Economy

Consultation: Draft Telecommunications Security Code of Practice

Contents

Structure of the draft Code of Practice

This draft Code of Practice contains three sections:

- Section 1 contains introductory and background information on this Code of Practice, including its legal status within Jersey's telecoms security framework, how it applies to Public Telecoms Providers, and its oversight in Jersey.
- Section 2 explains the key concepts that need to be understood by Public Telecoms Providers when applying the specific security measures contained within the Telecommunications (Security Measures) (Jersey) Order 202-[1] (hereafter referred to as 'the Order') and by those Public Telecoms Providers specified in the Order when applying the technical guidance measures within Section 3 of the Code of Practice.
- Section 3 contains the technical guidance measures and maps each individual guidance measure to the relevant security measures in the Order. It also sets out the implementation timeframes for the technical guidance measures, which those Public Telecoms Providers specified in the Order are expected to follow.

[1] The Order will be dated once made by the Minister for Sustainable Economic Development

Section 1: Introduction and background

Introduction

0.1 Government of Jersey's Digital Economy Strategy vision is "to unleash a thriving, innovative and inclusive digital future powered by world-class infrastructure and enabling legislation, that delivers sustainable growth for our Island economy."[2]

0.2 The strength of Jersey's economy, and reputation as an international financial services centre and a centre of innovation, are based not only on its laws and high standards but also on the secure and resilient digital connectivity provided by Jersey's telecommunications (telecoms) networks and services.

0.3 That digital connectivity underpins Jersey's vision of a consistently high-performing, environmentally sustainable and technologically advanced small Island economy. Providing reliable, secure access to the world while sitting at the heart of our Island community, digital connectivity is a key driver of sustainable economic growth and productivity. Economic growth and productivity are especially important to meet future challenges, around an ageing population digital connectivity will be at the heart of this growth and other wider service solutions.

0.4 Maintaining the security and resilience of Jersey telecoms networks and services in a rapidly changing world with ever more complex threats and risks is challenging and of crucial importance to Jersey, its businesses and all Islanders.

0.5 In recognising the scale and nature of those challenges, States Assembly agreed in September 2024, to amend the existing the Telecommunications (Jersey) Law 2002 in the interests of the security of Jersey and to closely align Jersey's approach to telecommunications security with that of the UK.

0.6 Jersey's relationship with the UK is deep and long-standing. Jersey's closet cultural, economic and diplomatic relationships are with the UK and Jersey looks to the UK Government for its defence and international representation. Jersey's Public Telecoms Providers use UK+44 phone numbers and work closely with UK Public Telecoms Providers and UK Government agencies to maintain the security of our networks and services.

0.7 Jersey has developed a telecoms security framework for Jersey's providers of public electronic communications networks and services (PECN / PECS)[3] that has much in common with the UK's framework introduced by the UK's Telecommunications (Security) Act 2021 (the Act).

0.8 Jersey remains an independent jurisdiction. The UK's Act does not apply to Jersey, nor do the UK's Electronic Communications (Security Measures) Regulations 2022, or the UK's Telecommunications Security Code of Practice issued December 2022. Ofcom has no telecoms security functions or duties for Jersey. Jersey's telecoms

[2] Digital Economy Strategy. Government of Jersey
[3] As defined in Article 24A of the Law.

security framework including the Order and this, Jersey's Code of Practice, are underpinned by Jersey legislation, the Telecommunications (Jersey) Law 2002, as amended (the Law).

0.9 Jersey's framework comprises three layers:

1. **Security duties on all Public Telecoms Providers**. These are set out in new Part 5A of the Law.

2. **Specific security measures** (hereafter referred to as 'requirements')**.** These are set out in the Order and detail the specified measures to be taken in addition to the overarching duties in the Law.

3. **Technical guidance.** This Code of Practice provides detailed guidelines to specified providers of PECN and PECS (hereafter referred to as 'Public Telecoms Providers') on the Government's preferred approach to demonstrating compliance with the duties in the Law and the requirements within the Order.

0.10 Meeting the duties and requirements of Jersey's framework will require Public Telecoms Providers to develop and maintain a positive cyber security culture. Leadership, active engagement and participation at all levels is required to achieve the desired outcome – a continuously improving security culture. Creating the right cultural conditions for security is important. Public Telecoms Providers should have regard to NCSC's guidance about how to create the cultural conditions in an organisation that support and encourage the desired cyber security behaviours.[4]

0.11 Public Telecoms Providers' Boards and executive teams must be engaged in the management of risks. Cyber security is a critical risk for boards and executive teams. A culture of cyber security starts with the Board. The need for Public Telecoms Providers to take a risk-based approach to securing data and systems should be led by the Board and executive teams.

0.12 The NCSC has published guidance about how Boards can deliver, communicate and champion strong cyber leadership including a Cyber Security Toolkit for Boards and Cyber Governance for Boards.

Technical Analysis

0.13 The technical content of this, Jersey's Code of Practice, is based on the UK's Code of Practice[5] published in December 2022 and is therefore informed by guidance developed by experts in the National Cyber Security Centre (NCSC). The NCSC provides advice and assistance to Jersey and the other Crown Dependencies as part of existing defence and security arrangements.

[4] Cyber security culture principles (NCSC, 2025)
[5] https://assets.publishing.service.gov.uk/media/6384d09ed3bf7f7eba1f286c/E02781980_Telecommunications_Security_CoP_Accessible.pdf

0.14 NCSC's guidance was produced following an extensive and detailed analysis of the security of the UK's telecoms sector. Government has worked closely with the NCSC to understand the extent to which the NCSC's guidance as set out the UK's Code of Practice is appropriate and proportionate for Jersey and Jersey's Public Telecoms Providers. This, Jersey's Code of Practice is, therefore, informed by the guidance provided by NCSC and contains a set of technical and procedural measures designed to ensure that security risks are appropriately managed by Jersey's Public Telecoms Providers.[6] NCSC's guidance stresses the need for organisations to take a risk-based approach to securing their networks and services.[7] Public Telecoms Providers shall, therefore, take a risk-based approach to securing their networks and services.

0.15 It is important that Public Telecoms Providers ensure that all of the risks they face including cyber, physical[8] and personnel[9] risks are assessed, appropriately managed, and that effective governance in in place. Public Telecoms Providers shall among other things consider NCSC's risk management guidance, the Cyber Assessment Framework, the Vendor Security Assessment guidance, and the guidance provided by the UK's National Protective Security Agency who, like the NCSC, provide advice to Jersey and the other Crown Dependencies.

0.16 The guidance, technical and procedural measures in this Code of Practice should be viewed and addressed holistically, not as separate, discrete elements or requirements to be understood and addressed in isolation.

0.17 Cyber and Telecoms security is constantly evolving and in response to rapidly changing and new threats. Public Telecoms Providers should in addition to this Code of Practice, consider and understand guidance, advice and information published by among others the NCSC, UK National Protective Security Authority, European Telecommunications Standards Institute (ETSI), and Jersey Cyber Security Centre (JCSC). Revisions and updates to the UK's Code of Practice that provide clarifications and introduce additional measures should also be considered and where appropriate addressed until such time they are incorporated into Jersey's Code of Practice.

0.18 The Order and this Code of Practice make that clear those persons – "responsible persons"- who have been given security-related tasks by Public Telecoms Providers shall be both competent to discharge the responsibility, and are given resources to enable them to do so.

0.19 It is equally important that Public Telecoms Providers continually improve their approach to risk management, considering risks posed by new and evolving technologies such as Artificial Intelligence, application programming interfaces and

[6] The NCSC published a summary of its security analysis for the telecoms sector in January 2020
[7] 10 Steps to Cyber Security - Risk Management (NCSC, 2021)
[8] Building Protection (NPSA)
[9] Personnel and People Security (NPSA, 2021)

eSIMs. Public Telecoms Providers should make use of threat intelligence, information sharing and analysis resources.

0.20 This Code of Practice does not contain guidance or measures about the application of Artificial Intelligence. Nevertheless, Public Telecoms Providers should have regard to guidance published by NCSC[10] and ETSI[11] in order to assess and address the risks arising from the use of Artificial Intelligence by themselves, suppliers and bad actors.

Roles and responsibilities of public authorities

0.21 *The Minister for Sustainable Economic Development (the Minister)* is responsible for setting and overseeing national policy on telecoms security and resilience. The Minister 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 the Jersey Competition Regulatory Authority (JCRA)[12] through its regular reporting on security to the Minister under Article 24Z of the Law.

0.22 Government has also published proposals for legislation to improve Jersey's cyber resilience.[13] Focussed on the intention for the JCSC to become an independent advisory and emergency response body, the proposed Jersey Cyber Security Law will require Operators of Essential Services to report significant cyber security incidents.[14]

0.23 *JCRA*: JCRA will regulate the new framework in accordance with its duty in Article 24V of the Law, to seek to ensure that Public Telecoms Providers comply with their security duties. This gives JCRA 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.

0.24 The Law gives JCRA the ability to monitor and enforce compliance with its new legal obligations in the telecoms security framework. It also gives JCRA new powers to request information from Public Telecoms Providers in order to carry out its functions.

0.25 *The NCSC:* The NCSC is the UK's national technical authority for cyber security and provides expert and impartial advice to the Government and its agencies including the JCRA.

