Department for
Digital, Culture,
Media & Sport

Draft Telecommunications Security Code of Practice

Department for Digital, Culture, Media and Sport

Draft Telecommunications Security Code of Practice

Presented to Parliament pursuant to Section 105F of the Communications Act 2003

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at

Department for Digital, Culture, Media and Sport
100 Parliament Street
London SW1A 2BQ
Tel: 020 7211 6000

ISBN 978-1-5286-3660-5
E02781980 09/22

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of Her Majesty's Stationery Office

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 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 0.11-0.16 below.
- Section 3 contains 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 as laid in parliament on 5 September 2022.

Section 1: Introduction and background

Introduction

0.1 The government's UK Telecoms Supply Chain Review Report ('the Review'), 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.

0.2 Since the Review was published, the government has put this recommendation into action, developing a new security framework for providers of public electronic communications networks or services (PECN/PECS)[3] through the Communications Act 2003 ('the Act') as amended by the Telecommunications (Security) Act 2021 ('the TSA'). This new security framework, set out in the amendments to the Act, the regulations and this code of practice, has been drafted by the government, taking into account its obligations under international law. The regulations and code of practice have been informed by a public consultation.

0.3 The framework established through the TSA comprises three layers:

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

ii. **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.

iii. **Technical guidance.** This code of practice provides detailed guidelines to large and medium-sized providers of PECN or 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

0.4 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) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf

[3] As defined in section 151 of the Communications Act 2003 https://www.legislation.gov.uk/ukpga/2003/21/section/151

[4] *Summary of the NCSC's security analysis for the UK telecoms sector* (NCSC, 2020) https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector

Roles and responsibilities of public authorities

0.5 *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.

0.6 *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 public networks and services and monitor their compliance.

0.7 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.

0.8 *The 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.

0.9 The NCSC will also continue to offer technical advice to telecoms providers. However, the NCSC will not report providers to Ofcom 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

0.10 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.

The tiering system

0.11 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.

0.12 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, but who are not micro-entities.

Application of the tiering system

0.13 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 for Tier 1 providers in Section 3.

[5] *Joint statement from Ofcom and the National Cyber Security Centre* (Ofcom and NCSC, 2021) https://www.ofcom.org.uk/__data/assets/pdf_file/0028/219628/ofcom-ncsc-joint-statement-telecoms-security-bill.pdf

- The measures in the code of practice also apply to medium-sized **(Tier 2)** public telecoms providers. They will have more time than Tier 1 providers to implement some of the measures set out in Section 3.
- 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.

0.14 Whilst the measures are intended to address the risk of security compromises 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 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 generated during the relevant period 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 last but one calendar year prior to the reporting cycle in question. So, for example, the relevant turnover generated in 2020 would 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

0.15 For the purposes of applying guidance set out in the code of practice, an existing tier designation will apply to a provider until the provider has been outside of their existing tier's range for at least two years.

0.16 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

0.17 The code of practice provides detailed technical guidance to public telecoms providers on the measures to be taken under sections 105A to 105D 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.

[6] *The definition of "relevant activity" for the purposes of administrative charging* (Ofcom) https://www.ofcom.org.uk/__data/assets/pdf_file/0017/80801/definition_of_relevant_acitvity_guidelines.pdf

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

0.18 The guidance set out in this code of practice is not the only way for providers to comply with the new security duties and specific security requirements that have been placed into law. We appreciate that where the regulations require public telecoms providers to take 'appropriate and proportionate' measures, what is appropriate and proportionate will depend on the particular circumstances of the provider.

0.19 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 their legal obligations under the security framework. Providers are obliged to explain those reasons to Ofcom under section 105I of the Act, where Ofcom has reasonable grounds for suspecting the public telecoms provider is failing or has failed to comply with the code of practice.

0.20 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 (see section 105H(3) of the Act).

0.21 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 (see section 105H(2) of the Act).

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

0.22 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.

0.23 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.

0.24 Further information on how Ofcom will use its powers and regulate the framework will be contained within its procedural guidance.

Implementation timeframes

0.25 Whilst the security duties, requirements in regulations and Ofcom oversight powers 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 timeframes 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.

0.26 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.

Implementation timeframes and the tiering system

0.27 For the majority of measures, the timeframes are the same for Tier 1 and 2 providers. However, a subset of the most straightforward measures have a shorter timeframe for Tier 1 providers in recognition of the fact that smaller providers with fewer resources may need more time to implement measures.

0.28 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-entities[7]. 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

0.29 There may be occasions when public telecoms providers either change tiers, or new public telecoms providers enter the market. Subject to the condition set out in paragraph 0.15 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

0.30 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 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.

0.31 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 the 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.

0.32 When published, this current 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.

[7] Micro-entities are defined as having two of the following three requirements under the Companies Act 2006: turnover of not more than £620,000; balance sheet total of not more than £316,000; not more than 10 employees.

Further information

0.33 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[8]
- The Telecommunications (Security) Act 2021[9]
- The Electronic Communications (Security Measures) Regulations 2022.

[8] *Security analysis for the UK telecoms sector* (NCSC, 2020) https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf

[9] Telecommunications (Security) Act 2021 https://www.legislation.gov.uk/ukpga/2021/31/enacted

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 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 meet the intent of the security requirements. This chapter covers the concepts of security critical functions and network oversight functions which apply throughout, as well as the overarching scope of the 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 the remainder of the code of practice. 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' 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 in the guidance 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 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 the code of practice

1.2 Measures contained within Section 3 of the code of practice apply to public telecoms providers and their public electronic communications networks and services[10]. 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;

[10] As defined in section 151 of the Communications Act 2003 https://www.legislation.gov.uk/ukpga/2003/21/section/151

- 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

1.3 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).

1.4 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 that could impact its proper operation 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.

1.5 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

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

1.7 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.

1.8 Network oversight functions include, but are not limited to, the following components of the network where such components oversee and control security critical functions:

- 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 (OSS).

Guidance

1.9 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.

1.10 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'

1.11 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

1.12 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

1.13 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.

1.14 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

1.15 An example of how network oversight functions and security critical functions can work together in the context of virtualisation workloads is set out below.[11]

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

- a 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.

1.17 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.

[11] More information on virtualisation and containerisation can be found in paragraphs 2.31-2.69.

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

Chapter Crossovers

1.19 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 network as a whole 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 such measures as are appropriate and proportionate 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 take such measures as are appropriate and proportionate to ensure that the network provider—
>
> (i) is able, without reliance on persons, equipment or stored data located outside the United Kingdom, to identify the risks of security compromises occurring,
>
> (ii) 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
>
> (iii) if it should become necessary to do so, 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 take such measures as are appropriate and proportionate to ensure 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.

2.6 Where there is a demonstrable plan at commencement of the regulations for the removal of specific network equipment and it would not be proportionate for that network equipment to meet specific measures within the code, providers shall be required to ensure compliance with their security duties by implementing those measures that remain proportionate, and by taking alternative measures as necessary, based on a detailed risk assessment. This may include earlier replacement of the network equipment with alternative equipment that mitigates the security risk. It is not appropriate to disregard the security of networks based on what may, or may not happen to them in the future.

The management plane

2.7 The management plane of a network 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

2.8 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).

2.9 Specific solutions and platforms which achieve the security objectives surrounding the management plane are open for providers to choose, as is the case for the rest of the security framework. The intention of this document is not to encourage or discourage the use of any specific services, but to ensure that any deployments use the appropriate security controls.

Background

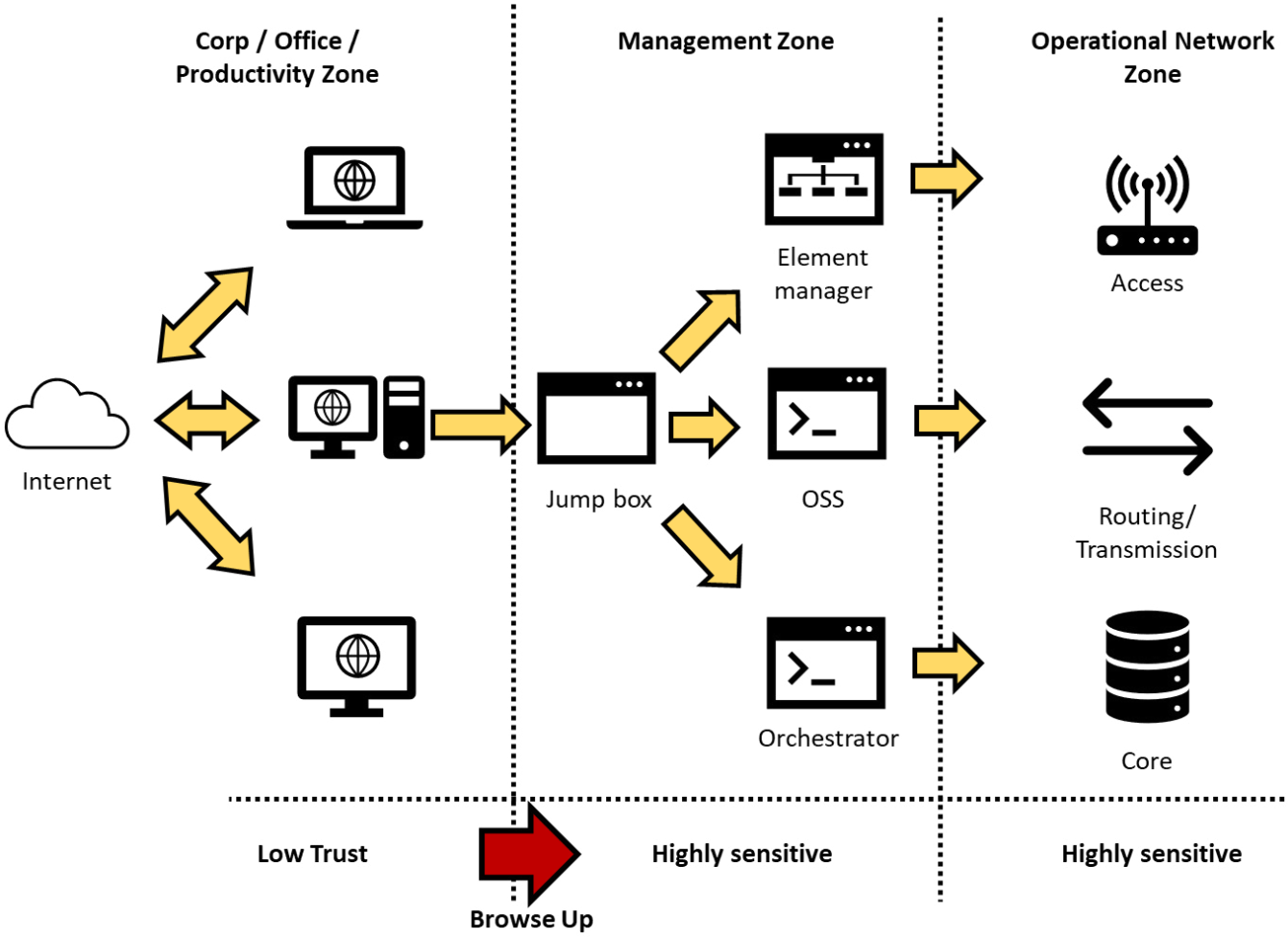
2.10 The management plane is the most powerful part of the network infrastructure, making it the primary target for any malicious attack intending to disrupt or otherwise compromise the operation of a network. Exploitation of the management plane could have a long-term impact on the availability and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

2.11 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.

2.12 As an example, on 17 August 2021 it was confirmed that T-Mobile was subject to a data breach which saw the personal data of nearly 50 million customers being exposed.[12] 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.

2.13 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[13].

Figure 1: Example of 'browse up' architecture



[12] *The Cyberattack Against T-Mobile and Our Customers: What happened, and what we are doing about it* (T-Mobile, 2021) https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers

[13] *Secure system administration* (NCSC, 2020) https://www.ncsc.gov.uk/collection/secure-system-administration

2.14 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

2.15 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 public telecoms providers. The following guidance in paragraphs 2.16-2.30 highlights the key aspects of management plane security for public telecoms providers to understand in order to appropriately secure networks. The guidance also contains 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.[14]

Isolating the management plane

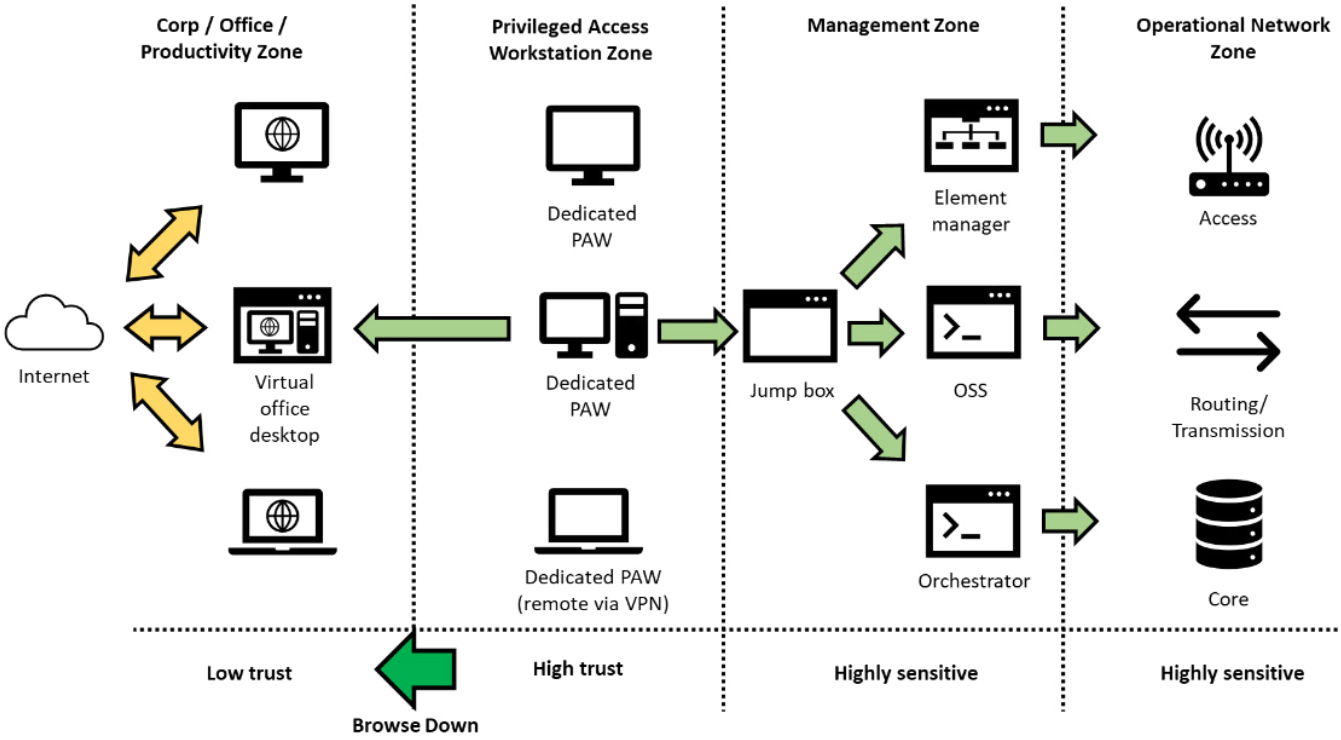
2.16 Given the risks, it is not appropriate for public telecoms providers to be using a 'browse-up' architecture. Instead, public telecoms providers shall architect, and operate, their management plane infrastructure to inhibit network compromise through administrative access.

2.17 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.

2.18 As public telecoms 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.

[14] *Secure system administration* (NCSC, 2020) https://www.ncsc.gov.uk/collection/secure-system-administration

Figure 2: Example of 'browse-down' architecture



2.19 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.

2.20 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.

Secure administration

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

2.22 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, 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.

2.23 Given that management traffic typically involves sensitive data 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 in preference to Telnet or HTTPS in preference to HTTP).

2.24 To ensure that compromise of network equipment does not result in onward access to further equipment via the management plane, public telecoms 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.

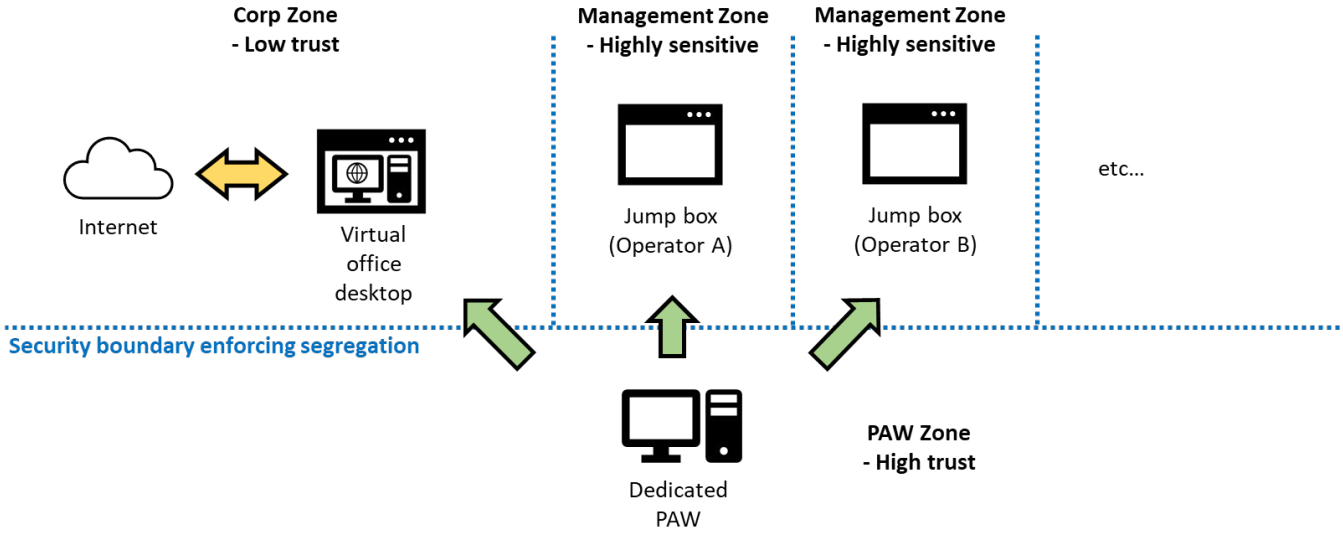
2.25 To protect management platforms (such as jump boxes, element managers, orchestrators, etc) from up-stream attacks from network equipment, the management plane shall be configured to ensure that only necessary connections are allowed. By default, the connections that should be allowed are those established from administrative functions to network equipment.

Third party administrators

2.26 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 public telecoms providers themselves, and ideally shall use the same methods.

