of the network infrastructure, making it the primary target for any malicious attack intending to disrupt or otherwise compromise the operation of a network. Exploitation of the management plane could have a long-term impact on the availability and confidentiality of the provider's services, including critical services.

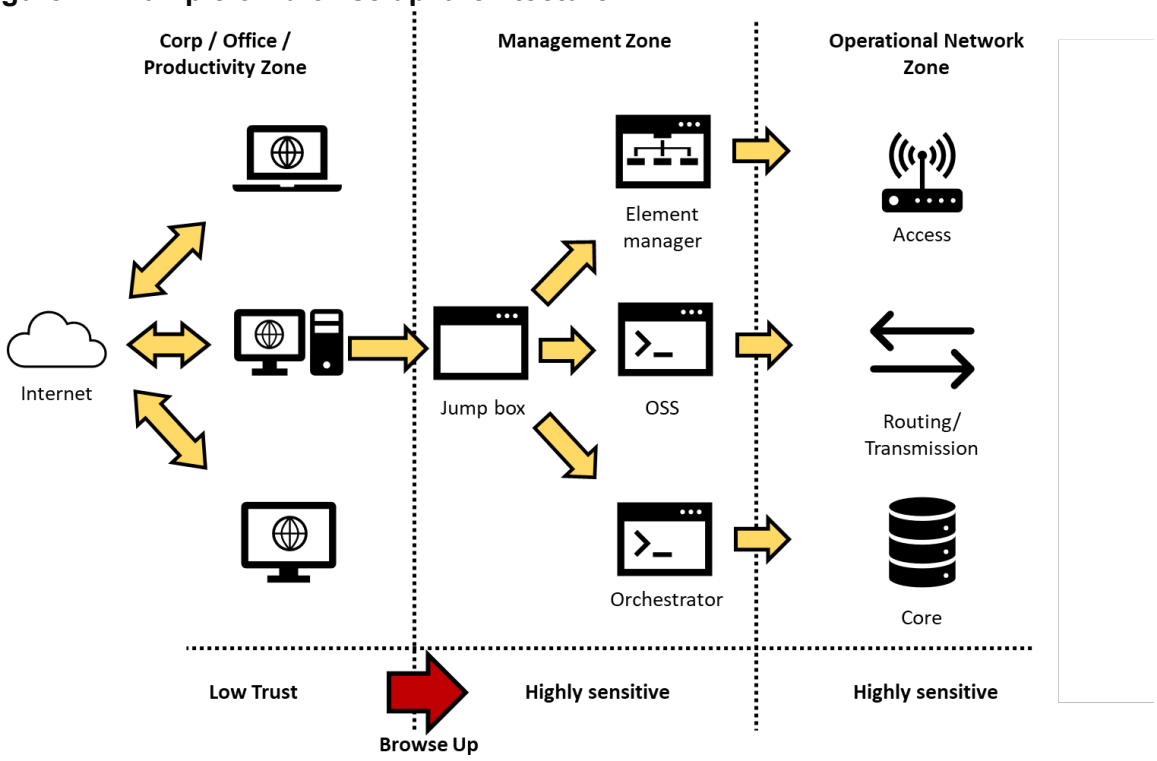
2.9 Attacks of this type tend not to be 'noisy', meaning that there may be no overt impact on the network, and they may be maintained for years, growing in scale and complexity over time.

2.10 As an example, on 17 August 2021 it was confirmed that T-Mobile was subject to a data breach which saw the sensitive data of nearly 50 million customers being exposed[10]. Evidence has shown that this compromise may have been caused by T-Mobile having the management plane of the core network directly exposed to the internet. It has been indicated that the exposed box was test equipment that was attached to the operational network, and from the test equipment the attacker had access to the LAN and could brute force the password on operational servers. This enabled a single hacker to access customer data within a number of weeks.

2.11 Historical management of telecoms networks has relied heavily upon standard corporate devices 'doubling up' as administrative workstations. Consequently, the computers that perform standard 'office' type functionality such as email, web access and the use of productivity tools are also defining the operation of the network. This is often referred to as a 'browse up' architecture, as shown in Figure 1 and described in the security architecture anti-patterns publication by the NCSC[11].

[10] *The Cyberattack Against T-Mobile and Our Customers: What happened, and what we are doing about it* (T-Mobile, 2021)
[11] *Secure system administration* (NCSC, 2020)

Figure 1: Example of 'browse up' architecture



2.12 A 'browse up' architecture brings with it significant risk. Where it is used, several 'commodity' classes of attack can be performed with relative ease upon administrative users, and these can achieve a significant impact. Several of these attack vectors exist (e.g. compromise via malicious websites and compromise via infected removable media) but the most notable being the possibilities afforded to an attacker via phishing attacks. Phishing of privileged user accounts, whether targeted or otherwise, can initially result in:

- credential loss (e.g. leading to unauthorised remote access or gathering of information for future exploitation);
- remote code execution (enabling an attacker to gain a foothold on machines used for administrative use); or
- further exploitation of networks or users (the potential to move laterally to other resources through use of privileged user accounts).

Guidance

2.13 Attacks via the management plane are likely to have a significant impact upon both the provider and the UK and hence securing the management plane should be treated as a priority by the providers. The following guidance in paragraphs 2.14-2.25 highlights the key aspects of management plane security for public telecoms providers to understand and implement, providing examples and further background information where appropriate. However, secure system administration is not solely a challenge within the

telecommunications sector, and general advice on this problem can be found on the NCSC website.[12]

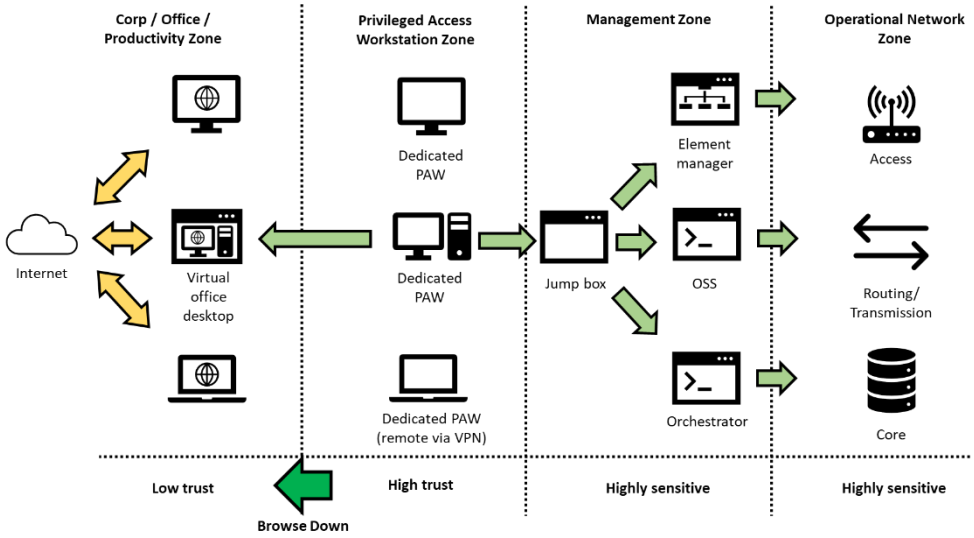
Isolating the management plane

2.14 Given the risks, it is not appropriate for providers to be using a 'browse-up' architecture. Instead, providers shall architect, and operate, their management plane infrastructure to inhibit network compromise through administrative access.

2.15 Workstations dealing with general office productivity tools and external access to external services over the internet shall be logically or physically separate from those with any access to the management plane. Any administrative users who previously performed these functions via a single device will need to operate differently to protect their network.

2.16 As providers prepare to isolate their management planes from corporate functions, it may help providers to consider their network infrastructure as divided into security 'zones', as shown in Figure 2. This can help providers ensure that anything that can impact the operational network cannot be compromised from the corporate zone.

Figure 2: Example of 'browse-down' architecture



2.17 To ensure the administrative zones are separated from corporate zones it will be necessary for separate enterprise services to be hosted within these zones. This will likely include, but is not limited to, authentication services, system update services and document stores..

2.18 In some instances remote access may be necessary (see paragraphs 3.6-3.7). More information on privileged access workstations can also be found in paragraphs 3.3-3.13.

[12] *Secure system administration* (NCSC, 2020)

Secure administration

2.19 Providers will need to ensure that administration is performed securely, using effective authorisation, authentication and encryption. Providers shall ensure that every administrative access is authorised and time-limited, linking that administrative access to a specific purpose or ticket.

2.20 Whenever administrators are gaining an ability to impact the operational network, providers shall ensure that multi-factor authentication (MFA) is used as part of the authentication process. MFA would normally be performed as administrators access management platforms (jump boxes, bastion hosts, orchestrators, etc) rather than individual hosts. The second factor should be generated or transmitted via a device separate to that being used to perform the administrative functionality. Public channels for delivery of the MFA token, such as SMS, are not appropriate for this use case.

2.21 Given that management traffic typically involves sensitive information and/or credentials being passed via these channels, it is essential that all management is performed over secure protocols. Third party suppliers with a mature approach to security will either provide equipment that is 'secure-by-default' on delivery, or will provide hardening guides to explain how to perform an effective lock down of the supplied network infrastructure. These should be followed to ensure the most secure variant of any given management protocol is used (for example SSH over Telnet or HTTPS over HTTP).

2.22 To ensure that compromise of network equipment does not result in onward access to further equipment via the management plane, providers shall restrict the ability of network elements to communicate with each other over the management plane. Network restrictions shall be put in place to ensure only equipment that needs to communicate is able to communicate over the management plane.

2.23 To protect management platforms (such as bastion hosts, jump boxes, element managers, orchestrators, etc) from up-stream attacks from network equipment, providers shall ensure that only outbound management traffic is permitted from management platforms.

Third party administrators

2.24 Managed service providers (MSPs) or third party administrators (3PAs) are prize targets for attackers, as they will often have privileged access to multiple networks. Because of this, where these third parties have access to the management plane, they shall have to meet the same security principles as those employed by providers themselves, and ideally shall use the same methods.

2.25 To ensure that security controls are applied correctly, it will be essential for providers to have contractual arrangements in place which oblige third party administrators to undertake this activity. It will also be necessary to have robust powers of audit to permit spot-checks and ongoing monitoring of security governance arrangements. Providers

shall ensure they are able to fully control and monitor access by third parties into their management plane independently of the third party.

Virtualisation and containerisation

2.26 Virtualisation refers to the creation of a virtual resource such as a server, desktop, operating system, file, storage or network. The use of this technology is growing significantly across the telecoms sector.

Scope

2.27 Background information and guidance on virtualisation and containerisation in paragraphs 2.28-2.64 applies to public network providers where they are making use of virtualisation or containerisation to abstract more than one piece of physical hardware from the operational software.

Background

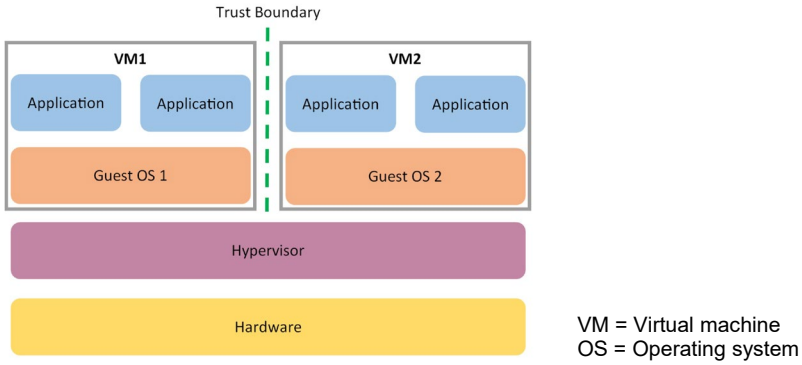
2.28 Prior to the emergence of virtualisation, network functions ran on their own dedicated hardware. Security controls were defined during design, and it was unlikely that these controls would change significantly throughout the equipment's lifetime. Virtualisation allows for greater flexibility. Operationally it allows services to scale up and down easily. In terms of network security, additional security controls can be added, interfaces can be monitored, or processes can be inspected without affecting on-going services.

2.29 Virtualisation generally establishes two architectural layers;

- the virtual functions or virtual instances (usually a set of applications and operating systems);
- the 'virtualisation fabric' or virtualisation platform, made up of a hardware abstraction layer, such as a hypervisor, and the physical servers and networking equipment used to host the virtualised workloads.

2.30 For the purposes of this document, 'virtualisation' is considered to be a system supported by a 'bare-metal' hypervisor, as shown in Figure 3. Bare-metal hypervisors run directly on a host machine's physical hardware and provide a fully abstracted layer between virtual workloads running within the hypervisor and the physical hardware's resources.

Figure 3: Example of bare-metal hypervisors

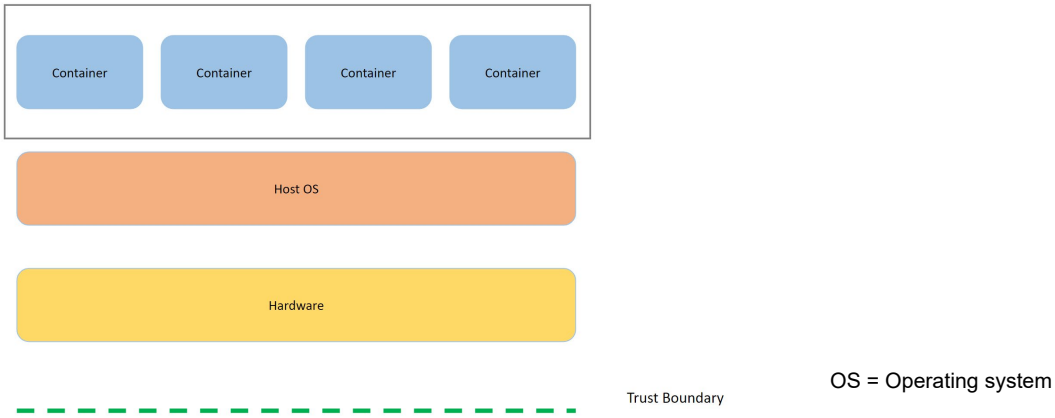


2.31 Virtualisation can be an effective tool for improving the security of a system. By enforcing separation between workloads, it can help prevent lateral movement. By abstracting the hardware, it can allow for better inspection of system behaviour and make the compromise of hardware more complex for an attacker. Virtualisation should also make a system more flexible, allowing security updates and improvements to be implemented more quickly.

2.32 However, in virtualised networks the integrity of the virtualisation fabric becomes critical. Compromise of the virtualisation fabric could result in the compromise or disruption of all workloads supported by that fabric. Virtualised networks are also highly configurable. While this is a strength, providers should be aware that the configuration of the virtualised environment can undermine its security properties.

2.33 In comparison, containerisation provides no hardware abstraction, but does provide a quick deployment and scaling opportunity to providers by packaging applications within a single host operating system (as shown in Figure 4). Access to resources is limited by the host operating system, but hardware resources are not abstracted, meaning the security benefit is limited.

Figure 4: Example of containers



2.34 Containerisation is viable for sharing and scaling workloads within the same security zone or trust domain (Figure 6). However, providers should assume that an attacker with access to one container will be able to compromise the host and all the other containers supported by that host.

2.35 Both virtualisation and containerisation are sometimes used together. Virtualisation may be used to abstract the hardware, while containers are used to scale workloads within the virtual function.

Guidance

2.36 Virtualisation security is an evolving subject, with new security solutions and design patterns emerging each year. The following guidance in paragraphs 2.37-2.64 highlights the key aspects of virtualisation security for telecommunications providers to understand and implement, providing examples and further background information where appropriate. When considering the guidance within the document, providers should also consider the latest virtualisation security best practices. Furthermore, additional advice on security design within virtualised environments can be found in the NCSC's virtualisation security design principles[13].

Limiting the impact of host compromise

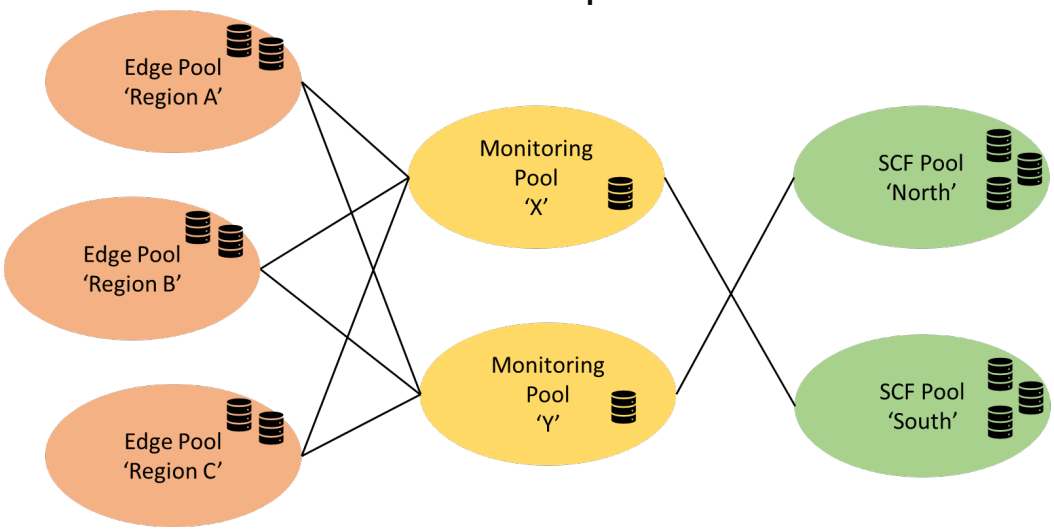
2.37 As previously noted, the compromise of a host within the virtualisation fabric poses a significant security risk to all virtual functions supported by the host. As it cannot be assumed that a host compromise will not occur, providers shall ensure that it is possible to reduce the impact from, and recover from, a host compromise.

2.38 To limit the impact of host compromise, providers should segregate both their virtualisation fabric and the virtual functions supported by that fabric. This ensures that the network's security architecture is not undermined by the dynamic nature of the virtualisation.

[13] *Virtualisation security design principles* (NCSC, 2019)

2.39 For this reason, providers will often break large host estates into groups based on risk. For the purposes of this document, these groups of hosts will be called host 'pools', an example of which is shown in Figure 5. All hosts within a pool should generally present a similar level of risk to the network. This risk may be based upon the host type, the security features of the host, or the host's physical location. Hosts may also be pooled for resilience purposes to ensure that load-balancing workloads are in physically separate locations.

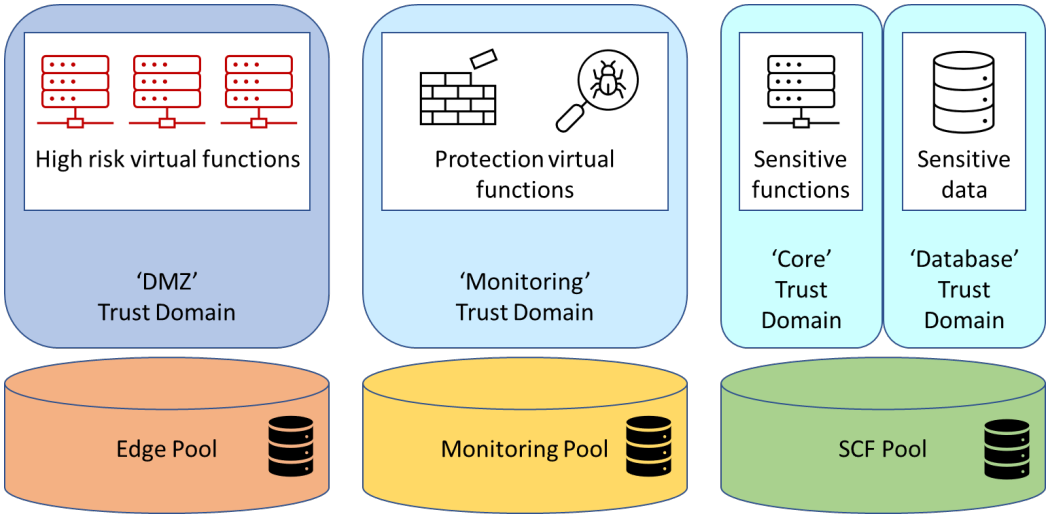
Figure 5: Virtualisation fabric broken into host 'pools'



2.40 Similarly, virtual functions can be grouped based on risk, for example due to exposure, criticality or sensitivity. For the purpose of this document, these groups of virtual functions are called trust domains.

2.41 By associating trust domains with host pools, providers can segregate their network, maintaining a physical security architecture within a virtualised network, as shown in Figure 6. These associations are sometimes known as 'affinity rules'.

Figure 6: Segregating trust domains using host pools



Management of the virtualisation fabric

2.42 As a compromise of physical hosts within a virtualisation fabric would likely compromise many workloads, the administration of hosts is particularly sensitive. Access should be actively monitored and shall be limited to the smallest number of trusted administrators. The host's network-accessible administration interfaces shall only accept connections from authorised management infrastructure.

2.43 It should rarely be necessary to directly administer physical hosts within an operational virtualised network, as most interaction should be performed by a central orchestration tool. This orchestration tool should be treated as a network oversight function. For resilience and security reasons, this central orchestration tool should not be hosted on the virtualisation fabric that it manages. Should it be hosted within the fabric, this could impede recovery should part or all of the fabric fail or be compromised.

2.44 It is possible that physical baseband management controllers (BMCs) or other integrated lights out (iLO) management interfaces are used to manage hosts. Such alternative administration networks should either use a dedicated network that is physically separated from the virtualisation fabric network or use a lights out management solution that supports secure management as detailed in this document.