---

[10] AI and cyber security what you need to know (NCSC, 2024), Guidelines for secure AI development (NCSC, 2023)
[11] New ETSI standard protects AI systems from evolving cyber threats (NCSC, 2025)
[12] The Jersey Competition Regulatory Authority was established as a body corporate by Article 2 of the Competition Regulatory Authority (Jersey) Law 2001
[13] Proposed Jersey Cyber Security Law (GoJ 2024)
[14] Operator of an Essential Service (OES) is defined as a person (which includes businesses) or any other service which is essential for the infrastructure of Jersey or the maintenance of critical societal or economic activities in Jersey

0.26 The NCSC will also continue to offer technical advice to Jersey's Public Telecoms Providers, to Government, JCRA, and to the JCSC. However, the NCSC will not report Public Telecoms Providers to JCRA in cases of non-compliance or advise Public Telecoms Providers on whether the measures they are taking amount to regulatory compliance.

0.27 *The JCSC:* JCSC is the local technical authority with regard to cyber security and provides expert and impartial advice to Government and its agencies including the JCRA. The JCSC and JCRA will agree a Memorandum of Understanding. The Memorandum will contain 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.

Scope of this Code of Practice

0.28 This Code of Practice provides guidance for those Public Telecoms Providers specified in the Order whose security is most crucial to the effective functioning of Jersey's telecoms critical national infrastructure (CNI). However, other Public Telecoms Providers could choose to adopt any aspects of the guidance that they consider would be appropriate to secure their networks and services.

Application of this Code of Practice

0.29 The guidance in this Code of Practice is intended to apply to Public Telecoms Providers in the following way:

- The measures in this Code of Practice apply to those Public Telecoms Providers specified in the Order, whose availability and security is critical to people and businesses across Jersey. We intend Public Telecoms Providers specified in the Order to implement measures to the timeframes set out in Section 3.
- Those Public Telecoms Providers not specified in the Order are not expected to follow the measures in this code of practice. However, they may choose to adopt the measures included within this Code of Practice where these are appropriate and proportionate to their networks and services.

0.30 In deciding whether a Public Telecoms Provider should be specified in the Order, the Minister uses market share information published by the JCRA as a measure that captures:

- severity of a security compromise as a product of the numbers of customers affected by the loss/disruption of the company's network or service,
- the importance of the network or service to those customers, and
- the wider importance to Jersey and its economy.

0.31 Market share also reflects the broad ability of a Public Telecoms Provider to bear the financial burden of following the guidance in the Code of Practice.

0.32 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 this Code of Practice where applicable.

Changes to the specified Public Telecoms Providers

0.33 The Minister will keep under review the need to make changes to those Public Telecoms Providers specified in the Order. Changes will only be made where there is a need to reflect a true change in the growth or reduction of a provider's business operations in the following circumstances:

- Where a telecoms market participant gains market share so that its market share is reported by JCRA in in its annual Statistics Report for a period of two years, the telecoms market participant will be included in Schedule 1 of the Order.
- Where a telecoms market participant loses market share so that its market share is not reported by JCRA in in its annual Statistics Report for a period of two years, the telecoms market participant will be removed from Schedule 1 of the Order.
- Where an telecoms market participant exits the market, the telecoms market participant will be removed from Schedule 1 of the Order.

Legal status of this Code of Practice

0.34 This Code of Practice provides detailed technical guidance to Public Telecoms Providers about the measures to be taken under Part 5A of the Telecoms Law. The processes for issuing, revising and withdrawing Codes of Practice are set out in Articles 24O and 24P of the Law and the legal effects of Codes of Practice are detailed in Article 24Q.

Non-compliance with the guidance measures in this Code of Practice

0.35 The guidance set out in this Code of Practice is not the only way for Public Telecoms Providers to comply with the security duties in the Law and the specific security requirements in the Order. Where the Order requires Public Telecoms Providers to take 'appropriate and proportionate' measures, what is appropriate and proportionate will depend on the particular circumstances of the Public Telecoms Provider.

0.36 A Public Telecoms Provider may choose to comply with its security duties and specific security requirements by adopting different technical solutions or approaches to those specified in this Code of Practice. When they do so, JCRA may require the Public Telecoms Provider to explain the reasons why they are not acting in accordance with the provisions of this Code of Practice in order to assess whether they are still meeting their duties under the Law. Public Telecoms Providers are obliged to explain those reasons to JCRA under Article 24R of the Law, where JCRA

has reasonable grounds for suspecting a Public Telecoms Provider is failing or has failed to comply with this Code of Practice.

0.37 In determining any question arising in connection with the carrying out by JCRA of a relevant function, JCRA must also take into account the provisions in this Code of Practice where they are relevant and in force at the time in which the question relates to (see Article 24Q(3) of the Law).

0.38 In determining any question arising in legal proceedings, a court must take the provisions in this Code of Practice into account where they are relevant and in force at the time in which the question relates to (see Article 24Q(2) of the Law).

Non-compliance with the security duties in the Law and/or requirements in the Order

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

0.40 In addition, in cases of non-compliance, including where a Public Telecoms Provider has not complied with a notification of contravention, JCRA can issue financial penalties. The level of the financial penalties that JCRA can impose in those instances is set out in the Law.

0.41 Further information on how JCRA will use its powers and regulate the framework will be contained within its Procedural Guidance required under Article 24Y of the Law.

Implementation timeframes

0.42 Whilst the overarching security duties that form the new telecoms security framework will come into force on a date to be confirmed, it would not be proportionate to expect Public Telecoms Providers to be in a position to meet all their obligations by that date. Instead, specific recommended compliance timeframes for individual measures are contained within this Code of Practice. These are the timelines by which Public Telecoms Providers would be expected to have taken relevant measures set out in this Code of Practice. Nevertheless, Public Telecoms Providers might well consider a risk-based approach that considers the threats to their networks and services means it is appropriate achieve compliance before the timelines set out in this Code of Practice.

0.43 It would not be appropriate, proportionate, or technically feasible, to expect Public Telecoms 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.

Public Telecoms Providers entering the market

0.44 New Public Telecoms Providers entering the market will be expected to follow the same timeframes as existing Public Telecoms Providers, irrespective of how recently they entered the market.

Updating this Code of Practice

0.45 Government intends to review and update this Code of Practice periodically. Updates will most likely be informed by the following broad categories of information:

- updates made by the UK Government to the UK's Code of Practice;
- security advice provided to the by the NCSC and JCSC 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 risks of security compromises; and
- security reports prepared by Ofcom and JCRA containing information and advice that will assist the Government with forming policy.

0.46 Where changes to this Code of Practice are proposed, Government will consult affected Public Telecoms Providers, JCRA and any other relevant parties. All proposed changes, regardless of their source, will be discussed with the NCSC and JCSC before being incorporated into the Code of Practice. After carrying out the consultation, and before issuing the Code of Practice, Government will lay a copy of the Code of Practice before the States Assembly.

0.47 When published, this current version of the Code of Practice provides guidance as to the measures to be taken by Public Telecoms Providers under Articles 24K to 24N of the Act, unless revised or withdrawn by the Government.

Further information

0.48 There are various documents that can be used to further understand the wider telecoms security framework and policy background of this Code of Practice. These include:

- NCSC's security analysis for the UK telecoms sector[15]
- The Telecommunications Law (Jersey) Amendment Regulations 2024
- The Telecommunications (Security Measures) (Jersey) Order 202-[16]

[15] Summary of NCSC's security analysis for the UK telecoms sector (NCSC, 2020)
[16] Once made the Order will be assigned a date.

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 Order. It is important that all Public Telecoms Providers fully understand these key concepts as it will enable them to properly apply the intent of the security requirements. This chapter covers the concepts of security critical functions and network oversight functions which apply throughout, as well as the overarching scope of this Code of Practice.

Explanation of terms

Where the term **'reduce'** is used in the Order, it is expected that the Public Telecoms 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 this 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 Order. 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 Public Telecoms 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 Public Telecoms Providers are likely to have multiple options, all of which could deliver a satisfactory solution and there are likely to be differences between Telecoms Providers in their implementation.

Scope of measures within this Code of Practice

1.2 Measures contained within Section 3 of this Code of Practice apply to Public Telecoms Providers. This includes, but is not limited to, the following elements where they are part of such networks and services:

- the systems and services involved in providing public telecommunications services to customers;
- proof of concepts or trials on the operational network;

- the use of data from the operational network for testing purposes;
- interconnection of development, test and operational systems - although this is an activity which is inappropriate in all scenarios;
- parts of the operational network operated by third parties on behalf of the Public Telecoms Provider, including as part of managed service arrangements;
- parts of the operational network hosted outside the British Islands; 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 Telecoms Provider’s 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” (Article 1 of the Order).

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, Public Telecoms 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 Public Telecoms Provider to understand the network, secure the network, or to recover the network. Scope will differ from Public Telecoms Provider to Public Telecoms Provider depending on the type of network and how those networks are architected.

1.7 Given their importance in allowing the Public Telecoms 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.

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 Public Telecoms Providers should establish the principle of 'assumed compromise'. This means that Public Telecoms Providers should normally assume network oversight functions to be subject to high-end attacks, which may not have been detected by the Public Telecoms 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 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 the Article 6 of the Order, Public Telecoms 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.

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

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

1.17 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.

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 Order. However, not all security critical functions can be considered as network oversight functions as many do not control or oversee other security critical functions.

2. Network Architecture

2.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 3 of the Order to design, construct (or where relevant, redesign and develop) and maintain networks securely.