2.27 This does not require MSPs and 3PAs to have separate devices for each public telecoms provider that they support. As is the case for the provider themselves, 3PAs will need to use trusted Privileged Access Workstations (PAWs) for administrative activity that is isolated from external attacks and signals (see guidance in Chapter 3). Given a trusted device, 3PAs can access securely-segregated, management systems for multiple providers, as shown in Figure 3. Critically, such an approach must maintain the security and integrity of the PAW, and segregation between each provider's management environment.

Figure 3: Third party administrator secure access to multiple providers



2.28 To ensure that security controls are applied correctly, it will be essential for public telecoms 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. Public telecoms providers shall ensure they are able to fully control and monitor access by third parties into their management plane independently of the third party.

Read only access

2.29 For some administrative tasks, administrators only require read-only access to the management plane. While it may seem that such access is lower risk, this access continues to pose a risk to the network. There remains a risk to network data and, as network equipment commonly treats the management interface as trusted, it may be relatively trivial for a read-only administrator to gain the ability to modify equipment behaviour.

2.30 Because of this, the recommended approach to support read-only administrative accesses to network equipment is to use administrative tools to extract the necessary data from network equipment and securely store this data away from the management plane via a cross-domain data transfer (see Chapter 3). This approach allows controlled access to network data without providing privileged access to the management plane, or necessitating the security controls associated with management plane access.

Virtualisation and containerisation

2.31 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

2.32 Background information and guidance on virtualisation and containerisation in paragraphs 2.33-2.69 applies to public telecoms providers where they are making use of virtualisation or containerisation to abstract more than one piece of physical hardware from the operational software.

Background

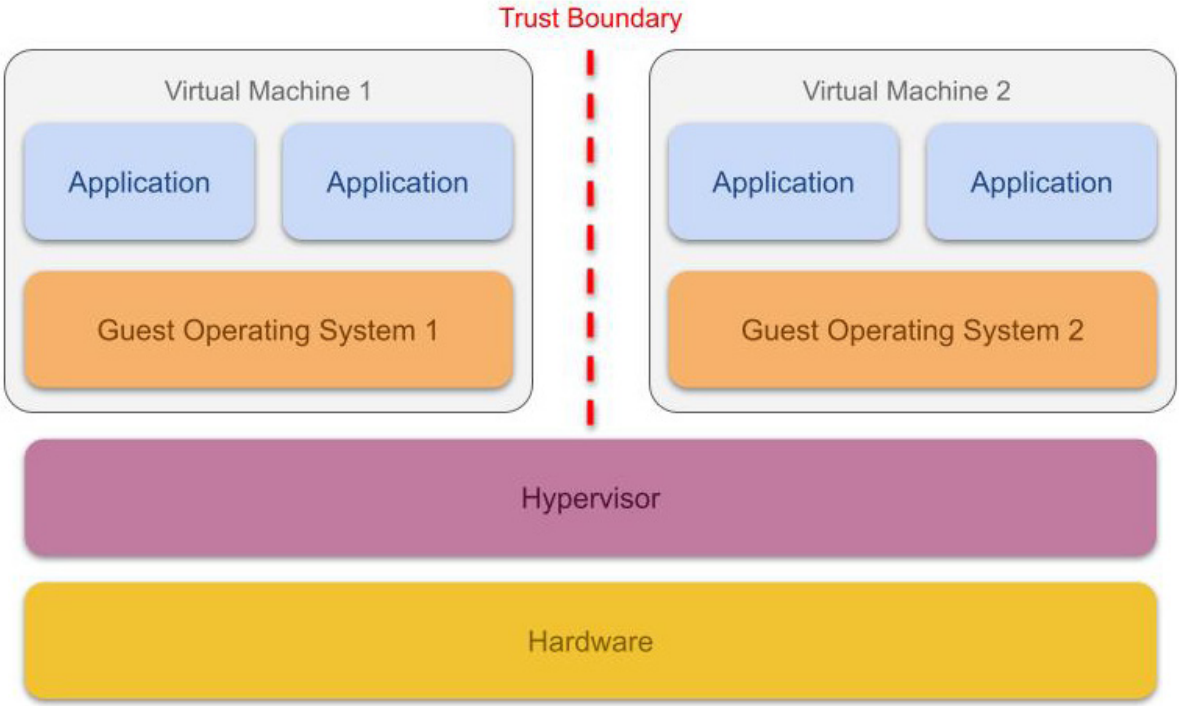
2.33 Prior to the emergence of virtualisation, network functions ran on their own dedicated hardware. Security controls were defined during design, and it was unlikely that these controls would change significantly throughout the equipment's lifetime. Virtualisation allows for greater flexibility. Operationally 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.

2.34 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.

2.35 For the purposes of this document, 'virtualisation' is considered to be a system supported by a 'bare-metal' hypervisor, as shown in Figure 4. 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 4: Example of bare-metal hypervisors

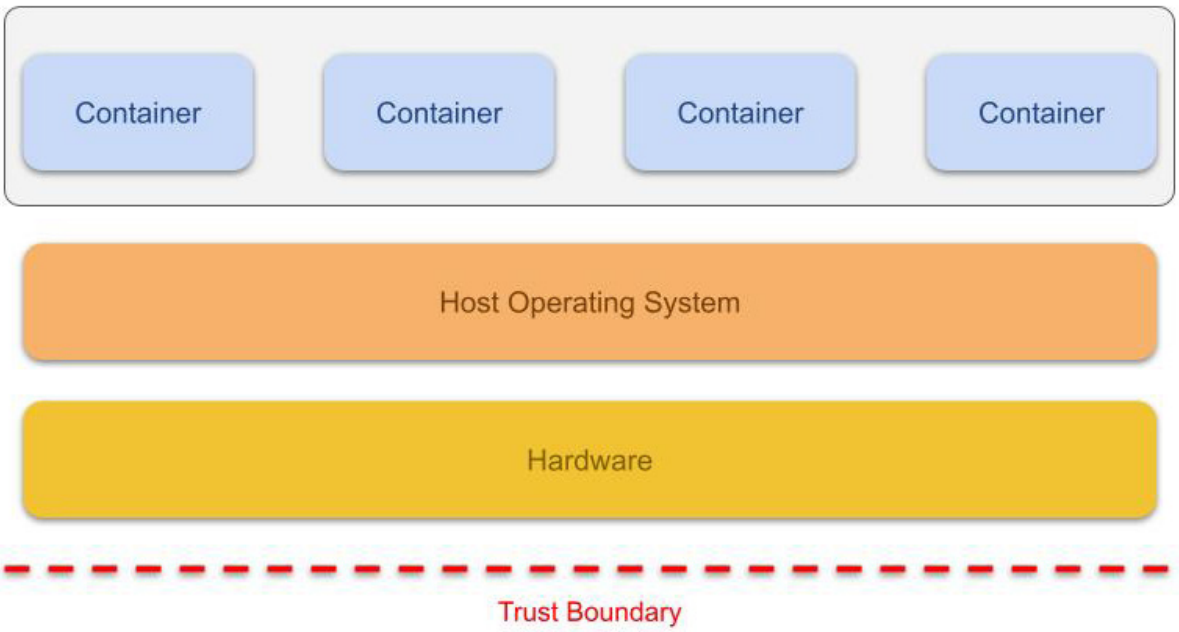


2.36 Virtualisation can be an effective tool for improving the security of a system. By enforcing separation between workloads, it can help prevent lateral movement. By abstracting the hardware, it can allow for better inspection of system behaviour and make the compromise of hardware more complex for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

2.37 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, public telecoms providers should be aware that the configuration of the virtualised environment can undermine its security properties.

2.38 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 5). Access to resources is limited by the host operating system, but hardware resources are not abstracted, meaning the security benefit is limited.

Figure 5: Example of containers



2.39 Containerisation is viable for sharing and scaling workloads within the same security zone or trust domain. However, public telecoms 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. Therefore, containers should never be considered as, nor used as, a security boundary.

2.40 Both virtualisation and containerisation are sometimes used together. Virtualisation may be used to abstract the hardware. Containers are used to scale workloads within the virtual function, but never as a security boundary.

Guidance

2.41 Virtualisation security is an evolving subject, with new security solutions and design patterns emerging each year. The following guidance in paragraphs 2.42-2.69 highlights the key aspects of virtualisation security for public telecoms providers to understand and implement, providing examples and further background information where appropriate. When considering the guidance within the document, public telecoms

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.[15]

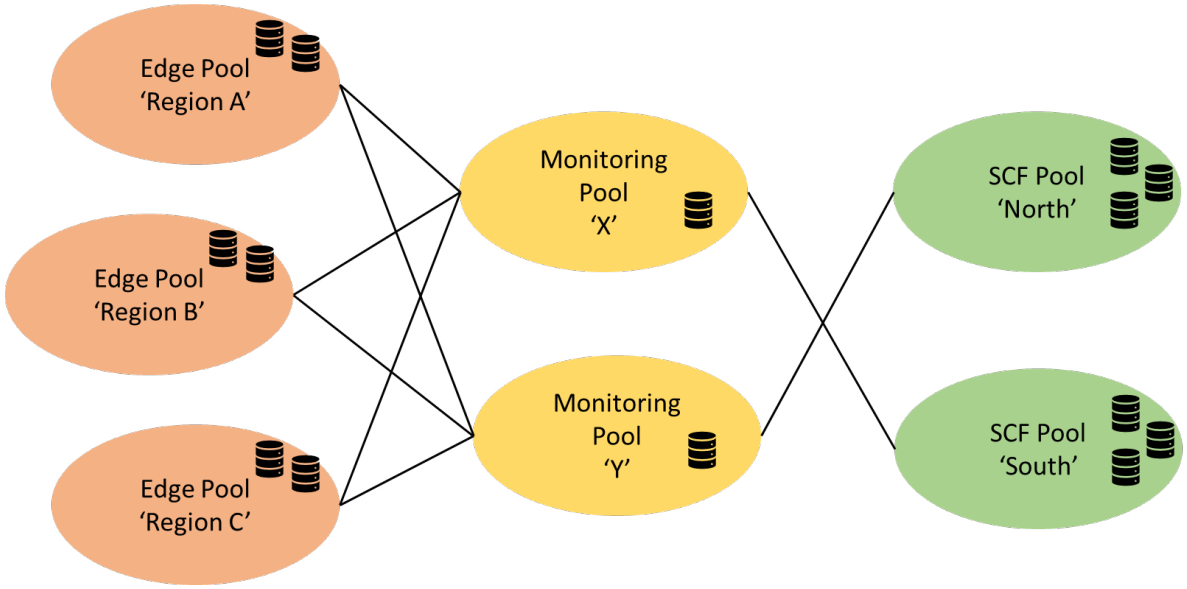
Limiting the impact of host compromise

2.42 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, public telecoms providers shall ensure that it is possible to reduce the impact from, and recover from, a host compromise.

2.43 To limit the impact of host compromise, public telecoms 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.

2.44 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 6. 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 6: Virtualisation fabric broken into host 'pools'

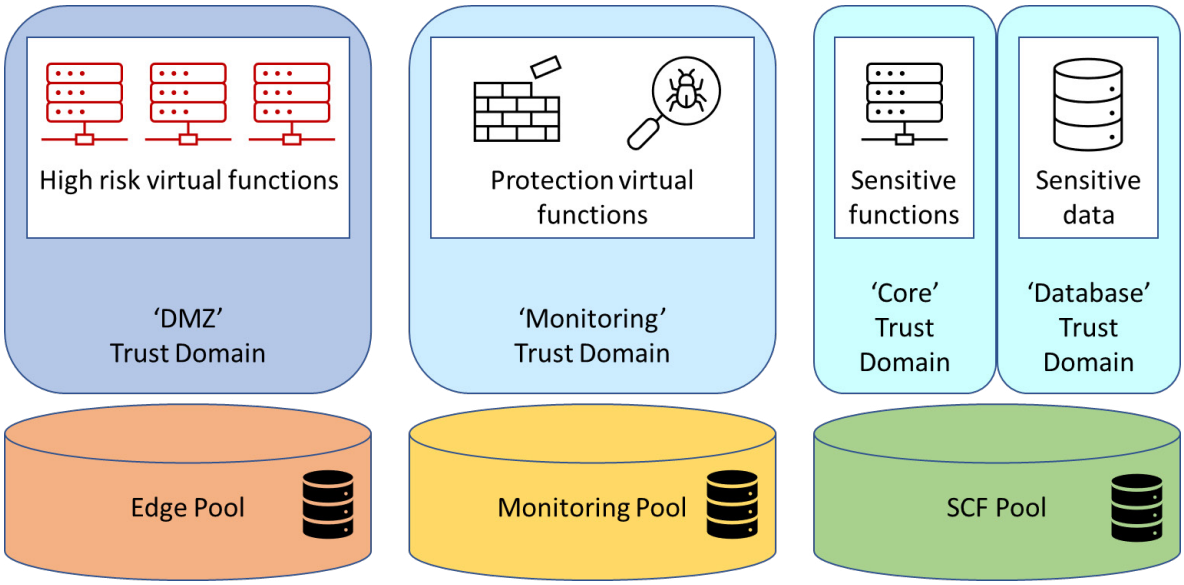


2.45 Similarly, virtual functions can be grouped based on risk, for example due to exposure, criticality or sensitivity. For the purpose of this document, these groups of virtual functions are called trust domains.

2.46 By associating trust domains with host pools, public telecoms providers can segregate their network, maintaining a physical security architecture within a virtualised network, as shown in Figure 7. These associations are sometimes known as 'affinity rules'.

[15] *Virtualisation security design principles* (NCSC, 2019) https://www.ncsc.gov.uk/blog-post/virtualisation-security-design-principles

Figure 7: Segregating trust domains using host pools



Management of the virtualisation fabric

2.47 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.

2.48 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.

2.49 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

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

2.51 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. Trusted Platform Module (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 public telecoms provider that the host can be trusted to host virtual functions.

2.52 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. Public telecoms providers should avoid configuring the virtualisation fabric in such a way as to inhibit the migration of virtual machines as required.

Choosing virtual functions

2.53 Public telecoms 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.

2.54 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.

2.55 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

2.56 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. Public telecoms 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

2.57 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 public telecoms provider to assume that it would be difficult for an attacker to move laterally between these virtual machines via the virtualisation fabric, as long as controls like the hypervisor are up-to-date and there are no known vulnerabilities in the hypervisor that can be exploited.

2.58 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.

2.59 In general, containers do not provide sufficient security separation to be relied upon to segregate virtual functions. Public telecoms 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.

2.60 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.

2.61 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

2.62 An essential part of a virtualised network is the understanding of that network. Public telecoms 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.

2.63 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.

2.64 From a physical perspective, public telecoms 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; and
- the trust domains that the host may support and the networks (VLANs/VXLANs) accessible from the host.

2.65 Within the virtual network, public telecoms 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; and
- the trust domains within the logical flow and the security enforcing functions splitting up that flow.

2.66 Public telecoms providers should also use the flexibility of virtualisation to enable greater monitoring of processes and flows within the virtualised system.

Network automation

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

2.68 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.

2.69 When automating, public telecoms 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 public telecoms 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

2.70 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

2.71 This code of practice applies to signalling traffic arriving from external signalling networks, signalling arriving from other networks that are not within the scope of the security framework and outgoing signalling traffic from a provider's network. This includes, but is not limited to: BGP, SS7/MAP/ISUP, DIAMETER, GTP-C, and SIP/IMS.

2.72 Controls apply to all international signalling, including signalling that 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.

2.73 Throughout the code of practice it should be noted that public telecoms 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

2.74 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, public telecoms 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. It should be noted, however, that where signalling messages are protected by end-to-end authentication, risk decisions and associated security controls may be determined based upon the authenticated source.

2.75 With respect to signalling networks, public telecoms 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 2.76-2.82 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

2.76 Public telecoms 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 in Table 1, along with descriptions of their purpose and function. This list is non-exhaustive.

Table 1: Signalling protocols

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. It is 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.
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.

Protocol	Purpose and function
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. It can also be used to modify the quality-of-service parameters. It is 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). It is 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

2.77 An attacker may seek to scan the provider's signalling networks to understand the network and inform further attacks. Public telecoms 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.

2.78 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, public telecoms providers should ensure that external signalling is fully parsed and processed before reaching a security critical function.

2.79 Architecturally, this may be achieved by public telecoms 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

2.80 Public telecoms providers should seek to prevent the disruption of service or the leaking of customer data, customer identifiers and network topology over signalling interfaces. Where the provider's customers are connected to the provider's network, the public telecoms provider shall implement mechanisms to protect the customer's service and data.

2.81 Where the public telecoms provider's customers have roamed onto another network, the public telecoms 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 public telecoms provider's (home) network.

2.82 Where another provider's customers have roamed onto the public telecoms provider's network, the public telecoms 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

2.83 Effective asset management is the basis of effective security risk management and effective security architectures. Public telecoms providers shall maintain their own asset management records, rather than relying on suppliers or third parties to maintain asset records. Public telecoms providers may, however, collate such information from suppliers and third parties as part of their own asset management records.

Guidance

2.84 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.

2.85 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.

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

2.87 Asset registers and network maps are sensitive data that would be valuable to an attacker seeking to traverse the network. Public telecoms providers should ensure that they are enforcing appropriate protections for this data. Further guidance on asset management can be found on the NCSC website.[16]

The exposed edge

2.88 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

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

2.90 To this end, public telecoms 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.

[16] *NCSC CAF guidance A:3 Asset management* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a-3-asset-management, and *Asset management* (NCSC, 2021) https://www.ncsc.gov.uk/guidance/asset-management

2.91 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.

Retaining national resilience

2.92 Regulation 3(3)(f) imposes certain requirements for national resilience. In particular, regulation 3(3)(f)(iii) requires network providers to take appropriate and proportionate measures to ensure that they would be able to operate the network without reliance on persons, equipment or stored data located outside the United Kingdom if it should become necessary to do so. 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

2.93 The resilience of the UK's national connectivity shall 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 network providers shall take appropriate and proportionate measures to ensure they are able to operate UK networks in emergency situations where there may be reduced international connectivity or travel, and factor this into business plans where they make use of offshored capabilities.

2.94 Whilst public telecoms network providers may be unable to maintain 100% of normal service connectivity in the event of loss of international connections, they shall 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 capabilities. In particular, if it becomes necessary to do so:

- Public telecoms network providers shall have the ability to maintain (as relevant, where they provide such forms of connectivity prior to the event) the following UK network connectivity for a period of one month in the event of loss of international connections:
  - fixed and mobile data connectivity to UK peering points;
  - mobile voice; and
  - text-based mobile messaging.
- Public telecoms network providers shall be able to transfer into the UK functions required by UK networks to maintain an operational service, should international bearers fail.