A secure virtualisation fabric

2.45 In the event that a host is potentially compromised, providers must be able to recover the integrity of the host infrastructure. As replacing the host hardware is expensive, providers can instead return the host to a known-good state. This may be achieved where hosts support 'secure boot'.

2.46 As part of a secure boot, physical hosts record their boot-up sequence from power on to hypervisor load. A hardware root-of-trust (e.g. TPM) signs this record before it is sent to an attestation service. The attestation service can then assess whether the state of the physical host has changed. If not, this gives confidence to the provider that the host can be trusted to host virtual functions.

2.47 Additionally, should the provider need to transfer hosts between host pools, a secure boot process can be used to give confidence to the provider that the host is ‘clean’ prior to performing the transfer. Providers should avoid configuring the virtualisation fabric in such a way as to inhibit the migration of virtual machines as required.

Choosing virtual functions

2.48 Providers should use virtual functions that are built for use within a virtualised environment as this provides significant security benefits. Network functions which are built to be virtual will run effectively on any virtualisation fabric or hypervisor and hence are likely to be more secure, avoiding platform-specific functionality or cut-throughs. They are likely to be more resilient, due to a lack of dependence on a specific platform. They also allow for the virtualisation fabric to be more secure, easily supporting migration between hosts to allow for updates and reconfiguration.

2.49 Pinning specific virtual network functions to specific hosts within the virtualisation fabric makes it significantly harder to update and patch those functions and hosts. As such, it should be avoided where possible.

2.50 Ideally, virtual functions will also support secure boot, using the trusted boot path provided by the underlying hosts and exposed securely to the virtual function via the hypervisor.

Authorising virtual functions

2.51 To prevent an attacker from running new virtual functions, or modifying existing virtual functions, only permitted virtual functions should be run by the virtualisation fabric. Providers should achieve this by ensuring all virtual functions are signed and authorised by the provider and configuring the virtualisation fabric to verify virtual functions prior to operation.

Separating virtual functions

2.52 As previously stated, virtualisation provides an effective means to provide security separation for different virtual functions running on a single host. Where virtual functions are within separate virtual machines, enforced by a bare-metal hypervisor, it is reasonable for a provider to assume that it would be difficult for an attacker to move laterally between these virtual machines via the virtualisation fabric.

2.53 For this reason, it is possible for a single host pool to support multiple trust domains as the separation between the trust domains is maintained by the virtualisation fabric.

2.54 In general, containers do not provide sufficient security separation to be relied upon to segregate virtual functions. Providers should assume that a virtual/physical host compromise or a container-to-container compromise is more likely in containerised environments. For this reason, all containers running on a single physical or virtual host

should be within a single trust domain. Additionally, where the containers are running directly on a physical host, the host pool should be treated as less trusted.

2.55 Similarly, bare-metal hypervisors are sometimes configured to allow specific virtual machines to address physical hardware directly. These are known as hypervisor 'cut-throughs'. Cut-throughs can have performance benefits, but they negate the security properties of the bare-metal hypervisor as a virtual machine is now able to directly access and control physical hardware without any of the hypervisor's security controls. On hosts supporting cut-throughs, the virtual functions should all be within a single trust domain, and the host pool should be treated as less trusted.

2.56 This guidance is not intended to discourage providers or third party suppliers from using containers where there is benefit in doing so, but to highlight that such containers should not be treated as a security boundary between trust domains. Similarly, where virtualisation is not being used to provide a security boundary, the security choices relating to the virtual network are less important.

Understanding the virtualised network

2.57 An essential part of a virtualised network is the understanding of that network. Providers should ensure that they can easily represent and explore the virtual and physical network architecture, including identifying how the security architecture is enforced both virtually and physically. This can be supported by well-defined, system-enabled processes.

2.58 As a virtualised network may change dynamically, the principles that define the security architecture should be defined within the orchestration systems that establish and modify the network.

2.59 From a physical perspective, providers shall ensure that they are able to access full details of hosts, including:

- type of host and supporting software (e.g. hypervisor) and software versions;
- the last boot time, boot status (e.g. a successful or failed secure boot) and any attested information;
- the host pool and security properties associated with the host;
- the trust domains that the host may support and the networks (VLANs/VXLANs) accessible from the host.

2.60 Within the virtual network, providers shall ensure that they are able to access the logical flows between virtualised workloads including:

- the protocols that should, and should not, flow over the virtualised interfaces;
- the physical hosts, equipment and links used to support the logical flow;
- the trust domains within the logical flow and the security enforcing functions splitting up that flow.

2.61 Providers should also use the flexibility of virtualisation to enable greater monitoring of processes and flows within the virtualised system.

Network automation

2.62 This guidance demonstrates that managing a secure virtualised environment is complex. However, the majority of the security requirements can be automated.

2.63 Automation also allows for rapid prototyping and testing of new features, security patches and changes. This approach supports network resilience by limiting errors caused by human interaction and by allowing quicker remediation should issues occur. The approach supports network security by increasing the speed at which updates and changes can be made, allowing the provider to keep pace with the threat environment.

2.64 When automating, providers should seek to use a secure, reproducible and comprehensible method of building and scaling a network. Orchestration and network management tools allow providers to define the network infrastructure as 'code', within which security requirements can be embedded. When automating the orchestration and configuration of virtual functions, it is essential that providers use modern development tools and techniques. As a minimum, this includes code versioning, continual integration, and delivery pipelines to maintain the security, integrity, and quality of automated builds.

The signalling plane

2.65 All public telecoms networks connect to each other over signalling networks. These signalling networks allow provider networks to connect to each other, reach each other's services and ultimately allow users to communicate with each other. The signalling plane of a network consists of protocols for control and support of the transmission plane functions. The signalling plane carries out the following functions:

- it controls the access connections to the network (e.g. GPRS attach and GPRS detach);
- it controls the attributes of an established network access connection (e.g. activation of a packet data protocol (PDP) address);
- it manages the routing of information for a dedicated network connection in order to support user mobility;
- it adapts network resources depending on the parameters; and
- it sets up calls and routes messages.

Scope

2.66 This code of practice applies to signalling traffic arriving from untrusted signalling networks and to signalling arriving from other networks which are not within the scope of the security framework. This includes, but is not limited to: BGP, SS7/MAP/ISUP, DIAMETER, GTP-C and SIP/IMS.

2.67 Controls apply to all international signalling, including signalling which arrives over national signalling interfaces (e.g. due to mobile number portability). Signalling from

Crown Dependencies (including the Channel Islands and Isle of Man) shall be treated as international signalling.

2.68 Throughout the code of practice it should be noted that providers' live networks should be considered in scope of the guidance measures which concern network signalling protections. This would cover, for example, any trials being conducted on a live network that may have implications for wider network availability, functionality or performance. Protections from risks arising from external signals will also apply to signals originating from the network edge or consumers.

Guidance

2.69 Traditionally, and to a degree currently, telecoms standards have been built on an assumption that all signalling from other telecoms networks can be trusted. However, that assumption is no longer valid as these international interfaces could be exploited by attackers to conduct attacks. Therefore, providers need to operate on the principle that incoming signalling networks are untrusted and build signalling security architecture that can validate incoming derived signalling without impacting critical core network functions.

2.70 With respect to signalling networks, providers should seek to increase the network's resilience to disruptive attacks from incoming signalling networks and to inhibit the leaking of subscriber or network data over incoming signalling networks. The following guidance in paragraphs 2.71-2.77 highlights the key aspects of signalling plane security for telecommunications providers to understand and implement, providing examples and further background information where appropriate.

Signalling protocols

2.71 Providers may use a combination of signalling protocols for different network functions, or variants of commonly accepted protocols. Examples of relevant protocols are listed below, along with descriptions of their purpose and function. This list is non-exhaustive.

Protocol	Purpose and function
Inter-network Mobile Application Part (MAP) and lower layer protocols (SS7/SIGTRAN)	MAP is used to facilitate mobility management, call handling, SMS and other functions in cellular networks. Commonly used between circuit-switched core network equipment (e.g. HLR, MSC, VLR), and between circuit-switched core networks and packet-switched core network equipment. Lower layer protocols may include TCAP, SCCP, MTP (1-3), M3UA, SCTP, IP, Ethernet.

Protocol	Purpose and function
Inter-network CAMEL Application Part (CAP) and lower layer protocols (SS7/SIGTRAN)	CAP provides additional provider services when the user is roaming across cellular networks. Lower layer protocols may include TCAP, SCCP, MTP (1-3), M3UA, SCTP, IP, Ethernet.
Inter-network GTP-C (and lower layer protocols)	The GPRS Tunnelling Protocol – Control plane (GTP-C) when used to establish, update and remove data sessions for transport of user traffic between cellular networks. Can also be used to modify the quality-of-service parameters. Commonly used between packet-switched core network equipment. Lower layer protocols will likely include UDP and IP, IP and IPSec.
Inter-network SIP/SDP (and lower layer protocols)	The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) when used for interconnection and roaming between the provider's IP Multimedia Subsystem (IMS) network and external SIP networks. SIP/SDP is commonly used to provide multimedia services in fixed and mobile networks. Lower layer protocols will likely include TCP/UDP, IP and IPSec.
Inter-network DIAMETER (and lower layer protocols)	A general authentication, authorisation and accounting protocol (AAA) extended for use in mobile networks to support mobility management, call handling (etc). Commonly used between packet-switched core network equipment in 3G and 4G networks. Lower layer protocols will likely include TLS, SCTP, TCP, IP and IPSec.
Inter-network BGP (and lower layer protocols)	Border Gateway Protocol (BGP) is a standardised exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the internet. BGP will announce the best route for traffic between two locations on the internet. Lower layer protocols include TCP/UDP and IP.

Protecting the network

2.72 An attacker may seek to scan the provider's signalling networks to understand the network and inform further attacks. Providers shall ensure that the internal network topology of their signalling is not exposed by ensuring that only 'hub' signalling addresses can be reached from external networks. These interfaces and addresses should be formally recorded.

2.73 Attackers may also send malformed signalling towards the provider's network in an attempt to disrupt or compromise the provider's service. To protect the network, providers should ensure that external signalling is fully parsed and processed before reaching a security critical function.

2.74 Architecturally, this may be achieved by network providers establishing an architectural demilitarised zone (DMZ) between incoming signalling networks and security critical functions, similar to the mechanism used to protect IP networks from any less-trusted sources (such as the internet). It could also be achieved by segregating the core network to limit the impact of any attack.

Protecting users

2.75 Providers should seek to prevent the disruption of service or the leaking of customer data over signalling interfaces. Where the provider's customers are connected to the provider's network, the provider shall implement mechanisms to protect the customer's service and data.

2.76 Where the provider's customers have roamed onto another network, the provider should support the visited network in protecting their customers by informing the visited network of the signalling addresses which will support the customers connection, and proxying call and SMS signalling via the provider's (home) network.

2.77 Where another provider's customers have roamed onto the provider's network, the provider should seek to protect the inbound roamer's service and data as well as can be achieved given the information available from the roamer's home network.

Asset management

2.78 Effective asset management is the basis of effective security risk management and effective security architectures. Providers shall maintain their own asset management records, rather than relying on suppliers or third-parties to maintain asset records.

Guidance

2.79 Due to its importance to network security, asset management should be automated whenever possible, and business processes should help to maintain the integrity of the asset register. Software tools can also be used to automatically enumerate the provider's network, to ensure that they have an up-to-date network map and that this aligns with the asset register.

2.80 An important aspect of asset management is an assessment of the criticality and sensitivity of network equipment and systems. As part of this process, providers will be able to identify their security critical functions and network oversight functions.

2.81 Asset management shall include the recording of any equipment in the provider's network that is out of mainline support, as this is likely to be more vulnerable to

compromise. Providers should have a plan to remove all equipment that is out of mainline support. To effectively manage the risk prior to removal, providers will need to implement a risk management plan for this equipment, which mitigates the increased risk of compromise.

2.82 Asset registers and network maps are sensitive data that would be valuable to an attacker seeking to traverse the network. Providers should ensure that they are enforcing appropriate protections for this data. Further guidance on asset management can be found on the NCSC website[14].

The exposed edge

2.83 The exposed edge of the network is the equipment that is either within customer premises, directly addressable from customer/user equipment, or is physically vulnerable. Physically vulnerable equipment includes equipment in road-side cabinets or attached to street furniture. For example, the following equipment is normally considered part of the exposed edge:

- Customer premises equipment (CPE) is equipment supplied to customers which is used, or intended to be used, as part of the network or service. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as routers, edge firewalls, SD-WAN equipment, and fixed wireless access kit;
- Base station equipment;
- Optical line terminal (OLT) equipment; and
- Multi-service access node / digital subscriber line access multiplexer (MSAN/DSLAM) equipment.

Guidance

2.84 Providers shall identify what equipment is in their exposed edge, and hence the equipment that is more accessible to potential attackers. Providers shall ensure that the compromise or disruption of parts of the exposed edge would not be a significant incident for them.

2.85 To this end, providers should physically and logically separate their exposed edge from security critical functions and ensure that no sensitive datasets are held within the exposed edge.

2.86 Given the increased likelihood of compromise, providers are strongly encouraged to implement secure boot mechanisms for all network elements in the exposed edge. This functionality allows equipment to be returned to a ‘known-good’ state, meaning that it becomes possible to recover from a compromise without requiring the physical replacement of network equipment.

[14] *NCSC CAF guidance* (NCSC, 2019) and *Asset management* (NCSC, 2021)

Retaining national resilience

2.87 Regulations 3(3)(f)-(h) impose certain requirements to ensure that network providers would be able to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom in emergency situations. In addition, the location of equipment performing each particular function, or type of function, or storing data relating to the function is one of the matters to be considered as part of providers' risk assessments under Regulation 3(3)(a).

Guidance

2.88 The resilience of the UK's national connectivity should be maintained by ensuring that a sustainable and critical level of security expertise, data and equipment are accessible from within the UK at all times. Public telecoms providers should ensure they are able to operate UK networks in emergencies where there may be reduced international connectivity or travel, and factor this into business plans where they make use of offshored capabilities. Providers should be able to restore, secure and run networks to the levels set out in this code of practice in the event they lose access to offshored facilities. In particular, guidance measures recommend that contingencies are in place so that should it become necessary to do so:

- providers have the ability to maintain 100% of normal service connectivity for a period of one month in the event of loss of international connections; and
- providers should be able to transfer into the UK functions required by UK networks to maintain an operational service, should international bearers fail.

2.89 Providers should also seek to ensure a UK-based capability to assess the risks of security compromise to the network. Such risks that could be assessed include:

- keeping network security and audit logs outside of the UK;
- approving procurement decisions on hardware and software for UK networks using overseas staff;
- relying on staff, equipment or data based outside the UK; and
- relying on third-party suppliers to ensure that basic first and second line support is available from them for the required period, where offshored expertise is lost.

Chapter crossovers

2.90 Information contained elsewhere in this code of practice is useful in understanding network architecture requirements. This includes:

- Security critical functions (Chapter 1)
- Network oversight functions (Chapter 1)
- Signalling (Chapter 2)
- Workstations (Chapter 3)
- Risk assessments (Chapter 10)

3. Protection of data and network functions

3.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 4 to protect data and network functions that could be at risk of security compromises.

3.2 Regulation 4 is set out below.

> 4. —(1) A network provider must use appropriate technical means—
>
> (a) to protect data which is stored by electronic means and relates to the operation of the public electronic communications network, in a manner which is appropriate to the data concerned, and
>
> (b) to protect functions of the public electronic communications network in a manner which is appropriate to the functions concerned.
>
> (2) A service provider must use appropriate technical means—
>
> (a) to protect data which is stored by electronic means and relates to the operation of the public electronic communications service, in a manner which is appropriate to the data concerned, and
>
> (b) to protect functions of the public electronic communications network by means of which the public electronic communications service is provided, so far as those functions are under the control of the service provider, in a manner which is appropriate to the functions concerned.
>
> (3) In paragraphs (1) and (2), “protect”, in relation to data or functions, means protect from anything involving a risk of a security compromise occurring in relation to the public electronic communications network or public electronic communications service in question.
>
> (4) The duties in paragraphs (1) and (2) include in particular duties to take such measures as are appropriate and proportionate—
>
> (a) to ensure that workstations through which it is possible to make significant changes to security critical functions are not exposed—
>
> (i) in the case of a public electronic communications network, to incoming signals,
>
> (ii) in the case of a public electronic communications service, to signals that are incoming signals in relation to the public electronic communications network by means of which the service is provided, or
>
> (iii) where, in either case, the workstation is operated remotely, to signals capable of being received by the workstation,
>
> (b) to monitor and reduce the risks of security compromises occurring as a result of incoming signals received in the network or, as the case may be, a network by means of which the service is provided, and
>
> (c) to monitor and reduce the risks of security compromises occurring as a result of the characteristics of any equipment supplied to customers which is used or intended to be used as part of the network or service.

(5) A network provider must use within the public electronic communications network signals which, by encryption, reduce the risks of security compromises occurring.

(6) A service provider must—

(a) monitor and reduce the risks of security compromises relating to customers' SIM cards occurring in relation to the public electronic communications network by means of which the public electronic communications service is provided, and

(b) replace SIM cards in cases where it is appropriate to do so in order to reduce such risks.

(7) In paragraph (6), "SIM card" means a subscriber identity module or other hardware storage device intended to store an International Mobile Subscriber Identity (IMSI) and associated cryptographic material, and the reference to replacing a SIM card includes a reference to the application to a SIM card of any process which permanently replaces one IMSI and associated cryptographic material with another.

Key concepts for understanding the requirements

Workstations and privileged access

3.3 A workstation is a computer device or an appropriately segregated and protected part of a computer device. A network can only be as secure as the devices that are able to administer the network, and so implementing an effective lock-down of administrative devices is essential. Such trusted, high-integrity devices are often known as privileged access workstations (PAWs). The following guidance in paragraphs 3.4-3.13 highlights the key aspects of workstation security for telecommunications providers to understand and implement, providing examples and background information where appropriate.

Guidance

3.4 When implementing a PAW-based lockdown, providers should include consideration of the following areas:

- Use of a 'clean' known-good operating system image to build PAWs from, rather than an OEM-provided image or other modified source;
- Approved application list - use of AppLocker or other OS-appropriate mechanisms to ensure that only authorised applications are permitted to run, minimising the potential for malicious code execution;
- Encryption - use of data at rest encryption to maintain security of data in case of theft or loss. This should incorporate use of a hardware-backed element such as a TPM, and in the case of full-disk encryption this should be unlocked with a PIN or passphrase prior to boot;
- Regular updates - security updates should be applied on a regular basis to both PAWs and management plane infrastructure to ensure vulnerabilities are patched in a timely manner;

- Approved removable media list - removable media use should be blocked by default, and only used by exception – regular data transfer should be performed via another method;
- Use of 'regular' user accounts - network administrators should use non-privileged accounts on their local PAW device for performing administrative activity within the network. This minimises the ability for malicious code to run and to compromise the entirety of the workstation, or for settings critical to security to be altered intentionally or otherwise; and
- Feed into monitoring - all PAW-like devices should be incorporated into available security monitoring systems for the detection of malicious or unusual activity.

3.5 Further information on the topic of device lockdown can be found online at NCSC's device security guidance pages[15] or secure system administration guidance[16] and for Windows devices at Microsoft's PAW guidance[17].

Remote PAWs

3.6 Sometimes it may be necessary to use PAWs remotely, rather than directly connected to the administrative zone. To protect the integrity of these devices, a standard solution would be to use an 'always on' virtual private network (VPN) to provide access to the administrative zone, without leaving the PAW vulnerable to internet-based attacks. Generic guidance and good practice around setting up VPNs and other methods for remote access can be found on the NCSC's website[18].

3.7 A remote PAW solution will likely be highly attractive to attackers as a potential route to the provider's management plane. For this reason, providers should consider implementing additional security controls to prevent and detect potential compromises. For example, when supporting remote PAWs, providers should monitor the time and location from which the PAW is accessing the network, alongside broader device health information. Remote PAWs could also implement additional logging and be patched within a minimal timeframe.

Cross-domain working and browse-down

3.8 Some administrative users may require access to corporate resources and services while simultaneously performing administrative activity. Assuming that this requirement cannot be fulfilled using a separate corporate device to the PAW, administrative users will require some form of cross-domain solution. The key requirement is to ensure that by granting access to these services, the security of the PAW is not compromised.

3.9 There are a range of solutions to providing access to corporate services to PAWs. One common solution is via the implementation of a virtualised environment existing within

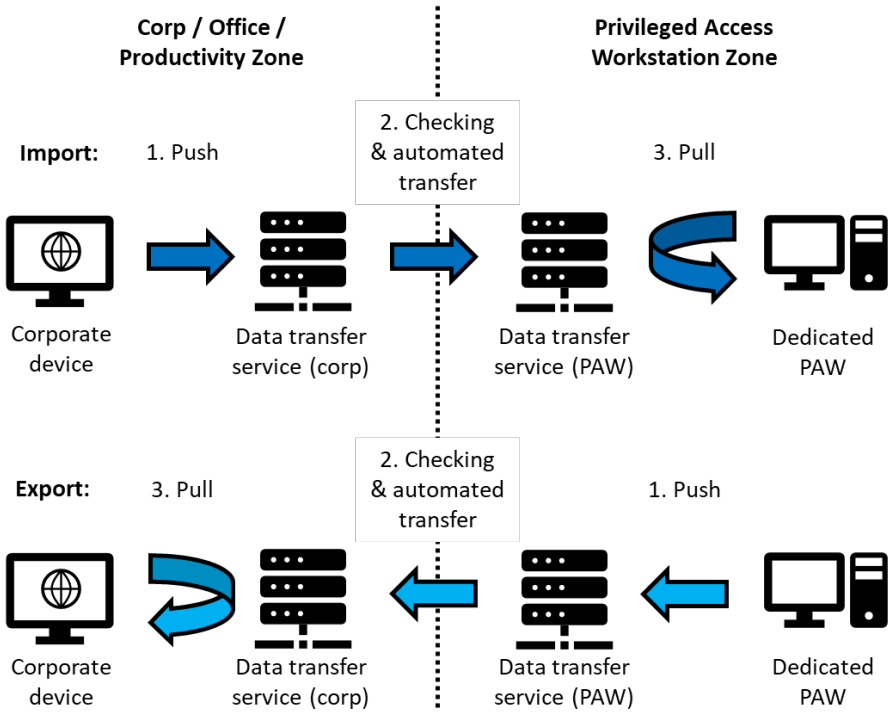
[15] *Device security guidance* (NCSC, 2021)
[16] *Secure system administration: Gain trust in your management devices* (NCSC,2020)
[17] *Securing devices as part of the privileged access story* (Microsoft, 2021)
[18] *Device security guidance: Virtual Private Networks* (NCSC, 2021) and *Device security guidance: network architectures* (NCSC, 2020)

the corporate security zone (see Figure 2). PAWs connect into a virtual machine to access corporate services, rather than accessing these services themselves.