2.2 Article 3 of the Order is set out below.

> 3 (1) A network provider must take appropriate and proportionate measures to ensure –
>
> (a) except in relation to an existing part of its public electronic communications network, that the network is designed and constructed in a way that reduces the risks of a security compromise occurring;
>
> (b) in relation to an existing part of its public electronic communications network, that the part is redesigned and developed in a way that reduces the risks of a security compromise occurring; and
>
> (c) that its public electronic communications network is maintained in a way that reduces the risks of a security compromise occurring.
>
> (2) An existing part of a public electronic communications network is a part that was brought into operation before the commencement of this Order.
>
> (3) The duty in paragraph (1) includes a duty to –
>
> (a) identify and reduce the risks of a security compromise to which the network as a whole, and each particular function or type of function of the network, may be exposed, giving consideration to –
>
> (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) make a written record, at least once in any 12-month period, of the risks identified under sub-paragraph (a);
>
> (c) identify and record the extent to which the network is exposed to incoming signals;
>
> (d) design and construct the network in a way that ensures that security critical functions are appropriately protected and that the equipment performing those functions is appropriately located;
>
> (e) take appropriate and proportionate measures in the procurement, configuration, management and testing of equipment to ensure the security of the equipment and functions carried out on the equipment; and

(f) take appropriate and proportionate measures to ensure that the network provider –

(i) is able, without reliance on persons, equipment or stored data located outside of the British Islands, to identify the risks of a security compromise 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 of the British Islands; 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 of the British Islands.

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

(5) A network provider or service provider must take appropriate and proportionate measures to ensure that its public electronic communications network or public electronic communications service is designed so that 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 Public Telecoms 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 Public Telecoms 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 Order for the removal of specific network equipment and it would not be proportionate for that network equipment to meet specific measures within this Code of Practice, Public Telecoms 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 networking system or device is the part of a system that configures, monitors and provides management, monitoring and configuration services to all layers of the network stack, and other parts of the system.

Scope

2.8 The scope will differ from Public Telecoms Provider to Public Telecoms 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 Public Telecoms 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 Public Telecoms 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 Public Telecoms 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.

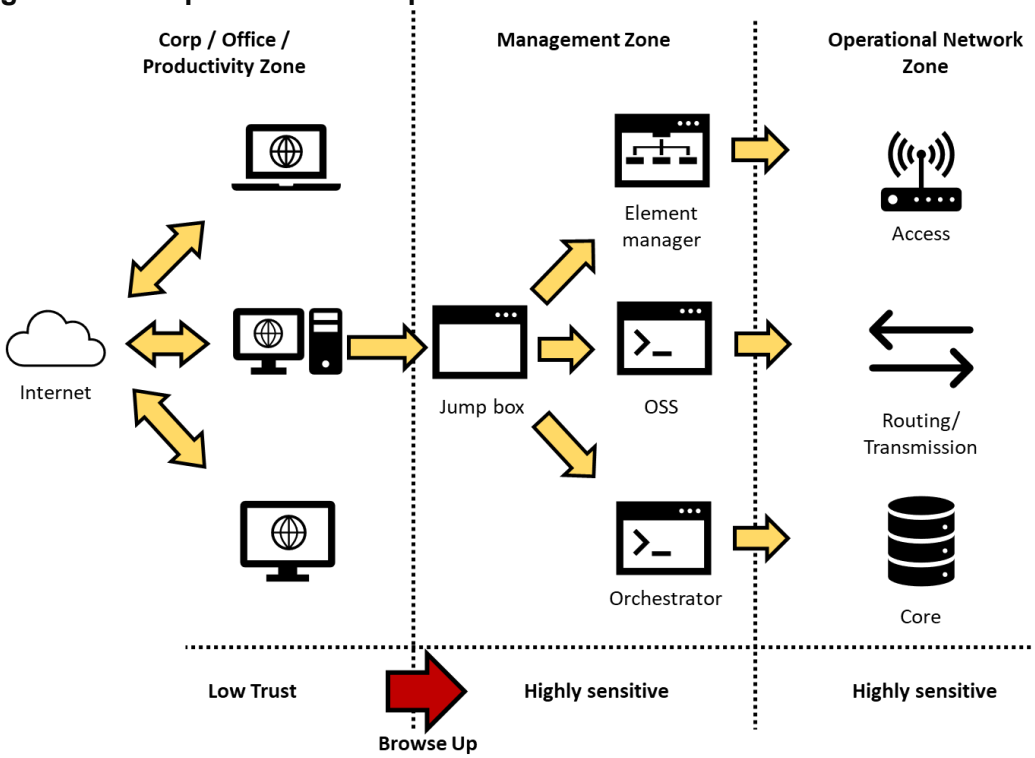
2.12 As an example, on 17 August 2021 it was confirmed that T-Mobile was subject to a data breach which saw the personal data of nearly 50 million customers being exposed[17]. Evidence has shown that this compromise may have been caused by T-Mobile having the management plane of the core network directly exposed to the internet. It has been indicated that the exposed box was test equipment that was attached to the operational

[17] *The Cyberattack Against T-Mobile and Our Customers: What happened, and what we are doing about it* (T-Mobile, 2021)

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[18].

Figure 1: Example of ‘browse up’ architecture



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

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

- 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 Public Telecoms Provider and Jersey and hence securing the management plane should be treated as a priority by Public Telecoms Providers. The following guidance 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.[19]

Isolating the management plane

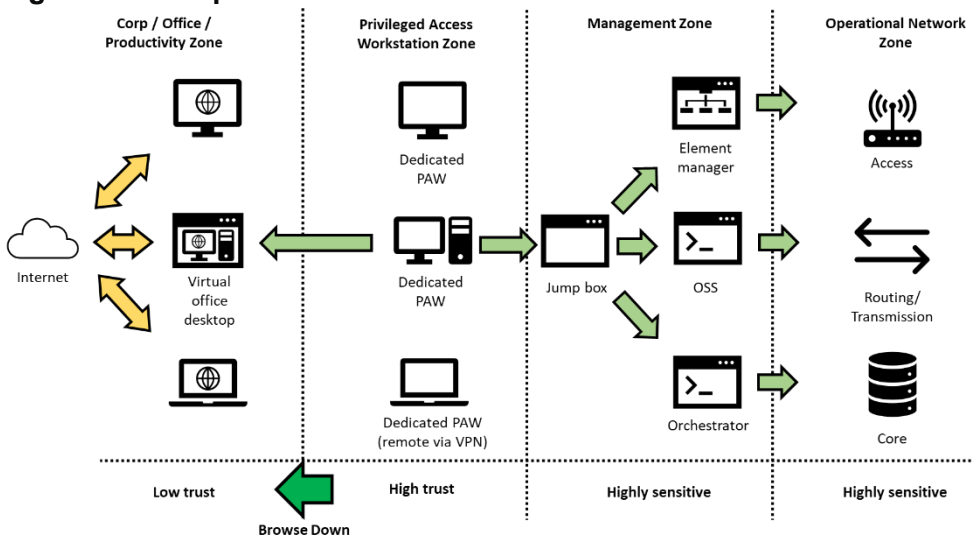
2.16 Given the risks, it is not appropriate for Public Telecoms Providers to be using a 'browse-up' architecture. Instead, Public Telecoms Providers shall architect, and operate, their management plane infrastructure to inhibit network compromise through administrative access.

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 Public Telecoms Providers ensure that anything that can impact the operational network cannot be compromised from the corporate zone.

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

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.

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, Public Telecoms 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.

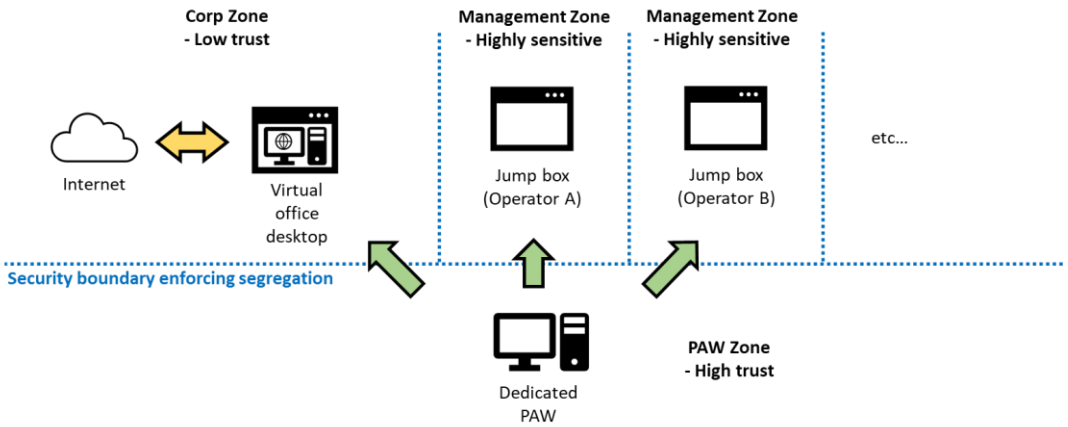
2.25 To protect management platforms (such as jump boxes, element managers, orchestrators, etc) from up-stream attacks from network equipment, the management plane shall be configured to ensure that only necessary connections are allowed. By default, the connections that should be allowed are those established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

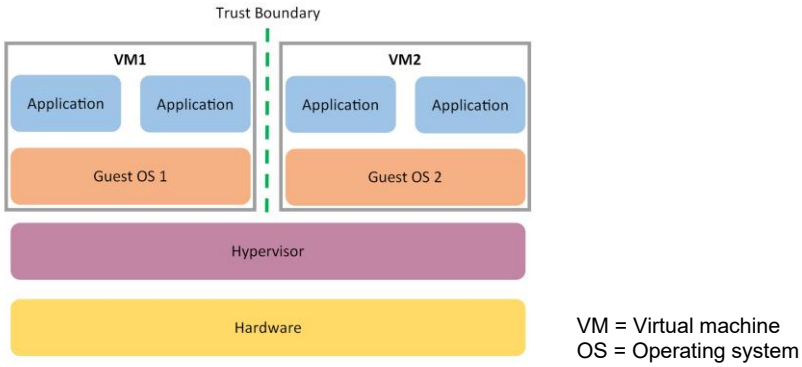
2.33 Prior to the emergence of virtualisation, network functions ran on their own dedicated hardware. Security controls were defined during design, and it was unlikely that these controls would change significantly throughout the equipment's lifetime. Virtualisation allows for greater flexibility. Operationally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