2.95 When assessing whether it is necessary to maintain the above network connectivity and transfer functions into the UK to maintain an operational service, providers can consider different scenarios in their business continuity planning that may be relevant to their decision. These could constitute emergency situations and may include:

i. loss of access to staff, equipment or data in a specific country or global region, where external factors such as natural hazards or geopolitics limit the access to a provider's resources in a particular country or global region, and those resources are required to operate the critical services set out in paragraph 2.94 above;

ii. compromise of non-UK group functions, where functions of a parent group that are located outside the UK suffer a security compromise, and those functions are required to operate the critical services set out in paragraph 2.94 above;

iii. disruption to connectivity or physical transport links between the UK and rest of the world, where external factors such as natural hazards or geopolitics limit the ability to access a provider's resources outside the UK, and those resources are required to operate the critical services set out in paragraph 2.94 above;

iv. failure of internet routing, where the failure of multiple major global providers, transit routes, or widespread hostile routing updates, or geopolitics cause failure of internet routing, or internet routing protocols, such as eBGP.

2.96 Public telecoms providers shall 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

2.97 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 plane (Chapter 2)
- Workstations and privileged access (Chapter 3)
- Risk assessments (Chapter 10).

3. Protection of data and network functions

3.1 This chapter provides guidance for public telecoms 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 such technical means as are appropriate and proportionate —

(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 such technical means as are appropriate and proportionate—

(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) where, in the case of a public electronic communications network, the workstation is directly connected to the network, to signals that are incoming signals in relation to the network,

(ii) where, in the case of a public electronic communications service, the workstation is directly connected to the public electronic communications network by means of which the service is provided, to signals that are incoming signals in relation to that network, or

(iii) where, in either case, the workstation is operated remotely, to signals other than those that the workstation has to be capable of receiving in order to enable changes to security critical functions authorised by the network provider or service provider to be made,

(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 public telecoms providers to understand when implementing solutions, providing examples and background information where appropriate.

Guidance

3.4 When implementing a PAW-based lockdown, public telecoms 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 to both PAWs and management plane infrastructure within such a period as is proportionate with the risk of the threat the update addresses (see Table 2) 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[17] or secure system administration guidance[18] and for Windows devices at Microsoft's PAW guidance[19].

[17] *Device Security Guidance* (NCSC, 2021) https://www.ncsc.gov.uk/collection/device-security-guidance

[18] *Secure system administration: Gain trust in your management devices* (NCSC,2020) https://www.ncsc.gov.uk/collection/secure-system-administration/gain-trust-in-your-management-devices

[19] *Securing devices as part of the privileged access story* (Microsoft, 2021) https://docs.microsoft.com/en-us/security/compass/privileged-access-devices

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.[20]

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, public telecoms providers should consider implementing additional security controls to prevent and detect potential compromises. For example, when supporting remote PAWs, public telecoms 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.

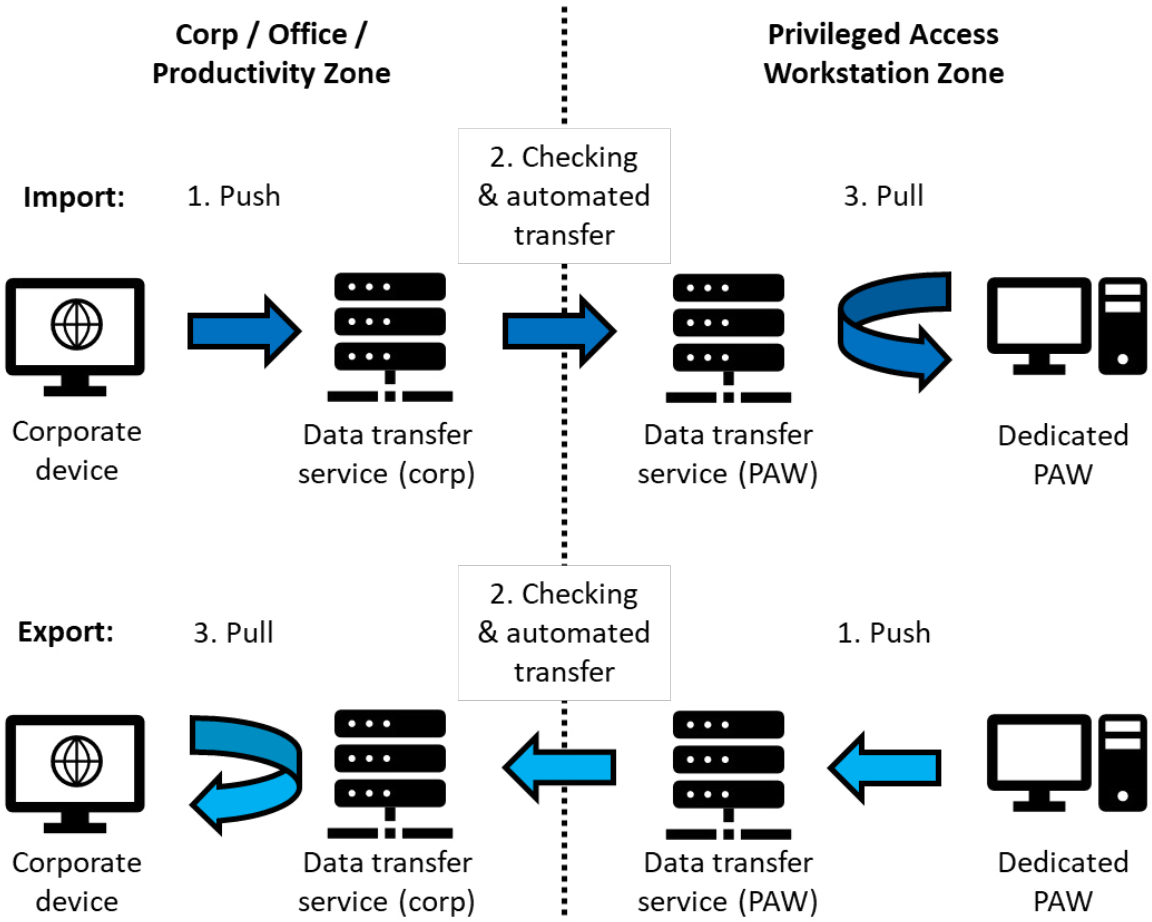
3.9 There are a range of solutions to providing access to corporate services to PAWs. One common solution is via the implementation of a virtualised environment existing within the corporate security zone (see Figure 2). PAWs connect into a virtual machine to access corporate services, rather than accessing 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. Public telecoms providers should not use unmanaged removable media for this task. Instead, public telecoms providers could consider using a push-pull mechanism to transfer data, as shown in Figure 8.

[20] *Device security guidance: Virtual Private Networks (VPNs)* (NCSC, 2021) https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks, and *Device security guidance: network architectures* (NCSC, 2020) https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/network-architectures

Figure 8: 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.[21]

SIM security

3.14 The intent of the SIM security 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 3.16-3.27 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.

[21] *Security principles for cross-domain solutions* (NCSC, 2021) https://www.ncsc.gov.uk/collection/cross-domain-solutions and *Pattern: safely importing data* (NCSC, 2018) https://www.ncsc.gov.uk/guidance/pattern-safely-importing-data

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 manufacturer's 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; and
- 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; and
- 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 it is adopted, any resilience risks to networks will need to be managed.

Guidance

3.22 Public telecoms providers should review existing SIM profiles that are in use. If vulnerabilities exist (in comparison with GSMA recommendations), public telecoms 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 encouraged to increase the overall security of the SIM population in the network.

3.23 Public telecoms 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, public telecoms 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, public telecoms 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 public telecoms provider shall only allow management (OTA) messages from permitted sources to reach SIM cards which are issued by the public telecoms provider and attached to the public telecoms provider's network.

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

3.27 Should providers be made aware of a compromise to customer SIMs, or the data within those SIMs, public telecoms providers shall inform the relevant customers as soon as is reasonably practicable.

Encryption

3.28 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

3.29 Public telecoms providers must ensure data is protected whether at-rest or in-transit. Where possible, public telecoms providers should protect this data through secure encryption. Where data is protected by other means, public telecoms providers should maintain a formal record of this, along with the means by which the data is protected.

3.30 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, public telecoms providers should consider the use of IPSec or TLS – detailed information and best practice guidance provided by NCSC can be found on its website.[22] 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.[23]

Customer Premises Equipment (CPE)

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

Scope

3.32 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 public telecoms provider. CPE provided to business customers is in scope alongside that provided to retail consumers.

Background

3.33 While public telecoms 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.

3.34 Additional protections to secure devices will be implemented through the Product Security and Telecommunications Infrastructure Bill.[24] 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

[22] *Using IPSec to protect data* (NCSC, 2016) https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data and *Using TLS to protect data* (NCSC, 2021) https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data

[23] *Guide to Storage Encryption Technologies for End User Devices* (NIST, 2007) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf

[24] Product Security and Telecommunications Infrastructure Bill https://bills.parliament.uk/bills/3069/publications

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:[25]

- ensuring that consumer connectable products do not use universal default passwords;
- implementing a means to manage reports of vulnerabilities; and
- providing transparency on how long, at a minimum, the product will receive security updates.

3.35 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.

3.36 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

3.37 Public telecoms 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, public telecoms providers shall ensure that the CPE has a secure default configuration, which should include limiting inbound connections by default. Public telecoms providers shall also ensure that the CPE will receive regular security updates throughout the device's lifetime.

3.38 Due to the possibility that exploitation of vulnerabilities in CPE devices could impact the provider's network at scale, or impact wider infrastructure, it is in the provider's interest to ensure that CPE remains in support and up to date. Acknowledging that providers are not responsible for customer behaviour, public telecoms providers shall take proactive measures that aim to ensure CPE devices are being kept up to date during the lifetime of the contract, such as by providing customers with CPE that will automatically update by default. Similarly, public telecoms providers shall take proactive measures that are likely to result in CPE devices being replaced once they go out-of-support.

3.39 Where the public telecoms provider performs on-going management of the CPE, they shall ensure that this is performed securely. In particular, the public telecoms 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

3.40 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 and the exposed edge (Chapter 2)
- Virtualisation fabric (Chapter 2)
- National resilience (Chapter 2).

[25] *Code of practice for consumer IoT security* (DCMS, 2018) https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

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) shall 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, or there is a reduction in existing risks associated with the countries listed in the Schedule, 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(b)(ii).

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);[26]

[26] *Building a Security Operations Centre (SOC)* (NCSC, 2022) https://www.ncsc.gov.uk/collection/building-a-security-operations-centre

- 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; and
- 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.

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 that may involve a risk of a security compromise occurring.
>
> (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 obtaining access,
>
> (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, and
>
> (f) to take measures to prevent activities that would restrict the monitoring and analysis required by this regulation.
>
> (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.[27]

Guidance

5.6 The following guidance in paragraphs 5.7-5.23 highlights the key aspects of monitoring and analysis for public telecoms providers to understand and implement, providing examples and further background information where appropriate.

Logging and monitoring

5.7 As a minimum, logging and monitoring should cover the following:

- who logged in (account or User ID);
- what they did (type of event/activity);
- when they logged in (date/time);
- where the login occurred (resource/source of the event such as location, IP address, terminal ID or other means of identification); and
- why the login occurred (a link to the specific ticket that necessitated the login).

It is just as important to log unsuccessful events as it is successful events. General guidance on what to log can be found on the NCSC website.[28]

Normal and anomalous activity

5.8 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.

5.9 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.

Network-based monitoring

5.10 Public telecoms 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.

5.11 What to monitor can only be defined by network providers themselves as they have the best knowledge of their networks. Public telecoms 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, public telecoms providers should consider factors such as:

- the criticality or sensitivity of interfaces and systems;
- the exposure of the systems or interfaces to attack;

---

[27] *NCSC CAF guidance: C.1 Security monitoring* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring

[28] *Introduction to logging for security purposes* (NCSC, 2018) https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes

- 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.

5.12 In determining where to monitor, public telecoms 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

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

5.14 Host-based monitoring may incorporate operating system, application, and virtual machine behaviour, including detailed information at the process level, especially where unexpected reboots/restarts have occurred as these event logs would help to investigate the cause. 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.

5.15 Public telecoms 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.[29]

Protection of monitoring data

5.16 Monitoring data provides information about network behaviour and can contain sensitive data such as administrative passwords. As such, public telecoms 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

5.17 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).

5.18 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

[29] *Device Security Guidance: Logging and protective monitoring* (NCSC, 2021) https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/logging-and-protective-monitoring

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).

5.19 Public telecoms 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.

5.20 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

5.21 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.

5.22 Analysts will need to be sufficiently skilled in understanding network and attacker behaviour. They will often benefit from access to threat intelligence feeds. When protecting large-scale networks, providers should have access to sufficient skilled analysts to support multiple investigations of anomalous behaviour at any one time.

5.23 General advice on proactive security monitoring can be found on the NCSC website.[30]

Border Gateway Protocol

5.24 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.[31]

Guidance

5.25 Public telecoms 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.

5.26 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 public telecoms 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.

5.27 To help ensure that routing information originating from the community is as accurate and secure as possible, public telecoms providers shall, at a minimum, implement the basic elements set out in Section 3.

---

[30] *NCSC CAF guidance: C.2 Proactive security event discovery* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-2-proactive-security-event-discovery

[31] *More details about the October 4 outage* (Meta, 2021) https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/

5.28 All address space and autonomous system (AS) resources allocated to a public telecoms provider should be correctly recorded in such a way that it is simple to identify and contact the 'owner' to assist in resolving issues. Contact details need to be current and accurate on all the Regional Internet Registries (e.g. RIPE) and other useful locations, such as PeeringDB. Note that all appropriate fields and record types should be secured appropriately, to prevent misuse.

5.29 Implementation of ingress and egress route filtering will help to ensure that only authorised and approved routes are used, and that IP address spoofing is prevented. Before accepting and onward advertising routes, transit providers should check on the relevant Regional Internet Registry (RIR) database(s). Other providers and/or AS 'owners' could also implement similar checks on RIR database(s) before accepting routes.

5.30 When implementing ingress and egress route filtering, service providers should pay special attention to:

- Special Use Addressing;
- BOGONs (although RFC 6441 should be considered);
- over-specific prefix lengths;
- their own prefixes;
- their own AS; and
- IXP LANs.

5.31 Accepting routes from unexpected sources could result in the provider propagating routing changes that have not come from the legitimate resource owner. One method to help address this is to limit where external BGP routing updates are accepted from.

5.32 Public telecoms providers should actively monitor BGP routing changes to detect and monitor incidents, including (but not limited to) hijacking and denial of service attacks. Tools such as BGP Spotlight are specifically designed for this purpose by NCSC, but other commercial and non-commercial tools are available.

5.33 Prefix origin validation by public telecoms providers using tools such as Resource Public Key Infrastructure (RPKI) will help to ensure that only valid BGP updates from the genuine owner of the address space will be acted on. If providers also aggregate routes where possible, this will minimise the number of routes advertised, minimising the number of route updates required.

5.34 In the event of a Global BGP failure, there will be a period of time when routers will be performing discovery and re-building their routing tables. This may take many hours. It is therefore incumbent on the UK service providers to ensure that they have in place a plan of maintaining UK internal traffic during this time. Route aggregation may help in speeding the return to normal. If RFC 3682 is implemented where it is available, it will help limit the possibility of resources on routers being overwhelmed. RFC 3682 provides a method of limiting the 'Time to Live' for BGP updates by implementing limits of valid BGP senders where the traffic is between routers that are next to each other, known as 'Peers'.

5.35 If routing equipment fails, there is the possibility of a route being withdrawn. Operators should advertise routes in such a way that this is unlikely to happen. One possible way to do this is by the use of static routes to non-physical, persistent interfaces.

5.36 Where it is available, TCP Authentication Option (TCP-AO) should be the preferred method of authentication. This will allow for stronger authentication algorithms and better, more agile, key management.

Threat hunting

5.37 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.

5.38 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 are also required, whether that be via existing skilled staff or appropriate training.

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

Regular scanning

5.40 Attackers are increasingly scanning networks to find exposed vulnerabilities. Public telecoms 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

5.41 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. The logs relating to security critical functions must be maintained for at least 13 months as this will ensure the retention of any changes made on a once-yearly basis, for example end of year processes.

5.42 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. Public telecoms providers should sanitise any customer data prior to storage.

Chapter Crossovers

5.43 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 public telecoms 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, takes appropriate measures for the purposes mentioned in section 105A(1) of the Act, in relation to goods, services or facilities supplied, provided or made available by the third party supplier to the primary provider, which are equivalent to the measures 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 the supply, provision or making available of goods, services or facilities by 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.[32]

Guidance

6.4 The intent of the security framework in this area is to ensure public telecoms providers fully understand and reduce supply chain risks. One of the key aims is to ensure that public telecoms 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 in terms of the specific goods, services or facilities it is supplying, providing or making available to the provider.

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

6.6 Public telecoms providers should also consider the support they may need from their suppliers should an incident or compromise occur, potentially via the supplier. As public telecoms 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 public telecoms 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, and the obligations set out in the regulations, 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, public telecoms 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 suppliers' systems may provide an attractive route to obtaining nationally significant datasets. In this context 'data' includes both user data and network data.

[32] *Supply chain security guidance* (NCSC, 2018) https://www.ncsc.gov.uk/collection/supply-chain-security

Guidance

6.9 Under normal governance practices, decisions relating to a dataset 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 public telecoms 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 public telecoms 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 public telecoms 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, including by using an encrypted and authenticated channel for data sharing.

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, public telecoms 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 Public telecoms 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. Public telecoms 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 data flows 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 Public telecoms 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.[33] 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.[34] 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 6.24-6.36 highlights the key areas that public telecoms providers need to understand when working with network equipment suppliers, providing examples and background information where appropriate.

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.

---

[33] *Government response to the call for views on supply chain cyber security* (DCMS, 2021) https://www.gov.uk/government/publications/government-response-on-supply-chain-cyber-security/government-response-to-the-call-for-views-on-supply-chain-cyber-security

[34] *Proposal for legislation to improve the UK's cyber resilience* (DCMS, 2022) https://www.gov.uk/government/consultations/proposal-for-legislation-to-improve-the-uks-cyber-resilience

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 faults, 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 public telecoms 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 (see Annex B). 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 shall 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. Any relevant updates that are made to the guidance in the VSA will be reflected in an updated Annex within future versions of the code of practice.

6.33 While public telecoms 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 encourage their suppliers to publish a response to the NCSC's VSA.

6.34 During procurement processes for security critical functions, public telecoms 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.