3.10 Virtualised environments can be implemented on the PAW device itself, but this can add significant complexity. An alternative is to host a set of virtualised desktops within the corporate zone that can be accessed by PAWs over a remote access protocol such as the remote desktop protocol (RDP).

3.11 Administrative users may also need to transfer data between the administrative zone and the corporate zone. Providers should not use unmanaged removable media for this task. Instead, providers could consider using a push-pull mechanism to transfer data, as shown in Figure 7.

Figure 7: Example of cross-domain data transfer



3.12 In this example, services are set up in each security zone with the responsibility of transferring data between them using automated scripts. However, user interaction (and associated authentication) will be required to both 'push' files into the sending device, and 'pull' it out at the opposite end. This method ensures that the transfer is a deliberate action of a user, and allows transfers to be filtered, verified and monitored.

3.13 Further general advice on the use of cross domain solutions and on data transfer can be found on the NCSC website.[19] [20]

[19] *Security principles for cross-domain solutions* (NCSC, 2021)
[20] *Pattern: safely importing data* (NCSC, 2018)

SIM security

3.14 The intent of the measures within this code of practice is to ensure that an at-scale compromise of SIM cards cannot be used to disrupt the UK's telecommunications networks, or to impact subscriber confidentiality. Regulation 4(6) sets out requirements that service providers must meet in relation to SIM cards.

3.15 The following background information and guidance in paragraphs 3.16-3.26 highlights the key aspects of SIM security for public telecoms providers to understand and implement, providing examples where appropriate.

Universal Integrated Circuit Cards (UICCs)

3.16 Universal Integrated Circuit Cards (UICCs) contain credentials of the SIM/USIM (Universal Subscriber Identity Module), which are used to authenticate subscribers' access to the telecommunications network.

3.17 Historically, UICCs were used in mobile devices but are increasingly being used for fixed access as well. It is also becoming more common for UICCs to be embedded in mobile and Internet of Things (IoT) devices (eUICC or eSIM), meaning that physical card replacement will not be feasible. In the case of IoT devices with removable UICC the cost of physically accessing the device to change the SIM card would not be financially viable.

3.18 Should a SIM fail to allow access to the network, the subscriber or device will be unable to gain connectivity beyond the default emergency service access. In this case the device could be anything from a car alarm, to a mobile phone, to critical national infrastructure. In some cases, without connectivity, the device will become inoperable. Consequently, at-scale disruption of SIM cards or SIM card infrastructure is a national security concern.

3.19 UICC and eUICC manufacture is performed globally. The addition of SIM information, such as algorithms and keys, is normally performed during the personalisation process in the SIM card manufacturers' premises. There are three disruptive attack vectors of concern:

- compromise of over the air (OTA) keys allowing an attacker to remotely corrupt SIM profiles;
- misuse of eSIM or remote SIM provisioning (RSP) functionality to corrupt UICCs and eUICCs with modifiable profiles;
- vulnerability in SIMs including the use of obsolete or weakly specified algorithms.

3.20 There are two attack vectors of concern relating to subscriber confidentiality:

- where the UICC is profile-modifiable, the profile could be modified to compromise the device's connection;
- where the cryptographic key (K/Ki) is compromised, the user's traffic could be decrypted over the air interface to generate spoofed traffic.

eSIMs

3.21 Efforts must also be made to inhibit the misuse of eSIM functionality (as defined by the GSM Association). As the GSMA has endeavoured to create an open market of eSIM services, these global services could be used to disrupt service or impact confidentiality, potentially at scale. eSIM technology is in an early phase of market adoption, therefore, as they are adopted, any resilience risks to networks will need to be managed.

Guidance

3.22 Providers should review existing SIM profiles used. If vulnerabilities exist (in comparison with GSMA recommendations), providers shall establish a plan for reducing the risk in an appropriate timeframe. Many providers globally have used the routine changing of SIM cards, form factor changes, or introduction of new services, to churn out older obsolete SIM cards for newer more secure profiles. This practice is to be encouraged to increase the overall security of the SIM population in the network.

3.23 Providers should ensure the security functionality of the SIM card meets or exceeds existing GSMA security recommendations. This is especially important for eUICCs which will be difficult or impossible to replace.

3.24 Where possible, and particularly for critical IoT applications, providers should seek to update the SIM credentials promptly after they are brought into live service to reduce the supply chain risk. Where this is not possible, providers shall ensure that the SIM Card manufacturer is sufficiently trustworthy to handle the SIM credentials given the risk.

3.25 Once operational, SIM cards should be protected from potentially malicious signals. The provider shall only allow management (OTA) messages from permitted sources to reach SIM cards which are issued by the provider and attached to the provider's network.

3.26 Where UICCs allow profiles to be modified more than once (e.g. through remote SIM provisioning) then providers shall ensure that only trustworthy services can add, remove or modify profiles on the provider's network. For any eSIMs issued by the provider, the provider should use certificate-pinning to allow only approved services to make profile modifications.

Encryption

3.27 Regulation 4(5) requires network providers to use within the public electronic communications network signals which, by encryption, reduce the risks of security compromises occurring.

Guidance

3.28 Providers must ensure data is protected whether at-rest or in-transit. Where possible, providers should protect this data through secure encryption. Where data is protected by

other means, providers should maintain a formal record of this, along with the means by which the data is protected.

3.29 Where data is encrypted either at rest or in transit, it should be encrypted in line with current industry best practice. For data in transit providers should consider the use IPSec or TLS - detailed information and best practice guidance provided by NCSC can be found on its website.[21] For data-at-rest providers should consider using AES used in GCM mode using keys at least 128-bits in length. NIST guidance for data at rest can be found on the NIST website.[22]

Customer Premises Equipment (CPE)

3.30 Customer premises equipment is supplied to customers and businesses to enable connectivity.

Scope

3.31 In relation to CPE and CPE configuration, the measures in Section 3 of the code of practice align with Regulation 4(4)(c) and only apply when these devices are supplied to customers by public network providers and are used, or intended to be used, as part of the public network or service. This excludes consumer electronic devices such as mobile phones and tablets. CPE in scope includes devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit, where these are provided and managed by the provider. CPE provided to business customers is in scope alongside that provided to retail consumers.

Background

3.32 While providers are responsible for the security of the default configuration of the devices they supply, they are not responsible for security weaknesses caused by customers independently adjusting the configuration of CPE after distribution.

3.33 Additional protections to secure devices will be implemented through the Product Security and Telecommunications Infrastructure Bill.[23] The Bill will give the government the necessary powers to set minimum security requirements for the manufacturers, importers, and distributors of consumer connectable products. It also defines the type of businesses that must comply with these security requirements, and prevent the sale of products that do not meet these requirements. The initial security requirements the government intends to set out for manufacturers of relevant connectable products will align to the top three guidelines in the code of practice for consumer IoT security:[24]

- ensuring that consumer connectable products do not use universal default passwords;

[21] *Using IPSec to protect data* (NCSC, 2016) and *Using TLS to protect data* (NCSC, 2021)
[22] *Guide to storage encryption technologies for end user devices* (NIST, 2007)
[23] *Product Security and Telecommunications Infrastructure Bill*
[24] *Code of practice for consumer IoT security* (DCMS, 2018)

- implementing a means to manage reports of vulnerabilities; and
- providing transparency on how long, at a minimum, the product will receive security updates.

3.34 For the customer, the CPE provides the separation between the internal network and the internet. Many customer devices rely on this separation to protect their local network.

3.35 If a CPE has security vulnerabilities, or has been configured in a way that leaves it vulnerable, it can lead to the following:

- either compromised CPEs or other consumer devices being used as part of botnets – threatening UK national infrastructure (for example, in 2016, the Mirai botnet was used to attack the DNS provider Dyn, as well as later targeting UK banks);
- compromise of devices owned by the customer, infringing on their privacy or product availability; and
- the CPE to be used to carry out cybercrime, allowing criminals to proxy their activities.

Guidance

3.36 Providers shall ensure a baseline level of security for CPE. This will help to ensure that both network infrastructure and customers are protected at the point where the CPE is distributed. Additionally, providers shall ensure that the CPE has a secure default configuration, which should include limiting inbound connections by default. Providers shall also ensure that the CPE will receive regular security updates throughout the device's lifetime.

3.37 Where the provider performs on-going management of the CPE, they shall ensure that this is performed securely. In particular, the provider shall prevent the CPE's management interfaces (e.g. TR-069) from being exposed wider than necessary, shall only allow the use of secure management protocols and shall ensure that their CPE credentials are unique to the device and not guessable.

Chapter crossovers

3.38 Information contained elsewhere in this code of practice is useful in understanding the protection of data and network functions. This includes:

- Security critical functions (Chapter 1)
- Network oversight functions and the principle of 'assumed compromise' (Chapter 1)
- Management plane, especially browse up architectures (Chapter 2)
- Signalling plane, especially risks from incoming signals & exposed edge (Chapter 2)
- Virtualisation fabric (Chapter 2)
- National resilience (Chapter 2)

4. Protection of certain tools enabling monitoring or analysis

4.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 5 to protect certain tools that enable the monitoring or analysis in real time of the use of the network or service, or the monitoring or analysis of the content of signals.

4.2 Regulation 5 is set out below.

> 5.—(1) This regulation applies in relation to a public electronic communications network or public electronic communications service if the network or service includes tools that enable—
>
> (a) the monitoring or analysis in real time of the use or operation of the network or service, or
>
> (b) the monitoring or analysis of the content of signals.
>
> (2) If the tools are stored on equipment located outside the United Kingdom, the network provider or service provider must take measures to identify and reduce the risks of security compromises occurring as a result of the tools being stored on equipment located outside of the United Kingdom.
>
> (3) The network provider or service provider must ensure that the tools—
>
> (a) are not capable of being accessed from a country listed in the Schedule, and
>
> (b) are not stored on equipment located in a country so listed.

Key concepts for understanding the requirements

Countries listed in the Schedule

4.3 The Schedule to the regulations sets out the countries that pose the greatest risk to the security of UK public telecoms networks and services. Monitoring and analysis tools of the type described in Regulation 5(1) may not be located in these listed countries due to the sensitivity of those tools and the access they provide to management of UK networks and services. Providers must also ensure that such monitoring and analysis tools are not capable of being accessed from those listed countries.

4.4 Tools that enable monitoring or analysis in real time under Regulation 5 include functions that allow the collection of traffic from the network (which are network oversight functions) and functions that include network monitoring of speech and data. These must not be accessible from any location listed in the Schedule to the regulations.

4.5 If new risks emerge from other countries in the future, the government may look to update the Schedule list. The code of practice sets out steps to help providers account for any such scenario, including the use of business continuity plans to cover that risk.

Risk assessment

4.6 Regulation 5(2) sets out the need for providers to take measures to identify and reduce the risks of security compromises occurring as a result of storing monitoring and analysis tools outside of the UK. Written assessments of these risks are addressed under Regulation 11(2)(b).

4.7 Relevant activity to consider for identifying such risks may include, for example, the risks associated with performing the following activity outside the UK:

- security analysis and anomaly detection, including the operation of security operation centres (SOCs);[25]
- network performance and diagnostic analysis, including the operation of network operation centres (NOCs);
- privileged access, where that privileged access grants potential access to real-time network information or the content of transmissions, such as through the interaction with network equipment;
- interaction with network or system probes;
- interaction with the virtualisation fabric;
- access to real-time network orchestration systems or controllers.

4.8 Relevant considerations may include the risk of unauthorised conduct, the risks associated with local laws or their enforcement, or a lack of appropriate understanding of UK-specific risks by local staff. This is not an exhaustive list and just a sample of activities that should make up part of a risk assessment.

Chapter crossovers

4.9 Information on monitoring and analysis in Chapter 5 may be useful in understanding the protection of tools enabling monitoring or analysis.

[25] *Security operations centre (SOC) buyers guide* (NCSC, 2016)

5. Monitoring and analysis

5.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 6 to monitor and analyse the use of their networks in order to identify any security compromises.

5.2 Regulation 6 is set out below.

> 6.—(1) A network provider must take such measures as are appropriate and proportionate to monitor and analyse access to security critical functions of the public electronic communications network for the purpose of identifying anomalous activity.
>
> (2) A network provider or service provider must take such measures as are appropriate and proportionate—
>
> (a) to monitor and analyse the operation of security critical functions of the public electronic communications network or public electronic communications service for the purpose of identifying the occurrence of any security compromise, using automated means of monitoring and analysis where possible, and
>
> (b) to investigate any anomalous activity in relation to the network or service.
>
> (3) The duty in paragraph (2) includes in particular a duty—
>
> (a) to maintain a record of all access to security critical functions of the network or service, including the persons responsible (where identifiable),
>
> (b) to identify and record all cases where a person's access to security critical functions of the network or service exceeds the person's security permission,
>
> (c) to have in place means and procedures for producing immediate alerts of all manual amendments to security critical functions,
>
> (d) to analyse promptly all activity relating to security critical functions of the network or service for the purpose of identifying any anomalous activity,
>
> (e) to ensure that all data required for the purposes of a duty under paragraph (1) or sub-paragraphs (a) to (c) is held securely for at least 13 months,
>
> (f) to take measures to prevent activities that would restrict the monitoring and analysis required by this regulation, and
>
> (4) A network provider or service provider must record the type, location, software and hardware information and identifying information of equipment supplied by the network provider or service provider which is used or intended to be used as part of the public electronic communications network or public electronic communications service.

Key concepts for understanding the requirements

Monitoring and analysis

5.3 While not directly a set of preventative controls, security monitoring fundamentally underpins the security posture of a network or system. Inadequate coverage of devices or networks from a logging and monitoring perspective will fundamentally limit the ability to identify and subsequently determine the root cause of anomalous activity and may also limit the ability to understand the extent of such activity without recourse to extremely labour intensive and expensive forensic work.

5.4 Enabling the collection of relevant information from appropriate devices or systems within a provider environment will permit post-event analysis to be undertaken with significantly more ease and allow providers to gain more confidence in their ability to respond to security-related events.

5.5 While collection of this information will permit a range of post-incident analysis and other such activity, proper implementation of monitoring and alerting capabilities on top of this will allow providers to identify malicious or unusual behaviour taking place in near real time, enabling response prior to a major or catastrophic event taking place. General guidance and principles on effective monitoring can be found on the NCSC website.[26]

Guidance

5.6 The following guidance in paragraphs 5.7-5.22 highlights the key aspects of monitoring and analysis for telecommunications providers to understand and implement, providing examples and further background information where appropriate.

Normal and anomalous activity

5.7 Effective monitoring of network behaviour is dependent on a detailed understanding of the network. This encompasses asset management, but also requires a clear security architecture and an understanding of the behaviour of network equipment. Providers are unlikely to be able to effectively monitor their networks without first collating this information.

5.8 This information is essential to determining a relative state of 'regular' activity and ‘anomalous’ activity, both between components within a network, and the behavioural state of network equipment. Anomalous activity is activity in a network which does not conform to regular network traffic, or conform to the regular behaviour of network equipment. Exactly what constitutes anomalous activity can only be defined by the network provider itself as they have the best knowledge of what normal activity looks like.

[26] *NCSC CAF guidance: C.1 Security monitoring* (NCSC, 2019)

Network-based monitoring

5.9 Providers should use network-based monitoring, specifically the monitoring of signals both internally and at the edge of the provider's network to determine anomalous behaviour.

5.10 What to monitor can only be defined by the network provider itself as they have the best knowledge of their networks. Providers should base this decision on risk, recording both details of their approach to monitoring and the justification for that approach. In making this decision, providers should consider factors such as:

- the criticality or sensitivity of interfaces and systems;
- the exposure of the systems or interfaces to attack;
- the vulnerability of interfaces and equipment, which may be higher for legacy and out-of-mainline support network equipment; and
- the approaches and interfaces used by security testers, or by attackers during past compromises.

5.11 In determining where to monitor, providers should give consideration to the following security boundaries:

- between the provider's network and external networks such as customer networks, partner networks, the internet and international telecommunications networks;
- between the provider's network and third-party administrator networks, such as those owned by network equipment suppliers and MSPs;
- between the provider's security critical functions, and functions in the access network or exposed edge; and
- between management networks and other networks, including internal networks.

Host-based monitoring

5.12 Host-based monitoring involves monitoring the behaviour of network equipment and supporting devices within the equipment to identify anomalous activity. Providers should utilise host-based monitoring wherever possible in their networks, and particularly in the protection of sensitive or critical functions.

5.13 Host-based monitoring may incorporate operating system, application, and virtual machine behaviour, including detailed information at the process level. This may involve deployment of an on-host agent to collect the required information, or simply the forwarding of existing operating system-level logging data.

5.14 Providers should be aware that should a host become compromised, the monitoring information produced by a host may also be compromised or may become unreliable. To protect this information, 'regular' administrative users should not be able to alter the collection of logging or audit data without 'high priority' alerts being raised to flag this event. Similarly, administrative users not responsible for maintenance of audit systems or analysis of its content should not be able to view or otherwise affect already-collected log data. Additionally, monitoring information should be exported from the device as

quickly as possible, ideally in real-time or near real-time. Further guidance on host-based logging can be found on the NCSC website.[27]

Protection of monitoring data

5.15 Monitoring data provides information about network behaviour and can contain sensitive data such as administrative passwords. As such, providers need to ensure that monitoring data is protected. Should there be any customer data recorded within any monitoring data, this data should be appropriately sanitised.

Effective Analysis

5.16 Security analysis allows benefit to be gained from monitoring by identifying anomalous activity. Providers frequently co-locate security analysts at a security operations centre (SOC).

5.17 For security analysts to identify anomalous activity, they will need access to detailed information about the network alongside monitoring data. Providing analysts with a clear picture of expected network activity provides them with context for the monitored environment, allows them to focus their activity, and maximises the protection they will be able to afford the network. The necessary network information will likely need to be collated from architectural design documentation, asset management systems, configuration management systems, product and interface specifications, network change plans and change systems (known as tickets).

5.18 Providers should also aim to provide analysts with monitoring data sourced from both network-based and host-based monitoring. To support effective analysis, there may be benefit in merging these datasets to provide a single picture of network activity and allow analysts to correlate information across a range of infrastructure.

5.19 Further, to help build a 'story' of activity, monitoring data should link administrative actions to network administrators and on to tickets. This applies whether the administrator is internal or employed by a third-party. With this information it becomes possible for analysts to build a chain of events, establish the root cause of incidents, and prevent a recurrence of that incident.

Proactive security monitoring

5.20 Analysis of monitoring data is sometimes viewed solely as a reactive exercise based upon configured alerting, or as a response to an incident. Providers should seek to perform proactive analysis, or threat hunting, to assess whether activity is present that would not necessarily trigger security alerts. Such analysis should consider behavioural information alongside security alerts.

5.21 Analysts will need to be sufficiently skilled in understanding network and attacker behaviour. They will often benefit from access to threat intelligence feeds. When

[27] *Device security guidance: Logging and protective monitoring* (NCSC, 2021)

protecting large-scale networks, providers should have access to sufficient skilled analysts to support multiple investigations of anomalous behaviour at any one time.

5.22 General advice on proactive security monitoring can be found on the NCSC website.[28]

Border Gateway Protocols

5.23 Border Gateway Protocol (BGP) is a signalling protocol which is used to route data between service providers. This protocol can be hijacked, resulting in traffic being deliberately misrouted round the internet. It occurs when either a false ownership claim, or a false route to an IP address is advertised externally by an entity that neither routes to, nor owns the address. As an example, BGP misrouting was a factor in the global outage of Facebook on 4 October 2021.[29]

Guidance

5.24 Providers are recommended to use a monitoring service/tool (e.g. NCSC's BGP Spotlight) to detect potential hijacks and to respond appropriately when hijacks are detected. It is recommended that providers ensure their network operation centres (NOCs) are alerted to hijacks and have plans to respond based on the type of hijack. In extremis, this should include blocking traffic from being routed to the hijacked destination.

5.25 Hijacks of internal UK-to-UK provider traffic shall be particularly inhibited, and UK-to-UK routes should be monitored for anomalous activity (such as the inclusion of unexpected transit networks). UK providers should share enough information with each-other to allow hijacks of internal traffic to be easily detected, and a fallback approach to routing should be established between providers in the event of a persistent hijack.

Threat hunting

5.26 Analysis of log information is sometimes viewed solely as a reactive exercise based upon configured alerting, or as a response to an incident. Collected log information should be used for proactive analysis to assess whether activity is present that would not trigger previously-configured alerts.