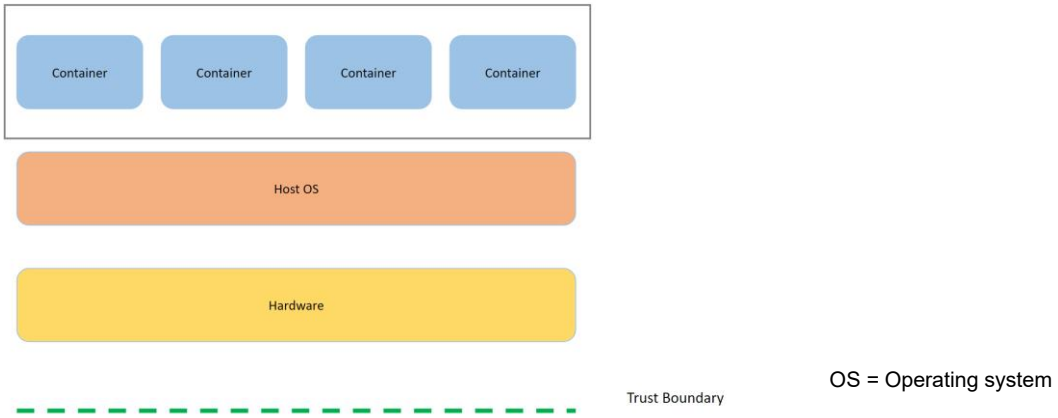


2.36 Virtualisation can be an effective tool for improving the security of a system. By enforcing separation between workloads, it can help prevent lateral movement. By abstracting the hardware, it can allow for better inspection of system behaviour and make the compromise of hardware more complex for 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 Public Telecoms 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 (Figure 6). 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 guidance in this Code of Practice 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[20].

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.

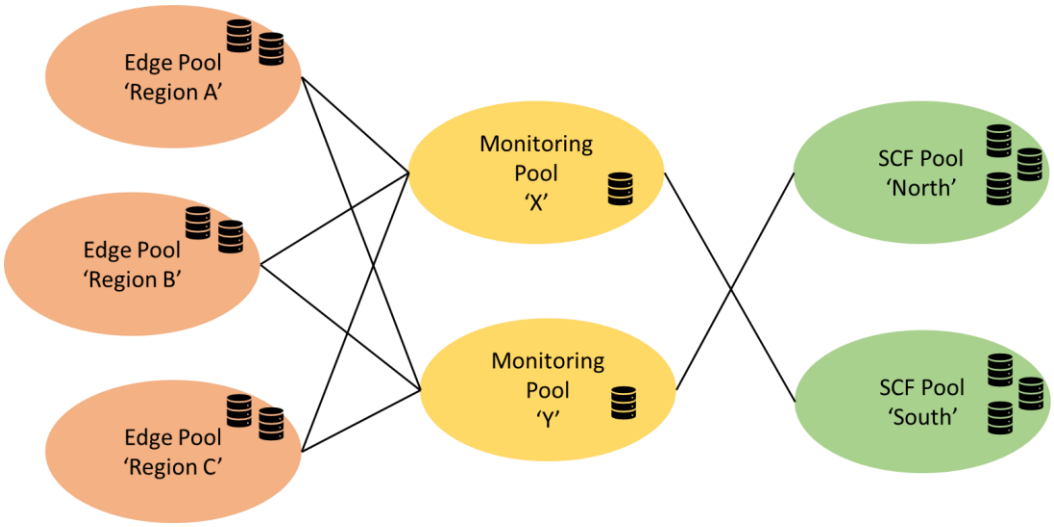
2.43 To limit the impact of host compromise, Public Telecoms Providers should segregate both their virtualisation fabric and the virtual functions supported by that fabric. This

[20] Security design principles and virtualisation (NCSC, 2019)

ensures that the network's security architecture is not undermined by the dynamic nature of the virtualisation.

2.44 For this reason, Public Telecoms 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.

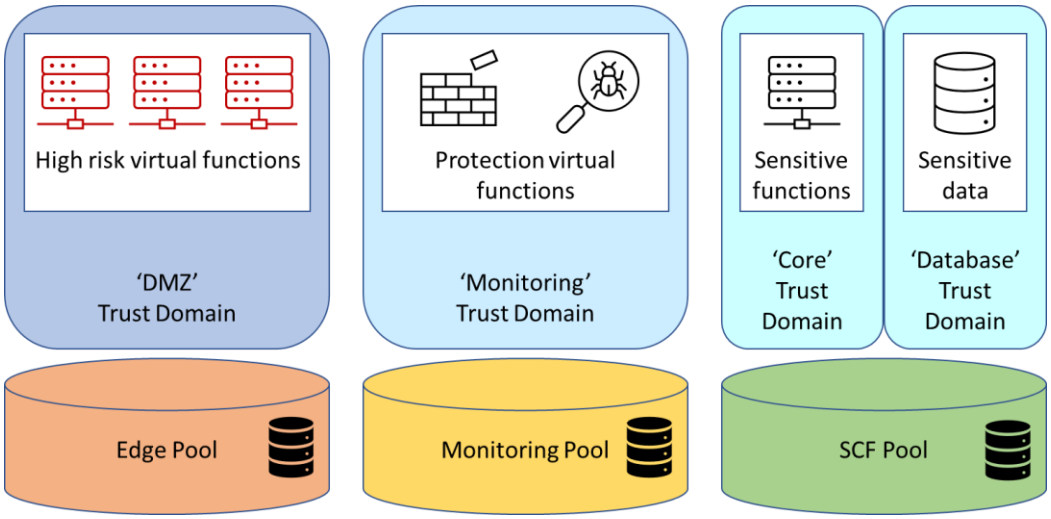
Figure 6: Virtualisation fabric broken into host 'pools'



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'.

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. 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 Public Telecoms Provider need to transfer hosts between host pools, a secure boot process can be used to give confidence to the Public Telecoms 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 Public Telecoms Providers 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 Providers 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 Public Telecoms 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;
- 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;
- 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 Public Telecoms 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 Public Telecoms 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 Providers’ networks connect to each other over signalling networks. These signalling networks allow Public Telecoms 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 which are not within the scope of the security framework and outgoing signalling traffic from a Public Telecoms 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 which arrives over national signalling interfaces (e.g. due to mobile number portability). Signalling from the other Crown Dependencies shall be treated as international signalling.

2.73 Throughout this 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 this Code of Practice highlights the key aspects of signalling plane security for Public Telecoms 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, along with descriptions of their purpose and function. This list is non-exhaustive.

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

Protecting the network

2.77 An attacker may seek to scan the Public Telecoms 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 Public Telecoms Providers network in an attempt to disrupt or compromise the Public Telecoms 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 Public Telecoms Providers' customers are connected to the Public Telecoms Providers' 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 Public Telecoms Providers' customers have roamed onto Public Telecoms Providers' 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 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 Public Telecoms 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, Public Telecoms 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 Public Telecoms Provider 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[21].

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.

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

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.

2.91 Given the increased likelihood of compromise, Public Telecoms 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 Article 3(3)(f) of the Order imposes certain requirements for national resilience. In particular, Article 3(3)(f)(iii) of the Order requires Public Telecoms 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 of the British Islands 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 Public Telecoms Providers' risk assessments under Article 3(3)(a) of the Order.

Guidance

2.93 The resilience of Jersey's national connectivity should be maintained by ensuring that a sustainable and critical level of security expertise, data and equipment are accessible from within the British Islands at all times. Public Telecoms Providers should take appropriate and proportionate measures to ensure they are able to operate Jersey's networks in emergency situations where there may be reduced off-Island connectivity or off-Island travel, and factor this into business plans where they make use of offshored capabilities.

2.94 Whilst Public Telecoms Providers may be unable to maintain 100% of normal service connectivity in the event of loss of off-Island connections, they should be able to restore, secure and run networks to the levels set out in this Code of Practice in the event they lose access to offshored capabilities. In particular, if it becomes necessary to do so:

- Public Telecoms Providers should have the ability to maintain (as relevant, where they provide such forms of connectivity prior to the event) the following Jersey on-Island connectivity for a period of one month in the event of loss of international connections:

- fixed and mobile data connectivity to Jersey peering points;
- on-Island mobile voice; and
- on-Island text-based mobile messaging.

■ Public Telecoms Providers should be able to transfer into Jersey functions required by Jersey 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 Jersey to maintain an operational service, Public Telecoms Providers can consider different scenarios in their business continuity and disaster recovery planning that may be relevant to their decision. These could constitute emergency situations and may include:

1. 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 Public Telecoms Provider's resources in a particular country or global region, and those resources are required to operate the critical services set out above.
2. Compromise of non-British Islands group functions, where functions of a parent group that are located outside the British Islands suffer a security compromise, and those functions are required to operate the critical services set out above.
3. Disruption to connectivity or physical transport links between Jersey and the British Islands and rest of the world, where external factors such as natural hazards or geopolitics limit the ability to access a Public Telecoms Provider's resources outside the British Islands, and those resources are required to operate the critical services set out above.
4. 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 should also seek to ensure a British Islands-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 British Islands;
■ approving procurement decisions on hardware and software for Jersey networks using overseas (non-British Islands) staff;
■ relying on staff, equipment or data based outside the British Islands; 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.