6.35 Where a third party supplier does, or omits, something which increases the risk of security compromise, the risk to the public telecoms provider will increase with the scale of deployment. Specifically, a high quantity of equipment or components in the network which share a supply chain risk increases the risk to the network. To limit the risk of security compromise, public telecoms providers shall consider whether the risk associated with the quantity of equipment or components is manageable given the supplier risk.

The 'Trojan horse' threat

6.36 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 public telecoms 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.

Interpretation of regulation 7(4)(a)(ii)

6.37 Where a network provider supplies its services to a different provider in a higher tier, it is expected that only the part of the network or service that is being supplied needs to meet the security standards of the provider in the higher tier. Where this is the case, providers also need to ensure that the relevant parts of the network or service are sufficiently segregated from the rest of their operations. This will avoid the risk of bringing the wider operations of the provider in a lower tier into the scope of regulation 7(4)(a)(ii) and having to hold more of their operations to the security standards of a higher tier.

Management of sites

6.38 Where public telecoms providers have network equipment and facilities within sites that are shared with other providers, it is recommended that all providers work together to set a consistent set of security measures that meet the regulations and that the site operator should follow.

Existing contracts and new contracts

6.39 In reference to the timeframes in Section 3, whether or not a contract with an existing supplier is 'new' should be defined in terms of whether the scope or scale of the contracted work changes. Therefore on this basis:

- a renewal of a contract to continue completing the same work would not be defined as new;
- software upgrades or service agreements that do not change the scope or scale of the work would not be defined as new (for example, a patch or general version of existing functionality would not be new);
- a renewal of a contract which resulted in a software upgrade that leads to a change in the quality of service or enables a new service to be delivered would be new;
- a renewal of a contract which resulted in the supply of updated, modified or new equipment hardware would be new;
- where there is a framework arrangement in place with individual statements of work under this agreement then a change in either the framework contract or the individual statements of work would be in scope of a new contract if they change the scope or scale of the work; and
- where an existing contract is amended to change the scope or scale of the work it would be new.

Chapter Crossovers

6.40 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)
- Keeping an offline copy (Chapter 8).

7. Prevention of unauthorised access or interference

7.1 This chapter provides guidance for public telecoms 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 reduce the risks of 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 the use of default credentials wherever possible, in particular by avoiding, as far as possible, the use of 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, and
>
> (g) to carry out changes to security critical functions through automated functions where possible.
>
> (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 such measures as are appropriate and proportionate 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 such measures as are appropriate and proportionate, including the avoidance of common credential creation processes, to ensure 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 public telecoms 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

Information necessary 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' networks and services are resilient to security compromises, such that the impacts to end-users are kept to a minimum. This should be fulfilled 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.[35] Without a trusted identity, ransomware should not be able to request access to a provider's 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.

[35] *Cloud security guidance – Principle 10: Identity and authentication* (NCSC, 2018) https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles/principle-10-identity-and-authentication

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.[36]

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.

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).

[36] *NCSC CAF guidance: D.1 Response and recovery planning* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-1-response-and-recovery-planning

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 and proportionate 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 and proportionate 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 9.5-9.9 highlights the key business processes for public telecoms providers to understand and implement, providing examples and background information where appropriate.

Top-to-bottom security governance

9.5 For a public telecoms 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 public telecoms 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. Public telecoms providers should refer to NCSC advice on security governance and security policies.[37]

9.6 Regulation 10(2)(d) requires public telecoms 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 public telecoms 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. So far as is appropriate and proportionate, 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.[38]

The Cyber Assessment Framework (CAF)

9.9 The relevant parts of the CAF that providers shall have regard to in order to ensure that they have appropriate business processes in place are contained within Annex C of this code of practice. Any relevant updates that are made to the guidance in the CAF will be reflected in an updated annex within future versions of the code of practice. Should any differences arise between the interpretation of the CAF measures in Annex C, and the guidance in the main body of the code of practice, the code shall take precedence.

Chapter Crossovers

9.10 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: A.1 Governance* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a1-governance and *NCSC CAF guidance: B.1 Service protection policies and processes* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-1-service-protection-policies-and-processes

[38] *NCSC CAF guidance: D.2 Lessons learned* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/d-2-lessons-learned

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, risks identified under regulation 3(3)(a),
>
> (ii) risks identified under regulation 5(2),
>
> (iii) risks identified under regulation 6(1),
>
> (iv) risks identified under regulation 7(1),
>
> (v) risks identified under regulation 10(4),
>
> (vi) the results of reviews carried out in accordance with sub-paragraph (a),
>
> (vii) the results of tests carried out in accordance with regulation 14, and
>
> (viii) any other relevant information.

Key concepts for understanding the requirements

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

10.3 In undertaking their annual reviews under Regulation 11(b), public telecoms providers must take into account the risks and results listed in Regulation 11(b)(i)-(viii) and "any other relevant information" (Regulation 11(b)(viii)). 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 Public telecoms providers should refer to the NCSC advice on risk management.[39] The risk assessment that these 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.

[39] *NCSC CAF guidance: A.2 Risk management* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/a2-risk-management

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).

11. Patching and updates

11.1 This chapter provides guidance for public telecoms 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 such measures as are appropriate and proportionate 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 for network equipment

11.3 Regulation 12(a) requires providers to take appropriate and proportionate measures to deploy any relevant patch or mitigation that 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". Table 2 contains guidance on which time periods for patching network equipment are appropriate in different situations, based on how critical the vulnerabilities are and whether they are internally or externally exposed interfaces. These timeframes are intended to ensure that patches are deployed in a way that is proportionate with the risk that the patch addresses. They also seek to counter the risks posed by threat actors who regularly target vulnerabilities soon after patches are made available, often by using easy, cheap and commercially available tools. Providers should act swiftly to close these vulnerabilities and in all cases should look to implement patches for network equipment as soon as is practicable and no later than the timeframes in Table 2.

Table 2: Criticality and exposure-adjusted maximum timeframes for application of patches (from supplier release date)

	Actively exploited in the wild	Critical vulnerability CVSS 9.0 – 10	High vulnerability CVSS 7.0 – 8.9	Other
Externally exposed interface	14 days	14 days	30 days	90 days
Internally exposed interface	14 days	30 days	90 days	As part of normal patching cycle

Guidance

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

11.5 Where relevant patches justifiably need more time than 14 days to be deployed (as outlined in Table 2), Regulation 12(c) 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).

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 for in-house staff 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 public telecoms provider is using a third party supplier, in-house staff of that provider need to be competent and able to take appropriate steps to identify and resolve security issues. This is to avoid public telecoms 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 Public telecom 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.[40]

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).

[40] *NCSC CAF guidance: B.6 Staff awareness and training* (NCSC, 2019) https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-6-staff-awareness-and-training

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 identifying 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 the risks of security compromises occurring 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 the persons mentioned in sub-paragraph (a) 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, the following criteria should be in place:

- testers or red teams should not be unnecessarily constrained;
- defensive teams should not be tipped-off in advance;
- monitoring teams should not know the testing is happening (to test their capabilities);
- defensive mechanisms should not be modified based on testers' plans;
- testing should be done by sufficiently skilled persons who are fully independent from the team that built and maintain the system under test, and should not be used for routine testing (and compliance); and
- scope, tests and results are transparent to Ofcom.

13.5 An example of this type of testing is Ofcom's TBEST scheme.[41]

[41] *Our network security and network resilience work* (Ofcom, 2021) https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work

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 that provide services into the UK meet best-practice standards. Advice produced by the Centre for the Protection of National Infrastructure (CPNI) should be consulted for physical and personnel-related security.[42]

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).

[42] *Physical security* (CPNI) https://www.cpni.gov.uk/physical-security

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—
>
> (a) be used or disclosed by the recipient otherwise than for the purpose 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, or
>
> (b) be retained by the recipient any longer than is necessary for that purpose.
>
> (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 providers to receive information from other providers that would help to reduce the risk of security compromises occurring (Regulation 15(1)). Whilst not required by regulation 15, providers may also consider whether it is 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, as envisaged by the regulations, 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:

- 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. Each individual guidance measure is also mapped to the relevant security requirements in the regulations, including regulations which may be indirectly linked to the guidance measure (for example, failing to block certain signals might suggest that the network has not been appropriately monitored).

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 is therefore only indicative and non-exhaustive.

The following measures should be completed by 31 March 2024 (Tier 1 providers) or by 31 March 2025 (Tier 2 providers).

Measure number	Description	Relevant Regulation(s)
Overarching security measures		
M1.01	Providers[43] 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)
M1.02	Security testing on externally-facing systems, excluding CPE, 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) 8(3) 14
M1.03	Equipment in the exposed edge shall not host sensitive data or security critical functions.	3(3)(a),(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b)
M1.04	Physical and logical separation shall be implemented between the exposed edge and security critical functions. Note that this measure may not be necessary once datasets and functions can be cryptographically-protected from compromise.	3(3)(c),(d),(e) 3(5) 4(4)(b)
M1.05	Security boundaries shall exist between the exposed edge and critical or sensitive functions that implement protective measures.	3(3)(c),(d) 3(5) 4(4)(b)

[43] References to 'providers' in Section 3 of the code are in reference to large ('Tier 1') and medium-sized ('Tier 2') providers of PECN or PECS, as outlined in paragraphs 0.12 and 0.13 of Section 1.

Measure number	Description	Relevant Regulation(s)
M1.06	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		
M2.01	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)
M2.02	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)
M2.03	Privileged access shall be via secure, encrypted and authenticated protocols whenever technically viable.	4(4) 8(4) 8(5)(e)
M2.04	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)
M2.05	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)
M2.06	The infrastructure used to support a provider's network shall be the responsibility of the provider, or another entity that adheres to the regulations, measures and oversight as they apply to the provider (such as a third party supplier with whom the provider has a contractual relationship). Where the provider or other entity adhering to the regulations has responsibility, this responsibility shall include retaining oversight of the management of that infrastructure (including sight of management activities, personnel granted management access, and management processes).	3(3)(d) 3(3)(f)(i),(ii),(iii) 3(5) 6(3)(d) 7(4)(a) 8(1) 8(6)
Signalling plane 1		
M3.01	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)
M3.02	Providers shall have an appropriate understanding of 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)

Measure number	Description	Relevant Regulation(s)
M3.03	Providers shall have an appropriate understanding of 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)
M3.04	Providers shall understand who they directly connect with over the signalling network and operate on the principle that incoming signals are from untrusted networks.	3(3)(a),(b) 6(1) 6(2)(a) 6(4) 7(1) 7(4)(a)(i),(ii),(iii)
M3.05	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)
M3.06	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 shall not be allowed by default.	3(3)(e) 4(4)(b),(c) 6(3)(d)
M3.07	Where the signalling message is protected by end-to-end authentication, risk decisions and associated security controls may be determined based upon the authenticated source.	3(3)(e) 4(4)(b) 6(3)(d)
M3.08	Where providers allow others to use number 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)
M3.09	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)
M3.10	Networks shall only send outgoing signalling in support of services permitted by the recipient. Guidance on what the GSMA has defined as permitted services is set out within Section 5 of GSMA's charging and accounting principles[44] and Section 10 of GSMA's interconnection and interworking charging principles[45].	4(4)(b) 6(1) 6(2)(a),(b)
M3.11	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)
M3.12	Any BGP misuse that impacts a provider's 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)

[44] *GSMA PRD BA27, Charging and Accounting Principles – Section 5*

[45] *GSMA IN.27, Interconnection and Interworking Charging Principles – Section 10*

Measure number	Description	Relevant Regulation(s)
M3.13	Providers shall ensure that contact details are current and accurate on all the Regional Internet Registries (e.g. RIPE) and should endeavour to keep other data sources accurate.	3(3)(e) 4(1)(a),(b) 4(2)(a),(b) 8(1)
M3.14	All address space and autonomous system number (ASN) resources allocated to a service provider shall be correctly recorded in such a way that it is simple to identify and contact the 'owner' to assist in resolving issues.	3(3)(e) 4(1)(a),(b) 4(2)(a),(b) 15(5)
M3.15	Providers shall implement ingress and egress route filtering.	3(3)(e) 4(2)(a),(b) 4(4)(b) 6(1) 6(2)(a) 8(1)
M3.16	Providers shall adopt and implement mechanisms that prevent IP address spoofing.	3(3)(e) 4(2)(a),(b) 4(4)(b) 6(1) 6(2)(a) 8(1)
M3.17	The provider shall share such details, as are appropriate and proportionate, of any BGP misuse with other providers where it may cause a connected security compromise.	6(3)(d) 15(1) 15(2) 15(3) 15(4)
M3.18	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)
M3.19	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

M4.01	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)

Measure number	Description	Relevant Regulation(s)
M4.02	During procurement of equipment, prior to contract award, it is recommended that providers should, as a minimum, use the guidance contained in NCSC's vendor security assessment to assess third party suppliers (as contained in Annex B).	3(3)(a),(b),(d),(e) 3(5) 7(1) 7(4)(a)(i) 10(1) 10(2)(a),(b) 10(4) 13(2)(d)(i),(ii) 14(1)
M4.03	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
M4.04	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) 7(5) 11
M4.05	The provider shall record all risk management processes undertaken. Guidance on risk management processes can be found on the NCSC website.[46]	3(1) 7(1) 7(4)(c) 7(5) 11
M4.06	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)
M4.07	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
M4.08	Providers shall phase out the use of SIMs that present an unmitigatable security risk, such as the use of deprecated security algorithms.	4(6)(b)

[46] *Risk management guidance* (NCSC, 2018) https://www.ncsc.gov.uk/collection/risk-management-collection

Measure number	Description	Relevant Regulation(s)
Supporting business processes		
M5.01	The provider shall implement appropriate business processes. In order to achieve this, providers shall have regard to implementing the parts of the CAF that define the provider's business processes. These are contained within Annex C. 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.	10(2) (a),(b),(c),(d),(e), (f) 10(4)
M5.02	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(5)(a),(b) 10(2) (a),(b),(c),(d),(e) 12(a)(b)(c) 13(1)(a)(b) 13(2)(a),(b)
M5.03	Providers shall maintain read-only backups of their infrastructure and information and shall be able to restore them. The backups should contain the information necessary to maintain the normal operation of the public electronic communications network or public electronic communications service.	3(3)(d) 4(1) 4(2) 4(4)(b) 7(1) 7(5)(a),(b) 8(5)(d) 9(2)(a),(b) 9(2)(c)(vii)
M5.04	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(1) 7(5)(a),(b) 9(2)(c)(iv) 10(2)(a),(b),(c),(d) 13(2)(a),(b)
M5.05	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(1) 7(5)(a),(b) (9)(2)(c)(i) 10(2)

Measure number	Description	Relevant Regulation(s)
M5.06	For significant incidents, providers shall share the high-level lessons learned with other providers, so far as is appropriate and proportionate.	15(1),(2),(3),(4)
M5.07	Lessons learned from previous security incidents shall be used to inform the security of new products and services.	3(3)(a),(b) 3(4) 10(2)(a),(b) 10(2)(e) 13(2)(a),(b),(c),(d)

The following measures should be completed by 31 March 2025.		
Measure number	**Description**	**Relevant Regulation(s)**
Management plane 2		
M6.01	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)
M6.02	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),(c)
M6.03	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)
M6.04	All break-glass privileged user accounts must have unique, strong credentials per individual piece of network equipment.	3(1)(a),(b),(c) 8(2)(b) 8(5)(a),(b),(c) 9(2)(c)(vi)
M6.05	Default and hardcoded accounts shall be disabled.	8(2)(d),(e) 8(4) 8(5)(b),(c)
Signalling plane 2		
M7.01	Any incoming or outgoing message type that should not be sent over international or external signalling networks shall be blocked at the logical edge of the provider's network. For example, GSMA CAT 1 messages[47] shall be blocked for SS7 networks, and equivalent messages shall be blocked for other signalling protocols such as Diameter,[48] GTP,[49] Interconnect[50] and SS7/SIGTRAN[51].	3(3)(e) 3(3)(f)(i) 4(4)(b) 6(1) 6(3)(d) 8(3) 8(6)

[47] *FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines* (GSMA, 2019) https://www.gsma.com/security/resources/fs-11-ss7-interconnect-security-monitoring-and-firewall-guidelines-v6-0/

[48] *FS.19 DIAMETER Interconnect Security* (GSMA, 2019) https://www.gsma.com/security/resources/fs-19-diameter-interconnect-security-v7-0/

[49] *FS.20 GPRS Tunnelling Protocol (GTP) Security* (GSMA, 2019) https://www.gsma.com/security/resources/fs-20-gprs-tunnelling-protocol-gtp-security-v3-0/

[50] *FS.21 Interconnect Signalling Security Recommendations* (GSMA, 2019) https://www.gsma.com/security/resources/fs-21-interconnect-signalling-security-recommendations-v6-0/

[51] *FS.07 SS7 and SIGTRAN Network Security* (GSMA, 2017) https://www.gsma.com/security/resources/fs-07-ss7-and-sigtran-network-security-v4-0/

Measure number	Description	Relevant Regulation(s)
M7.02	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)
M7.03	Providers shall have in place the means for recipients of their BGP routing updates to validate that the BGP routing update originated from the legitimate owner.	3(3)(e) 4(2)b 4(4)(b) 6(1) 6(2)(a) 8(1)
M7.04	Where the necessary information is available, providers shall validate that any BGP route updates they receive have originated from the legitimate owner.	3(3)(e) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 6(1) 6(2)(a) 8(1)

Third party supplier measures 2

M8.01	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(4)(a)(i) 10(1) 10(2)(a),(b) 10(4) 13(2)(d)(i),(ii) 14(1)
M8.02	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(4)(a)(i) 13(2)(d)(i),(ii) 14(1) 14(2)
M8.03	Any third party testing in relation to the security of the network equipment 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(4)(a)(i) 12 13(2)(d)(i),(ii) 14(1) 14(2) 14(3)

Measure number	Description	Relevant Regulation(s)
M8.04	Providers shall ensure that security considerations are a significant factor in determining the procurement outcome for security critical functions, 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(1) 7(4)(a)(i)
M8.05	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) 7(1) 7(5) 11(b)(i),(iii),(v),(vii) 13(2)(d)(i),(ii)
M8.06	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)
M8.07	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)
M8.08	Providers shall prioritise critical security patches over functionality upgrades wherever possible.	7(4)(c) 7(5) 12
M8.09	When assessing the risk due to SIM card suppliers, including during procurement, providers' risk assessment shall include the risk due to the loss of sensitive SIM card data.	3(3)(a),(e) 4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a) 8(6) 11
M8.10	When transferring the provider's SIM key material from SIM card vendors, transport keys shall not be shared across multiple SIM vendors. Where possible, a range of transport keys shall be used with each SIM card vendor.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a) 8(6)
M8.11	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)
M8.12	For fixed-profile SIM cards, the provider shall ensure that sensitive SIM data is appropriately protected throughout its lifecycle, by both the SIM card vendor 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)

Measure number	Description	Relevant Regulation(s)
M8.13	For fixed-profile SIM cards, the confidentiality, integrity and availability of the sensitive SIM card data shared with the SIM card vendor shall be protected at every stage of their lifecycle.	4(6) 7(1) 7(4)(a)(i) 7(4)(b) 8(5)(a)
M8.14	For fixed-profile SIM cards, providers shall ensure that the security of the SIM card vendor has been independently audited. For example, using the GSMA's SAS scheme provides a means to accredit the security of SAS suppliers.[52]	4(6) 7(1)
M8.15	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 vendor. 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 vendor.	4(6)(a),(b)
M8.16	When under the provider's control, the provider shall ensure that the SIM card can only be modified by specifically allowed servers (for example, determined by IP address and certificate stored on the SIM card).	4(6)(a),(b)
Customer premises equipment		
M9.01	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)
M9.02	The provider shall ensure that all CPE provided to customers are still supported by the network equipment supplier. For any provider-provided CPE that go out of third party supplier support, customers shall be informed prior to, and once the equipment goes out of support, and proactively offered a replacement as soon as reasonably practicable. This shall apply only whilst the provider provides the associated service.	4(4)(c) 12
M9.03	WAN CPE management interfaces shall only be accessible from specified management locations (e.g. URL or IP address).	3(3)(a) 4(4)(c)
M9.04	Management of the CPE shall use a secure protocol (e.g. TLS 1.2 or newer).	3(3)(a) 4(4)(c)
M9.05	By default, the CPE's customer-facing management interfaces shall only be accessible from within the customer's network.	3(3)(a) 4(4)(c)
M9.06	By default, all unsolicited incoming connections towards the customer's network shall be blocked by the CPE.	3(3)(a) 4(4)(b),(c) 9(2)(c)(iii)

[52] *Security accreditation scheme* (SAS) (GSMA, 2021) https://www.gsma.com/security/security-accreditation-scheme/

The following measures should be implemented on all new contracts after 31 March 2024 (Tier 1 providers) or 31 March 2025 (Tier 2 providers), and on all contracts by 31 March 2027 (all providers).