5.27 Threat intelligence information feeds will likely be required as reference material for potential attacker behaviour, and a good knowledge of the typical behaviour of monitored networks and the capabilities of monitoring systems will be necessary. Suitably skilled staff to operate these feeds is also required, whether that be via existing skilled staff or appropriate training.

5.28 Proactive analysis will need to be based upon assessed threat information relating to likely attacks and risks to a provider's network or service. The risks should be chosen by

[28] *NCSC CAF guidance: C.2 Proactive security event discovery* (NCSC, 2019)
[29] *More details about the October 4 outage* (Meta, 2021)

individual providers for this purpose based upon their threat profile and will likely change over time.

Regular scanning

5.29 Attackers are increasingly scanning networks to find exposed vulnerabilities. Providers should regularly, ideally continuously, scan their networks to detect vulnerabilities, mistakenly exposed services and ports, or out-of-date equipment.

Retaining equipment logs for 13 months

5.30 The retention of logging data ensures that if there is a security compromise it is possible to identify any changes in the network that may have contributed to the compromise. These logs must be maintained for 13 months as this will ensure the retention of any changes made on a once-yearly basis, for example end of year processes.

5.31 Equipment logs are produced by network equipment to record the equipment's behaviour and the actions taken by administrative staff in relation to that equipment. Equipment logs do not normally contain customer data. Providers should sanitise any customer data prior to storage.

Chapter crossovers

5.32 Information contained elsewhere in this code of practice is useful in understanding monitoring and audit requirements. This includes:

- Security critical functions (Chapter 1)
- Network oversight functions (Chapter 1)
- Countries listed in the Schedule (Chapter 4)
- Testing (Chapter 13)

6. Supply chain

6.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 7 to identify and reduce the security risk arising from actions taken or not taken by third party suppliers.

6.2 Regulation 7 is set out below.

> 7.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service as a result of things done or omitted by third party suppliers.
>
> (2) In this Regulation, “third party supplier”, in relation to a network provider or service provider, means a person who supplies, provides or makes available goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.
>
> (3) The risks referred to in paragraph (1) include—
>
> (a) those arising during the formation, existence or termination of contracts with third party
>
> suppliers, and
>
> (b) those arising from third party suppliers with whom the network provider or service provider has a contractual relationship contracting with other persons for the supply, provision or making available of any goods, services or facilities for use in connection with the provision of the public electronic communications network or public electronic communications service.
>
> (4) A network provider or service provider (“the primary provider”) must take such measures as are appropriate and proportionate—
>
> (a) to ensure, by means of contractual arrangements, that each third party supplier—
>
> (i) takes appropriate measures to identify the risks of security compromises occurring in relation to the primary provider’s network or service as a result of the primary provider’s use of goods, services or facilities supplied, provided or made available by the third party supplier, to disclose any such risks to the primary provider, and to reduce any such risks,
>
> (ii) where the third party supplier is itself a network provider and is given access to the primary provider’s network or service or to sensitive data, take measures for the purposes mentioned in section 105A(1) of the Act equivalent to those that the primary provider is required to take in relation to the primary provider’s network or service,

(iii) takes appropriate measures to enable the primary provider to monitor all activity undertaken or arranged by the third party supplier in relation to the primary provider's network or service, and

(iv) takes appropriate measures to co-operate with the primary provider in the resolution of incidents which cause or contribute to the occurrence of a security compromise in relation to the primary provider's network or service or of an increased risk of such a compromise occurring,

(b) to ensure that all network connections and data sharing with third party suppliers, or arranged by third party suppliers, are managed securely, and

(c) to have appropriate written plans to manage the termination of, and transition from, contracts with third party suppliers while maintaining the security of the network or service.

(5) A network provider must—

(a) ensure that there is in place at all times a written plan to maintain the normal operation of the public electronic communications network in the event that supply or support from a third party supplier is interrupted, and

(b) review that plan on a regular basis.

Key concepts for understanding the requirements

Management of third party suppliers

6.3 A supply chain involves contractual arrangements between the provider and third party supplier, or between third party suppliers. If used and managed correctly, these contractual arrangements can help improve the understanding of the supply chain, assist in investigations of security incidents and assist testing of security mitigations or processes. More general advice on supply chain security can be found on the NCSC website.[30]

Guidance

6.4 The intent of the security framework in this area is to ensure providers fully understand and reduce supply chain risks. One of the key aims is to ensure that providers flow-down security requirements to third party suppliers by means of contractual arrangements, ensuring the third party supplier is working to the same security standards.

6.5 Providers should consider whether they may require their third party suppliers' support to perform effective network audits and effective security testing of the provider's network. For example, where the provider's network and a third party supplier's network

[30] *Supply chain security guidance* (NCSC, 2018)

are closely integrated, security testers will better simulate attacker behaviour if they are permitted to test both networks simultaneously.

6.6 Providers should also consider the support they may need from their suppliers should an incident or compromise occur, potentially via the supplier. As providers are responsible for the risk to their network or service, they should ensure that suppliers inform them about incidents that may affect the provider's network or service, and that they can access the data required to effectively investigate incidents relating to their network or service, including accessing any relevant data that may be owned by the supplier.

6.7 It should also be noted that network and service providers are ultimately responsible for the security of their networks and cannot outsource this responsibility to third parties. Where providers do outsource aspects of operations to a third party, responsibility to comply with the obligations contained within new sections 105A-D of the Communications Act 2003 remain with the provider. The provider therefore needs to have sufficient internal capacity to meet those obligations.

Data sharing

6.8 When working with external suppliers, providers need to effectively manage the risk to any data that needs to be shared with the supplier. Suppliers are often targeted by attackers interested in their supply chain, and compromising supplier's systems may provide an attractive route to obtaining nationally significant datasets. In this context 'data' includes both user data and network data.

Guidance

6.9 Under normal governance practices, decisions relating to a data set will be taken by a 'data owner' who is responsible for the data's protection. As a first principle, data sharing should be limited to only the data necessary for the purpose. In most scenarios, the sharing of data from the operational network is unnecessary and should be avoided. Where data relating to the operational network needs to be shared, it will often need to be sanitised or anonymised first to protect user and network data.

6.10 It is recommended that providers establish systems that allow the provider to retain its data within its control whenever possible. This allows the provider to authenticate and authorise any access to their data using MFA, understand full details of that access, control any movement of data, and monitor and detect compromises. Any such data-sharing system is ideally separate from the provider's corporate and operational systems, ensuring that the data-sharing requirement does not give suppliers wider access to other systems.

6.11 If data must be transferred off the provider's network and into the supply chain, there should be a process to authorise the transfer, validate that the data has arrived, and ensure that it is deleted irretrievably when the reason for the transfer is completed. The

provider should confirm by both audit and testing that the security of their data, wherever it is held in the supply chain, is appropriately protected.

Third party administrators

Background

6.12 Administrative access presents a significant security risk to electronic communications networks. Providers grant administrative access to third party administrators for a variety of reasons. Administrative services provided by an external company within a broader umbrella business or provider group should be considered as third-party administrators. Third party administrators may also be MSPs as part of a managed service contract, or equipment supplier as part of a third-line support function.

6.13 Due to their nature, third party administrators may gain access to multiple electronic communications networks. This means that a single set of administrators, and administrative systems, can negatively impact multiple networks. This makes third party administrators particularly attractive to attackers. Should third party administrator systems be compromised, or a third party administrator be malicious, multiple UK networks could be exploited or disrupted simultaneously.

6.14 As an example, in December 2018 the government attributed a Chinese espionage operation against global MSPs to threat group APT10. This operation was of unprecedented size and scale, targeting several global MSPs, with attacks ongoing since at least 2016. After compromising the MSP, the group exfiltrated a large volume of data from multiple victims, exploiting compromised MSP networks and those of their customers through trusted connections. This indirect approach of reaching many through only a few targets provides a high-profile example of a supply chain attack and a new level of cyber espionage maturity.

6.15 While both managed service access and third-line support can present a risk to UK networks, the risks associated with managed service access is particularly significant due to increased scope and frequency of network access, and frequency of data access. The use of third-party administrators by UK networks almost certainly increases the overall threat of cyber-attack, requiring careful risk management by industry.

6.16 The use of third party administrators also creates a risk due to the dependence of the provider on the third party administrator for the continued operation of networks. Should the third party administrator be no longer able to provide the service, this is likely to have an operational impact.

Guidance

6.17 Overall, providers should be looking to reduce the risks to networks due to third-party administrators, and specifically reduce the risk that a single attack within a third party administrator could negatively impact multiple networks.

6.18 Providers should ensure that the third-party administrator is enforcing separation to prevent its network from being connected to another provider's networks via the third-party administrator. Providers will require a robust security boundary between their network and the third-party administrator, including the ability to control access to infrastructure, control any dataflows and limit any administrative accesses across the boundary. Such controls should be applied even when the third-party administrator is part of the same umbrella company or provider group.

6.19 Providers should ensure that a compromise of the third-party administrator cannot compromise or disrupt multiple providers. Administrative workstations within third-party administrators should only be able to access a single provider's network. Such workstations may be virtualised, allowing a single device to support multiple operators.

6.20 Further government work is ongoing to address the security risks associated with MSPs. In November 2021, the government published its response to a call for views on the government's preliminary proposals for managing the cyber risks associated with MSPs.[31] Those proposals included education and awareness campaigns, certification or assurance marks, minimum requirements in public procurement and legislation. All proposals received positive feedback, and the government responded by recognising that a range of audience-specific interventions will be needed when addressing the security of managed services.

6.21 The government has also published proposals for legislation to improve the UK's cyber resilience.[32] This included the proposal to add 'managed services' to the list of 'digital services' regulated under the Network and Information Systems (NIS) Regulations 2018. This change would require MSPs to comply with the duties currently set out in the NIS regulations, including taking appropriate and proportionate measures to manage risks, and reporting relevant incidents to the Information Commissioner's Office (ICO) as the relevant regulator.

Network equipment suppliers

Guidance

6.22 Providers procure their network equipment from a set of suppliers. Equipment and contracting risks should therefore be considered as part of relationships with third party suppliers.For the purposes of this guidance, third party supplier 'equipment' includes both hardware and software.

6.23 The following guidance in paragraphs 6.24-6.35 highlights the key areas that telecommunications providers need to understand when working with network equipment suppliers, providing examples and background information where appropriate.

[31] *Government response to the call for views on supply chain cyber security* (DCMS, 2021)
[32] *Proposal for legislation to improve the UK's cyber resilience* (DCMS, 2022)

Third party supplier dependency

6.24 Network equipment supply should not be viewed as a single transaction. There are four components:

- supply of the equipment;
- an essential flow of technical information as part of a support contract - comprising training, fixes, updates, enhancements, advice, direct network troubleshooting and replacement of failed equipment;
- the upgrade/replacement of the equipment during a network refresh; and
- the decommissioning of equipment.

6.25 Where the equipment will be difficult to replace due to time and cost, the provider is establishing a long-term reliance on the supplier. To some degree, the provider is now reliant on the third party supplier to ensure that the provider's network stays secure. Providers should ensure that the quantity of equipment procured from any network equipment supplier is kept to an acceptable level to limit reliance on the network equipment supplier, and to limit the associated resilience risks.

6.26 The equipment that is most difficult to replace tends to be within nationally distributed networks, particularly the access network. In this network it is costly and time-consuming for providers to replace equipment as there is a very large quantity of equipment and it is geographically distributed. The following subcomponents are involved in 'access' networks:

- mobile access (base stations and antennas);
- fixed access (DSLAMs, MSANs, OLTs etc); and
- transport (fibre and microwave links and equipment).

Fault or vulnerability in network equipment

6.27 Low product quality could result in disruptive security compromises within providers' networks. This risk includes two types of cyber event:

- systemic failure due to software or firmware fault which could involve multiple third party suppliers if they use a common component; and
- equipment vulnerability exploited by an attacker to cause disruptive effect or compromise the network.

6.28 If there are product quality issues (be it from legacy build environments, poor software development processes or poor vulnerability management), a flaw in one or more products could potentially result in widespread equipment failure or be turned into an exploitable vulnerability, allowing the attacker to gain control of network equipment.

6.29 Regulation 7 is intended to ensure that third party supplier security and quality is sufficiently valued by providers to reduce the risk of security compromise to their networks and services and drive security improvements in third party suppliers. This can

be achieved through providers regularly performing an evidence-based assessment of network equipment suppliers' equipment security, recognising the supplier's positive and negative security behaviours, and ultimately valuing a network equipment supplier's good security practises during procurement.

The Vendor Security Assessment

6.30 The NCSC's Vendor Security Assessment (VSA) provides advice on how providers should assess network equipment suppliers' security processes and the security of their equipment, alongside their usual assessments of network equipment supplier performance and interworking. The purpose of the approach is for providers to objectively quantify the cyber risk due to use of the network equipment supplier's equipment. This is performed by gathering objective, repeatable evidence on network equipment suppliers' security processes and the security of the network equipment.

6.31 Evidence on the network equipment supplier's security practices should be based on the network equipment supplier's implemented practices, rather than its documentation. Given this, one valuable method of assessing the security of network equipment suppliers' equipment is through testing. This should include positive testing, negative testing and fuzzing of the equipment's interfaces. Ideally this should be automated and repeated at scale to stress test the equipment's interfaces.

6.32 The VSA will be updated periodically in the future, to keep pace with new threats and technologies. On its own, the VSA does not form part of the code and will not be necessary or sufficient to meet new supply chain legal requirements, but it is important advice that providers can use to help their compliance.

6.33 While providers are responsible for ensuring the equipment that they use is sufficiently secure, achieving secure equipment is best achieved through collective security research and transparency. To this end, it is highly recommended that providers ensure that their suppliers publish a response to the NCSC's VSA, which affords the provider with sufficient information to allow them to make an informed decision about the security of network equipment suppliers' equipment.

6.34 During procurement processes for security critical functions, providers shall ensure that security considerations are a significant factor in determining the procurement outcome. These security considerations should relate to the information gathered during the vendor security assessment, recognising the benefit of any security features that will provide measurable improvement to the security of the network, and the additional costs of mitigating any additional risks or unknowns.

The 'Trojan horse' threat

6.35 This threat covers malicious functionality added to equipment either intentionally by the third party supplier or covertly by a hostile actor who has access to the third party supplier's hardware design or manufacture, or software development systems. As part of the provider's governance of their supply chain, they should assess whether the third

party supplier's corporate and development systems are sufficiently trustworthy given the sensitivity of the equipment being supplied and the information that will be made available to the third party supplier.

Chapter crossovers

6.36 Information contained elsewhere in this code of practice is useful in understanding the supply chain requirements. This includes:

- Customer premises equipment (Chapter 3)
- Countries listed in the Schedule (Chapter 4)
- Online and offline copy (Chapter 8)

7. Prevention of unauthorised access or interference

7.1 This chapter provides guidance for providers on the measures to be taken in accordance with Regulation 8 to prevent the occurrence of security compromises that consist of unauthorised access to their networks or services.

7.2 Regulation 8 is set out below.

> 8.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to prevent the occurrence of security compromises that consist of unauthorised access to the public electronic communications network or public electronic communications service.
>
> (2) The duty in paragraph (1) includes in particular a duty—
>
> (a) to ensure that persons given responsibility for the taking of measures on behalf of the network provider or service provider for the purposes mentioned in section 105A(1) of the Act ("the responsible persons") have an appropriate understanding of the operation of the network or service,
>
> (b) to require multi-factor authentication for access to an account capable of making changes to security critical functions,
>
> (c) to ensure that significant or manual changes to security critical functions must, before the change is made, be proposed by one person authorised by the network provider or service provider in question and approved by another person from among the responsible persons,
>
> (d) to avoid using default credentials wherever possible, in particular by avoiding, as far as possible, using devices and services with default credentials that cannot be changed,
>
> (e) where, despite sub-paragraph (d), default credentials have been used, to assume, for the purpose of identifying the risks of security compromises occurring, that any such default credentials are publicly available,
>
> (f) to ensure that information which could be used to obtain unauthorised access to the network or service (whether or not stored by electronic means) is stored securely,
>
> (g) to carry out changes to security critical functions through automated functions where possible, and
>
> (3) A network provider must have in place, and use where appropriate, means and procedures for isolating security critical functions from signals which the provider does not believe on reasonable grounds to be safe.
>
> (4) A network provider or service provider must limit, so far as is consistent with the maintenance and operation of the public electronic communications network or the provision of the public electronic communications service, the number of persons given security permissions and the extent of any security permissions given.

(5) A network provider or service provider must also—

(a) ensure that passwords and credentials are—

(i) managed, stored and assigned securely, and

(ii) revoked when no longer needed,

(b) take all appropriate and proportionate measures to ensure that each user or system authorised to access security critical functions uses a credential which identifies them individually when accessing those functions,

(c) take appropriate measures, including the avoidance of common credential creation processes, for the purpose of ensuring that credentials are unique and not capable of being anticipated by others,

(d) keep records of all persons who—

(i) in the case of a network provider, have access to the public electronic communications network otherwise than merely as end-users of a public electronic communications service provided by means of the network, and

(ii) in the case of a service provider, have access to the public electronic communications service otherwise then merely as end-users of the service, and

(e) limit the extent of the access to security critical functions given to a person who uses the network or service to that which is strictly necessary to enable the person to undertake the activities which the provider authorises the person to carry on.

(6) A network provider or service provider must ensure—

(a) that no security permission is given to a person while the person is in a country listed in the Schedule, and

(b) that any security permission cannot be exercised while the person to whom it is given is in a country so listed.

Key concepts for understanding the requirements

Explaining “access” to the PECN or PECS

7.3 In this context, “access” to a PECN or PECS covers both logical/virtual access and physical access by an individual as well as machine-to-machine access.

Chapter crossovers

7.4 Information contained elsewhere in this code of practice is useful in understanding the prevention of unauthorised access or interference. This includes:

- Security critical functions (Chapter 1)
- Network oversight functions (Chapter 1)
- Management plane, especially browse up architectures (Chapter 2)
- Countries listed in the Schedule (Chapter 4)
- Third party administrators (Chapter 6).

8. Preparing for remediation and recovery

8.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 9 to prepare for the occurrence of security compromises with a view to limiting the adverse effects of security compromises and being able to recover from them.

8.2 Regulation 9 is set out below.

> 9.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to prepare for the occurrence of security compromises with a view to limiting the adverse effects of security compromises and enabling the provider to recover from security compromises.
>
> (2) The duty in paragraph (1) includes in particular a duty—
>
> (a) to create or acquire, for the purposes mentioned in that paragraph, and to retain within the United Kingdom—
>
> (i) an online copy of information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service, and
>
> (ii) so far as is proportionate, an offline copy of that information,
>
> (b) to replace copies held for the purpose of sub-paragraph (a) with reasonable frequency, appropriate to the assessed security risk of the network or service,
>
> (c) to have means and procedures in place—
>
> (i) for promptly identifying the occurrence of any security compromise and assessing its severity, impact and likely cause,
>
> (ii) for promptly identifying any mitigating actions required as a result of the occurrence of any security compromise,
>
> (iii) where the occurrence of a security compromise gives rise to the risk of a connected security compromise, for preventing the transmission of signals that give rise to that risk,
>
> (iv) for dealing with the occurrence of a security compromise within a reasonable period appropriate to the assessed security risk of the network provider or service provider, and without creating any risk of a further security compromise occurring,
>
> (v) for ensuring that, if the network provider or service provider is unable to take steps for the purposes of preventing any adverse effects (on the network or service or otherwise) arising from the occurrence of a security compromise within the period of 14 days beginning with the day on which it occurs, the network provider or service provider is able to prepare a written plan as to how and when the provider will take such measures,
>
> (vi) for dealing with any unauthorised access to, or control over, security critical functions by taking action as soon as reasonably possible, and without creating

any risk of a further security compromise occurring, to ensure that only authorised users have access to the network or service, and

(vii) for replacing information damaged by security compromises with the information contained in the copy referred to in sub-paragraph (a).

(3) For the purposes of paragraph (2)(a)—

(a) an "online copy" is a copy that is held on the public electronic communications network or public electronic communications service in question, and

(b) an "offline copy" is a copy that is stored in such a way that it is not exposed to signals conveyed by means of the network or service in question.

Key concepts for understanding the requirements

The necessary information to maintain the normal operation of the network/service

8.3 Regulation 9(2)(a)-(b) sets out requirements in relation to the information that providers must create or acquire, retain within the UK and replace with reasonable frequency in order to ensure the normal operation of the relevant network or service. As to the format of such information, providers must hold:

- a copy of this information on the network or service in question (i.e. an "online copy") and;
- so far as is proportionate, a copy that is stored in such a way that it is not exposed to signals conveyed by means of the network or service in question (i.e. an "offline copy").

8.4 The aim of these requirements is to ensure that providers can maintain the normal operation of a network or service by having access to the information which is necessary to get networks or services back up and running. For the avoidance of doubt, these requirements are not in place to ensure that providers replace all user data that may have been lost during a security compromise.

Keeping an offline copy

8.5 Regulation 9(3)(b) defines an "offline copy" as "a copy that is stored in such a way that it is not exposed to signals conveyed by means of the network or service in question". Keeping an offline copy of this information could be achieved through cloud backups, where the cloud service is not itself a part of the network it is backing up and not exposed to signals from the network.

8.6 When the offline backup is not in use it needs to be digitally disconnected. Unlike conventional backup storage, it is not possible to take cloud storage offline by simply unplugging it. However, steps can be taken to apply a similar level of protection:

- Identity management - the first step to protect cloud storage is secure account identity. All users able to access cloud backups should be properly protected in

line with NCSC advice.[33] Without a trusted identity, ransomware should not be able to request access to a providers' cloud storage and encrypt it without the provider's permission.