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 Article 4 of the Order to protect data and network functions that could be at risk of security compromises.

3.2 Article 4 of the Order is set out below.

> 4 (1) A network provider must use appropriate and proportionate technical means to –
>
> (a) protect data that is stored by electronic means and relates to the operation of its public electronic communications network, in a way that is appropriate to that data; and
>
> (b) protect functions of its public electronic communications network in a way that is appropriate to those functions.
>
> (2) A service provider must use appropriate and proportionate technical means to –
>
> (a) protect data that is stored by electronic means and relates to the operation of its public electronic communications network, in a way that is appropriate to that data; and
>
> (b) protect functions of the public electronic communications network used to provide the public electronic communications service, to the extent that those functions are under the control of the service provider, in a way that is appropriate to those functions.
>
> (3) In paragraphs (1) and (2), "protect" 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 duties to take appropriate and proportionate measures –
>
> (a) to ensure that workstations through which it is possible to make significant changes to security critical functions are not exposed –
>
> (i) if, 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) if, in the case of a public electronic communications service, the workstation is directly connected to the public electronic communications network through which the service is provided, to signals that are incoming signals in relation to that network; or
>
> (iii) if, in either case, the workstation is operated remotely, to signals other than those that the workstation must 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 a security compromise occurring as a result of incoming signals received in the network or in a network that is used to provide the service; and

(c) to monitor and reduce the risks of a security compromise occurring as a result of the characteristics of any equipment supplied to customers that is used or intended to be used as part of the network or service.

(5) A network provider must use within its public electronic communications network signals that, by encryption, reduce the risks of a security compromise occurring.

(6) A service provider must –

(a) monitor and reduce the risks of a security compromise relating to customers' SIM cards occurring in relation to the public electronic communications network used to provide the public electronic communications service; and

(b) replace SIM cards if it is appropriate to do so in order to reduce the 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 applying to a SIM card any process that permanently replaces an 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).

3.4 Public Telecoms Providers shall apply the NCSC's March 2025 guidance on PAWs. NCSC's guidance sets out principles about how to design and securely build management devices for high-risk system maintenance and administration.[22]

In addition to any current or future NCSC PAW guidance, Public Telecoms Providers should have regard to the ETSI's technical specification: Cyber Security (CYBER); Privileged Access Workstations; Part 1: Physical Device, and any future ETSI technical specifications for PAWs.[23]

[22] *Principles for secure privileged access workstations (PAWS)* (NCSC, 2025)
23 Cyber Security (CYBER); Privileged Access Workstations; Part 1: Physical Device (ETSI, 2024)

3.5 ETSI's guidance covers the PAW device and the technical specification that would ensure the confidentiality of the end user device. Additional documents will cover other aspects of PAWs that can work in conjunction with each other to meet the needs of the overall system architecture and the relevant security aims

SIM security

3.6 The intent of the measures within this Code of Practice is to ensure that an at-scale compromise of SIM cards cannot be used to disrupt Jersey's Public Telecoms Providers, or to impact subscriber confidentiality. Article 4(6) of the Order sets out requirements that Public Telecoms Providers must meet in relation to SIM cards.

3.7 The following background information and guidance highlights the key aspects of SIM security for Public Telecoms Providers to understand and implement, providing examples where appropriate.

Universal Integrated Circuit Cards (UICCs)

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

3.9 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.

3.10 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.

3.11 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;
- vulnerability in SIMs including the use of obsolete or weakly specified algorithms.

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

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

eSIMs

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

3.14 Public Telecoms Providers should ensure they have regard to and apply any guidance or advice about eSIMs published by NCSC or ETSI.

Guidance

3.15 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 Telecoms Providers globally have used the routine changing of SIM cards, form factor changes, or introduction of new services, to churn out older obsolete SIM cards for newer more secure profiles. This practice is to be encouraged to increase the overall security of the SIM population in the network.

3.16 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.

3.17 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.

3.18 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 Providers' network.

3.19 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 Public Telecoms Provider, the Public Telecoms Provider should use certificate-pinning to allow only approved services to make profile modifications.

3.20 Should Public Telecoms 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

3.21 Article 4(5) of the Order requires Public Telecoms Providers to use within the public electronic communications network signals which, by encryption, reduce the risks of security compromises occurring.

Guidance

3.22 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.

3.23 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 IPSec or TLS - detailed information and best practice guidance provided by NCSC can be found on its website.[24] For data-at-rest Public Telecoms 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.[25]

Customer Premises Equipment (CPE)

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

Scope

3.25 In relation to CPE and CPE configuration, the measures in Section 3 of this Code of Practice align with Article 4(4)(c) of the Order and only apply when these devices are supplied to customers by Public Telecoms 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.

[24] *Using IPSec to protect data* (NCSC, 2016) and *Using TLS to protect data* (NCSC, 2021)
[25] *Guide to storage encryption technologies for end user devices* (NIST, 2007)

Background

3.26 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.

3.27 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.

3.28 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 Jersey 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

3.29 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.

3.30 Due to the possibility that exploitation of vulnerabilities in CPE devices could impact the Public Telecoms Provider's network at scale, or impact wider infrastructure, it is in the Public Telecoms Provider's interest to ensure that CPEs remain in support and up to date. Acknowledging that Public Telecoms 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 CPEs 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.

3.31 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.

4. Protection of certain tools enabling monitoring or analysis

4.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 5 of the Order 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 Article 5 of the Order is set out below.

> 5 (1) This Article 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 of the British Islands, the network provider or service provider must take measures to identify and reduce the risks of a security compromise occurring as a result of the tools being stored on equipment located outside of the British Islands.
>
> (3) The network provider or service provider must ensure that the tools –
>
> (a) are not capable of being accessed from a country listed in Schedule 2; and
>
> (b) are not stored on equipment located in any of those countries.

Key concepts for understanding the requirements

Countries listed in the Schedule

4.3 The Schedule 2 to the Order sets out the countries that pose the greatest risk to the security of Public Telecoms Providers. Monitoring and analysis tools of the type described in Article 5(1) of the Order may not be located in these listed countries due to the sensitivity of those tools and the access they provide to management of Jersey's networks and services. Public Telecoms 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 Article 5 of the Order 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 2 to the Order.

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 Schedule 2 to the Order, the Government may look to update the Schedule 2 list. This Code of Practice sets out steps to help Public Telecoms Providers account for any such scenario, including the use of business continuity and disaster recovery plans to cover that risk.

Risk assessment

4.6 Article 5(2) of the Order sets out the need for Public Telecoms 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 British Islands. Written assessments of these risks are addressed under Article 11(b)(ii) of the Order.

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

- security analysis and anomaly detection, including the operation of security operation centres (SOCs);[26]
- network performance and diagnostic analysis, including the operation of network operation centres (NOCs);
- privileged access, where that privileged access grants potential access to real-time network information or the content of transmissions, such as through the interaction with network equipment;
- interaction with network or system probes;
- interaction with the virtualisation fabric;
- access to real-time network orchestration systems or controllers.

4.8 Relevant considerations may include the risk of unauthorised conduct, the risks associated with local laws or their enforcement, or a lack of appropriate understanding of Jersey - 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.

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

5. Monitoring and analysis

5.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 6 of the Order to monitor and analyse the use of their networks in order to identify any security compromises.

5.2 Article 6 of the Order is set out below.

> 6 (1) A network provider must take appropriate and proportionate measures to monitor and analyse access to security critical functions of its 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 appropriate and proportionate measures to –
>
> (a) monitor and analyse the operation of security critical functions of its public electronic communications network or public electronic communications service for the purpose of identifying the occurrence of a security compromise, using automated means of monitoring and analysis where possible; and
>
> (b) investigate any anomalous activity in relation to the network or service.
>
> (3) The duty in paragraph (2) includes a duty to –
>
> (a) maintain a record of all access to security critical functions of the network or service, including the persons obtaining access;
>
> (b) 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) have in place means and procedures for producing immediate alerts of all manual amendments to security critical functions;
>
> (d) analyse promptly all activity relating to security critical functions of the network or service for the purpose of identifying anomalous activity;
>
> (e) 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) take measures to prevent activities that would restrict the monitoring and analysis required by this Article.
>
> (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 that is used or intended to be used as part of its 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 Public Telecoms Provider's environment will permit post-event analysis to be undertaken with significantly more ease and allow Public Telecoms 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 Public Telecoms 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 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 UserID);
- 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].

[27] *NCSC CAF guidance: C.1 Security monitoring* (NCSC, 2019)
[28] *NCSC Introduction to logging for security purposes* (NCSC, 2018)

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. Public Telecoms 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 Public Telecoms Providers 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 Public Telecoms Provider’s network to determine anomalous behaviour.

5.11 What to monitor can only be defined by the Public Telecoms Provider itself 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;
- 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 Public Telecoms Provider’s network and external networks such as customer networks, partner networks, the internet and international telecommunications networks;
- between the Public Telecoms Provider’s network and third-party administrator networks, such as those owned by network equipment suppliers and MSPs;
- between the Public Telecoms 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. Public Telecoms 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

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

be able to afford the network. The necessary network information will likely need to be collated from architectural design documentation, asset management systems, configuration management systems, product and interface specifications, network change plans and change systems (known as tickets).

5.19 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. Public Telecoms 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, Public Telecoms 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 Protocols

5.24 Border Gateway Protocol (BGP) is a signalling protocol which is used to route data between Public Telecoms 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]

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

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 Public Telecoms 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 British Islands Public Telecoms Provider traffic shall be particularly inhibited, and British Islands routes should be monitored for anomalous activity (such as the inclusion of unexpected transit networks). 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 Public Telecoms 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.