Measure number	Description	Relevant Regulation(s)
Third party supplier measures 3		
M10.01	The provider shall maintain records of third party suppliers' 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)
M10.02	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)
M10.03	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)
M10.04	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)
M10.05	Providers shall retain control and oversight of their network and user data.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(iii) 7(4)(b)
M10.06	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
M10.07	When making network or user data available to third party suppliers outside of a secure privileged access system, the provider's environment that is used to hold and make the network and user data available to the third party shall be secure and segregated from the provider's wider 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)
M10.08	Providers shall avoid transferring control of their network and user data to third parties, except where necessary. Any such transfer of control should be limited to the necessary and defined purpose. Where a data 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

Measure number	Description	Relevant Regulation(s)
M10.09	Where network or user data leaves a provider's control, the provider shall contractually require and verify that the data is properly 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)
M10.10	When sharing user or network data, providers and suppliers shall use 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
M10.11	Providers shall contractually oblige third party suppliers to notify the provider within 48 hours 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
M10.12	Providers shall contractually require third party suppliers to support the provider in investigations of incidents that 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
M10.13	Providers shall contractually require the third party suppliers to find and report on the root cause of any security incident that could result in a security compromise in the UK within 30 days, and rectify any security failings found.	7(4)(a)(iv) 9(1) 9(2)(c) (i),(ii),(iv),(v),(vi) 9(4) 9(5) 15
M10.14	Where third party suppliers cannot quickly resolve security failings, 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
M10.15	Where third party suppliers do not resolve security failings 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)
M10.16	Providers shall contractually require third party suppliers to support, as far as appropriate, 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)
M10.17	Providers shall flow down appropriate 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)

Measure number	Description	Relevant Regulation(s)
M10.18	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)
M10.19	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)
M10.20	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)
M10.21	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)
M10.22	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)
M10.23	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)
M10.24	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.	4(1) 4(2) 7(1) 7(4)(a)(i),(ii) 7(4)(b) 9(2)(c)(iii),(v)
M10.25	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)

Measure number	Description	Relevant Regulation(s)
M10.26	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)
M10.27	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)
M10.28	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)
M10.29	Providers shall contractually require that third party administrators implement logically-independent privileged access workstations per provider.	4(4)(a) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
M10.30	Providers shall contractually require that third party administrators implement independent administrative domains and accounts per provider.	7(1) 7(4)(a)(i),(ii)
M10.31	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)
M10.32	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)
M10.33	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)
M10.34	The provider shall contractually require from the third party administrator all logs relating to the security of the 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) 7(4)(a)(iii),(iv) 8(5)(d)(i),(ii) 9(1) 9(2)(c)(iv),(v)

Measure number	Description	Relevant Regulation(s)
M10.35	Providers shall require that networks of the third party administrator 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)
M10.36	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. It is recommended that any such declaration should cover all aspects described within the Vendor Security Assessment (VSA) (see Annex B), and providers should encourage their suppliers to publish a response to the VSA.	3(3)(a),(b),(e) 7(4)(a)(i),(iii),(iv) 7(4)(b)
M10.37	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)
M10.38	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)
M10.39	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)
M10.40	Providers shall contractually require network equipment suppliers 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)
M10.41	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)
M10.42	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)

Measure number	Description	Relevant Regulation(s)
M10.43	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)
M10.44	Where relevant to a provider's particular usage of equipment, providers shall contractually require third party suppliers to remediate all security issues that pose a security risk to a provider's network or service 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)
M10.45	Providers shall record where third party suppliers fail to meet these security obligations.	7(4)(iii),(iv)
M10.46	Providers shall ensure that their contracts allow details of security issues to be shared as appropriate to support the identification and reduction of 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.	7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c)
M10.47	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)
M10.48	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)
M10.49	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)
M10.50	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)
M10.51	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

Measure number	Description	Relevant Regulation(s)
M10.52	Providers shall deploy all security related patches and patches with a security element in a way that is proportionate to the risk of security compromise that the patch is intended to address (see Table 2). Should this not be possible, patches shall be deployed as soon as practicable and effective alternative mitigations put in place until the relevant patch has been deployed. Where a patch addresses an exposed, actively-exploited vulnerability, providers shall ensure that such patches are deployed as soon as can reasonably be achieved, and at most within 14 days of release.	7(4)(c) 7(5) 12
M10.53	Providers shall ensure that network equipment continues to meet the requirements in M8.04, M8.05, M8.06, M10.48 and M10.49 throughout its lifecycle including after an upgrade or patch.	7(4)(c) 7(5) 12
M10.54	The provider shall verify that their third party network equipment suppliers have 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

The following measures should be completed by 31 March 2027.		
Measure number	**Description**	**Relevant Regulation(s)**
Management plane 3		
M11.01	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)
M11.02	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)
M11.03	Central storage for persistent credentials shall be protected by hardware means. For example, on a physical host the drive could be encrypted with the use of a TPM. Where a virtual machine (VM) is used to provide a central storage service, that VM and the data included in it shall also be encrypted, use secure boot and be configured to ensure that it can only be booted within an appropriate environment. This is to ensure that data cannot be removed from the operational environment and accessed.	3(3)(a),(b),(d) 3(5) 6(2) 6(3)(b),(d) 8(1) 8(2)(f) 8(5)(a)
M11.04	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)
M11.05	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)
M11.06	While open, tickets shall be updated daily as a record of why privileged access granted to a user remains required, and shall be closed once privileged access is no longer required.	8(4) 8(5)(a),(e)
M11.07	Privileged access shall be automatically revoked once the ticket is closed.	8(4) 8(5)(a),(b),(e)
M11.08	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)
M11.09	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)

Measure number	Description	Relevant Regulation(s)
M11.10	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(3)(a),(b),(c) 3(5) 6(3)(a) 8(1) 8(3) 9(1) 9(2)(c) 11(a)
M11.11	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(5) 8(4) 8(5)(b),(d) 9(2)(c)(v)
M11.12	Break-glass privileged user account credentials should be single-use and changed after use.	3(1)(a),(b),(c) 8(5)(a),(b),(c) 9(2)(c)(v)
M11.13	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)
M11.14	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)
M11.15	Privileged access to network equipment shall be via a centralised element manager or equivalent configuration 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)
M11.16	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)
M11.17	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 M11.23.	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(4) 8(5)(a),(e)

Measure number	Description	Relevant Regulation(s)
M11.18	The management plane shall be configured to ensure that only necessary connections are allowed. Specifically, element managers and other administrative functions shall only be able to communicate with the network equipment that they administer. Further, network equipment shall only be able to communicate with its administrative functions and its ability to establish a connection with these functions shall be limited.	3(3)(d) 3(5) 6(3)(d) 8(4) 8(5)(e)
M11.19	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)
M11.20	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)
M11.21	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)
M11.22	The provider's 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)
M11.23	The management plane shall be segregated in such a way that a disruption to a segment shall not affect the entirety of the provider's UK network.	3(3)(d) 3(5) 8(1)
M11.24	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)
M11.25	The PAW shall only have access to internal-only business systems (e.g. not corporate email).	3(3)(c) 4(4)(a)
M11.26	A PAW shall support secure boot, boot-attestation, data-at-rest encryption backed by a hardware root-of-trust.	4(1) 9(1)
M11.27	A PAW shall be kept patched and up-to-date with a supported OS throughout its lifetime.	12

Measure number	Description	Relevant Regulation(s)
M11.28	Security critical patches shall be applied to PAWs within 14 days.[53] Should this not be possible, patches shall be deployed to PAWs as soon as practicable and robust alternative mitigations put in place until the relevant patch has been deployed.	12
M11.29	A PAW shall prevent the execution of unauthorised code such as binaries or macros within documents.	3(3)(c) 4(1)
M11.30	A PAW shall use data-at-rest encryption.	4(1) 4(2)
M11.31	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)
M11.32	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)
M11.33	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(3)(b) 8(4) 10(2)(d),(f) 11(b)
M11.34	Security protocols and algorithms shall not be proprietary whenever technically viable.	8(4)
M11.35	Each network equipment shall have strong, unique credentials for every account.	8(2)(b),(d) 8(4) 8(5)(b),(c)
Signalling plane 3		
M12.01	Incoming and outgoing signalling traffic shall be monitored.	4(4)(b) 5(3) 6(1) 6(2)(a),(b) 6(3)(a),(d)
M12.02	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)
M12.03	Security analysis shall be performed on signalling traffic to find and address anomalous signalling and malicious signalling.	4(4)(b) 6(1) 6(2)(a),(b) 6(3)(a),(d),(f) 8(1)

[53] Unlike the patching of network equipment, patching of PAWs is a standard enterprise function which does not require additional time as described in Table 2.

Measure number	Description	Relevant Regulation(s)
M12.04	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
M12.05	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 that this measure applies to, including existing equipment). The provider shall test that the live configuration prevents malformed, inconsistent, unexpected, or abnormally high volumes of signalling messages from disrupting security critical functions.	3(3)(a)(iv) 3(3)(c),(d),(e) 3(3)(f)(i),(ii) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b),(c) 6(1) 14(1) 14(2)
Virtualisation 1		
M13.01	The virtualisation fabric shall be robustly locked-down, shall use the latest patch for the software version and shall be in support.[54]	3(1)(a),(b),(c) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 12(a),(b),(c)
M13.02	It shall be possible to update the virtualisation fabric without negatively impacting the network functionality.	3(1)(a),(b),(c) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 12(a),(b),(c)
M13.03	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 or to support the virtualisation function. 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(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 6(1) 6(2)(a),(b) 8(1)

[54] This measure to keep the virtualisation fabric up-to-date is in addition to the measures to apply security critical patches within appropriate timeframes as defined in Table 2.

Measure number	Description	Relevant Regulation(s)
M13.04	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(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 8(1) 12(a)
M13.05	Modification of databases and systems that define the operation of the network shall require sign off by two authorised persons.	3(1)(a),(b),(c) 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)
M13.06	As part of the virtualisation fabric, physically separate ports shall be used to segregate internal interface and external interface network traffic.	3(1)(a),(b),(c) 3(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 12(a),(b),(c)
M13.07	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(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b)
M13.08	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(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b)
M13.09	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(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b) 4(5) 7(4)(b) 8(1)
M13.10	Where there is risk of exposure during transmission, the virtualisation fabric shall be configured to securely encrypt data in transit. Examples and guidance on the use of encryption can be found on the NCSC website.[55]	3(1)(a),(b),(c) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b) 4(5)

[55] *Using TLS to protect data* (NCSC, 2021) https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data

Measure number	Description	Relevant Regulation(s)
M13.11	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(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 8(1)
M13.12	Virtual workloads shall be authorised, tagged with a specific trust domain, and signed prior to use. The specific trust domain shall be based on the risks associated with the workload.	3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 8(1)
M13.13	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(3)(d) 4(1)(a),(b) 4(2)(a),(b)
M13.14	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. The virtualisation fabric shall verify that the virtual workload is signed and complies with policy prior to use, including that the virtual workload's trust domain is permitted to execute within the host's pool.	3(1)(a),(b),(c) 3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(c)
M13.15	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(3)(d) 3(3)(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(c) 6(1) 6(3)(b)
M13.16	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(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b)
M13.17	Containerised hosts shall only support a single trust domain.	3(1)(a),(b),(c) 3(3)(d) 3(5) 4(1)(a),(b) 4(2)(a),(b)
M13.18	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)
M13.19	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)

Measure number	Description	Relevant Regulation(s)
M13.20	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)
M13.21	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)
M13.22	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)
M13.23	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)
M13.24	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)
M13.25	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)
M13.26	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)
M13.27	Network oversight functions shall not share trust domains or host pools with workloads that are not network oversight functions.	3(3)(d) 3(5)

Measure number	Description	Relevant Regulation(s)
M13.28	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 4		
M14.01	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)
M14.02	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		
M15.01	Network oversight functions shall be robustly locked-down, in support and patched within such period as is proportionate to the risk of security compromise that the patch is intended to address (see Table 2). Should this not be possible, patches shall be deployed on network oversight functions as soon as practicable and robust alternative mitigations put in place until the relevant patch has been deployed.	3(3)(a),(d),(e) 3(5) 4(1)(b) 4(2)(b) 8(3) 12
M15.02	Any service that supports or contains 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
M15.03	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
M15.04	Network oversight functions shall run on trusted platforms.	3(3)(a),(d),(e) 4(1)(b) 4(2)(b) 8(3) 12
M15.05	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)

Measure number	Description	Relevant Regulation(s)
M15.06	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)
M15.07	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)
M15.08	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)
M15.09	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)
M15.10	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)

Measure number	Description	Relevant Regulation(s)
M15.11	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)
M15.12	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)
M15.13	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

M16.01	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)
M16.02	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)(viii) 14(1)
M16.03	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)
M16.04	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)

Measure number	Description	Relevant Regulation(s)
M16.05	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)
M16.06	Providers shall monitor physical and logical interfaces between networks that operate at different trust levels, as well as 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)
M16.07	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)
M16.08	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)
M16.09	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)
M16.10	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)
M16.11	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)

Measure number	Description	Relevant Regulation(s)
M16.12	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)
M16.13	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)
M16.14	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)
M16.15	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 provider's 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)
M16.16	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)
M16.17	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)
M16.18	Logs shall be processed and analysed in near real-time (in any case within five 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)

Measure number	Description	Relevant Regulation(s)
M16.19	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)
M16.20	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)
M16.21	Indications of potential anomalous activity, and potential malicious 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)
M16.22	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 2028.		
Measure number	**Description**	**Relevant Regulation(s)**
Management plane 4		
M17.01	Administrators should not need privileged access to network equipment to make administrative changes. Administrators should instead have privileged access to administrative systems (e.g. OSS) which make the necessary changes on the administrator's behalf. Administrative systems should group administrative changes to automate administrative processes and minimise administrator input and risk. When an administrator uses a privileged access into a security critical function, which is not an administrative system, this shall create a security alert.	3(5) 6(2) 6(3)(c),(d) 8(1) 8(2)(g)
Signalling plane 4		
M18.01	The provider shall ensure that their critical, core and signalling security systems are highly resilient to signalling attacks. Signalling messages shall be validated at the logical edge of the network prior to being forwarded to critical or core nodes. Messages that are not encoded in a normal manner, or that are unrelated to a normal operation or call flow in the network, shall be blocked. All exceptions to this shall be understood, justified, and documented.	3(3)(a)(iv) 3(3)(c),(d),(e) 3(4) 4(1)(b) 4(2)(b) 4(4)(b) 8(3)
M18.02	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)
M18.03	With the exception of SS7 and GTP-C, 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)
M18.04	Outgoing signalling shall be authenticated where this is supported by international standards.	4(4)(b) 6(1) 6(2)(a),(b)
M18.05	Customer data and customer identifiers shall be obfuscated before being released over an external signalling network, except where it is functionally essential to provide this information.	4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 4(5) 6(1) 6(2)(a) 8(1) 8(5)(a)

Measure number	Description	Relevant Regulation(s)
M18.06	In protocols other than SS7 and GTP-C, signalling network topology information shall be obfuscated before being released over an external signalling network, except where it is functionally essential to provide this information.	4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 4(5) 6(1) 6(2)(a) 8(1) 8(2)(f) 8(5)(a)

Virtualisation 2

M19.01	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(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 8(5)(a) 12(a),(b),(c)
M19.02	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(3)(d),(e) 3(5) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 8(3) 8(4) 12
M19.03	Where the virtualisation fabric allows virtual functions to have direct access to the physical hardware (cut-throughs), it shall not be treated as a security boundary.	3(1)(a),(b),(c) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b)
M19.04	Where possible, the virtualisation fabric shall be built and updated through an automated and verifiable process.	3(3)(d),(e) 8(2)(g) 12
M19.05	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)
M19.06	Where possible, administration of the virtualisation fabric shall be automated during normal operation.	8(2)(g)
M19.07	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)

Measure number	Description	Relevant Regulation(s)
Monitoring and analysis 2		
M20.01	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		
M21.01	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 2022.	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)
M21.02	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)(i)
M21.03	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)
M21.04	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) 3(3)(f)(i),(ii),(iii) 5(2) 11
M21.05	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) 3(3)(f)(i),(ii),(iii) 5(3) 10(2)
M21.06	If it should become necessary to do so, the provider shall have the ability to maintain (as relevant, where it provides such a form of connectivity prior to the event) the following UK network connectivity for a period of one month in the event of loss of international connections: fixed and mobile data connectivity to UK peering points; mobile voice; and text-based mobile messaging.	3(3)(f)(iii) 5(2)
M21.07	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)(f)(iii) 5(2)

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 is 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 host's operating system but on the "bare metal" of the host's hardware.
Container	The environment created by the Type 2 (Hosted) hypervisor in which a Virtual Machine runs.
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.
Core nodes	The main network elements that process data and store information.
Corporate Security Domain	A system or group of systems that all have the same level of security which protects the provider's own data.
Cryptographically attested	Identity, security and integrity of a system or sub system is confirmed by an encrypted algorithm.
Customer Premises Equipment (CPE)	Customer Premises Equipment refers to equipment provided to customers by the provider, and managed by the provider, that 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 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.
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 that 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.
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.
GSMA's Network Equipment Security Assurance Scheme (NESAS)	An industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry.
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	Pieces 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 that need to communicate with other providers (e.g. 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.
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.
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 network management.
Management Plane	The interfaces and connectivity and supporting equipment that allows network equipment to be managed.
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.
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.