- Client management - a backup client is a device with credentials to access cloud storage. Cloud backup clients should not have valid credentials while the cloud storage is not in use. The number of backup clients should also be kept to a minimum with standard user devices unable to modify cloud backups directly. If this practice is followed, a ransomware infection can only compromise the cloud backup if it occurs on an authorised client and while the cloud backup is being used.
- Access control - access control should be configured to only allow authorised clients to create new backups (or append to existing ones) and deny connection requests while the storage is not in use ('cold' storage). If a ransomware infection occurs while the cloud backup is offline, it will be denied connection requests. This means it will not be able to reach the cloud storage, giving the same level of confidence as unplugging an on-premises storage drive.
- Back up plan - some cloud storage services allow a user to restore modified data back to an older version and recover deleted data for a limited time after it was deleted. If ransomware does manage to affect the cloud backup, these features can be used to restore back to the last known-good state.

Recovery

8.7 Backups should be created on a regular basis. The more frequently backups are created, the less data is required to be recovered in the event of an incident. Backups should also be regularly tested to check they allow the data and network to be recovered effectively. For more information, providers should refer to NCSC advice on response and recovery planning.[34]

Retention of copies within the UK

8.8 For resilience and continuity purposes, Regulation 9(2)(a) requires providers to retain copies of information within the UK which is necessary to maintain the normal operation of the network or service. This does not prevent copies being held elsewhere as part of a global business operation.

[33] *Cloud security guidance: 10. Identity and authentication* (NCSC, 2018)
[34] *NCSC CAF guidance: D.1 Response and recovery planning* (NCSC, 2019)

Chapter crossovers

8.9 Information contained elsewhere in this code of practice is useful in understanding remediation and recovery. This includes:

- Security critical functions (Chapter 1)
- National resilience (Chapter 2)
- Countries listed in the Schedule (Chapter 4)

9. Governance

9.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 10 to ensure appropriate management of the persons who are given security-related tasks. This is intended to ensure that providers employ the appropriate security governance and business processes to protect UK networks and services.

9.2 Regulation 10 is set out below.

> 10.—(1) A network provider or service provider must ensure appropriate management of persons given responsibility for the taking of measures on behalf of the provider for the purposes mentioned in section 105A(1) of the Act.
>
> (2) The duty in paragraph (1) includes in particular a duty—
>
> (a) to establish, and regularly review, the provider's policy as to measures to be taken for the purposes mentioned in section 105A(1) of the Act,
>
> (b) to ensure that the policy includes procedures for the management of security incidents, at varying levels of severity,
>
> (c) to have a standardised way of categorising and managing security incidents, and
>
> (d) to ensure that the policy provides channels through which risks identified by persons involved at any level in the provision of the network or service are reported to persons at an appropriate governance level,
>
> (e) to ensure that the policy provides for a post-incident review procedure in relation to security incidents and that the procedure involves consideration of the outcome of the review at an appropriate governance level and the use of that outcome to inform future policy, and
>
> (f) to give a person or committee at board level (or equivalent) responsibility for—
>
> (i) supervising the implementation of the policy, and
>
> (ii) ensuring the effective management of persons responsible for the taking of measures for the purposes mentioned in section 105A(1) of the Act.
>
> (3) In paragraph (2) "security incident" means an incident involving—
>
> (a) the occurrence of a security compromise, or
>
> (b) an increased risk of a security compromise occurring.
>
> (4) A network provider or service provider must take such measures as are appropriate and proportionate to identify and reduce the risks of security compromises occurring as a result of unauthorised conduct by persons involved in the provision of the public electronic communications network or public electronic communications service.

Key concepts for understanding the requirements

Supporting business processes

9.3 Having an effective security governance framework ensures that procedures, personnel, physical and technical controls continue to work through the lifetime of a network. Without effective governance, it is likely that security improvements will not be sustained or consistent. Any technical controls deployed outside of an effective security governance framework will be fundamentally undermined.

9.4 The following guidance in paragraphs 9.5-9.8 highlights the key business processes for telecommunications providers to understand and implement, providing examples and background information where appropriate.

Top-to-bottom security governance

9.5 For a provider to effectively deliver the requirements of the security framework, it is critical that the whole business has the proper processes and business functions in place to backup and support the appropriate security measures. As such, the security direction of providers must have buy-in at all levels. A nominated person or committee at board level (or a person or committee having an equivalent level of responsibility and status) shall have overall responsibility and accountability for security and should champion all security initiatives throughout the organisation. Providers should refer to NCSC advice on security governance and security policies.[35] [36]

9.6 Regulation 10(2)(d) requires providers to ensure that their security policy "provides channels through which risks identified by persons involved at any level in the provision of the network or service are reported to persons at an appropriate governance level". This requirement aims to ensure (among other things) that providers' policies include a way to communicate security issues and risks to the top of the organisation, without risk of dilution.

Security and operational changes

9.7 Given the scale of some providers' networks, one of the greatest challenges may be ensuring that security teams are aware of the changes being made by operational teams. Before any decision is made that could impact the network, its operation, or management, the risks should be assessed with the support of the security team. Ideally this should be part of an automated process.

Learning from incidents

9.8 Security incidents that occur within providers' networks are not only a learning opportunity for providers, but also for the sector as a whole. Whenever possible,

[35] *NCSC CAF guidance: A.1 Governance* (NCSC, 2019)
[36] *NCSC CAF guidance: B.1 Service protection policies and processes* (NCSC, 2019)

providers should share information about significant past issues or compromises with other providers via suitable trusted groups. Providers are also strongly encouraged to feedback their findings from incidents to enhance future versions of this document and the security of the sector as a whole. More information for providers on learning from incidents can be found on the NCSC website.[37]

Chapter crossovers

9.9 Information contained elsewhere in this code of practice is useful in understanding governance. This includes:

- Security critical functions (Chapter 1)
- Competency (Chapter 12)

[37] *NCSC CAF guidance: D.2 Lessons learned* (NCSC, 2019)

10. Reviews

10.1 This chapter provides guidance for providers on the measures to be taken in accordance with Regulation 11 to ensure that regular reviews of their security measures are undertaken.

10.2 Regulation 11 is set out below.

> 11. A network provider or service provider must—
>
> (a) undertake regular reviews of the provider's security measures in relation to the public electronic communications network or public electronic communications service, taking into account relevant developments relating to the risks of security compromises occurring, and
>
> (b) undertake at least once in any period of 12 months a review of the risks of security compromises occurring in relation to the network or service in order to produce a written assessment of the extent of the overall risk of security compromises occurring within the next 12 months, taking into account—
>
> (i) in the case of a network provider, the risks identified under regulation 3(3)(a),
>
> (ii) the risks identified under regulation 5(2),
>
> (iii) the risks identified under regulation 6(1),
>
> (iv) the risks identified under regulation 10(4),
>
> (v) the results of reviews carried out in accordance with sub-paragraph (a),
>
> (vi) the results of tests carried out in accordance with regulation 14, and
>
> (vii) any other relevant information.

Key concepts for understanding the requirements

Clarifying 'any other relevant information' in Regulation 11(b)(vii)

10.3 In undertaking their annual reviews under Regulation 11(b), providers must take into account the risks and results listed in Regulation 11(b)(i)-(vi) and "any other relevant information" (Regulation 11(b)(vii)). This latter category of information may include, for example, 'event correlation analysis' where relevant. This is where security incidents have been identified by providers which may not have amounted to security compromises, but showed similar root causes and can be classified as near misses. These security incidents are important in assessing the risks of security compromises going forward and should therefore be integrated into the reviews process.

Risks to be considered within risk assessments

10.4 Providers should refer to the NCSC advice on risk management.[38] The risk assessment that providers must carry out as a part of the reviews process under Regulation 11 should be looking at not only the risks to the provider's business and network, but also the risks to end users. This includes, but is not limited to, the risks of loss of availability and of personal data leaks.

Chapter crossovers

10.5 Information contained elsewhere in this code of practice is useful in understanding Reviews. This includes:

- Security critical functions (Chapter 1)
- Signalling plane (Chapter 2)
- Third party administrators (Chapter 6)
- Governance (Chapter 9)

[38] *NCSC CAF guidance: A.2 Risk management* (NCSC, 2019)

11. Patching and updates

11.1 This chapter provides guidance for network and service providers on the measures to be taken in accordance with Regulation 12 to deploy patches or mitigations (including software updates and equipment replacement) as well as the necessary security updates and equipment upgrades.

11.2 Regulation 12 is set out below.

> 12. A network provider or service provider must—
>
> (a) where the person providing any software or equipment used for the purposes of the public electronic communications network or public electronic communications service makes available a patch or mitigation relating to the risks of security compromises occurring (including software updates and equipment replacement), take proportionate measures to deploy the patch or mitigation within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise which the patch or mitigation addresses,
>
> (b) identify any need for a security update or equipment upgrade and implement the necessary update or upgrade within such period as is appropriate, having regard to the assessed security risk of the network provider or service provider, and
>
> (c) arrange for any decision as to what period the network provider or service provider considers appropriate—
>
> (i) for the purposes of sub-paragraph (a), in a case where the network provider or service provider considers in relation to a particular patch or mitigation that a period of more than 14 days beginning with the day on which the patch or mitigation becomes available is appropriate, or
>
> (ii) for the purposes of sub-paragraph (b), in a case where there is a significant risk of a security compromise occurring to be taken at an appropriate governance level and recorded in writing.

Key concepts for understanding the requirements

Guidance on the appropriate patching period

11.3 Regulation 12(a) requires providers to take proportionate measures to deploy any relevant patch or mitigation which becomes available “within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise which the patch or mitigation addresses”. Some guidance measures in Section 3 recommend that providers deploy security patches or mitigations relevant to the security of the provider’s network within 14 days of the patch or mitigation being made available from the network equipment supplier, wherever possible. This is to counter the risks posed by threat actors who regularly target vulnerabilities soon after

they are made available, often by using easy, cheap and commercially available tools. Providers should act swiftly to close these vulnerabilities.

Guidance

11.4 To achieve this objective, it is recommended that providers request that network equipment suppliers provide important security patches separately to feature updates. It is also recommended that providers establish automated and scaled testing processes. This will allow the provider to validate that patches will not disrupt the resilience of the network in a timely manner, and accelerate rollout. Providers shall ensure that they remove any dependence upon any features that are due to be deprecated.

11.5 Where patches justifiably need more time than 14 days to be deployed, Regulation 12(c)(i) requires providers to arrange for any such decisions to be taken at an appropriate governance level and recorded in writing. Providers should ensure that these decisions are based on a rigorous risk assessment process and that robust alternative mitigations are put in place until the relevant patch has been deployed.

Governance for decisions about routine maintenance

11.6 Security should form part of the network's routine maintenance. If a routine security update is postponed, for example, due to a network incident then it must be implemented in the next round of updates or sooner. Should any security functionality be reduced and lead to a significant risk of a security compromise occurring, then providers must ensure that the associated risk assessment and the acceptance of the additional risk is signed off by a nominated person or committee at board level (or a person or committee having an equivalent level of responsibility and status), as in Regulation 12(c)(ii).

Chapter crossovers

11.7 Information contained elsewhere in this code of practice is useful in understanding patching. This includes:

- Customer premises equipment (Chapter 3)
- Governance (Chapter 9)

12. Competency

12.1 This chapter provides guidance for providers on the measures to be taken in accordance with Regulation 13 to ensure that the persons who have been given security-related tasks can appropriately discharge their duties.

12.2 Regulation 13 is set out below for reference.

> 13.—(1) A network provider or service provider must take such measures as are appropriate and proportionate to ensure that persons given responsibility for the taking of measures on behalf of the provider for the purposes mentioned in section 105A(1) of the Act ("the responsible persons")—
>
> (a) are competent to discharge that responsibility, and
>
> (b) are given resources to enable them to do so.
>
> (2) The duty in paragraph (1) includes in particular a duty to take such measures as are appropriate and proportionate—
>
> (a) to ensure that the responsible persons have appropriate knowledge and skills to perform their responsibilities effectively,
>
> (b) to ensure that the responsible persons are competent to enable the network provider or service provider to perform the provider's duties under regulation 6, and are given resources for that purpose,
>
> (c) to ensure that the responsible persons—
>
> (i) are competent to show appropriate understanding and appraisal of the activities of third party suppliers and of any recommendations made by third party suppliers for the purposes of identifying and reducing the risk of security compromises occurring,
>
> and
>
> (ii) are given resources for that purpose, and
>
> (d) where new equipment is supplied, provided or made available by a third party supplier—
>
> (i) to ensure that the equipment is set up according to a secure configuration approved by appropriately trained security personnel, following procedures which enable it to be demonstrated that the configuration has been carried out in that way, and
>
> (ii) to record any failure to meet recommendations of the third party supplier as to the measures that are essential to reduce the risk of security compromises occurring as a result of the way in which the equipment is set up.
>
> (3) In paragraph (2)(c) and (d) "third party supplier" has the meaning given by regulation 7(2).

Key concepts for understanding the requirements

In-house competency

12.3 Regulation 13(2)(c)-(d) sets out competency requirements in relation to the activities of third-party suppliers, their recommendations and the equipment supplied, provided or made available by them.

Guidance

12.4 Where a network or service provider is using a third party supplier, in-house staff of the network or service provider need to be competent and able to take appropriate steps to identify and resolve security issues. This is to avoid providers relying on the competency of third party administrators or third party suppliers, as those third parties may not always be available to address security issues.

12.5 Providers should also ensure that adequate, appropriate and relevant security training is undertaken by anyone who interacts with security critical functions or sensitive data. For those involved in the security of security critical functions, focussed cyber security training and evaluation should be carried out, including providing staff with an understanding of how a telecommunications network is compromised. Further advice on staff training can be found in NCSC advice.[39]

Chapter crossovers

12.6 Information contained elsewhere in this code of practice is useful in understanding Competency. This includes:

- Security critical functions (Chapter 1)
- Supporting business processes (Chapter 9)
- Monitoring and analysis (Chapter 5)
- Third party administrators (Chapter 6)

[39] *NCSC CAF guidance: B.6 Staff awareness and training* (NCSC, 2019)

13. Testing

13.1 This chapter provides guidance for providers on the measures to be taken in accordance with Regulation 14 to carry out, or arrange for a suitable person to carry out, appropriate tests.

13.2 Regulation 14 is set out below.

> 14.—(1) A network provider or service provider must at appropriate intervals carry out, or arrange for a suitable person to carry out, such tests in relation to the network or service as are appropriate and proportionate for the purpose of assessing the risks of security compromises occurring in relation to the public electronic communications network or public electronic communications service.
>
> (2) The tests must involve simulating, so far as is possible, techniques that might be expected to be used by a person seeking to cause a security compromise.
>
> (3) The network provider or service provider must ensure, so far as is reasonably practicable—
>
> (a) that the manner in which the tests are to be carried out is not made known to the persons involved in identifying and responding to security compromises in relation to the network or service or the persons supplying any equipment to be tested, and
>
> (b) that measures are taken to prevent any of those persons being able to anticipate the tests to be carried out.
>
> (4) The references to tests in relation to the network or service include references to tests in relation to—
>
> (a) the competence and skills of persons involved in the provision of the network or service, and
>
> (b) the possibility of unauthorised access to places where the network provider or service provider keeps equipment used for the purposes of the network or service.

Key concepts for understanding the requirements

Penetration testing

13.3 The purpose of testing, or ‘red team’ exercising, is to verify the security defences of the network, and identify any security weaknesses prior to any potential attackers. For this reason it is essential that the testing simulates, so far as possible, real world attacks.

Guidance

13.4 To achieve this, testers or red teams should not be constrained unnecessarily, defensive teams should not be tipped-off in advance, and defensive mechanisms should not be modified based on tester’s plans.

13.5 An example of this type of testing is Ofcom's TBEST scheme[40].

Tests against equipment locations

13.6 The tests covered by Regulation 14 include those in relation to "the possibility of unauthorised access to places where the network provider or service provider keeps equipment used for the purposes of the network or service" (Regulation 14(4)(b)). This requirement should be read in conjunction with other security requirements concerning the equipment location, such as Regulation 3(3)(a)(iii).

Guidance

13.7 Testing should ensure that the physical security of the buildings, server rooms and network equipment meets best-practice standards. Advice produced by the Centre for the Protection of National Infrastructure (CPNI) should be consulted for physical and personnel-related security.[41]

13.8 The code of practice does not cover safety planning such as fire drills, as these should be covered by the general planning and health and safety requirements for buildings.

Chapter crossovers

13.9 Information contained elsewhere in this code of practice is useful in understanding Testing. This includes:

- Signalling plane (Chapter 2)
- Third party administrators (Chapter 6)
- Prevention of unauthorised access or interference (Chapter 7)
- Competency (Chapter 12)

[40] *Our network security and network resilience work* (Ofcom, 2021)
[41] *Physical security* (CPNI)

14. Assistance

14.1 This chapter provides guidance for providers on the measures to be taken in accordance with Regulation 15 to reduce the risk of security compromise by seeking and providing appropriate assistance.

14.2 Regulation 15 is set out below.

> 15.—(1) Where—
>
> (a) a security compromise occurs in relation to a public electronic communications network or public electronic communications service, and
>
> (b) it appears to the network provider or service provider ("the relevant person") that the security compromise is one that may cause a connected security compromise in relation to another public electronic communications network or public electronic communications service,
>
> the relevant person must, so far as is appropriate and proportionate, provide information about the security compromise to the network provider or service provider in relation to the other network or service.
>
> (2) Information provided under paragraph (1) which relates to a particular business may not, without the consent of the person carrying on the business, be used or disclosed by the recipient for any purpose other than that of identifying or reducing the risk of security compromises occurring in relation to the recipient's network or service or preventing or mitigating the adverse
>
> effects of security compromises that have occurred in relation to the recipient's network or service.
>
> (3) A network provider ("provider A") must, when requested by a service provider or another network provider ("provider B"), give provider B such assistance as is appropriate and proportionate in the taking by provider B of any measure required by these Regulations in relation to anything that—
>
> (a) has occurred in relation to provider A's public electronic communications network,
>
> (b) is a security compromise in relation to that network, and
>
> (c) may cause a connected security compromise in relation to provider B's public electronic communications network or public electronic communications service.
>
> (4) A service provider ("provider A") must, when requested by a network provider or another service provider ("provider B"), give provider B such assistance as is appropriate and proportionate in the taking by provider B of any measure required by these Regulations in relation to anything that—
>
> (a) has occurred in relation to provider A's public electronic communications service,
>
> (b) is a security compromise in relation to that service, and

(c) may cause a connected security compromise in relation to provider B's public electronic communications network or public electronic communications service.

(5) A network provider or service provider must, where necessary to reduce the risk of security compromises occurring in relation to the provider's public electronic communications network or public electronic communications service, request another person to give any assistance which paragraph (3) or (4) will require the other person to give.

Key concepts for understanding the requirements

Sharing information

14.3 In certain circumstances it is appropriate for different providers to receive information from providers which would help to reduce the risk of security compromises occurring (Regulation 15(1)). It may also be appropriate in certain circumstances to share information with other types of bodies/organisations such as:

- educational institutions;
- security organisations; and
- UK government cyber security experts.

14.4 All information to be provided under Regulation 15 (1) should be shared swiftly to ensure recipients are able to address risks effectively.

Guidance

14.5 Subject to competition law, providers should establish agreements with other providers around mutual assistance and information sharing in the event of an incident or compromise. By establishing such agreements in advance, assistance can be given to other providers during an incident without compromising the security of their own networks, systems or data.

Chapter crossovers

14.6 Information contained elsewhere in this code of practice is useful in understanding assistance. This includes:

- The supply chain (Chapter 6)
- Governance (Chapter 9)

Section 3: Technical guidance measures

Specific technical measures to be taken by providers are set out below, grouped by the date by which they are expected to be completed.

It should be noted, however, that the extent to which each technical guidance measure can contribute to ensuring compliance with any specific regulation will depend on the facts of each case. The mapping of measures to regulations in this section are therefore only indicative.