5.28 All address space and address space 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 Peering DB. 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 Public Telecoms 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, Public Telecoms 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;
- IXP LANs.

5.31 Accepting routes from unexpected sources could result in the Public Telecoms Providers 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 Public Telecoms 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 Public Telecoms Providers to ensure that they have in place a plan of maintaining Jersey 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 is 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 Public Telecoms 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.

6. Supply Chain

6.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 7 of the Order to identify and reduce the security risk arising from actions taken or not taken by third party suppliers.

6.2 Article 7 of the Order is set out below.

> 7 (1) A network provider or service provider must take appropriate and proportionate measures to identify and reduce the risks of a security compromise occurring in relation to its public electronic communications network or public electronic communications service as a result of an act by a third-party supplier.
>
> (2) 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 its public electronic communications network or public electronic communications service.
>
> (3) A network provider or service provider (the "primary provider") must take appropriate and proportionate measures to –
>
> (a) ensure, by means of contractual arrangements, that each third-party supplier –
>
> (i) takes appropriate measures to –
>
> (A) identify the risks of a security compromise 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;
>
> (B) disclose those risks to the primary provider; and
>
> (C) reduce those risks;
>
> (ii) if the third-party supplier is 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 Article 24K(1) of the Law, in relation to goods, services or facilities supplied, provided or made available by the third-party supplier to the primary provider, that 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 an incident that causes or contributes to the occurrence of a security compromise in relation to the primary provider's network or service or of an increased risk of a compromise occurring;

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

(c) 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.

(4) A network provider must –

(a) ensure that there is in place at all times a written plan to maintain the normal operation of its 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 and amend it if required by the review.

Key concepts for understanding the requirements

Management of third party suppliers

6.3 A supply chain involves contractual arrangements between the Public Telecoms 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]

6.4 Public Telecoms Providers cannot delegate or outsource responsibility for their duties under the Law or the Order to third party suppliers through contractual arrangements. Public Telecoms Providers remain responsible for ensuring compliance with the duties imposed by the Law and Order.

Guidance

6.5 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.

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

6.6 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 Public Telecoms Provider's network. For example, where the Public Telecoms 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.

6.7 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 Public Telecoms Providers 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.

6.8 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 Public Telecoms Providers do outsource aspects of operations to a third party, responsibility to comply with the obligations contained within the Law, and the obligations set out in the Order, remain with the Public Telecoms Provider. The Public Telecoms Provider therefore needs to have sufficient internal capacity to meet those obligations.

Data sharing

6.9 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 supplier's systems may provide an attractive route to obtaining nationally significant datasets. In this context 'data' includes both user data and network data.

Guidance

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

6.11 It is recommended that Public Telecoms Providers establish systems that allow the Public Telecoms Providers to retain its data within its control whenever possible. This allows the Public Telecoms 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 Public Telecoms Provider's corporate and operational systems, ensuring that the data-sharing requirement does not give suppliers wider access to other systems.

6.12 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

6.13 Administrative access presents a significant security risk to electronic communications networks. Public Telecoms 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 Public Telecoms Provider's 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.

6.14 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 networks could be exploited or disrupted simultaneously.

6.15 As an example, in December 2018 the UK 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.

6.16 While both managed service access and third-line support can present a risk to Jersey's 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 Jersey networks almost certainly increases the overall threat of cyber-attack, requiring careful risk management by industry.

6.17 The use of third party administrators also creates a risk due to the dependence of the Public Telecoms Providers 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

6.18 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.

6.19 Public Telecoms Providers should ensure that the third-party administrator is enforcing separation to prevent its network from being connected to another Public Telecoms 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 dataflows and limit any administrative accesses across the boundary. Such controls should be applied even when the third-party administrator is part of the same umbrella company or Public Telecoms Provider group.

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

6.21 In October 2023, the NCSC published supply chain guidance. Broken down into Foundations, Application and Consolidation sections, the NCSC's Supply Chain Guidance sets out essential information, guidance and advice on securing supply chains.[33]

Network equipment suppliers

Guidance

6.22 Public Telecoms 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 highlights the key areas that Public Telecoms Providers need to understand when working with network equipment suppliers, providing examples and background information where appropriate.

[33] Supply Chain Guidance (NCSC, 2023)

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 Public Telecoms Provider is establishing a long-term reliance on the supplier. To some degree, the Public Telecoms Provider is now reliant on the third party supplier to ensure that the Public Telecoms Provider's network stays secure.

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 Public Telecoms Providers to replace equipment as there is a 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 (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 Public Telecoms Providers' networks. This risk includes two types of cyber event:

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

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

6.29 Article 7 of the Order is intended to ensure that third party supplier security and quality is sufficiently valued by Public Telecoms 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 have published advice on how to assess the security of network equipment.[34] The NCSC's Vendor Security Assessment (VSA) provides advice on how Public Telecoms 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.

6.31 The purpose of the approach is for Public Telecoms 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.

6.32 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.

6.33 The VSA will be updated periodically, to keep pace with new threats and technologies. Public Telecoms Providers should ensure they are aware of any relevant updates that are made to the NCSC's VSA advice and access the latest version of the VSA as published on NCSC's website.

6.34 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.

6.35 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.

6.36 Where a third-party supplier does, or omits, something which increases the risk of security compromise, the risk to the Public Telecoms Providers 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

[34] NCSC Vendor Security Assessment

associated with the quantity of equipment or components is manageable given the supplier risk.

The 'Trojan horse' threat

6.37 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.

Management of sites

6.38 Where Public Telecoms Providers have network equipment and facilities within sites that are shared with other Public Telecoms Providers, it is recommended that all Public Telecoms Providers work together to set a consistent set of security measures that meet the Order 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;
- where an existing contract is amended to change the scope or scale of the work it would be new.

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 Article 8 of the Order to prevent the occurrence of security compromises that consist of unauthorised access to their networks or services.

7.2 Article 8 of the Order is set out below.

> (1) A network provider or service provider must take appropriate and proportionate measures to reduce the risks of the occurrence of a security compromise that consists of unauthorised access to its public electronic communications network or public electronic communications service.
>
> (2) The duty in paragraph (1) includes a duty –
>
> (a) to ensure that 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 1 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) if, despite sub-paragraph (d), default credentials have been used, to assume, for the purpose of identifying the risks of a security compromise occurring, that those default credentials are publicly available;
>
> (f) to ensure that information that 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 that the provider does not reasonably believe are safe.
>
> (4) A network provider or service provider must limit, so far as is consistent with the maintenance and operation of its public electronic communications network or the provision of its 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 appropriate and proportionate measures to ensure that each user or system authorised to access security critical functions uses a credential that identifies them individually when accessing those functions;

(c) take appropriate and proportionate measures, 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 its public electronic communications network other 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 its public electronic communications service other than 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 that the provider authorises the person to carry on.

(6) A network provider or service provider must ensure that –

(a) no security permission is given to a person while the person is in a country listed in Schedule 2; and

(b) a security permission cannot be exercised while the person to whom it is given is in in a country listed in Schedule 2.

Key concepts for understanding the requirements

Explaining “access” to the Public Telecoms Provider

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

Application Programming Interfaces

7.4 Application programming interfaces (APIs) underpin a great range of digital functions, and facilitate seamless data exchange between systems and services. NCSC has reported that an increased use of APIs provides attackers with greater opportunities to exploit vulnerabilities within their design and implementation.[35]

[35] New guidance on securing HTTP-based APIs (NCSC, 2025)

7.5 In response to the increased threats NCSC has published guidance on securing HTTP-based APIs. Public Telecoms Providers shall follow the NCSC's guidance when designing or building secure applications that offer an HTTP API.[36]

7.6 Public Telecoms Providers remain responsible for ensuring the security of APIs supplied by vendors and third parties. Public Telecoms Providers should ensure that those supplying APIs and software are aware of and follow NCSC's guidance on securing HTTP-based APIs.

[36] Securing HTTP-based APIs

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 Article 9 of the Order 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 Article 9 of the Order is set out below.

> 9 (1) A network provider or service provider must take appropriate and proportionate measures to prepare for the occurrence of a security compromise, with a view to limiting the adverse effects of any security compromise and enabling the provider to recover from a security compromise.
>
> (2) The duty in paragraph (1) includes a duty –
>
> (a) to create or acquire, for the purposes mentioned in that paragraph, and to retain –
>
> (i) within the British Islands, an online copy of information necessary to maintain the normal operation of its public electronic communications network or public electronic communications service; and
>
> (ii) in Jersey, an offline copy of that information so far as is proportionate;
>
> (b) to replace, with the most recent version, copies held for the purpose of sub-paragraph (a) with reasonable frequency, appropriate to the assessed security risk of its network or service; and
>
> (c) to have the means and procedures in place –
>
> (i) for promptly identifying the occurrence of a 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 a security compromise;
>
> (iii) if 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 to prevent 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 they will take those steps;
>
> (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 a

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 a security compromise 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 a way that ensures it is not exposed to signals conveyed by means of the network or service in question.

Key concepts for understanding the requirements

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

8.3 Article 9(2)(a)-(b) of the Order sets out requirements in relation to the information that Public Telecoms Providers must create or acquire, retain 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, Public Telecoms Providers must hold:

- Within the British Islands a copy of this information on the network or service in question (i.e. an "online copy"); and
- so far as is proportionate, in Jersey 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 Public Telecoms Providers 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 Public Telecoms Providers replace all user data that may have been lost during a security compromise.