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 that connects customers' telephone lines to the core network, to provide telephone, ISDN, and broadband, all from a single platform.
National Cyber Security Centre (NCSC)	The UK's technical authority for cyber security. 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 the results are monitored for potential vulnerabilities.
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 and documents that help to describe the network and the equipment in the network.
Network Function Virtualisation	A way to virtualise network services, such as routers, firewalls, and load balancers, that have traditionally been run on proprietary hardware.
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.
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 standard user or customer. Any access over the management plane, or to management ports of network equipment is privileged access.
Privileged Access Workstation (PAW)	An appropriately secured device that 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. A profile-modifiable SIM card is also a SIM that is able to support encryption key changes.
Remote Desktop Protocol (RDP)	A proprietary protocol which provides a user with a graphical interface to connect to another computer over a network connection.
RFC3682	The specification for the Generalised 'Time to live' (TTL) Security Mechanism (GTSM).
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.
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.
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.
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.
Third party administrators (3PA)	Managed service providers, provider group functions, or external support for third party supplier equipment (e.g. third-line support function).
Third Party Supplier Equipment or Network Equipment	Either a 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. It includes both virtual machines and physical hardware.
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 that has the characteristics defined in NCSC's secure by default platforms guidance.[56]
Trusted Platform Module (TPM)	Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM. The most common TPM functions are used for system integrity measurements and for key creation and use. During the boot process of a system, the boot code that is loaded (including firmware and the operating system components) can be measured and recorded in the TPM. The integrity measurements can be used as evidence for how a system started and to make sure that a TPM-based key was used only when the correct software was used to boot the system.
Trusted Platform / Trusted Computing Platform	A platform that uses roots of trust to provide reliable reporting of the characteristics that determine its trustworthiness.

[56] *Secure by default platforms* (NCSC, 2016) https://www.ncsc.gov.uk/information/secure-by-default-platforms

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.
Vendor's End-Of-Life Date	The end of the vendor's standard, global support for the equipment. It is the point at which no further security patches will be provided.
Virtualisation Administrators	Administrators who are granted privileged access to virtualisation infrastructure (NFVi), or the functions which manage virtualisation infrastructure.
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 Fabric	The physical servers and networking equipment used to provide the resources for virtualised workloads to run on.
Virtual Extensible LAN (VXLAN)	A network virtualisation technology that attempts to address the scalability problems associated with large cloud computing deployments.
Virtual LAN (VLAN)	Any broadcast domain that is partitioned and isolated in a computer network at the data link layer.
Wide Area Network (WAN)	A data network that extends over a large geographic area for the primary purpose of computer networking.

Annex B – Vendor Security Assessment

Introduction

The security of equipment deployed within a network is critical to the protection of that network. When selecting equipment that will support a critical service or critical infrastructure, public telecommunications providers should make an assessment of the security of that equipment and consider that assessment as part of their procurement and risk management processes.

This Annex provides advice on how to assess the security of network equipment. It provides guidance to support public telecommunications providers (the providers of Public Electronic Communications Networks and Services), in meeting their duties under the Telecommunications (Security) Act 2021, and the Electronic Communications (Security Measures) Regulations 2022. For example, under Regulation 3(3)(e), the network provider is required:

> "*to take such measures as are appropriate and proportionate in the procurement, configuration, management and testing of equipment to ensure the security of the equipment and functions carried out on the equipment*".

The guidance in this Annex should be used when making selection decisions for network equipment. However, security is an ongoing activity. As with other areas of performance, public telecoms providers should continue to assess and retain evidence of the vendor's track record in security during the equipment's lifetime, as this will support future security assessments.

The guidance in this Annex does not take account of, and cannot mitigate, the threats that may arise because of additional risks specific to a particular vendor in the supply chain. These risks include the degree to which it might be susceptible to being influenced or required to act contrary to the interests of the customer or their national security. In such circumstances, additional controls specific to the vendor in question may be required.

The guidance below is taken from the NCSC's Vendor Security Assessment (VSA) Version 1.0, which was published in March 2022. Any references to 'customers' should be interpreted as 'public telecoms providers' in the context of this code of practice.

Summary of approach to assessment

This document provides guidance on how to assess a vendor's security processes and their supplied network equipment. The purpose of the approach is to objectively assess the cyber risk due to use of the vendor's equipment. This is performed by gathering objective, repeatable evidence on the security of the vendor's processes and network equipment.

Assessing the cyber risk due to a vendor requires:

- evidence from the vendor themselves;
- testing to validate the vendor's claims;
- third party evidence.

For each criterion in this document, there are a range of product-specific spot checks that may be performed and evidence may be obtained directly from lab-tests on the product itself. These three components together will help build an understanding of how well a vendor is building a new product.

However, such an approach will always be fallible. While evidence will be customer-driven, it can only provide examples of vendor behaviour. To be effective, both the approach and security standards need to be sustained over many years, with evidence of good and bad practice recorded to support future security assessments and procurement decisions.

When assessing vendor security practices, the NCSC recommends operators to not rely exclusively upon vendor documentation to assess vendor security. Security assessments should be based on the vendor's implemented security behaviour. This includes product-line specific spot checks, and objective evidence extracted from the product.

External audits and international schemes

One of the biggest challenges when assessing the security of network equipment is the industry practice of producing regional or operator-specific versions of products. Where vendors follow this practice, international customers cannot share the burden of gaining evidence or assurance about product quality or security, whether through working with each other or through international testing schemes.

It may be possible to rely on independent, external sources to provide some of the required evidence, provided:

- it is applicable to the customer's product (specifically the same hardware and code base);
- all evidence can be revalidated by the customer, and some evidence has been randomly selected to be revalidated.

Generally, vendor audits or evaluations that rely on vendor documentation are unlikely to provide useful evidence unless it is possible to verify that the audit relates to the security of the network equipment. For the same reason, audits or evaluations where the evidence behind the audit is not widely available and testable should also not be considered. For example, as currently defined, the private, paper-based assessments performed under GSMA's NESAS[57] scheme are unlikely to provide useful evidence in support of the customer's assessment of product security.

Support from the security research community

Given the range, scale and complexity of network equipment, participation from the global security research community (including both commercial labs and academia) is essential to support customers in understanding security risk. For this reason, vendors should be encouraged to be transparent and open about their security practices, and should be encouraged to support responsible, independent security researchers in performing their own testing and analysis.

To support the development of increasingly secure and open telecommunications equipment, DCMS has stated that it intends to establish a UK Telecoms Lab (UKTL). This will be a secure research facility that will bring together telecommunications operators, existing and new suppliers, academia, and the government to create representative networks in which to research and test new ways of increasing security and interoperability.

[57] *GSMA Network Equipment Security Assurance Scheme* (NESAS) https://www.gsma.com/security/network-equipment-security-assurance-scheme/

The approach to assessment

Assessing a vendor's approach to security requires a four-tiered approach:

Assess

Assessing a Security Declaration provided by the vendor. This should state the vendor's approach to security, and the security promises that the vendor makes to its customers. In the interests of developing the security ecosystem, the NCSC recommends that the vendor openly publishes their Security Declaration. This provides confidence to customers that the vendor's approach is consistent for all customers and product lines, and allows the wider security community to participate in the security discussion.

Check

Performing Spot Checks on the vendor's implemented security processes for specific, independently chosen product releases. As all details should be readily available to the vendor within their own systems, providing advance notice of the choice should not be necessary.

Analyse

Performing Lab Tests against equipment. The tests should either be against all equipment or the equipment should be randomly selected from the equipment provided by the vendor. Lab tests should be automated wherever possible so they can be easily repeated at low cost. Lab tests performed independent of the customer should be against the same product version track, hardware, software, firmware, and configuration as used by the customer.

Sustain

Holding vendors to the standard in the Security Declaration throughout the entire period of the customer's relationship with the vendor. Customers should analyse root causes of issues and record the vendor's security performance to ensure future assessments are made with a rigorous evidence base.

Recommendations for applying this four-tiered approach are provided below.

Assessing vendor security performance

When assessing vendor security practises one essential source of data is the vendor's security performance. Customers should consider both the vendor's security culture and behaviour as evidenced by:

- maturity of vendor risk assessment and security assessment processes;
- vendor transparency, openness, and collaboration with the security research community;
- vendor assessment, management, and support to customers in relation to any security vulnerabilities and incidents;
- vendor compliance with security obligations and requirements;
- vendor approach to product and component support.

Security incidents in themselves are not evidence of poor security practice. All major companies are likely to be impacted by security incidents and depending on their cause and how they are handled, security incidents may provide an example of good practice. The customer should consider whether the incident could have been reasonably avoided, or its impact could have been reasonably reduced.

Similarly, product security vulnerabilities or issues are not in themselves evidence of poor security practice as such issues will occur in all products. However, where issues are simplistic, or due to poor product management or maintenance, this may be evidence of poor practice.

Vendor security assessment criteria

The following table can be used to assist in assessing the security processes of vendors and their network equipment. The table describes the information that customers should expect within the Security Declaration, Spot Checks that should be considered to collect evidence, and the Lab Testing that customers or third parties should consider making against equipment. For Spot Checks and Lab Testing, it is assumed that the customer will be given sufficient access to vendor processes and equipment to perform an effective evaluation prior to making decisions based upon this evaluation.

When third parties are used, the customer should satisfy themselves that the third party was sufficiently independent, had sufficient technical competence, and gained sufficient information about the vendor's day-to-day practices to provide them with the confidence required reliable evidence.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.A: Product lifecycle management					
V.A: Overall aim	*The vendor's products are properly supported throughout the lifetime of the product.*	*To provide confidence that a product will be maturely managed by the vendor, receiving updates and security critical fixes for the supported lifetime of the product.*	*As part of the Security Declaration, the vendor describes how products are supported.*	-	-
V.A.1: Product lifecycle process	The vendor clearly identifies the lifecycle for each product. Vendors should have an End of Life Policy which details how long products will be supported after End of Sale.	To provide confidence that products will be supported until a given date. Also, that the vendor's support dates apply globally, meaning that the vendor is likely to continue to invest in product maintenance throughout this period.	The vendor describes their product's lifecycle within the Security Declaration. For each release within a product line, the vendor publishes End of Sale dates on their website as soon as they become applicable. The End of Life Policy should detail how long, and in what way, products will be supported after the End of Sale date has been announced. The location of this information is referenced in the Security Declaration.	Check product release history. Explore how the vendor is keeping components up-to-date.	-

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.A.2: Software maintenance	Each product is maintained through its published life cycle. This maintenance, as a minimum, covers security fixes for the product.	To provide confidence that products can be patched against security issues discovered in the product throughout its supported lifetime.	The vendor clearly describes how they will support products during their lifetime, including what support they will provide under each support class.	View records showing the history of security fixes applied to the product, including a roadmap for resolution of any outstanding vulnerabilities.	Pick a sample of known vulnerabilities for a customer-selected product and check how and when they were patched in accordance with the vendor's policies. (see V.A.7). Test the product to verify that the equipment is no longer vulnerable to the vulnerability or variants of the vulnerability.
V.A.3: Software version control	Each product has a version-controlled code repository which logs every code modification. This audit log will detail: what code has been modified, added, or removed; why the change was made; who made the change; when the change was made; and which version of the code has been built into the released product.	To provide confidence that the vendor can track exactly what code is being deployed within products. It is essential for effective investigation of supply chain attacks.	The vendor describes how they maintain the integrity of their code base.	The vendor demonstrates how changes are made based on normal processes, and how changes via other means would be rejected. Explore a change and verify that processes were followed.	
V.A.4: Software releases	Each product goes through a rigorous software release cycle including internal testing before a version is released for general availability. Software will not be released if it does not comply with the Secure Engineering requirements detailed below. Each product should have regular external testing carried out on it by an independent third party.	This requirement exists to provide confidence that vendors test their software releases and validate that their internal secure engineering processes have been followed. The tests should also ensure that previously-resolved security vulnerabilities are not reintroduced.	The vendor describes their software release cycle, including the gates, and the testing performed.	View the build and test process. Review the testing performed against a customer-chosen product line and version. Check that testing tools are well configured and view the test results. Verify that tests are included to check for previously-resolved vulnerabilities and issues. The vendor demonstrates that issues were correctly fixed as a result of any failed tests.	Check accuracy of a set of the vendor's test results by repeating the tests in the customer's or third party's lab.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.A.5: Development processes and feature development	There is one primary release train of the product. Forking of new versions is minimised. Where necessary, customer-specific functionality is provided as optional modules. Any new features are brought into the main product line during the standard development roadmap.	This requirement exists to provide confidence that the vendor is shipping them a generally available version of the product, so they know the product can be supported throughout its lifetime using the general support routes. It is highly unlikely that the vendor will be able to properly support a proliferation of feature-specific product versions.	The Security Declaration describes the vendor's development process, including how and when new product versions are released, and how the number of versions is kept to a manageable level.	-	-
V.A.6: International release and forking	The vendor maintains a single, global version line for each product. There are a minimal number of other versions (ideally none).	This requirement exists to provide the confidence that the product is globally supported and that any issues discovered can easily be mitigated It is highly unlikely that the vendor will be able to properly support a proliferation of customer-specific product versions.	The vendor publishes details of all released versions of their products, including binary hashes. It is expected that this information will be on the vendor's website. The vendor references its public list of product versions within its Security Declaration.	The vendor describes the full release train of the product, including why each version was created.	Based on the vendor's published information, or otherwise, test that product versions supplied by the vendor are the 'global' versions and have matching binary hashes.
V.A.7: Use of tools, software and libraries	Third party tools (e.g. code compilers), software components and software libraries that are used within and in the development of the product are inventoried. Any of the above that are material to the security of the vendor's software are maintained throughout its lifetime.	Out-of-support tools, software components, software, or libraries are unlikely to use modern security features. If exposed, they can cause known vulnerabilities to be embedded in the product. Vulnerabilities in critical security protections of the product must be patched, to minimise the impact of exploits.	The Security Declaration describes how third-party software components are maintained, explicitly stating when, if ever, out-of-support components will be included in any product versions, stating justifications.	For a customer-selected product, the vendor provides a list of third-party components that are material to the security of the product, (e.g. those components exposed via interfaces). Verify that these components are still actively maintained, and there is a support plan for the lifetime of the product.	Scan product interfaces to inventory known third party tools and determine if they are being maintained. Examine the product to verify that the vendor's component list appears accurate.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.A.8: Software documentation	The vendor provides up-to-date and technically accurate documentation alongside new releases of the product. This documentation, as a minimum, shall detail how to securely configure, manage, and update the product.	This provides the customer with the information they require to help them securely deploy and manage the product throughout its lifetime in their networks, and independently assess the security of that configuration. This helps to reduce the customer's on-going dependence on the vendor.	The Security Declaration makes commitments about the release of product documentation to customers.	-	Using documentation, set-up, operate, configure, and update the product without support from the vendor.
V.B: Product security management					
V.B: Overall aim	*Products will be developed in a "secure by default" manner.*	*These requirements exist to provide confidence that a product they deploy has been developed using standard security mitigations and secure coding techniques.*	-	-	-
V.B.1: Security culture	The vendor has a security culture which ensures that security principles are followed.	This provides confidence that developers within the company are known to follow the security principles and development requirements.	The Security Declaration describes the senior ownership of the security culture within the vendor, and the mechanisms that exist to allow staff to raise security concerns.	-	-
V.B.2: Secure development lifecycle	The vendor has a Secure Development Lifecycle[58] to embed security into product development. All development teams follow, and can evidence that they follow, the Secure Development Lifecycle processes.	This provides confidence that security is embedded in the development process and that there is a consistent security culture within the company.	The Security Declaration describes how the vendor develops secure products, including how the vendor verifies that its secure coding standards are followed.	The vendor demonstrates how they gain confidence that the Secure Development Lifecycle has been followed by developers. The vendor describes how they ensure their code is of high quality. Verify examples of security controls built into the product development processes.	Search for signs that the vendor's security controls built into their Secure Development Lifecycle are working (e.g. that subcomponents are resistant to malformed inputs).