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
Overarching security measures		
1.01	Providers shall maintain accurate records of all externally-facing systems.	3(3)(c),(d),(e) 3(4) 3(5) 4(4)(b) 6(4) 8(3)
1.02	Security testing on externally-facing systems should normally be performed at least every two years, and in any case shortly after a significant change occurs.	3(3)(a)(iv) 3(3)(c),(d),(e) 3(5) 4(4)(b) 6(4) 8(3) 14
1.03	Equipment in the exposed edge shall not host sensitive data or security critical functions.	3(3)(a),(d) 3(5) 4(1)(a) 4(2)(a) 4(4)(b)
1.04	Physical and logical separation shall be implemented between the exposed edge and security critical functions. (Note that this requirement may not be necessary once datasets and functions can be cryptographically-protected from compromise)	3(3)(c),(d),(e) 3(5) 4(4)(b)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
1.05	Security boundaries shall exist between the exposed edge and critical or sensitive functions which implement protective measures.	3(3)(c),(d) 3(5) 4(4)(b)
1.06	Equipment in the exposed edge shall not be able to impact operation or routing within the core network. As an example, the exposed edge shall not be a PE-node within the provider's IP core.	3(3)(c),(d) 3(5) 4(4)(b)
Management plane 1		
2.01	Non-persistent credentials (e.g. username and password authentication) shall be stored in a centralised service with appropriate role-based access control which shall be updated in line with any relevant changes to roles and responsibilities within the organisation.	3(3)(a),(b),(d) 3(5) 6(2) 6(3)(b),(d) 8(1) 8(2)(f) 8(5)(a)
2.02	Privileged access shall be via accounts with unique user ID and authentication credentials for each user and these shall not be shared.	8(2)(b) 8(4) 8(5)(a),(b),(e)
2.03	For accounts capable of making changes to security critical functions, the following measures shall be adopted relating to multi-factor authentication: (a) the second factor shall be locally generated, and not be transmitted; and (b) the multi-factor authentication mechanism shall be independent of the provider's network and PAW. Soft tokens (e.g. authenticator apps) may be used.	8(4) 8(2)(b) 8(5)(a),(b),(e)
2.04	Privileged user access rights shall be regularly reviewed and updated as part of business as usual management. This shall include updating privileged user rights in line with any relevant changes to roles and responsibilities within the organisation.	8(4) 8(5)(a),(b),(e) 11(a)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
2.05	All break-glass privileged user accounts must have unique, strong credentials per network equipment.	3(1)(a),(b),(c) 3(2) 8(2)(b) 8(5)(a),(b),(c) 9(2)(c)(vi)
2.06	All privileged access shall be logged.	4(4)(b) 6(2)(a),(b) 6(3)(a),(b) 8(5)(a) 8(5)(d)(i),(ii)
2.07	Privileged access shall be via secure, encrypted and authenticated protocols whenever technically viable.	4(4) 8(4) 8(5)(e)
2.08	Default and hardcoded accounts shall be disabled.	8(2)(d),(e) 8(4) 8(5)(b),(c)
2.09	Management protocols that are not required shall be disabled on all network functions and equipment.	3(3)(e) 7(4)(a)(ii) 8(4) 8(5)(e)
2.10	Default passwords shall be changed upon initialisation of the device or service and before its use for the provision of the relevant network of service.	7(4)(b) 8(2)(d) 8(4) 8(5)(b),(c)
Signalling plane 1		
3.01	Providers shall understand how incoming signalling arrives into their network, and outgoing signalling leaves their network. Specifically, the interfaces over which signalling enters and leaves the network, and the equipment which sends and processes external signalling.	3(3)(a),(b),(c) 4(4)(b),(c) 8(2)(a)
3.02	Providers shall understand what network equipment could be impacted by malicious signalling.	3(3)(a),(b),(d) 4(6)(a) 6(1) 6(4) 7(4)(a)(i)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
3.03	Providers shall understand what network and user data could be compromised through malicious signalling.	3(3)(a),(b) 4(1)(a) 6(1) 6(2)(a),(b) 6(4) 8(2)(a)
3.04	Providers shall understand who they directly connect with over the signalling network.	3(3)(a),(b) 6(1) 6(2)(a) 6(4) 7(1) 7(4)(a)(i),(ii),(iii)
3.05	Any incoming or outgoing message type that should not be sent over international signalling networks shall be blocked at the logical edge of the provider's network. For example, GSMA CAT 1 messages[42] shall be blocked for SS7 networks, and equivalent messages shall be blocked for other signalling protocols such as Diameter[43], GTP[44], Interconnect[45] and SS7/SIGTRAN[46].	3(3)(e),(f) 4(4)(b) 6(1) 6(3)(d) 8(3) 8(6)
3.06	At edge signalling nodes, providers shall block any incoming message using any source address internal to the provider's network.	3(3)(a),(d),(e) 4(4)(b) 6(3)(d)
3.07	Trust shall not be assumed based on the source of any incoming message. For example, 'UK' source addresses (e.g. +44 global titles in SS7) shall not be assumed to be trusted and allowed by default.	3(3)(e) 4(4)(b),(c) 6(3)(d)
3.08	Trust in source addresses may be assumed where the signalling is authenticated by the sender.	3(3)(e) 4(4)(b) 6(3)(d)

[42] *FS.11 SS7 interconnect security monitoring and firewall guidelines* (GSMA, 2019)
[43] *FS.19 DIAMETER interconnect security* (GSMA, 2019)
[44] *FS.20 GPRS tunnelling protocol (GTP) security* (GSMA, 2019)
[45] *FS.21 Interconnect Signalling Security Recommendations* (GSMA, 2019)
[46] *FS.07 SS7 and SIGTRAN Network Security* (GSMA, 2017)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
3.09	Where providers allow others to use numbers ranges that have been allocated to them (e.g. GTs, IMSIs), they remain responsible for the activity related to that number range, and any further security implications. This does not apply in the case of MSISDNs shared through MNP.	3(3)(e) 4(1)(a),(b) 4(4)(b) 6(3)(d)
3.10	Any outgoing message that uses a source address that should not transit or leave the provider's network shall not be permitted to leave the provider's network.	4(1)(a) 4(2)(a) 4(4)(a) 6(1) 8(1)
3.11	When sent over signalling networks, the external exposure of customer data, customer identifiers and network topology information shall be minimised.	4(1)(a),(b) 4(2)(a),(b) 4(4)(a) 4(4) 6(1) 8(1) 8(2)(f) 8(5)(a)
3.12	Networks shall only send outgoing signalling in support of permitted services in line with the GSMA guidelines for interconnectivity.	4(4)(b) 6(1) 6(2)(a),(b)
3.13	External BGP updates shall be monitored for evidence of misuse.	3(3)(e) 4(4)(b) 6(3)(a),(c),(d),(e) 9(2)(c)(i)
3.14	Any BGP misuse that impacts their network or services shall be mitigated in a timely manner, and at least within 12 hours whenever technically possible.	3(3)(e) 4(4)(b) 6(3)(a),(d) 8(1)
3.15	Best practices in the use of BGP shall be implemented as defined in NCSC BGP best practice guidance.[47]	3(3)(e) 4(4)(b) 6(3)(d) 8(1) 9(2)(c)

[47] *Technical report: responsible use of the border gateway protocol (BGP) for ISP interworking (version 1.0)* (NCSC)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
3.16	The provider shall share details of any BGP misuse with other providers where it may cause a connected security compromise.	3(3)(e) 6(3)(d) 15(1) 15(2) 15(3) 15(4) 15(5)
3.17	An external path update that includes a prefix owned by the provider shall not be accepted.	3(3)(e) 4(4)(b) 6(3)(d) 8(1) 8(3)
3.18	End-users shall not be able to spoof IPs over the data plane (e.g. in line with BCP38).	3(3)(e) 4(4)(b) 6(1) 6(2)(a) 8(1)
Third party supplier measures 1		
4.01	The provider shall ensure the risks included in Regulation 7(3) are assessed prior to contract, and this assessment is documented. This assessment shall inform both risk management and procurement processes.	3(3)(e) 7(1) 7(4)(a)(i)
5.01	During procurement of equipment, prior to contract award, providers should, as a minimum, use the guidance contained in NCSC's vendor security assessment[48] to assess third party suppliers.	3(3)(a),(b),(d),(e) 3(5) 7(3)(a),(b) 7(4)(a)(i) 10(1) 10(2)(a)(b) 10(4) 13(2)(d)(i),(ii) 14(1)

[48] *NCSC Vendor Security Assessment* (NCSC, 2022)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
5.02	During procurement of equipment, prior to contract award, providers shall ensure the security functionality of all equipment has been tested.	3(3)(a),(b),(d),(e) 3(5) 7(1) 7(3)(a)(b) 7(4)(a)(i) 10(1) 10(2)(a)(b) 10(4) 13(2)(d)(i)(ii) 14(1)
5.03	During procurement of equipment, prior to contract award, providers shall ensure negative testing and fuzzing of equipment interfaces has been performed.	3(3)(a),(b),(d),(e) 3(5) 7(1) 7(3)(a)(b) 7(4)(a)(i) 13(2)(d)(i),(ii) 14(1) 14(2)
5.04	Any third party testing shall only be accepted as evidence by the provider if it is repeatable, performed independently of the network equipment supplier and is clearly applicable to the provider's deployment (e.g. relates to the hardware, software and configuration that is being supplied).	3(3)(a),(b),(d),(e) 3(4) 3(5) 7(1) 7(3)(a),(b) 7(4)(a)(i) 12 13(2)(d)(i),(ii) 14(1) 14(2) 14(3)
5.05	Providers shall ensure that security considerations are a significant factor in determining the procurement outcome, considering available evidence from testing, recognising the benefit of any security features that will provide measurable improvement to the security of the network.	3(3)(e) 7(3)(a) 7(4)(a)(i)
5.06	Providers shall record all equipment deployed in their networks, and proactively assess, at least once a year, their exposure should the third party supplier be unable to continue to support that equipment.	3(1)(a),(b),(c) 3(2) 11(b)(i),(iv),(vi) 13(2)(d)(i),(ii)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
5.07	Providers shall remove or change default passwords and accounts for all devices in the network, and should disable unencrypted management protocols. Where unencrypted management protocols cannot be disabled, providers shall limit and mitigate the use of these protocols as far as possible.	3(3)(e) 4(5) 8(2)(d) 13(2)(d)
5.08	Providers shall ensure that all security relevant logging is enabled on all network equipment and sent to the network logging systems.	3(3)(e) 6(2)(a)
5.09	Providers shall prioritise critical security patches over functionality upgrades wherever possible.	7(4)(c) 7(5) 12
5.10	The provider shall record all equipment that remains in use but has reached the vendor's end-of-life date. Providers shall regularly review their use of this equipment, with a view to reducing the risk of a security compromise occurring as a result of unsupported equipment remaining in use.	3(3)(a),(b) 3(4) 7(1) 7(4)(c) 11
5.11	The provider shall produce a plan to replace the unsupported equipment at an appropriate time, dependent on the level of risk.	3(3)(a),(b) 3(4) 7(1) 7(4)(c) 11
5.12	The provider shall record all risk management processes undertaken. Guidance on risk management processes can be found on the NCSC website[49].	3(1) 7(1) 7(4)(c)
6.01	When assessing the risk due to SIM card suppliers, providers shall consider the risk due to the loss of sensitive SIM card data.	3(3)(a),(e) 4(5) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a) 8(6) 11

[49] *Risk management guidance* (NCSC, 2018)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
6.02	Different SIM transport keys shall be used with each SIM card vendor. A range of transport keys shall be used with each SIM card vendor. Providers shall not share transport keys across multiple SIM vendors.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a) 8(6)
6.03	When providers define new SIM authentication algorithm parameters (e.g. for MILENAGE), the default values shall not be used.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a)
6.04	Providers shall only store SIM credentials and SIM transport keys within secured systems that ensure data integrity and prevent 'read' access to key material.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a)
6.05	Providers shall review the security of existing SIM cards on an annual basis, including the supplier, the protection of keys, the algorithms used by the SIM, and the applets provisioned and running on SIMs.	3(3)(a) 4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a) 8(6) 11
6.06	Providers shall phase out the use of SIMs which present an unmitigatable security risk, such as the use of deprecated security algorithms.	4(6)(b)
6.07	For fixed-profile SIM cards, the provider shall ensure that sensitive SIM data is appropriately protected throughout its lifecycle, by both the SIM card manufacturer and within the operator network, given the risk to network resilience and confidentiality should this information be lost.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a)
6.08	For fixed-profile SIM cards, the confidentiality, integrity and availability of the sensitive SIM card data shared with the SIM card manufacturer shall be protected at every stage of their lifecycle.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
6.09	For fixed-profile SIM cards, providers shall ensure the SIM card manufacturer has been accredited through the GSMA's SAS scheme.[50]	4(6) 7(1)
6.10	For profile-modifiable SIM cards, the provider shall, within the first year of use, update with a new profile (including K/Ki, and OTA keys) that has not been provided externally, including to the SIM card manufacturer. Providers should aim to ensure that all new UICCs can be updated with new K/Ki and OTA keys after receipt from the SIM card manufacturer.	4(6)(a),(b)
6.11	When under the provider's control, the provider shall ensure that the SIM card can only be modified by specifically allowed servers (as determined by IP address and certificate stored on the SIM card).	4(6)(a),(b)
Supporting business processes		
7.01	The provider shall implement appropriate business processes. Specifically, the provider shall meet the 'achieved' column in relation to the parts of the CAF which define the provider's business processes. These are: A1: Governance, A2: Risk Management, A3: Asset Management, B5: Resilient Networks and Systems, B6: Staff Awareness and Training, D1: Response and Recovery Planning, D2: Lessons Learned[51].	4(1) 4(2) 4(4)(b) 7(3) 7(5) 9(2)(c)(iv),(vi),(vii) 10(2)(a),(b),(c),(d),(e),(f) 10(4) 13(1) 13(2)(a),(b),(c),(d)

[50] *Security accreditation scheme (SAS)* (GSMA, 2021)
[51] *NCSC CAF guidance (version 3.0)* (NCSC, 2019)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
7.02	Security changes shall be prioritised and postponements of security changes shall be minimised. Where security changes are postponed, these may need to be recorded as a business risk as appropriate.	3(3)(a),(b) 3(4) 4(1) 4(2) 4(4)(b) 7(1) 7(3)(a),(b) 7(5)(a),(b) 10(2)(a),(b),(c),(d),(e) 12(a)(b)(c) 13(1)(a)(b) 13(2)(a),(b)
7.03	In addition to the requirements in CAF B.5.c, providers shall maintain both online and offline backups of their infrastructure and information and shall be able to restore from either. These backups should be sufficient to resume normal service.	3(3)(d) 4(1) 4(2) 4(4)(b) 7(3)(a),(b) 7(5)(a),(b) 8(5)(d) 9(2)(a),(b) 9(2)(c)(vii)
7.04	In addition to the requirements in CAF D.1.a, providers shall have clear, exercised and implemented processes for managing security incidents, at varying levels of severity.	3(3)(d) 4(1) 4(2) 4(4)(b) 7(3)(a),(b) 7(5)(a),(b) 9(2)(c)(iv) 10(2)(a),(b),(c),(d) 13(2)(a),(b)
7.05	In addition to the requirements in CAF D.2 providers shall perform a root-cause analysis of all security incidents. Outcomes of this analysis shall be escalated to an appropriate level, which may include the provider's board.	3(3)(a),(b),(d) 3(4) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(3)(a),(b) 7(5)(a),(b) 10(2)(f) 10(2)(a),(b) 10(2)(c),(d),(e)

The following measures should be completed by 31 March 2023 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
7.06	In addition to the requirements in CAF D.2 , for significant incidents, providers shall share the high-level lessons learned with other providers.	15
7.07	Lessons learned from previous security incidents shall be used to inform the security of new products and services.	3(3)(a),(b) 3(4) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 10(2)(a)(b) 10(2)(e) 13(2)(a),(b),(c),(d)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
Third party supplier measures 2		
8.01	The provider shall maintain records of third party supplier's details, including their third-parties and the major components which are used in the provision of goods/services/facilities for the provider.	7(1) 7(4)(a)(i) 11(a)
8.02	The provider shall clearly express the security needs placed on third party suppliers. These shall be defined and agreed in contracts.	7(1) 7(4)(a),(b) 9(1) 9(2)(c)(ii),(iv),(vi)
8.03	There shall be a clear and documented shared-responsibility model between the provider and third party suppliers.	7(1) 7(4)(a) 9(1) 9(2)(c)(ii),(iv),(vi)
8.04	The provider's incident management process and that of their third party suppliers shall provide mutual support in the resolution of incidents.	7(4)(a)(i),(iv) 9(1) 9(2)(c)(ii),(iv),(vi)
8.05	Providers shall retain network and user data within their own environment wherever possible.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(iii) 7(4)(b)
8.06	The provider shall define what information is made accessible to any third party supplier, ensuring that it is the minimum necessary to fulfil their function. Providers shall place controls on that information and limit third party access to the minimum required to fulfil the business function.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii),(iii) 7(4)(b) 8(5)(e) 15

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
8.07	The environment used to hold the network and user data made available to third party suppliers shall be within a system segregated from the rest of the provider's internal systems and data.	3(3)(a),(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(iii) 7(4)(b)
8.08	Providers shall prevent transfer of network and user data outside their environment, except where necessary. Where transfer is necessary, it shall be through a defined process.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii),(iii) 7(4)(b) 15
8.09	Where network or user data leaves a provider’s control, providers shall contractually require and verify that the data is property protected as a consequence. This shall include assessing the third party supplier's controls to ensure provider data is only visible or accessible to appropriate employees and from appropriate locations.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii),(iii) 7(4)(b)
8.10	All data sharing with third party suppliers shall be over an encrypted and authenticated channel.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii),(iii) 7(4)(b) 15
8.11	Providers shall contractually oblige third party suppliers to notify the provider within 48 hours (or less), of becoming aware of any security incidents that may have caused or contributed to the occurrence of a security compromise, or where they identify an increased risk of such a compromise occuring. This includes, but is not limited to, incidents in the supplier's development network or their corporate network.	7(4)(a)(i),(iv) 9(1) 9(2)(c)(i) 15

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
8.12	Providers shall contractually require third party suppliers to support the provider in investigations of incidents which cause or contribute to the occurrence of a security compromise in relation to the primary provider, or of an increased risk of such a compromise occurring.	7(4)(a),(iv) 9(1) 9(2)(c)(i),(ii),(iii),(iv),(v),(vi) 15
8.13	Providers shall contractually require the third party suppliers to find and report on the root cause of any security incident within 30 days, and rectify any weaknesses found.	7(4)(a)(iv) 9(1) 9(2)(c)(i),(ii),(iv),(v),(vi) 9(4) 9(5) 15
8.14	Where third party suppliers cannot quickly resolve weaknesses, the provider shall work with the third party supplier to ensure the issue is mitigated until resolved.	7(4)(a)(iv) 9(1) 9(2)(c)(ii),(iv),(v) 15
8.15	Where third party suppliers do not resolve weaknesses within a reasonable timeframe, the provider shall have a break clause with the third party supplier to allow exit from the contract without penalty.	7(4)(c)
8.16	Providers shall contractually require third party suppliers to support, as far as appropriate and reasonable, any security audits, assessments or testing required by the provider in relation to the security of the provider's own network, including those necessary to evaluate the security requirements in this document.	7(1) 7(4)(a)(i),(iii),(iv) 14(1)
9.01	Providers shall flow down security measures to the third party administrator. Providers shall ensure that the third party administrator applies controls that are at least as rigorous as the provider when the third party administrator has access to the provider's network or service or to sensitive data.	7(3)(a) 7(3)(b) 7(4)(a)(i),(ii)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
9.02	The provider shall retain the right to determine permissions of the accounts used to access its network by third party administrators.	7(1) 7(4)(a)(ii),(iii) 7(4)(b)
9.03	Providers shall ensure that they retain sufficient in-house expertise and technical ability to re-tender their managed services arrangements at any time and shall produce and maintain a plan for moving the provided services back in-house, or to another third party supplier.	7(1) 7(4)(a)(ii) 7(5) 8(2)(a) 8(4) 13(1) 13(2)(a) 13(2)(c)(i)
9.04	Providers shall maintain an up-to-date list of all third party administrator personnel that are able to access its network, including their roles, responsibilities and expected frequency of access.	7(1) 7(4)(a)(ii),(iii) 7(4)(b) 8(4) 8(5)(d),(e) 8(6)(a),(b)
9.05	Providers shall have the contractual right to control the members of third party administrator personnel who are involved in the provision of the third party administrator services, including to require the third party administrator to ensure that any member of personnel no longer has access to the network.	7(1) 7(4)(a)(i),(iii) 7(4)(b) 8(4) 8(5)(d),(e) 8(6)(a),(b)
9.06	Providers shall not allow routine, direct access to network equipment by third party administrators. Access shall be via mediation points owned and operated by the provider.	3(1)(a),(b),(c) 3(3)(e) 4(1)(b) 4(2)(b) 4(4)(b) 7(1) 7(4)(b) 8(4)
9.07	Providers shall implement and enforce security enforcing functions at the boundary between the third party administrator network and the provider network.	3(1)(a),(b),(c) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 7(4)(b)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
9.08	Providers shall contractually require that the third party administrators implement technical controls to prevent one provider or their network from adversely affecting any other provider or their network.	7(1) 7(4)(a)(i),(ii) 7(4)(b) 9(2)(c)(iii),(v)
9.09	Providers shall contractually require that the third party administrators implement logical separation within the third party administrator network to segregate customer data and networks.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
9.10	Providers shall contractually require that the third party administrators implement separation between third party administrator management environments used for different provider networks.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
9.11	Providers shall contractually require that the third party administrators implement and enforce security enforcing functions at the boundary between the third party administrator network and the provider network.	4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
9.12	Providers shall contractually require that the third party administrators implement technical controls to limit the potential for users or systems to negatively impact more than one provider.	4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
9.13	Providers shall contractually require that the third party administrators implement logically-independent privileged access workstations per provider.	4(4)(a) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
9.14	Providers shall contractually require that the third party administrators implement independent administrative domains and accounts per provider.	7(1) 7(4)(a)(i),(ii)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
9.15	Providers shall ensure that the elements of the provider network that are accessible by the third party administrator shall be the minimum required to perform its contractual function.	7(1) 7(4)(a)(i),(ii) 8(4) 8(5)(e)
9.16	Providers shall both log and record all third party administrator access into its networks.	6(1), 6(2)(a),(b) 6(3)(a) 7(4)(a)(iii),(iv) 8(5)(d)(i),(ii) 9(1) 9(2)(c)(iv),(v)
9.17	The provider shall contractually require the third party administrator to monitor and audit the activities of the third party administrator's staff when accessing the provider's network.	6(1) 6(2)(a),(b) 7(4)(a)(iii),(iv) 8(5)(d)(i),(ii) 9(1) 9(2)(c)(iv),(v)
9.18	The provider shall contractually require from the third party administrator all logs relating to the security of third party administrator's network to the extent that such logs relate to access into the provider's network.	6(1) 6(2)(a),(b) 6(3)(a),(g) 7(4)(a)(iii),(iv) 8(5)(d)(i),(ii) 9(1) 9(2)(c)(iv),(v)
9.19	Providers shall require that the third party administrator networks that could impact the provider undergo the same level of testing as the provider applies to themselves (e.g. TBEST testing as set for the provider by Ofcom from time to time).	7(4)(a)(i),(iii) 14(1) 14(2)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
10.01	Providers shall contractually require network equipment suppliers to share with them a 'security declaration' on how they produce secure equipment and ensure they maintain the equipment's security throughout its lifetime. The security declaration shall cover all aspects described within the Vendor Security Assessment.[52]	3(3)(a),(b),(e) 3(3)(b) 3(3)(e) 7(4)(a)(i),(iii),(iv) 7(4)(b)
10.02	As part of the security declaration, any differences in process across product lines shall be recorded.	3(3)(a),(b) 3(3)(e) 7(4)(a)(i),(iii),(iv) 7(4)(b)
10.03	Providers shall ensure, by contractual arrangements, that the network equipment supplier's security declaration is signed-off at an appropriate governance level.	3(3)(a),(b),(e) 7(4)(a)(i),(iii),(iv) 7(4)(b)
10.04	Where the network equipment supplier claims to have obtained any internationally recognised security assessments or certifications of their equipment (such as Common Criteria or NESAS), providers shall contractually require equipment suppliers to share with them the full findings that evidence this assessment or certificate.	3(3)(a),(b),(e) 7(4)(a)(i),(iii),(iv) 7(4)(b)
10.05	Providers shall contractually require network equipment supplier to adhere to a standard no lower than the network equipment supplier's 'security declaration'.	3(3)(a),(b) 3(4) 7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c)
10.06	Providers shall contractually require network equipment suppliers to supply up-to-date guidance on how the equipment should be securely deployed.	3(3)(a),(b) 3(4) 7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c) 12(a) 13(2)(d)(i),(ii)