Keeping an offline copy

8.5 Article 9(3)(b) of the Order 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.[37] Without a trusted identity, ransomware should not be able to request access to a Public Telecoms Providers' cloud storage and encrypt it without the Public Telecoms Provider's permission.
- Client management - a backup client is a device with credentials to access cloud storage. Cloud backup clients should not have valid credentials while the cloud storage is not in use. The number of backup clients should also be kept to a minimum with standard user devices unable to modify cloud backups directly. If this practice is followed, a ransomware infection can only compromise the cloud backup if it occurs on an authorised client and while the cloud backup is being used.
- Access control - access control should be configured to only allow authorised clients to create new backups (or append to existing ones) and deny connection requests while the storage is not in use ('cold' storage). If a ransomware infection occurs while the cloud backup is offline, it will be denied connection requests. This means it will not be able to reach the cloud storage, giving the same level of confidence as unplugging an on-premises storage drive.
- Back-up plan - some cloud storage services allow a user to restore modified data back to an older version and recover deleted data for a limited time after it was deleted. If ransomware does manage to affect the cloud backup, these features can be used to restore back to the last known-good state.

Recovery

8.7 Backups should be created on a regular basis. The more frequently backups are created, the less data is required to be recovered in the event of an incident. Backups should also be regularly tested to check they allow the data and network to be recovered effectively. For more information, Public Telecoms Providers should refer to NCSC advice on response and recovery planning.[38]

Retention of copies within the British Islands and Jersey

8.8 For resilience and continuity purposes, Article 9(2)(a) of the Order requires Public Telecoms Providers to retain online copies of information within the British Islands which is necessary to maintain the normal operation of the network or service and an offline copy of that information in Jersey. This does not prevent copies being held elsewhere as part of a global business operation.

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

9. Governance

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

9.2 The NCSC has published guidance about how Boards can deliver, communicate and champion strong cyber leadership including a Cyber Security Toolkit for Boards[39], Cyber Governance for Boards[40] and about the key role of culture[41].

9.3 Article 10 of the Order is set out below.

> 10 (1) A network provider or service provider must ensure appropriate and proportionate management of responsible persons.
>
> (2) The duty in paragraph (1) includes a duty to –
>
> (a) establish, and regularly review, the provider's policy as to measures to be taken for the purposes mentioned in Article 24K(1) of the Law;
>
> (b) ensure that the policy includes procedures for the management of security incidents, at varying levels of severity;
>
> (c) have a standardised way of categorising and managing security incidents;
>
> (d) 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) ensure that the policy provides for a post-incident review procedure in relation to security incidents and that the procedure involves consideration of –
>
> (i) the outcome of the review at an appropriate governance level; and
>
> (ii) the use of that outcome to inform future policy; and
>
> (f) 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 responsible persons.
>
> (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.

[39] Cyber Security Toolkit for Boards (NCSC, 2023)
[40] Cyber Governance for Boards (NCSC)
[41] Cyber security culture principles (NCSC 2025)

(4) A network provider or service provider must take appropriate and proportionate measures to identify and reduce the risks of a security compromise 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

9.4 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.

9.5 The following guidance 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

9.6 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.[42][43]

9.7 Article 10(2)(d) of the Order 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 Public Telecoms Providers policies include a way to communicate security issues and risks to the top of the organisation, without risk of dilution.

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

Security and operational changes

9.8 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

9.9 Security incidents that occur within Public Telecoms Providers' networks are not only a learning opportunity for Public Telecoms Providers, but also for the sector as a whole. So far as is appropriate and proportionate, Public Telecoms Providers should share information about significant past issues or compromises with other Public Telecoms Providers via suitable trusted groups. Public Telecoms 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 Public Telecoms Providers on learning from incidents can be found on the NCSC website.[44]

The Cyber Assessment Framework (CAF)

9.10 Public Telecoms Providers should have regard to the CAF in order to ensure that they have appropriate business processes in place.[45] Should any differences arise between the interpretation of the CAF, and the guidance in the main body of this Code of Practice, this Code of Practice shall take precedence.

[44] *NCSC CAF guidance: D.2 Lessons learned* (NCSC, 2019)
[45] *NCSC Cyber Assessment Framework* (NCSC, 2024)

10. Reviews

10.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 11 of the Order to ensure that regular reviews of their security measures are undertaken.

10.2 Article 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 its public electronic communications network or public electronic communications service, taking into account relevant developments relating to the risks of a security compromise occurring; and
>
> (b) undertake at least once in any 12-month period a review of the risks of a security compromise occurring in relation to the network or service and produce a written assessment of the extent of the overall risk of a security compromise occurring within the next 12 months, taking into account –
>
> (i) in the case of a network provider, risks identified under Article 3(3)(a);
>
> (ii) risks identified under Article 5(2);
>
> (iii) risks identified under Article 6(1);
>
> (iv) risks identified under Article 7(1);
>
> (v) risks identified under Article 10(4);
>
> (vi) the results of reviews carried out under sub-paragraph (a);
>
> (vii) the results of tests carried out under Article 14; and
>
> (viii) any other relevant information.

Key concepts for understanding the requirements

Clarifying 'any other relevant information' in Article 11(b)(vii) of the Order

10.3 In undertaking their annual reviews under Article 11(b) of the Order, Public Telecoms Providers must take into account the risks and results listed in Article 11(b)(i)-(vii) of the Order and "any other relevant information" (Article 11(b)(viii) of the Order). This latter category of information may include, for example, 'event correlation analysis' where relevant. This is where security incidents have been identified by Public Telecoms 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.[46] The risk assessment that these Public Telecoms Providers must carry out as a part of the reviews process under Article 11 of the Order should be looking at not only the risks to the Public Telecoms 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.

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

11. Patching and updates

11.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 12 of the Order to deploy patches or mitigations (including software updates and equipment replacement) as well as the necessary security updates and equipment upgrades.

11.2 Article 12 of the Order is set out below.

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

Key concepts for understanding the requirements

Guidance on the appropriate patching period for network equipment

11.3 Article 12(a) of the Order requires Public Telecoms Providers to take appropriate and proportionate measures to deploy any relevant patch or mitigation which becomes available “within such period as is appropriate in the circumstances having regard to the severity of the risk of security compromise which the patch or mitigation addresses”. Figure 9 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 of the threat 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. Public Telecoms 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 Figure 9.

Figure 9: 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 Providers 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 Figure 9), Article 12(c)(i) of the Order requires Public Telecoms Providers to arrange for any such decisions to be taken at an appropriate governance level and recorded in writing. Public Telecoms 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 Public Telecoms 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 Article 12(c)(ii) of the Order.

12. Competency

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

12.2 Article 13 of the Order is set out below for reference.

> 13. (1) A network provider or service provider must take appropriate and proportionate measures to ensure that responsible persons –
>
> (a) are competent to discharge their responsibility; and
>
> (b) are given sufficient resources to enable them to do so.
>
> (2) The duty in paragraph (1) includes a duty to take appropriate and proportionate measures –
>
> (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 Article 6, and are given sufficient 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 risks of a security compromise occurring; and
>
> (ii) are given sufficient resources for that purpose; and
>
> (d) if 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 that 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 risks of a security compromise occurring as a result of the way in which the equipment is set up.

Key concepts for understanding the requirements

In-house competency

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

Guidance

12.4 Where a Public Telecoms Providers is using a third party supplier, in-house staff of that Public Telecoms Providers 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 Telecoms Providers must ensure that those involved in the security and resilience of networks and services have the appropriate level of qualifications and experience necessary to mitigate the risks to networks, services and data. Public Telecoms Providers should put in place and maintain processes for determining and verifying the competency of those involved in network or service security, for example, through registration with the Cyber Security Council.[47]

12.6 Public Telecoms 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.[48]

[47] *UK Cyber Security Council. Professional registration*
[48] *NCSC CAF guidance: B.6 Staff awareness and training* (NCSC, 2019)

13. Testing

13.1 This chapter provides guidance for Public Telecoms Providers on the measures to be taken in accordance with Article 14 of the Order to carry out, or arrange for a suitable person to carry out, appropriate tests.

13.2 Article 14 of the Order 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, tests in relation to the network or service that are appropriate and proportionate for the purpose of identifying the risks of a security compromise occurring in relation to its 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 way in which the tests are to be carried out is not made known to –
>
> (i) the persons involved in identifying and responding to the risks of a security compromise occurring in relation to the network or service; or
>
> (ii) the persons supplying any equipment to be tested; and
>
> (b) that measures are taken to prevent the persons mentioned in sub-paragraph (a) being able to anticipate the tests to be carried out.

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 tester's 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 JCRA.

13.5 An example of this type of testing is Ofcom's TBEST scheme [4950]. In considering threat intelligence-led penetration testing schemes, Public Telecoms Providers should have regard to appropriateness of those schemes and providers.