[58] The 'Secure Development Lifecycle' is the process through which the vendor integrates security considerations throughout the product development lifecycle.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.B.3: Internal component management	Any shared internal components or libraries are kept up to date and only the latest stable, supported version is used. These components and libraries are not to be modified for specific builds and are supported for the lifetime of the product.	This provides confidence that any internal shared components being used within a product will be maintained throughout the lifetime of the main product.	The Security Declaration makes clear commitments around the maintenance of internal components.	For a customer-selected product, the vendor can list the product's software and hardware components. Verify that only recently released versions of shared internal components and libraries are used. Explore whether the product line has forked any shared libraries.	In a lab, verify that the released product contains only one version of each internal software component or library, and that all internal components have been recently built.
V.B.4: External component management	Only supported external components are used within a product. The vendor monitors the external component's changelog so that only the latest supported, stable version is used within the product. Additionally, the vendor monitors the external component's security advisories and pull in any security fixes and integrate them into their product with a security update.	This provides confidence that any third-party component a vendor chooses to use will be currently supported, and that any security issue discovered with the component will be patched. Extended support contracts are likely to increase security risk and should be avoided.	The Security Declaration makes clear commitments on the use of supported external components.	For a customer-selected product release, verify that it is only using supported versions of external components and libraries. Explore how these components will be updated when they reach end-of-life. Explore whether the product line has forked any externally-developed code, and if so, explore how it is maintained.	In a lab, verify that the released product is only using fully supported versions of all external components. Search for evidence of internally-forked external components or libraries.
V.B.5: Unsafe functions	There are no unsafe functions used within the vendor's released code. Unsafe functions are those commonly associated with security vulnerabilities or those considered unsafe by industry best practice.	These functions are frequently the cause of product vulnerabilities .	The Security Declaration clearly states whether unsafe functions are used within the vendor's code base.	Request code metrics on use of unsafe functions	-

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.B.6: Redundant and duplicate code	The vendor's source tree is maintained to a level that there is limited redundant or duplicate code.	Redundant code makes a product more difficult to understand and maintain. Increases the likelihood that security critical changes won't be applied to access the product.	The Security Declaration makes clear statements about how the vendor produces code to reduce complexity and increase maintainability.	Request code metrics on how much duplicated code exists within the source tree.	-
V.B.7: File structure	The vendor's source tree is maintained to a level where code complexity is minimised, and functions perform single, clear, actions.	Code clarity reduces the risk of error or vulnerability and makes issues easier to spot.	The Security Declaration makes clear statements about how the vendor produces code to reduce complexity and increase maintainability.		-
V.B.8: Debug functionality	There is no engineering debug functionality present within the vendor's released products that could weaken or bypass the product's security mechanisms.	Engineering debug functionality may be used by an attacker to exploit a product.	The Security Declaration makes clear statements confirming that no engineering debug functionality is present within a released version of a product.	Ask the vendor to demonstrate that inclusion of debug functionality within a release build results in a build failure.	-
V.B.9: Comments	The source tree has suitable and understandable comments through it, explaining what the code is for and why it performs its actions.	Commenting helps ensure products can be easily supported in the future and speeds up vulnerability fixes.	- The Security Declaration makes clear statements about how the vendor produces code to reduce complexity and increase maintainability.	-	
V.C: Protected development and build environments					
V.C: Overall aim	*The NCSC expects the product is developed within a secure environment*	*A secure environment helps to maintain the integrity of the product and reduces the risk of supply chain attack.*	*The Security Declaration describes how the vendor maintains the integrity of its products through securing the development and build environments.*	-	-
V.C.1: Segregation of development environment	Development environment is segregated from corporate network and protected from the internet.	This protects the development environment from compromise via straight-forward attacks.	-	Ask to see details of penetration-tests or red team[59] exercises, where the objective was to modify the vendor's codebase or development environment.	-

[59] A 'red-team' exercise is one where responsible penetration testers are seeking to gain access to an asset within the vendor's network, such as their development environment.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.C.2: Segregation of build environment	Build environment is segregated from corporate network and protected from the internet. Very few people can make changes.	This protects the build environment from compromise via straight-forward attacks.	-	Ask to see details of penetration-tests or red team exercise , where the objective was to modify the vendor's build environment.	-
V.C.3: Build environments and automation	Build environments are simple, and the build process is automated.	Simple build environments and an automated build process makes the product build easier to understand, less likely to have errors and reduces the risk of compromise.	The Security Declaration describes how the vendor build process can be understood and maintained.	For a customer-selected product release, the vendor explains the build environment and its dependencies, and demonstrates the automated process via which a build is performed.	-
V.C.4: Role-based access	Only individuals with a need have access to the internal code base, and access is controlled and limited based on role.	Minimising access reduces the impact of a malicious insider.	The Security Declaration describes how the vendor enforces role-based access controls to its development and build environments.	The vendor demonstrates that access to the development and build environment is limited.	-
V.C.5: Code review	All code is independently reviewed prior to acceptance. Feedback processes exist.	Code review is essential to maintaining coding standards, and to reduce the risk due to a malicious insider.	The Security Declaration describes how and when the vendor carries out internal code review and audit.	For any change made to the code, the vendor can demonstrate how that change was reviewed or audited.	-
V.C.6: Repeatable builds	All builds of released software can be replicated at a future date	Replicated builds allow the vendor to demonstrate what components were included in a past build. Tracking of each build, what components are built into it and which versions of the components were used is critical to verifying the integrity of a build.	The Security Declaration makes clear statements about how the vendor maintains their build environment and code base to enable repeated builds with a minimal number of differences – with an explanation for each difference.	The vendor reproduces a previous build and confirms that it is functionally identical to a version that was released. The vendor demonstrates that they have retained copies of any external dependencies necessary for the build.	A released build and a reproduced build are compared to verify functional equivalence.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.D: Exploit mitigations					
V.D: Overall aim	*The vendor implements standard security mitigations used in a modern product.*	*Each of these mitigations has a demonstrable positive impact on the security of a product by helping to mitigate well known vulnerability classes. Modern platforms, operating systems, development languages, libraries and development tools regularly offer security enhancing technologies to both minimise the occurrence of security defects, and to minimise their impact should they occur.*	*The Security Declaration describes the vendor's policy with respect to the use of defensive security techniques.*	-	-
V.D.1: Heap protections	The vendor makes use of modern heap protection mitigations to help prevent heap-based memory corruption attacks against the product.	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products use heap protections throughout their product.	-	Verify that heap mitigations are enabled by (automatically) inspecting the product for this mitigation
V.D.2: Stack protections	The vendor only ships executable code that has been compiled using modern stack mitigations.	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products use stack protections throughout their product.	-	Verify that stack mitigations are enabled by (automatically) inspecting the product for this mitigation
V.D.3: Data execution prevention	The vendor supports hardware-enforced data execution prevention (for example DEP or NX).	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products use hardware-enforced data execution prevention throughout their product.	-	Verify that data execution prevention mitigations are enabled by (automatically) inspecting the product for this mitigation
V.D.4: Address space layout randomisation	The vendor only ships executable code that has been compiled using modern ASLR techniques.	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products use ASLR throughout their product.	-	Verify that address space layer randomisation mitigations are enabled by (automatically) inspecting the product for this mitigation.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.D.5: Memory mapping protections	The vendor's product will have no memory pages mapped by default as both "Writeable" and "Executable". This excludes areas of the code required to do Just-In-Time code compilation.	Widely used to make it more difficult for an attacker to exploit any security issues.	The Security Declaration states whether the vendor's products have any read-write memory pages. If any Just-In-Time code compilation is required, this should be described in the security declaration.	-	Verify that there are no executables that map memory pages as both writeable and executable by (automatically) inspecting the product.
V.D.6: Least privilege code	The vendor follows a "least privilege" methodology when developing and executing code within their products. The vendor ensures that their product only runs at or requests the minimum privilege level required for it to fulfil its advertised purpose. If higher privilege levels are ever required, then the product implements segregations to elevate privilege for the specific task.	Products that run at higher privilege levels than required can provide a route for attackers to exploit a host system.	The Security Declaration states the vendor's 'least privilege' methodology.	-	Verify that executable code running on the vendor's platform runs with the least level of privilege required Verify that any privileged executables drop privilege after completing their privileged task.
V.D.7: Security improvement and secure execution environments	The vendor has plans to continue to improve its product's security. As an example, this may include detailing how and when they plan to implement secure execution environments[60].	Product security needs to continue to evolve to keep pace with the threat environment.	-	Explore the vendor's future security roadmap, discussing how the vendor's product security will increase over time.	-
V.E: Secure updates and software signing					
V.E: Overall aim	*The source of the code that runs on the device is known, and the mechanisms to change the code on the device are secure*	*Reduces the risk of supply chain attack between code production by the vendor, and delivery to the device.*	-	-	-

[60] Secure execution environments are a significant upcoming security technology that increases product security by enabling execution of sensitive workloads on untrusted hardware.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.E.1: Software and firmware signing	Vendor's software and firmware is digitally-signed.	Signing of software and firmware provides strong evidence that the developer produced the code.	The Security Declaration describes whether software and firmware are digitally signed, and any processes for allowing customers to deploy their own code.	-	Test that shipped executable code (binaries, scripts, etc) are digitally signed using the vendor's public code signing certificate by automatically inspecting each file.
V.E.2: Signature verification	Software signatures are verified before binaries are executed.	Allows the device to check the source of the code.	The Security Declaration describes how signatures are checked prior to code execution. States whether that check is hardware-backed.		Test that a modification of a signed binary results in the device refusing to run the binary.
V.E.3: Secure update	Updates are delivered via a secure channel that is mutually authenticated between the device and the update server.	Using a secure channel reduces the risk of an attacker exploiting the update mechanism.	The Security Declaration describes the security properties of the update mechanism. .	-	Perform the update process, verifying that updates are delivered over a secure channel.
V.E.4 Downgrade protection	Built-in detection capabilities alert whenever software is downgraded during an install process.	Publicly known vulnerabilities in an older version of the product are common causes of exploit and compromise.	The Security Declaration describes how downgrade attacks are prevented by the vendor.		Test that a signed update which is of an older version to that currently installed produces a log message or other alert likely be seen by the system administrator.
V.F: Hardware roots of trust and secure boot					
V.F: Overall aim	*The vendors use a secure hardware root of trust within their products. These are commonly referred to as one of the following: TEE (Trusted Execution Environment), TPM (Trusted Platform Module), or DSC (Dedicated Security Component).*	*A hardware root of trust enables the vendor to use modern security mitigations such secure boot and code signing.*	*The Security Declaration describes the vendor's approach to the provision of hardware-backed security.*	-	-
V.F.1: Hardware root-of-trust	The equipment contains a hardware root-of-trust for identity and storage.	A hardware root-of-trust is necessary to provide hardware-backed functionality that cannot be remotely modified by an attacker.	The Security Declaration states the presence and properties of any hardware root of trust with the products.	-	Test that private keys associated with identity or device secrets are not stored in the filesystem in clear text.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.F.2: Secure boot	Each product will support a secure boot process, initiated by the hardware root-of-trust (V.F.1) to bring the equipment into a known-good state on restart.	Secure boot makes it harder for any compromise of the device to persist after a power-cycle. Should devices be compromised, secure boot is required to restore trust in the equipment. Otherwise, the equipment may need to be scrapped.	The Security Declaration describes the vendor's support of a secure boot, and how the vendor's products can be returned to a known-good state in the event of compromise.	-	Verify that the product can be returned to a 'known-good' state. Test that the device fails to boot should one or more of the signed binaries or scripts used during the boot process be modified.
V.F.3: Securing JTAG	Each compute element on a product will have debug interfaces (such as JTAG and UART) access disabled	With physical access, debug interfaces like JTAG can be used to circumvent the integrity of a product or steal device secrets.			Test that JTAG equipment cannot establish communication with any of the system's JTAG TAP controllers.
V.G: Security testing					
V.G: Overall aim	*The vendor rigorously tests the security of their products prior to release.*	*Through security testing and resolution, the number of vulnerabilities in the product is reduced, as is the risk of exploitation.*	*The Security Declaration describes the vendor's approach to security testing across its product range.*	-	-
V.G.1: Automated testing	Once developed, extensive security tests are automatically run against all versions of applicable products.	This ensures that testing is at a scale comparable to that employed by an attacker.	The Security Declaration describes the automated tests run against every product version.	For a customer-chosen product release, ask to see the test results from automated testing.	The customer, or third party, applies their own automated tests where possible.
V.G.2: Testing rigour	Developers cannot modify the build environment to hide or disregard build issues, or issues detected by automated tests. Failing builds are automatically rejected. Therefore, code used in released products do not create any compiler errors or security related warnings during build.	Developers may seek to bypass checks if permitted, leading to more vulnerable products.	The Security Declaration states whether tests can be bypassed.	For a customer-chosen product release, ask to see build results. Verify that the results do not highlight issues that should not be accepted in a released build.	-

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.G.3: Security testing	Security functionality is tested to demonstrate correct operation.	If security functionality is mis-implemented, the device will likely be vulnerable.	The Security Declaration states whether security testing is performed to verify correct operation.	For a customer-chosen product release, ask to see the results from security testing. Verify that issues were resolved, including root-causes.	Repeat tests of security functionality.
V.G.4: Negative testing	Extensive negative testing is performed against every product release, including a wide range of potential failure cases, inappropriate message sequencing and malformed messages.	By testing with extensive negative test cases, the vendor is more likely to catch easy-to-detect issues.	The Security Declaration states whether negative testing is performed and describes the scale of this testing.	For a customer-chosen product release, ask to see the test results from negative testing. Verify that issues were resolved, including root-causes.	Perform negative tests against the product, ideally using a distinct toolset to the vendor.
V.G.5: Fuzzing	Fuzzing is performed against the product, especially focusing on interfaces which cross security boundaries. The approach is sophisticated enough to ensure that a high proportion of code is tested.	A specific form of negative testing, the vendor tests their products against randomly-generated, malformed data, to catch easy-to-detect issues.	The Security Declaration states whether fuzz testing is performed and indicates the scope of this testing.	For customer-chosen product release, ask to see the test results from fuzzing, alongside data on code coverage. Verify that issues were resolved, including root-causes.	Perform fuzzing of the product, ideally using a distinct toolset to the vendor.
V.G.6: External testing	External security research teams perform testing against a selection of major product releases. Some of this testing is un-scoped.	By subjecting the device to an external third party, vulnerabilities are more likely to be detected and remediated.	The Security Declaration contains explicit details about how the vendor partners with external labs and academics to ensure the security of their products is independently tested.	Ask to see the results from external tests. Verify that issues were resolved, including root-causes.	-
V.G.7: Dynamic application security testing (DAST)[61]	The vendor has a DAST solution integrated into the vendor's test process	Applying DAST during testing can identify different types of vulnerabilities to that of fuzzing and negative testing.	The Security Declaration states how the vendor performs dynamic application security testing.	Ask to see the results from the DAST suite. Verify that issues were resolved, including root-causes.	Perform dynamic application security testing on the product, ideally using a distinct toolset to the vendor.

[61] Dynamic Application Security Testing (DAST) a procedure that actively investigates running applications with penetration tests to detect possible security vulnerabilities.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.H: Secure management and configuration					
V.H: Overall aim	*Any product can be easily setup to run securely.*	*Insecurely configured products are more likely to be exploited.*	*The Security Declaration describes the vendor's approach to helping operators securely configure products. This includes whether products are released in a 'secure' configuration.*	-	-
V.H.1: Product hardening	The product can be easily hardened into a secure configuration . Documentation exists to help customers perform this hardening process. Alerts are created should the device be taken out of the hardened state.	Insecurely configured products are more likely to be exploited.	The Security Declaration states whether products can be easily hardened into a secure configuration.	Verify that guidance is provided on secure configuration for provided products.	Test that the hardening guide can be easily deployed as-is to the product without impacting necessary functions. Test that alerts are created should the device be taken out of the hardened state.
V.H.2: Protocol standardisation	The product can be configured to only use standardised protocols.	Proprietary protocols do not allow for thorough, independent security testing, or correct behaviour to be understood by the customer.	-	-	Analyse traffic from the equipment to ensure that there are no proprietary protocols in use.
V.H.3: Management plane security	By default, the product is configured to only use up-to-date, secure protocols on the management plane.	Without secure protocols and user-based access it is not possible to securely manage equipment and associate administrative changes with a specific administrator.	The Security Declaration confirms whether the product only uses secure management protocols by-default.	-	Test that no weak or deprecated security protocols are enabled on the management plane.
V.H.4: Management access	Access to the management plane is user-based and supports asymmetric-key-based (e.g. X.509 certificates or SSH keys).	This allows customers to limit administrative privilege and investigate potentially malicious changes. The use of asymmetric key based authentication allows for more secure authentication and helps mitigate the risk of password sharing.	-	-	Test that the management plane gives administrators user-based access and supports asymmetric-key-based authentication.

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.H.5: No unencrypted protocols	Secure protocols are used whenever possible (e.g. SSH and HTTPS). If an unencrypted protocol is enabled, and a secure alternative exists, the product warns the administrator, and provides the option to create a security alert.	To prevent the use of insecure protocols, which increases the risk of exploitation.	-	-	Test that there are no unencrypted protocols and services are enabled by default on the product. Test that enabling an unencrypted protocol on the product results in appropriate warnings and alerts.
V.H.6: No un-documented administrative mechanisms	The product does not have any undocumented administrator accounts. Examples include, but are not limited to, hard coded passwords, access key pairs (SSH keys) or other administrative access tokens.	Undocumented administrative accounts may be exploited without customer awareness.	The Security Declaration explicitly states whether there are any undocumented administrative accounts on the product.	-	Search for evidence of undocumented administrator accounts in released products.
V.H.7: No un-documented administrative features	The product does not have any undocumented administration features.	Undocumented administrative features may be exploited without customer awareness.	The Security Declaration explicitly states whether there are any undocumented administrative features on the product.	-	Search for evidence of undocumented administrator features in released products.
V.H.8: No default credentials	No default passwords are left on the device after the initial setup. For clarity, this also means there are no administrative accounts coded into the vendor's software.	Failure to disable any non-unique or hardcoded accounts renders the equipment highly vulnerable to exploitation.	The Security Declaration explicitly states how default credentials are removed from all devices, and whether hard-coded administrative accounts exist.	-	Test that there are no default credentials on the device after initial setup. Scan products for potential hardcoded password strings.
V.H.9: Good practice guidance	The vendor is explicit about the threats to the equipment that they have sought to mitigate, and those they have not. The vendor provides detailed configuration and notes on how the equipment can be protected in networks.	By helping understand the security decisions taken by the vendor, and setup the equipment securely, security mistakes are less likely to be made.	The Security Declaration describes the vendors approach to security analysis, and how they support customers in minimising risk.	For a customer-chosen product, explore the vendor's product security analysis, and consider whether the vendor has understood the risk environment and established appropriate mitigations.	-

Topic	Security Expectation	Why it matters	Evaluation: Security Declaration	Evaluation: Customer or third-party Spot-checks	Evaluation: Customer or third-party lab test
V.J: Vulnerability and Issue Management					
V.J: Overall aim	*Effective processes exist to manage security issues and vulnerabilities. These issues are quickly and effectively resolved.*	*Products are most vulnerable from when an issue is discovered until it is patched. Effective issue management reduces this risk.*	*The Security Declaration describes the vendors approach to resolving issues.*	-	-
V.J.1: Issue tracking and remediation	The vendor has a process for issuing remediation. This ensures the vulnerability is resolved in all impacted products. Vulnerabilities are patched within appropriate timeframes.	If issues are not resolved across all versions of all product lines, the same issue may continue to be exploitable in some product version.	The Security Declaration provides the vendor's timescales on the resolution of security issues and describes how the vendor traces vulnerabilities across all products.	Assuming a software component is vulnerable, ask to see all products that contain that component.	Test whether a previously reported and resolved vulnerability may still be exploited across a range of products.
V.J.2: Issue comprehension	For issues, the vendor identifies the root cause analysis of the issue and is able to detail the origin of the vulnerability.	Proper vulnerability management requires the vendor to understand its own product and quickly assess impact of a vulnerability.	-	For a customer-chosen vulnerability, the vendor can provide details of the vulnerability, the root cause of the vulnerability, and how and when the vulnerability was correctly resolved.	-
V.J.3: Vulnerability reporting	The vendor provides a publicly advertised route for disclosure of security issues that links into their vulnerability management process.	This allows external people and organisations to responsibly disclose security issues to the vendor.	The Security Declaration describes how vulnerabilities may be reported to the vendor.	Explore how the vendor resolved a previously reported issue.	-
V.J.4: Issue transparency	The vendor is transparent about their patching of security issues.	In the sector, most security issues are patched without customers becoming aware of their existence. This makes it difficult for customers to judge risk.	The Security Declaration provides metrics on security issues, both reported and resolved. A list of all patched security issues in the product is available.	-	-
V.J.5 **Product Security Incident Response Team (PSIRT)**[62]	The vendor has set up the PSIRT structures within its organisation	Product security is not restricted to R&D. PSIRT brings together R&D, QM, TAC, OPS to be responsible for secure product operation by customers.	The Security Declaration describes how to contact vendor's PSIRT team.	Ask the vendor for Product Security Incident Response plan of selected release.	When vulnerabilities are found during lab testing, report these to the PSIRT team and verify that the vendor's response is effective.