[52] *NCSC Vendor Security Assessment* (NCSC, 2022)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
10.07	Providers shall contractually require network equipment suppliers to support all equipment and all software and hardware subcomponents for the length of the contract. The period of support of both hardware and software shall be written into the contract.	3(3)(a),(b) 3(4) 7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c) 12(a) 13(2)(d)(i),(ii)
10.08	Providers shall contractually require network equipment suppliers to provide details (product and version) of major third party components and dependencies, including open source components and the period and level of support.	3(3)(a),(b) 3(4) 7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c) 12(a) 13(2)(d)(i),(ii)
10.09	Where relevant to a provider's particular usage of equipment, providers shall contractually require third party suppliers to remediate all security issues with a CVSS score of 7.0 or above discovered within their products within a reasonable time of being notified, providing regular updates on progress in the interim. This shall include all products impacted by the vulnerability, not only the product for which the vulnerability was reported.	3(3)(a),(b) 3(4) 7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c) 12(a) 12(c)(i),(ii) 15(1) 15(4)
10.10	Providers shall record where third party suppliers fail to meet these security obligations.	7(4)(iii)(iv)
10.11	Providers should ensure that their contracts allow details of security issues to be shared with the UK government, the regulator and other providers.	7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c)

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
10.12	Providers shall contractually require network equipment suppliers to deliver critical security patches separately to feature releases, to maximise the speed at which the patch can be deployed.	3(3)(a),(b) 3(4) 7(1) 7(4)(a)(i) 7(4)(c) 12(a) 12(c)(i),(ii)
10.13	Providers shall ensure their equipment is in a secure-by-default configuration, based on the principle that only required services are made available.	3(3)(e) 13(2)(d)
10.14	Providers shall ensure that all deployed equipment either meets the network equipment supplier's recommended secure configuration (as a minimum), or that any variations are recorded and the risk assessed.	3(3)(e) 11 13(2)(d)
10.15	Providers shall implement necessary mitigations based on identified equipment risks (e.g. use of an out-of-support component), such that these equipment risks do not increase the overall risk to their networks.	3(3)(e) 11 13(2)(d)
10.16	Providers shall update all supported equipment within such period as is appropriate of any relevant and appropriate version being released.	7(4)(c) 7(5) 12
10.17	Providers shall deploy all security related patches within 14 days. Should this not be possible, patches shall be deployed as soon as practicable and robust alternative mitigations put in place until the relevant patch has been deployed.	7(4)(c) 7(5) 12
10.18	Providers shall ensure that network equipment continues to meet the requirements in 5.05, 5.06, 5.07, 10.13 and 10.14 throughout its lifecycle including after an upgrade or patch.	7(4)(c) 7(5) 12

The following measures should be implemented on all new contracts after 31 March 2023 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2025 (Tier 1 providers) or 31 March 2027 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
10.19	The provider shall verify that the third party supplier has a vulnerability disclosure policy. This shall include, at a minimum, a public point of contact and details around timescales for communication.	4(4)(c) 7(4)(a)(i) 12
Customer Premises Equipment		
11.01	Once the CPE has been configured at the customer site, it shall only contain credentials that are both unique to that CPE, and not guessable from CPE metadata.	4(4)(c) 8(5)(c)
11.02	The provider shall ensure that all CPEs provided to customers are still supported by the network equipment supplier. For any provider-provided CPEs that go out of third party supplier support, customers shall be proactively offered a replacement as soon as reasonably practicable and at no extra cost. This shall apply only whilst the provider provides the associated service.	4(4)(c) 6(4) 12
11.03	WAN CPE management interfaces shall only be accessible from specified management locations (e.g. URL or IP address).	3(3)(a) 4(4)(c)
11.04	Management of the CPE shall use a secure protocol (e.g. TLS 1.2 or newer)	3(3)(a) 4(4)(c)
11.05	By default, the customer-facing management interfaces shall only be accessible from within the customer's network.	3(3)(a) 4(4)(c)
11.06	By default, all unsolicited incoming traffic towards the customer's network shall be blocked.	3(3)(a) 4(4)(b),(c) 9(2)(c)(iii)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
Management plane 2		
12.01	All parts of the provider's management plane shall be under the ultimate control and oversight of the provider. This includes the architecture of the management plane, equipment attached to the management plane, and administrative access to the management plane. Providers shall retain ultimate control and oversight even when administrative actions are performed by third-parties.	3(3)(d),(f),(g),(h) 3(5) 6(3)(d) 7(4)(a) 8(1) 8(6)
12.02	Operational changes shall only be made according to a formal change process except under emergency or outage situations.	3(3)(d) 3(5) 6(2) 6(3)(d) 8(1) 8(2)(b),(c),(g) 10(2)(b)
12.03	Any persistent credentials and secrets (e.g., for break glass access) shall be protected and not available to anyone except for the responsible person(s) in an emergency.	3(3)(a),(b),(d) 3(5) 6(2) 6(3)(b),(d) 8(1) 8(2)(f) 8(5)(a)
12.04	The central storage for any persistent credentials and secrets (e.g., for break glass access) shall be protected within hardware-protected storage and not be readable except for the relevant person(s) in an emergency.	3(3)(a),(b),(d) 3(5) 6(2) 6(3)(b),(d) 8(1) 8(2)(f) 8(5)(a)
12.05	Privileged users are only granted specific privileged accounts and associated permissions which are essential to their business role or function.	8(4) 8(5)(a),(e)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
12.06	Privileged access shall be temporary, time-bounded and based on a ticket associated with a specific purpose. Administrators shall not be able to grant themselves privileged access to the network.	8(4) 8(5)(a),(b),(e)
12.07	Privileged access shall be granted for a maximum period of 12 hours. Access after 12 hours may be immediately reauthorised provided the initiating ticket remains open.	8(4) 8(5)(a),(e)
12.08	Privileged access shall be automatically revoked once the ticket is closed.	8(4) 8(5)(a),(b),(e)
12.09	Privileged user accounts are generated from a least privilege role template and modified as required. The permissions associated with this account shall not be copied from existing users.	8(4) 8(5)(a),(b),(e)
12.10	Given a business need, administrators can have multiple roles, each with its own account, provided the risk of doing so has been considered and accepted as part of the provider's risk management processes.	8(5)(a),(b),(e) 8(6)(a),(b)
12.11	When an emergency occurs, security requirements may temporarily be suspended. Clean-up steps shall be performed after the emergency is resolved to ensure the suspension of these requirements has not compromised the network. Where an ‘emergency’ event occurs, this shall be recorded and audited, along with the reason and time period for which controls were suspended.	3(1)(a),(b),(c) 3(2) 3(3)(a),(b),(c) 3(5) 6(3)(a) 8(1) 8(3) 9(1) 9(2)(c) 11(a)
12.12	Break-glass privileged user accounts should be present for emergency access outside of change windows, but alerts shall be raised when these are used, the circumstances investigated, and all activity logs audited post emergency.	3(1)(a),(b),(c) 3(3)(a),(b),(c) 3(2) 3(5) 8(4) 8(5)(b),(d) 9(2)(c)(v)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
12.13	Break-glass privileged user account credentials should be single use and changed after use.	3(1)(a),(b),(c) 3(2) 8(5)(a),(b),(c) 9(2)(c)(v)
12.14	All privileged access activity undertaken during a management session shall be fully recorded.	4(4)(b) 6(2)(a),(b) 6(3)(a),(b) 8(5)(a) 8(5)(d)(i),(ii)
12.15	A device that is not necessary to perform network management or support management operations shall not be able to logically access the management plane.	3(3)(d) 3(5) 6(3)(d) 8(3) 8(5)(e)
12.16	Privileged access to network equipment shall be via a centralised element manager or equivalent config deployment system. For example, privileged users shall not be provided with direct access to any management terminal, except where network connectivity is not available (e.g. break-glass situations).	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(4) 8(5)(a),(e)
12.17	It shall not be possible to directly communicate between managed elements over the management plane.	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(4) 8(5)(e)
12.18	The management plane shall be segregated by third party supplier, and between access networks and core networks (e.g. by VLAN). This would not preclude the use of a single orchestration and management solution, provided it is compliant with measure 12.24.	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(4) 8(5)(a),(e)
12.19	Element managers shall not be able to communicate with elements that they do not administer (and vice-versa).	3(3)(d) 3(5) 6(3)(d) 8(4) 8(5)(e)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
12.20	The function authorising privileged user access (e.g. the root authentication service) shall be within a trusted security domain (not the corporate network).	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(5)(a)
12.21	Multi-factor authentication supporting and authorisation functions shall be treated as a network oversight function and shall be within a separate security domain to the corporate security domain.	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(5)(a)
12.22	Testing procedures shall be established and utilised to verify that management networks enforce these controls.	3(3)(d),(e) 3(5) 6(3)(d) 8(2)(f) 8(4) 8(5)(a),(e) 14(1)
12.23	The wider network outside of the management plane shall be continuously scanned to detect and remediate unnecessary open management protocols, ports and services.	3(3)(d) 3(5) 6(3)(b) 6(3)(d) 8(2)(f) 8(4) 8(5)(a),(e) 14(1)
12.24	The management plane used for access networks shall be segregated such that disruption of one management plane segment shall only impact a single UK region.	3(3)(d) 3(5) 8(1)
12.25	A PAW shall only have access to the internet to the extent it is needed to carry out changes to security critical functions, and such access shall be secured (e.g. via VPN).	3(3)(c) 4(4)(a)
12.26	The PAW shall only have access to internal-only business systems (e.g. not corporate email).	3(3)(c) 4(4)(a)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
12.27	A PAW shall support secure boot, boot-attestation, data-at-rest encryption backed by a hardware root-of-trust.	4(1) 9(1)
12.28	A PAW shall be kept patched and up-to-date with a supported OS throughout its lifetime.	12
12.29	Security critical patches shall be applied to PAWs within 14 days, or within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise.	12
12.30	A PAW shall prevent the execution of unauthorised code such as binaries or macros within documents.	3(3)(c) 4(1)
12.31	A PAW shall use data-at-rest encryption.	4(1) 4(2)
12.32	Health attestation of the PAW shall be used wherever possible, and particularly where the PAW is located outside the UK.	3(3)(c) 8(6)
12.33	All new deployments of equipment shall be administered via secure, encrypted and authenticated protocols. Insecure or proprietary security protocols shall be disabled.	3(1) 3(3)(e) 13(2)(d)
12.34	Where administrative access is not via secure channels, the risk this poses and the mitigation applied shall be justified, fully documented and reported at board level.	3(3)(a) 3(b) 8(4) 10(2)(d),(f) 11(b)
12.35	Security protocols and algorithms shall not be proprietary whenever technically viable.	8(4)
12.36	Each network equipment shall have strong, unique credentials for every account.	8(2)(b),(d) 8(4) 8(5)(b),(c)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
Signalling plane 2		
13.01	Incoming and outgoing signalling traffic shall be monitored.	4(4)(b) 5(3) 6(1) 6(2)(a),(b) 6(3)(a),(d),(e) 6(4)
13.02	Signalling records are sensitive data and shall be protected from misuse or extraction.	3(3)(a)(i) 4(1)(a) 4(2)(a) 4(4)(b) 5(3) 6(1) 6(2)(b) 6(3)(a),(d)
13.03	Security analysis shall be performed on signalling traffic to find and address malicious signalling.	4(4)(b) 6(1) 6(2)(a),(b) 6(3)(a),(d),(f) 8(1)
13.04	Providers shall establish an effective means to alert each other to malicious signalling where there could be a connected security compromise.	4(4)(b) 6(1) 6(2)(a),(b) 6(3)(d),(e) 15
13.05	Detailed negative testing and fuzzing shall be performed for all interfaces that process data provided over an external signalling interface (This applies to all equipment which this measure applies to, including existing equipment).	3(3)(a)(iv) 3(3)(c),(d),(e),(f),(g) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b),(c) 6(1) 4(1) 14(2)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
13.06	Malformed, inconsistent or unexpected signalling messages shall be blocked.	3(3)(a)(iv) 3(3)(c),(d),(e) 3(4) 4(1)(b) 4(2)(b) 4(4)(b) 6(1) 8(3)
Virtualisation 1		
14.01	The virtualisation fabric shall be kept up to date.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 12(a),(b),(c)
14.02	It shall be possible to update the virtualisation fabric without negatively impacting the network functionality.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 12(a),(b),(c)
14.03	All interfaces on physical hosts shall be locked down to restrict access. The only incoming connection to the physical host shall be for management purposes. There shall be no outgoing connections except to support virtual workloads. Communication between physical hosts shall be inhibited other than as part of data flows between virtual workloads.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 6(1) 6(2)(a),(b) 8(1)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
14.04	Controls shall be in place to ensure that only known physical hosts can be added to the virtualisation fabric.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 8(1) 12(a)
14.05	Modification of databases and systems that define the operation of the network shall require two authorised-person sign-off.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 8(2)(b),(c) 12(a),(b),(c)
14.06	As part of the virtualisation fabric, physically separate ports shall be used to segregate internal and external network traffic.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 12(a),(b),(c)
14.07	The virtualisation fabric shall be configured to limit the exposure of virtual workloads (e.g. disable virtual span ports by default).	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b)
14.08	The virtualisation fabric shall be configured to prevent use of hard-coded MAC addresses by default e.g. by individual VNFs.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
14.09	Where providers cannot guarantee the security of the physical environment (e.g. within the exposed edge, or within a shared data centre/exchange), the virtualisation fabric shall be configured to encrypt data-at-rest (no data is written to the host's storage unencrypted and data is encrypted when the host is powered off).	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b) 4(5) 7(4)(b) 8(1)
14.10	Where there is risk of exposure during transmission, the virtualisation fabric shall be configured to encrypt data-in-transit in line with NCSC TLS[53] and IPsec[54] guidance.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b) 4(5)
14.11	All physical hosts shall be placed into a host security 'pool'. Pools may be defined based on the environment within which that host resides, the type of host, resilience and diversity, purpose etc.	3(1)(a),(b),(c) 3(2) 3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 8(1)
14.12	Virtual workloads shall be tagged with a specific trust domain within the orchestrator or relevant virtualisation stack, based on the risks associated with the workload.	3(2) 3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 8(1)
14.13	There shall be separation between trust domains. This separation may be enforced by the virtualisation fabric, provided virtualisation cut-throughs are not used.	3(1)(a),(b),(c) 3(2) 3(3)(d) 4(1)(a),(b) 4(2)(a),(b)
14.14	Host pools shall be tagged with trust domains they can execute. This will be based on risk and ensure that sensitive functions are not executed alongside vulnerable functions, or in physically-exposed locations.	3(1)(a),(b),(c) 3(2) 3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(c)

[53] *Using TLS to protect data* (NCSC, 2021)
[54] *Using IPSec to protect data* (NCSC, 2016)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
14.15	A physical host shall not be able to impact hosts in other host pools. This includes, but is not limited to, spoofing VLAN/VXLANs of virtual networks.	3(1)(a),(b),(c) 3(2) 3(3)(d) 3(3)(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(c) 6(1) 6(3)(b)
14.16	Containers shall not be used to implement separation between trust domains. To implement separation between trust domains, providers shall use Type-1 hypervisors (without cut-throughs) or discrete physical hardware.	3(1)(a),(b),(c) 3(2) 3(3)(d) 3(5) 3(3)(d) 4(1)(a),(b) 4(2)(a),(b)
14.17	Containerised hosts shall only support a single trust domain.	3(1)(a),(b),(c) 3(2) 3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b)
14.18	The control and orchestration functions for virtualisation are network oversight functions and shall reside in a trusted physical and logical location.	3(3)(d) 3(5)
14.19	The administration network of the virtualisation fabric is a management plane and shall be protected as such.	3(3)(d) 3(5) 4(1) 4(2)
14.20	Privileged access to the virtualisation fabric shall only be available over authenticated and encrypted channels.	3(3)(a) 3(3)(d) 3(5) 4(1) 4(2) 8(5)(e)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
14.21	Functions that support the administration and security of the virtualisation fabric shall not be run on the fabric it is administering.	3(3)(a) 3(3)(d) 3(5) 4(1) 4(2)
14.22	Functions that support the administration and security of the virtualisation fabric are network oversight functions and shall reside in a trusted physical and logical location.	3(3)(a) 3(3)(d) 3(5) 4(1) 4(2)
14.23	The number of privileged accounts for the virtualisation fabric shall be constrained to the minimum necessary to meet the provider's needs.	3(3)(d) 4(1)(b) 4(2)(b) 7(1) 8(1) 8(2)(a) 8(4)
14.24	Virtualisation fabric administrator accounts shall not have any privileged rights to other services within the provider, or vice-versa.	3(3)(d) 4(1)(b) 4(2)(b) 7(1) 8(1) 8(2)(a) 8(4)
14.25	Virtualisation fabric administrator accounts shall only be provided with the privileges and accesses required to carry out their role.	3(3)(d) 4(1)(b) 4(2)(b) 7(1) 8(1) 8(2)(a) 8(4)
14.26	Virtualisation fabric administrator accounts shall not have access to the provider’s workloads running within the virtualised environment.	3(3)(d) 4(1)(b) 4(2)(b) 7(1) 8(1) 8(2)(a) 8(4)
14.27	Network oversight functions shall not share trust domains or host pools with workloads that are not network oversight functions.	3(3)(d) 3(5)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
14.28	Containers shall not be used to enforce separation between different network oversight functions and between network oversight functions and other functions.	3(3)(d) 3(5)
Third party supplier measures 3		
15.01	Once equipment reaches the vendor's end-of-life date, providers shall only continue to use the equipment if the following conditions are met: a) the equipment's configuration is rarely modified, and modifications are reviewed; b) either the addressable interfaces of the unsupported equipment are monitored and use of those interfaces can be explained, or there is no realistic possibility that exploitation of all unsupported equipment would have an impact on the network; and c) the network exposure (attack surface) of the unsupported equipment is minimal (e.g. some transport equipment).	3(3)(a),(b),(e) 3(4) 6(2) 6(3) 7(1) 7(4)(c)
16.01	The provider shall block and record any SIM OTA messages sent to their own SIMs, except where these are sent from allowed sources.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a) 8(6)
Network Oversight Functions		
17.01	Network oversight functions shall be robustly locked-down and patched within such period as is appropriate in the circumstances, having regard to the severity of the risk of security compromise which the patch or mitigation addresses.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 8(3) 12