[62] Product Security Incident Response Team (PSIRT) is the common name for the vendor's team that handles the receipt, investigation and public reporting of security vulnerability information relating to the vendor's products.

Annex C – Extracts from the Cyber Assessment Framework

Introduction

The information in this Annex is taken from the NCSC's Cyber Assessment Framework Version 3.1, which was published on 11 April 2022. Any references in this Annex to 'essential functions' should be considered as 'security critical functions' for the purpose of this code of practice.

CAF – Outline Approach

Each top-level NCSC security and resilience principle defines a fairly wide-ranging cyber security outcome. The precise approach organisations adopt to achieve each principle is not specified as this will vary according to organisational circumstances. However, each principle can be broken down into a collection of lower-level contributing cyber security and resilience outcomes, all of which will normally need to be achieved to fully satisfy the top-level principle.

An assessment of the extent to which an organisation is meeting a particular principle is accomplished by assessing all the contributing outcomes for that principle. In order to inform assessments at the level of contributing outcomes:

1. each contributing outcome is associated with a set of indicators of good practice (IGPs) and;
2. using the relevant IGPs, the circumstances under which the contributing outcome is judged 'achieved', 'not achieved' or (in some cases) 'partially achieved' are described.

For each contributing outcome the relevant IGPs have conveniently been arranged into table format. The resulting tables, referred to as IGP tables, constitute the basic building blocks of the CAF. In this way, each principle is associated with several IGP tables, one table per contributing outcome

Using CAF IGP Tables

Assessment of contributing outcomes is primarily a matter of expert judgement and the IGP tables do not remove the requirement for the informed use of cyber security expertise and sector knowledge. Indicators in the IGP tables will usually provide good starting points for assessments but should be used flexibly and in conjunction with the NCSC guidance associated with the top-level cyber security and resilience principles. Conclusions about an organisation's cyber security should only be drawn after considering additional relevant factors and special circumstances.

The 'achieved' (GREEN) column of an IGP table defines the typical characteristics of an organisation fully achieving that outcome. It is intended that all the indicators would normally be present to support an assessment of 'achieved'.

The 'not achieved' (RED) column of an IGP table defines the typical characteristics of an organisation not achieving that outcome. It is intended that the presence of any one indicator would normally be sufficient to justify an assessment of 'not achieved'.

When present, the 'partially achieved' (AMBER) column of an IGP table defines the typical characteristics of an organisation partially achieving that outcome. It is also important that the partial achievement is delivering specific worthwhile cyber security benefits. An assessment of 'partially achieved' should represent more than giving credit for doing something vaguely relevant.

The following table summarises the key points relating to the purpose and nature of the indicators included in the CAF IGP tables:

	Indicators in CAF IGP are…	**Indicators in CAF IGP are not…**
Purpose	…intended to help inform expert judgement.	…a checklist to be used in an inflexible assessment process.
Scope	…important examples of what an assessor will normally need to consider, which may need to be supplemented in some cases.	… an exhaustive list covering everything an assessor needs to consider.
Applicability	…designed to be widely applicable across different organisations, but applicability needs to be established.	…guaranteed to apply verbatim to all organisations.

CAF – Objective A – Managing security risk

Appropriate organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

Principle A1 Governance

The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

A1.a Board Direction

You have effective organisational security management led at board level and articulated clearly in corresponding policies.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
The security of network and information systems related to the operation of essential functions is not discussed or reported on regularly at board-level. Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance. The security of networks and information systems supporting your essential functions are not driven effectively by the direction set at board level. Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.	Your organisation's approach and policy relating to the security of networks and information systems supporting the operation of essential functions are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation. Regular board discussions on the security of network and information systems supporting the operation of your essential function take place, based on timely and accurate information and informed by expert guidance. There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level. Direction set at board level is translated into effective organisational practices that direct and control the security of the networks and information systems supporting your essential function.

A1.b Roles and Responsibilities

Your organisation has established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
Key roles are missing, left vacant, or fulfilled on an ad-hoc or informal basis. Staff are assigned security responsibilities but without adequate authority or resources to fulfil them. Staff are unsure what their responsibilities are for the security of the essential function.	Necessary roles and responsibilities for the security of networks and information systems supporting your essential function have been identified. These are reviewed periodically to ensure they remain fit for purpose. Appropriately capable and knowledgeable staff fill those roles and are given the time, authority, and resources to carry out their duties. There is clarity on who in your organisation has overall accountability for the security of the networks and information systems supporting your essential function.

A1.c Decision-making

You have senior-level accountability for the security of networks and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of essential functions are considered in the context of other organisational risks.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
What should be relatively straightforward risk decisions are constantly referred up the chain, or not made. Risks are resolved informally (or ignored) at a local level when the use of a more formal risk reporting mechanism would be more appropriate. Decision-makers are unsure of what senior management's risk appetite is, or only understand it in vague terms such as "averse" or "cautious". Organisational structure causes risk decisions to be made in isolation. (e.g. engineering and IT don't talk to each other about risk). Risk priorities are too vague to make meaningful distinctions between them. (e.g. almost all risks are rated 'medium' or 'amber').	Senior management have visibility of key risk decisions made throughout the organisation. Risk management decision-makers understand their responsibilities for making effective and timely decisions in the context of the risk appetite regarding the essential function, as set by senior management. Risk management decision-making is delegated and escalated where necessary, across the organisation, to people who have the skills, knowledge, tools, and authority they need. Risk management decisions are periodically reviewed to ensure their continued relevance and validity.

Principle A2 Risk Management

The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.

A2.a Risk Management Process

Your organisation has effective internal processes for managing risks to the security of network and information systems related to the operation of essential functions and communicating associated activities.

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
Risk assessments are not based on a clearly defined set of threat assumptions. Risk assessment outputs are too complex or unwieldy to be consumed by decision-makers and are not effectively communicated in a clear and timely manner. Risk assessments for critical systems are a "one-off" activity or not done at all. The security elements of projects or programmes are solely dependent on the completion of a risk management assessment without any regard to the outcomes. There is no systematic process in place to ensure that identified security risks are managed effectively. Systems are assessed in isolation, without consideration of dependencies and interactions with other systems. (e.g. interactions between IT and OT environments). Security requirements and mitigations are arbitrary or are applied from a control catalogue without consideration of how they contribute to the security of the essential function. Risks remain unresolved on a register for prolonged periods of time awaiting senior decision making or resource allocation to resolve.	Your organisational process ensures that security risks to networks and information systems relevant to essential functions are identified, analysed, prioritised, and managed. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential function. The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security. Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals. You conduct risk assessments when significant events potentially affect the essential function, such as replacing a system or a change in the cyber security threat. You perform threat analysis and understand how generic threats apply to your organisation.	Your organisational process ensures that security risks to networks and information systems relevant to essential functions are identified, analysed, prioritised, and managed. Your approach to risk is focused on the possibility of adverse impact to your essential function, leading to a detailed understanding of how such impact might arise as a consequence of possible attacker actions and the security properties of your networks and information systems. Your risk assessments are based on a clearly understood set of threat assumptions, informed by an up-to-date understanding of security threats to your essential function and your sector. Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential function. The output from your risk management process is a clear set of security requirements that will address the risks in line with your organisational approach to security. Significant conclusions reached in the course of your risk management process are communicated to key security decision-makers and accountable individuals.

Not achieved	Partially Achieved	Achieved
		Your risk assessments are dynamic and updated in the light of relevant changes which may include technical changes to networks and information systems, change of use and new threat information. The effectiveness of your risk management process is reviewed periodically, and improvements made as required. You perform detailed threat analysis and understand how this applies to your organisation in the context of the threat to your sector and the wider CNI.

A2.b Assurance

You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to essential functions.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
A particular product or service is seen as a "silver bullet" and vendor claims are taken at face value. Assurance methods are applied without appreciation of their strengths and limitations, such as the risks of penetration testing in operational environments. Assurance is assumed because there have been no known problems to date.	You validate that the security measures in place to protect the networks and information systems are effective and remain effective for the lifetime over which they are needed. You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential functions. Your confidence in the security as it relates to your technology, people, and processes can be justified to, and verified by, a third party. Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way. The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.

Principle: A3 Asset Management

Everything required to deliver, maintain or support networks and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

A3.a Asset Management

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
Inventories of assets relevant to the essential function are incomplete, non-existent, or inadequately detailed. Only certain domains or types of asset are documented and understood. Dependencies between assets are not understood (such as the dependencies between IT and OT). Information assets, which could include personally identifiable information or other sensitive information, are stored for long periods of time with no clear business need or retention policy. Knowledge critical to the management, operation, or recovery of essential functions is held by one or two key individuals with no succession plan. Asset inventories are neglected and out of date.	All assets relevant to the secure operation of essential functions are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date. Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded. You have prioritised your assets according to their importance to the operation of the essential function. You have assigned responsibility for managing physical assets. Assets relevant to essential functions are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.

CAF – Objective B – Protecting against cyber-attack

Proportionate security measures are in place to protect the networks and information systems supporting essential functions from cyber attack.

Principle: B5 Resilient Networks and Systems

The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and management of systems that support the operation of essential functions.

B5.a Resilience Preparation

You are prepared to restore the operation of your essential function following adverse impact.

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
You have limited understanding of all the elements that are required to restore operation of the essential function. You have not completed business continuity and/or disaster recovery plans for your essential function's networks, information systems and their dependencies. You have not fully assessed the practical implementation of your disaster recovery plans.	You know all networks, information systems and underlying technologies that are necessary to restore the operation of the essential function and understand their interdependence. You know the order in which systems need to be recovered to efficiently and effectively restore the operation of the essential function.	You have business continuity and disaster recovery plans that have been tested for practicality, effectiveness and completeness. Appropriate use is made of different test methods, e.g. manual fail-over, table-top exercises, or red-teaming. You use your security awareness and threat intelligence sources, to make immediate and potentially temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.

B5.b Design for Resilience

You design the network and information systems supporting your essential function to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
Operational networks and systems are not appropriately segregated. Internet services, such as browsing and email, are accessible from essential operational systems supporting the essential function. You do not understand or lack plans to mitigate all resource limitations that could adversely affect your essential function.	Operational systems that support the operation of the essential function are logically separated from your business systems, e.g. they reside on the same network as the rest of the organisation, but within a DMZ. Internet access is not available from operational systems. Resource limitations (e.g. network bandwidth, single network paths) have been identified but not fully mitigated.	Operational systems that support the operation of the essential function are segregated from other business and external systems by appropriate technical and physical means, e.g. separate network and system infrastructure with independent user administration. Internet services are not accessible from operational systems. You have identified and mitigated all resource limitations, e.g. bandwidth limitations and single network paths. You have identified and mitigated any geographical constraints or weaknesses. (e.g. systems that your essential function depends upon are replicated in another location, important network connectivity has alternative physical paths and service providers). You review and update assessments of dependencies, resource and geographical limitations and mitigations when necessary.

B5.c Backups

You hold accessible and secured current backups of data and information needed to recover operation of your essential function.

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
Backup coverage is incomplete and does not include all relevant data and information needed to restore the operation of your essential function. Backups are not frequent enough for the operation of your essential function to be restored within a suitable time-frame.	You have appropriately secured backups (including data, configuration information, software, equipment, processes and knowledge). These backups will be accessible to recover from an extreme event. You routinely test backups to ensure that the backup process functions correctly and the backups are usable.	Your comprehensive, automatic and tested technical and procedural backups are secured at centrally accessible or secondary sites to recover from an extreme event. Backups of all important data and information needed to recover the essential function are made, tested, documented and routinely reviewed.

Principle: B6 Staff Awareness and Training

Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of essential functions.

B6.a Cyber Security Culture

You develop and maintain a positive cyber security culture.

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
People in your organisation don't understand what they contribute to the cyber security of the essential function. People in your organisation don't know how to raise a concern about cyber security. People believe that reporting issues may get them into trouble. Your organisation's approach to cyber security is perceived by staff as hindering the business of the organisation.	Your executive management understand and widely communicate the importance of a positive cyber security culture. Positive attitudes, behaviours and expectations are described for your organisation. All people in your organisation understand the contribution they make to the essential functions' cyber security. All individuals in your organisation know who to contact and where to access more information about cyber security. They know how to raise a cyber security issue.	Your executive management clearly and effectively communicates the organisation's cyber security priorities and objectives to all staff. Your organisation displays positive cyber security attitudes, behaviours and expectations. People in your organisation raising potential cyber security incidents and issues are treated positively. Individuals at all levels in your organisation routinely report concerns or issues about cyber security and are recognised for their contribution to keeping the organisation secure. Your management is seen to be committed to and actively involved in cyber security. Your organisation communicates openly about cyber security, with any concern being taken seriously. People across your organisation participate in cyber security activities and improvements, building joint ownership and bringing knowledge of their area of expertise.

B6.b Cyber Security Training

The people who support the operation of your essential function are appropriately trained in cyber security. A range of approaches to cyber security training, awareness and communications are employed

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
There are teams who operate and support your essential function that lack any cyber security training. Cyber security training is restricted to specific roles in your organisation. Cyber security training records for your organisation are lacking or incomplete.	You have defined appropriate cyber security training and awareness activities for all roles in your organisation, from executives to the most junior roles. You use a range of teaching and communication techniques for cyber security training and awareness to reach the widest audience effectively. Cyber security information is easily available.	All people in your organisation, from the most senior to the most junior, follow appropriate cyber security training paths. Each individual's cyber security training is tracked and refreshed at suitable intervals You routinely evaluate your cyber security training and awareness activities to ensure they reach the widest audience and are effective. You make cyber security information and good practice guidance easily accessible, widely available and you know it is referenced and used within your organisation.

CAF – Objective D – Minimising the impact of cyber security incidents

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

Principle: D1 Response and Recovery Planning

There are well-defined and tested incident management processes in place that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D1.a Response Plan

You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function and covers a range of incident scenarios.

Not achieved	Partially Achieved	Achieved
At least one of the following statements is true	*All the following statements are true*	*All the following statements are true*
Your incident response plan is not documented. Your incident response plan does not include your organisation's identified essential function. Your incident response plan is not well understood by relevant staff.	Your incident response plan covers your essential functions. Your incident response plan comprehensively covers scenarios that are focused on likely impacts of known and well-understood attacks only. Your incident response plan is understood by all staff who are involved with your organisation's response function. Your incident response plan is documented and shared with all relevant stakeholders.	Your incident response plan is based on a clear understanding of the security risks to the networks and information systems supporting your essential function. Your incident response plan is comprehensive (i.e. covers the complete lifecycle of an incident, roles and responsibilities, and reporting) and covers likely impacts of both known attack patterns and of possible attacks, previously unseen Your incident response plan is documented and integrated with wider organisational business and supply chain response plans. Your incident response plan is communicated and understood by the business areas involved with the operation of your essential functions.

D1.b Response and Recovery Capability

You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function. During an incident, you have access to timely information on which to base your response decisions.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
Inadequate arrangements have been made to make the right resources available to implement your response plan. Your response team members are not equipped to make good response decisions and put them into effect. Inadequate back-up mechanisms exist to allow the continued operation of your essential function during an incident	You understand the resources that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available. You understand the types of information that will likely be needed to inform response decisions and arrangements are in place to make this information available. Your response team members have the skills and knowledge required to decide on the response actions necessary to limit harm, and the authority to carry them out. Key roles are duplicated, and operational delivery knowledge is shared with all individuals involved in the operations and recovery of the essential function. Back-up mechanisms are available that can be readily activated to allow continued operation of your essential function (although possibly at a reduced level) if primary networks and information systems fail or are unavailable. Arrangements exist to augment your organisation's incident response capabilities with external support if necessary (e.g. specialist cyber incident responders).

D1.c Testing and exercising

Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
Exercises test only a discrete part of the process (e.g. that backups are working), but do not consider all areas. *Incident response exercises are not routinely carried out or are carried out in an ad-hoc way.* *Outputs from exercises are not fed into the organisation's lessons learned process.* *Exercises do not test all parts of the response cycle*	Exercise scenarios are based on incidents experienced by your and other organisations or are composed using experience or threat intelligence. Exercise scenarios are documented, regularly reviewed, and validated. Exercises are routinely run, with the findings documented and used to refine incident response plans and protective security, in line with the lessons learned. Exercises test all parts of your response cycle relating to your essential functions (e.g. restoration of normal function levels).

Principle: D2 Lessons Learned

When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.

D2.a Incident Root Cause Analysis

When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
You are not usually able to resolve incidents to a root cause. *You do not have a formal process for investigating causes.*	*Root cause analysis is conducted routinely as a key part of your lessons learned activities following an incident.* *Your root cause analysis is comprehensive, covering organisational process issues, as well as vulnerabilities in your networks, systems or software.* *All relevant incident data is made available to the analysis team to perform root cause analysis*

D2.b Using Incidents to Drive Improvements

Your organisation uses lessons learned from incidents to improve your security measures.

Not achieved	Achieved
At least one of the following statements is true	*All the following statements are true*
Following incidents, lessons learned are not captured or are limited in scope. Improvements arising from lessons learned following an incident are not implemented or not given sufficient organisational priority.	You have a documented incident review process/policy which ensures that lessons learned from each incident are identified, captured, and acted upon. Lessons learned cover issues with reporting, roles, governance, skills and organisational processes as well as technical aspects of networks and information systems. You use lessons learned to improve security measures, including updating and retesting response plans when necessary. Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly. Analysis is fed to senior management and incorporated into risk management and continuous improvement.

E02781980
978-1-5286-3660-5