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
17.02	Any service that supports or contains a network oversight functions shall be rebuilt from an up-to-date known-good software state every 24 months. This includes the operating system and application software. This can be performed in line with a system upgrade.	3(3)(a),(d),(e) 4(1)(b) 4(2)(b) 8(3) 12
17.03	Any workstations or functions (e.g. jump boxes) through which it is possible to make administrative changes to network oversight functions shall be rebuilt from an up-to-date known-good software state on a yearly-basis. This applies to the workstation or function's operating systems and above.	3(3)(a),(d),(e) 4(1)(b) 4(2)(b) 8(3) 12
17.04	Network oversight functions shall run on trusted platforms.	3(3)(a),(d),(e) 4(1)(b) 4(2)(b) 8(3) 12
17.05	Where providers cannot guarantee the security of the physical environment (e.g. within the exposed edge, or within a shared data centre/exchange) network oversight functions shall not be deployed.	3(3)(a),(d),(e) 4(1)(b) 4(2)(b) 8(3)
17.06	Network oversight functions shall only be managed by a minimal set of trusted privileged users.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 4(4)(a) 8(2)(a),(f) 8(4) 8(5)(a),(b),(e) 8(6)
17.07	The management functions (e.g. jump-box) used to manage network oversight functions shall only be accessible from designated PAWs.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 4(4)(a) 8(2)(f) 8(3) 8(4) 8(5)(a),(e)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
17.08	Dedicated management functions shall be used to manage network oversight functions.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 8(3) 8(4)
17.09	The management plane used to manage network oversight functions shall be isolated from other internal and external networks, including the management plane used by other equipment.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 8(2)(f) 8(4) 8(5)(a),(e)
17.10	All management accesses to network oversight functions shall be pre-authorised by a limited set of people who have been assigned with an appropriate role.	3(3)(a),(d) 3(5) 4(1)(b) 4(2)(b) 6(2)(a),(b) 6(3)(a),(b) 8(2)(a),(c),(f) 8(4) 8(5)(b),(e) 8(6) 13(2)(a),(b)
17.11	Changes to network oversight functions shall be monitored in real-time (e.g. Syslog).	3(3)(d) 4(1)(b) 4(2)(b) 4(4)(a) 5(3) 6(2)(a),(b) 6(3)(a),(b),(c),(d),(f) 8(2)(c) 8(5)(b),(d)
17.12	The designated PAWs, dedicated management functions and the network oversight functions themselves shall be monitored for signs of exploitation.	3(3)(d) 4(1)(b) 4(2)(b) 4(4)(a) 5(3) 6(2)(a),(b) 6(3)(a),(b),(c),(d),(f) 8(2)(c) 8(5)(b),(d)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
17.13	Network oversight functions shall only access services (e.g. AAA, network time, software updates) over internally-facing interfaces.	3(3)(a),(d) 3(5) 4(1)(b) 4(2)(b) 8(2)(f)
Monitoring and analysis 1		
18.01	Providers shall use appropriately-skilled and dedicated resources to understand and analyse security-related network activity. These resources may be provided by a third party supplier.	8(2)(a) 13(2)(a),(b),(c) 14(1)
18.02	Providers shall ensure that threat hunting is periodically performed using available logging and monitoring data.	6(1) 6(2)(a),(b) 6(3)(d) 10(2)(a) 11(a) 11(b)(vii) 14(1)
18.03	Providers may outsource threat hunting to an independent third party, but, if possible, should not outsource audit or threat hunting to any party involved in operating the network.	10(1) 14(1) 14(4)(a)
18.04	Asset management and network monitoring systems shall be kept up to date to enable security staff to identify and track down anomalies within networks. This shall include comprehensive details of normal system and traffic behaviour (e.g. source and destination, frequency of communication, protocols and ports used, and expected bandwidth consumed).	3(1)(c) 3(3)(e) 4(1)(b) 4(2)(b) 6(3)(a),(b),(c),(d),(e),(f) 6(4) 9(1) 9(2)(c)(i),(v) 11(a)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
18.05	Network changes that could impact network security shall be notified to those monitoring the network. Monitoring processes shall be maintained and modified if necessary.	3(1)(c) 3(3)(a) 4(1)(b) 4(2)(b) 5(2) 5(3) 6(2)(a),(b) 6(3)(a),(b),(c),(d),(e),(f) 6(4) 8(2)(c) 9(1) 9(2)(c)(i),(v) 11(a) 11(b)
18.06	Physical and logical interfaces between networks that operate at different trust levels shall be monitored, and between groups of network functions (e.g. core networks and access networks).	3(3)(a) 4(1)(b) 4(2)(b) 5(2) 5(3) 6(2)(a),(b) 6(3)(a),(b),(c),(d),(e),(f) 6(4) 9(1) 9(2)(c)(i),(v)
18.07	Systems that collect and process logging and monitoring data shall be treated as network oversight functions.	3(3)(a),(d) 3(5) 4(1)(a),(b) 4(2)(a),(b)
18.08	The integrity of logging data shall be protected, and any modification alerted and attributed.	3(3)(a),(d) 4(1)(a) 4(2)(a) 8(2)(b),(c) 8(5)(b)
18.09	All actions involving stored logging or monitoring data (e.g. copying, deleting, modification, or viewing) shall be traceable back to an individual user.	3(3)(a),(d) 4(1)(a) 4(2)(a) 8(2)(c) 8(5)(a),(b),(c),(d)
18.10	Logging datasets shall be synchronised, using common time sources, so separate datasets can be correlated in different ways.	3(3)(a),(d),(e) 4(1)(a) 4(2)(a)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
18.11	An alarm shall be raised if logs stop being received from any network equipment.	3(3)(a),(d),(e) 4(1)(a) 4(2)(a)
18.12	Logs for network equipment in security critical functions shall be fully recorded and made available for audit for 13 months.	3(3)(a),(d),(e) 4(1)(b) 4(2)(b) 6(2)(a),(b) 6(3)(a)(b),(c),(e),(f) 6(4) 9(2)(c)(i),(iv)
18.13	Network-based and host-based sensors shall be deployed and run throughout networks to obtain traffic to support security analysis.	6(1) 6(2)(a),(b) 6(3)(a),(d),(e),(f) 9(2)(c)(i),(iv)
18.14	Access events to network equipment shall be collected. Unauthorised access attempts shall be considered a security event.	4(4)(b),(c) 6(1) 6(2)(a),(b) 6(3)(a),(b),(d),(e) 7(4)(a)(iii) 8(5)(d) 9(2)(c)(i),(iv) 13(2)(a)
18.15	Logging data shall be enriched with other network knowledge and data. In order to successfully analyse logging data it must be used in conjunction with knowledge of the providers' network as well as other pertinent data needed for understanding log entries.	6(1) 6(2)(a),(b) 6(3)(e) 9(2)(c)(i),(iv)
18.16	Network equipment configurations shall be regularly and automatically collected and audited to detect unexpected changes.	3(3)(e) 6(1) 6(2)(a),(b) 6(3)(c),(d),(e) 6(4) 8(2)(g) 9(2)(c)(i) 12(b) 14(1)

The following measures should be completed by 31 March 2025 (Tier 1 providers) or by 31 March 2027 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
18.17	Logs shall be linked back to specific network equipment or services.	6(1) 6(2)(a) 6(3)(a),(e) 6(4) 9(2)(c)(i),(iv)
18.18	Logs shall be processed and analysed in near real-time (in any case within 5 minutes) and generate security relevant events.	4(4)(b) 5(1)(a) 6(1) 6(2)(a),(b) 6(3)(c),(d),(e) 9(2)(c)(i),(iv) 11(a)
18.19	The provider shall ensure that tools and techniques are utilised to support analysts in understanding the data collected.	6(1) 6(2)(a),(b) 6(3)(c),(e) 7(4)(iv) 9(1) 11(a)
18.20	Providers shall regularly review access logs and correlate this data with other access records and ticketed activity.	6(1) 6(2)(a),(b) 6(3)(a),(b),(c),(d),(e) 8(5)(d) 9(2)(c)(i),(iv)
18.21	Indications of potential anomalous activity shall be promptly assessed, investigated and addressed.	6(1) 6(2)(a),(b) 6(3)(d),(e) 9(2)(c)(i),(ii),(iv),(v)
18.22	Logging data shall be correlated with data within asset management systems to detect anomalies. Models shall be developed to characterise ‘normal’ traffic within networks, including type and volume.	6(1) 6(2)(a),(b) 6(3)(a),(d),(e) 9(2)(a) 9(2)(c)(i),(iv)

The following measures should be completed by 31 March 2026 (Tier 1 providers) or by 31 March 2028 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
Management plane 3		
19.01	Administrative processes shall be automated wherever possible. All manual administration shall create an alert where amendments have been made to security critical functions.	3(5) 6(2) 6(3)(c),(d) 8(1) 8(2)(g)
Signalling plane 3		
20.01	Signalling messages shall be validated at the logical edge of the network prior to being forwarded to core nodes. The validation shall verify compliance with the signalling protocol in use, preventing malformed messages from entering the provider's network. Valid incoming signalling messages shall be reconstructed (rather than copied), when forwarding to core nodes.	3(3)(a)(iv) 3(3)(c),(d),(e) 3(4) 4(1)(b) 4(2)(b) 4(4)(b) 8(3)
20.02	A signalling failure for an externally-facing service shall not impact core nodes or security critical functions.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 4(4)(b) 8(3)
20.03	Only ‘hub’ signalling addresses shall be exposed externally. This shall be done in such a way that internal signalling addresses of critical core nodes are not shared or exposed externally.	4(1)(a) 4(2)(a) 4(4)(a) 4(5) 6(1) 8(1)
20.04	Outgoing signalling shall be authenticated where this is supported by international standards.	4(4)(b) 6(1) 6(2)(a),(b)

The following measures should be completed by 31 March 2026 (Tier 1 providers) or by 31 March 2028 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
20.05	Customer data, customer identifiers and network topology information shall be obfuscated before it is released over an external signalling network, except where it is functionally essential to provide this information.	4(4)(b) 8(1) 8(2)(f) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 4(5) 6(1) 6(2)(a) 8(1) 8(5)(a)
Virtualisation 2		
21.01	All non-ephemeral secrets, passwords and keys shall be stored in hardware-backed secure storage.Where providers are not able to apply this measure to existing networks and services they must set out what mitigating steps they are taking.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 8(5)(a) 12(a),(b),(c)
21.02	Only physical hosts that have cryptographically attested to be in a known-good state can be provisioned into the virtualisation fabric.	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 8(3) 8(4) 12
21.03	Where the virtualisation fabric provides a security boundary, it shall not be able to directly access the physical hardware (no cut-throughs).	3(1)(a),(b),(c) 3(2) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b)
21.04	Where possible, the virtualisation fabric shall be built and updated through an automated and verifiable process.	3(3)(d),(e) 8(2)(g) 12

The following measures should be completed by 31 March 2026 (Tier 1 providers) or by 31 March 2028 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
21.05	Where possible, only automated and verifiable methods of configuration shall be used for administration of the virtualisation fabric (authorised API calls etc).	3(3)(e) 8(2)(g)
21.06	Where possible, administration of the virtualisation fabric shall be automated during normal operation.	8(2)(g)
21.07	Manual administration of the virtualisation fabric (e.g. access to a command line on host infrastructure) shall produce an immediate alert	6(3)(c) 8(2)(g)
Monitoring and analysis 2		
22.01	Automated tools shall be used to find and prioritise events that require manual analysis.	3(3)(a) 4(1)(b) 4(2)(b) 5(3) 6(2)(a),(b) 6(3)(d),(f) 9(1) 9(2)(c)(i),(iv),(v),(vi)
Retaining national resilience and capability		
23.01	Procedures should ensure contingencies are in place in the event that further locations are added to the Schedule of the Electronic Communications (Security Measures) Regulations.	3(3)(a)(iii) 3(3)(d),(e) 3(5) 5(2) 5(3) 7(1) 7(5) 8(1) 8(2)(a) 8(6)

The following measures should be completed by 31 March 2026 (Tier 1 providers) or by 31 March 2028 (Tier 2 providers)		
Measure number	**Description**	**Relevant Regulation(s)**
23.02	The measures to be taken by the provider under Regulation 3(3)(f) should normally include ensuring, so far as is reasonably practicable, that the equipment performing provider's network oversight functions is located within the UK, and operated using UK-based staff.	3(3)(f)
23.03	The provider shall retain a UK-based technical capability to provide subject matter expertise on the operation of the provider's UK networks and the risks to the provider's UK networks.	3(3) 13(1)
23.04	Where data is stored offshore, the provider shall maintain a list of locations where the data is held. The risk due to holding the data in these locations, including any risk associated with local data protection law, shall be managed as part of the provider's risk management processes.	3(3)(a),(f),(g),(h) 5(2) 11
23.05	Decisions about holding outside of the UK data relating to more than 100,000 UK subscribers, the operation of the large parts of the network, or the operation of network oversight functions, shall be taken at an appropriate governance level and recorded in writing. The sign-off for these decisions should normally be given by a person or committee at board level (or equivalent).	3(3)(a),(f),(g),(h) 5(3)
23.06	If it should become necessary to do so, the provider shall have the ability to maintain 100% of normal service connectivity for a period of one month in the event of loss of international connections.	3(3)(h)
23.07	If it should become necessary to do so, the provider shall be able to transfer into the UK functions required by UK networks to maintain an operational service, should international bearers fail.	3(3)(h)

Annex A: Glossary of terms

The terms listed below are used throughout the code of practice.

Access Network	The part of the network that connects directly to customers. This includes, but not limited to, the Radio Access Network, Passive Optical Network (PON), and copper access networks.
Bare Metal Hypervisor	Another name for a Type 1 hypervisor, so called as it does not run on top of a hosts operating system but on the “bare metal” of the hosts hardware.
Customer Premises Equipment (CPE)	The Customer Premises Equipment provided and managed by the provider to the customer. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit.
Cyber Assessment Framework (CAF)	The CAF provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. NCSC CAF guidance - NCSC.GOV.UK
Containerisation	The term for the use of a Type 2 hypervisor (or Hosted Hypervisor) environment. This type of hypervisor runs inside the operating system of a physical host machine.
Container	The environment created by the Type 2 (Hosted) hypervisor in which a Virtual Machine runs.
Core nodes	The main network elements that processes data and store information
Corporate Security Domain	A system or group of systems that all have the same level of security which protects the providers own data.
Cryptographically attested	Identity, security and integrity of a system or sub system is confirmed by an encrypted algorithm.

DeMilitarised Zone (DMZ)	A perimeter network that protects and adds an extra layer of security to an organisation's internal local-area network from external untrusted traffic.
Digital Subscriber Line Access Multiplexer (DSLAM)	A network device that receives signals from multiple customer Digital Subscriber Line (DSL) connections and puts the signals on a high-speed backbone line using multiplexing techniques.
Exposed Edge	Equipment that is either within customer premises, directly addressable from customer/user equipment, or is physically vulnerable. Physically vulnerable equipment includes mobile base sites, equipment in road-side cabinets or attached to street furniture.
Externally-Facing Interface	Any system interface which is accessible to people or systems outside of the provider's direct control.
Externally-Facing System or Service	Any system or service with an externally-facing interface.
Fixed-Profile SIM	A Subscriber Identity Module Card where the credentials used to authenticate access to the network cannot be modified.
Fuzzing	An automated software testing technique that involves providing invalid, unexpected, or random data as inputs to assess a system's vulnerability to them.
The Global System for Mobile Communications (GSM)	A digital mobile network that is widely used by mobile phone users in Europe and other parts of the world.
Home Location Register (HLR)	A database containing pertinent data regarding subscribers authorised to use a global system for mobile communications (GSM) network. Including their last known location and service they are allowed to use.
Host-based sensors	Piece of code installed in a computer or other devices to collect and forward information on system activity.
Hub signalling address	The parts of the network which need to communicate with other providers (eg for roaming or number portability).

Insecure Protocols	An insecure protocol should be considered to be any protocol where a more secure or encrypted variant of that protocol exists, Some examples are to use HTTPS rather than HTTP, SSH rather than Telnet, TaACACS+ rather than TACACS. This is not an exhaustive list and is constantly evolving.
Internally-Facing interface	Any system interface that is only accessible by people and systems within the provider's direct control.
Jump Boxes	A system on a network used to access and manage devices in a separate security zone.
Logical edge of the network	The furthest element of the network that can be electronically reached.
Media Access Control address (MAC)	A unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.
Management Access	Access to control or modify the operation of a device or network.
Management Networks	A collective term for systems that are responsible for the network management
Management Plane	The interfaces and connectivity and supporting equipment that allows Network Equipment to be managed.
Multi Factor Authentication (MFA)	An authentication method that requires the user to provide two or more verification factors to gain access to a resource
Multi-Service Access Node (MSAN)	A device which connects customers' telephone lines to the core network, to provide telephone, ISDN, and broadband, all from a single platform.
Mobile Switching Centre (MSC)	The MSC connects calls between subscribers by switching the digital voice packets between network paths. It also provides information needed to support mobile subscribers services that the home location register has given access to.

Malformed signalling messages	Signalling messages should be correctly formed and only directed to the appropriate parts of the network from parts of the network which are authorised and expected to initiate them. Malformed messages can be caused by transmission faults, but they may also be deliberate attempts to attack a network and as such should be blocked. See also 'Fuzzing'.
Managed Service Provider (MSP)	Any entity that delivers services, such as network, application, infrastructure and security, via ongoing and regular management, support and active administration on customers' premises, in their MSP's data centre (hosting), or in a third-party data centre.
National Cyber Security Centre (NCSC)	The UK's technical authority for cyber threats. It is part of the Government Communications Headquarters (GCHQ)
Negative Testing	The process of validating the application against invalid inputs. Invalid data is used in testing to compare the output against the given input and results monitored for potential vulnerabilities.
The GSMA's Network Equipment Security Assurance Scheme (NESAS)	An industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry.
Network and Information Systems Regulations (NIS Regulations)	These regulations provide legal measures to protect essential services and infrastructure by improving the security of their network and information systems and maturing their resilience.
Network-based sensors	A component installed in a network to collect and forward information on system activity.
Network Data	The network identifiers, logs, documents that help to describe the network and the equipment in the network
Network Operations Centre (NOC)	A physical or logical location from where network engineers can continuously monitor the performance and health of a network.

Network Oversight Function	Network oversight functions are the components of the network that oversee and control the security critical functions, which make them vitally important in overall network security. They are essential for the network provider to understand the network, secure the network, or to recover the network.
Network Function Virtualisation	A way to virtualize network services, such as routers, firewalls, and load balancers, that have traditionally been run on proprietary hardware.
Optical Line Terminal (OLT)	The endpoint hardware device in a passive optical network
Privileged Access / Administrative Access	An access to network equipment where greater capabilities are granted than a basic maintenance engineer. The misuse of privileged access could negatively impact the network. Any access over the management plane, or to management ports of network equipment is privileged access.
Privileged Access Workstation (PAW)	An appropriately secured device which is able to make changes to security critical functions via a management plane.
Privileged User / Administrator	A person who is granted privileged access, through their role, access and credentials, or through any other means.
Profile-Modifiable SIM	A SIM card where the SIM profile credential used to authenticate access to the network can be modified or deleted, or where new SIM profiles and credentials may be added.
Remote Desktop Protocol (RDP)	A proprietary protocol which provides a user with a graphical interface to connect to another computer over a network connection.

Scanning the wider network	Only the appropriate ports should be available on any component. The network provider should ensure that all other ports are closed. Similarly, all protocols should be unavailable except for those specifically required by the network provider. Scanning should flag any of these which are available and unless specifically recorded as required, these must be shut down immediately as they are unnecessary and present a risk to security.
Software Defined – Wide Area Network (SD-WAN)	A virtual WAN architecture that allows enterprises to leverage any combination of transport services to securely connect users to applications.
Secure Channel	A communications flow which is encrypted using industry best practice such as TLS 1.2, SSHv2, or IPsec with industry best practice cipher suites. This is not an exhaustive list and is constantly evolving.
Security Analysis	Considering data or information with the intent of detecting a threat actor or understanding the behaviour of a threat actor. Used to determine mitigating actions.
SIM Card	A Subscriber Identity Module (SIM) is a unique hardware component or token, and associated software, used to authenticate the subscriber's access to the network. As used in this document, the SIM encompasses the hardware UICC/eUICC, the SIM/USIM/ISIM applications, eSIM and RSP functionality and any SIM applets. Note that this is a broader definition than the true technical definition (which defines the SIM to be the GSM authentication application running on a UICC). Instead, we are using the term 'SIM' as it is commonly used in the public domain to refer to the token in a device in its entirety.
SIM OTA	SIM Over-The-Air - technology that updates and changes data in a profile modifiable SIM card without having to physically replace it.
SIM Profile	The provider-defined identity, credential, algorithms, parameters and applets stored on the SIM card.

Signalling System No7 (SS7 or CCITT #7)	A telecommunications signalling architecture traditionally used for the set up and clear down of telephone calls and services in fixed or mobile telecommunications networks.
Third party administrators (3PA)	Managed service providers, provider group functions, or external support for third party supplier equipment (e.g. third-line support function).
Transport Layer Security (TLS)	A widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.
Trusted Platform	A secure platform which has the characteristics defined in Secure by default platforms - 22 September 2016
Trusted Platform / Trusted Computing Platform	A platform that uses roots of trust to provide reliable reporting of the characteristics that determine its trustworthiness.
Trust levels	Where all the devices at the same level have the same standard of security, integrity and availability.
UICC	Any physical card SIM-like credential allowing network access, including permanently soldered-in UICCs in some handsets and IoT devices. (An eSIM does not require a UICC)
Up-to-date known-good software state	A piece of software that is proven to be current, supported and unmodified from the agreed standard
Third party supplier Equipment or Network Equipment	Either software or hardware component of the provider's network that transmits or receives data or provides supporting services to components of the provider's network that transmit or receive data. Includes both virtual machines and physical hardware.
Vendor's End-Of-Life Date	The end of the vendor's standard, global support for the equipment. The point at which no further security patches will be provided.

Virtualisation "Cut-Through" and Paravirtualization	Paravirtualization is when specific guest OS kernel modifications are made to replace non-virtualizable instructions with hypercalls that communicate directly with the virtualisation layer hypervisor. The hypervisor also provides hypercall interfaces for other critical kernel operations such as memory management, interrupt handling and time keeping). These are often referred to as "cut-throughs".
Virtualisation Administrators	Administrators who are granted privileged access to virtualisation infrastructure (NFVi), or the functions which manage virtualisation infrastructure.
Virtualisation Fabric	The physical servers and networking equipment used to provide the resources for virtualised workloads to run on.
Virtual LAN (VLAN)	Any broadcast domain that is partitioned and isolated in a computer network at the data link layer.
Virtual Extensible LAN (VXLAN)	A network virtualisation technology that attempts to address the scalability problems associated with large cloud computing deployments.
Wide Area Network (WAN)	A data network that extends over a large geographic area for the primary purpose of computer networking.