Tests against equipment locations

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

Guidance

13.7 Testing should ensure that the physical security of the buildings, server rooms and network equipment that provide services into Jersey meet best-practice standards. Advice produced by the National Protective Security Authority (NPSA) should be consulted for physical and personnel-related security.[51]

13.8 This 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.

[49] *Our network security and network resilience work* (Ofcom, 2021)
[50] Jersey's Public Telecoms Providers cannot participate in the TBEST scheme that Ofcom runs in partnership with NCSC, UK Government and UK Public Telecoms Providers. Jersey's Public Telecoms Providers can engage UK providers of TBEST threat intelligence-led penetration testing services.
[51] *Physical security* (NPSA)

14. Assistance

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

14.2 Article 15 of the Order is set out below.

> 15. (1) A network provider or service provider (the "relevant provider") must, so far as is appropriate and proportionate, provide information about a security compromise to another network provider or service provider if –
>
> (a) the security compromise occurs in relation to the relevant provider's public electronic communications network or public electronic communications service; and
>
> (b) it appears to the relevant provider that the security compromise may cause a connected security compromise in relation to the other network or service.
>
> (2) Information provided under paragraph (1) that relates to a particular business must not, without the consent of the person carrying on the business –
>
> (a) be used or disclosed by the recipient, except for the purposes of –
>
> (i) identifying or reducing the risks of a security compromise occurring in relation to the recipient's network or service; or
>
> (ii) preventing or mitigating the adverse effects of a security compromise that has occurred in relation to the recipient's network or service; or
>
> (b) be retained by the recipient any longer than is necessary for those purposes.
>
> (3) A network provider ("network provider A") must, when requested by a service provider or another network provider ("network provider B"), give network provider B assistance that is appropriate and proportionate in the taking by network provider B of a measure required by this Order in relation to anything that –
>
> (a) has occurred in relation to network provider A's public electronic communications network;
>
> (b) is a security compromise in relation to that network; and
>
> (c) could cause a connected security compromise in relation to network provider B's public electronic communications network or public electronic communications service.
>
> (4) A service provider ("service provider A") must, when requested by a network provider or another service provider ("service provider B"), give service provider B assistance that is appropriate and proportionate in the taking by service provider B of any measure required by this Order in relation to anything that –
>
> (a) has occurred in relation to service provider A's public electronic communications service;
>
> (b) is a security compromise in relation to that service; and

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

(5) A network provider or service provider must, if necessary to reduce the risks of a security compromise occurring in relation to the provider's public electronic communications network or public electronic communications service, request another person to give any assistance that paragraph (3) or (4) requires the other person to give.

Key concepts for understanding the requirements

Sharing information

14.3 In certain circumstances it is appropriate for different Public Telecoms Providers to receive information from Public Telecoms Providers serving the British Islands which would help to reduce the risk of security compromises occurring (Article 15(1) of the Order). Whilst not required by Article 15 of the Order, Public Telecoms Providers may also consider whether it is appropriate in certain circumstances to share information with other types of bodies/organisations such as:

- educational institutions;
- UK and Jersey security organisations;
- JCRA;
- JCSC; and
- UK and Crown Dependency government cyber security experts.

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

Guidance

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

Section 3: Technical guidance measures

Specific technical measures to be taken by Public Telecoms 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 Order, including Articles 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 Article of the Order will depend on the facts of each case. The mapping of measures to Articles of the Order in this section is therefore only indicative and non-exhaustive.

The following measures should be completed by 31 March 2027		
Measure number	**Description**	**Relevant Article(s)**
Overarching security measures		
M1.01	Public Telecoms Providers [52] 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)

[52] References to 'Public Telecoms Providers' in section 3 of this Code of Practice are those specified in Schedule 1 of the Order

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 which implement protective measures.	3(3)(c),(d) 3(5) 4(4)(b)
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 Public Telecoms 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 Public Telecoms Provider’s network shall be the responsibility of the Public Telecoms Provider, or another entity that adheres to	3(3)(d) 3(3)(f)(i),(ii)(iii) 3(5) 6(3)(d)

	the Articles, measures and oversight as they apply to the Public Telecoms Provider (such as a third party supplier with whom the Public Telecoms Provider has a contractual relationship with). Where the Public Telecoms Provider or other entity adhering to the Articles 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).	7(4)(a) 8(1) 8(6)

Signalling plane 1

M3.01	Public Telecoms 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	Public Telecoms 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)
M3.03	Public Telecoms 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	Public Telecoms 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, Public Telecoms Providers shall block any incoming message using any source address internal to the Public Telecoms 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	3(3)(e) 4(4)(b),(c) 6(3)(d)

	global titles in SS7) shall not be assumed to be trusted and allowed by default.	
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 Public Telecoms Providers allow others to use numbers ranges that have been allocated to them (e.g. GTs, IMSIs), they remain responsible for the activity related to that number range, and any further security implications. This does not apply in the case of MSISDNs shared through MNP.	3(3)(e) 4(1)(a),(b) 4(4)(b) 6(3)(d)
M3.09	Any outgoing message that uses a source address that should not transit or leave the Public Telecoms Provider's network shall not be permitted to leave the Public Telecoms 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 their charging and accounting principles[53] and Section 10 of their interconnection and interworking charging principles[54].	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 their network or services shall be mitigated in a timely manner, and at least within 12 hours whenever technically possible.	3(3)(e) 4(4)(b) 6(3)(a),(d) 8(1)
M3.13	Public Telecoms 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	3(3)(e)

[53] GSMA PRD BA27, Charging and Accounting Principles - Section 5

[54] GSMA IN.27, Interconnection and Interworking Charging Principles - Section 10

	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.	4(1)(a)(b) 4(2)(a)(b) 15(5)
M3.15	Public Telecoms 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	Public Telecoms 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 Public Telecoms Provider shall share such details, as are appropriate and proportionate, of any BGP misuse with other Public Telecoms 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 Public Telecoms Providers 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 Public Telecoms Provider shall ensure the risks included in Article 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)
M4.02	During procurement of equipment, prior to contract award, it is recommended that Public Telecoms Providers should, as a minimum, use the guidance contained in NCSC’s vendor security assessment to	3(3)(a),(b),(d),(e) 3(5) 7(1) 7(4)(a)(i) 10(1)

	assess third party suppliers (See NCSC published advice).	10(2)(a)(b) 10(4) 13(2)(d)(i),(ii) 14(1)
M4.03	The Public Telecoms Provider shall record all equipment that remains in use but has reached the vendor's end-of-life date. Public Telecoms 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 Public Telecoms 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 Public Telecoms Provider shall record all risk management processes undertaken. Guidance on risk management processes can be found on the NCSC website[55].	3(1) 7(1) 7(4)(c) 7(5) 11
M4.06	Public Telecoms 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	Public Telecoms 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	Public Telecoms Providers shall phase out the use of SIMs that present an unmitigable security risk, such as the use of deprecated security algorithms.	4(6)(b)

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

Supporting business processes

M5.01	The Public Telecoms Provider shall implement appropriate business processes. In order to achieve this, Public Telecoms Providers shall have regard to implementing the parts of the CAF which define the Public Telecoms Provider's business processes.	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	Public Telecoms Providers shall maintain read only backups of their infrastructure and information and shall be able to restore them. The backup should be sufficient to resume normal 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	Public Telecoms 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	Public Telecoms 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 Public Telecoms 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)
M5.06	For significant incidents, Public Telecoms	15(1),(2),(3),(4)

	Providers shall share the high-level lessons learned with other Public Telecoms Providers, so far as is appropriate and proportionate.	
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 2027		
Measure number	**Description**	**Relevant Article(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 Public Telecoms 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 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 Public Telecoms Provider's network. For example,	3(3)(e) 3(3)(f)(i) 4(4)(b) 6(1) 6(3)(d) 8(3) 8(6)

	GSMA CAT 1 messages[56] shall be blocked for SS7 networks, and equivalent messages shall be blocked for other signalling protocols such as Diameter[57], GTP[58] Interconnect[59] and SS7/SIGTRAN[60].	
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	Public Telecoms Providers shall have in place the means for recipients of their BGP routing updates to validate 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, Public Telecoms 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, Public Telecoms 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, Public Telecoms Providers shall ensure negative testing and fuzzing of	3(3)(a),(b),(d),(e) 3(5) 7(1)

[56] *FS.11 SS7 interconnect security monitoring and firewall guidelines* (GSMA, 2019)
[57] *FS.19 DIAMETER interconnect security* (GSMA, 2019)
[58] *FS.20 GPRS tunnelling protocol (GTP) security* (GSMA, 2019)
[59] *FS.21 Interconnect Signalling Security Recommendations* (GSMA, 2019)
[60] *FS.07 SS7 and SIGTRAN Network Security* (GSMA, 2017)

	equipment interfaces has been performed.	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 Public Telecoms Provider if it is repeatable, performed independently of the network equipment supplier and is clearly applicable to the Public Telecoms 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)
M8.04	Public Telecoms 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	Public Telecoms 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	Public Telecoms 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, Public Telecoms 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	Public Telecoms 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	Public Telecoms 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, Public Telecoms Providers risk assessment shall include the risk due to the loss of	3(3)(a),(e) 4(6) 7(1) 7(4)(a)(i)

	sensitive SIM card data.	7(4)(b) 8(5)(a) 8(6) 11
M8.10	When transferring the Public Telecoms 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 Public Telecoms 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 Public Telecoms 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)
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, Public Telecoms 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.[61]	4(6) 7(1)
M8.15	For profile-modifiable SIM cards the Public Telecoms 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. Public Telecoms 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 Public Telecoms Provider's	4(6)(a),(b)

[61] *Security accreditation scheme (SAS)* (GSMA, 2021)

	control, the Public Telecoms 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).	

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 Public Telecoms Provider shall ensure that all CPEs provided to customers are still supported by the network equipment supplier. For any Public Telecoms Provider - provided CPEs 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 Public Telecoms 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)

The following measures should be implemented on all new contracts after 31 March 2027 (and on all contracts by 31 March 2029		
Measure number	**Description**	**Relevant Article(s)**
Third party supplier measures 3		
M10.01	The Public Telecoms Provider shall maintain records of third party supplier's details, including their third-parties and the major components which are used in the provision of goods/services/facilities for the Public Telecoms Provider.	7(1) 7(4)(a)(i)
M10.02	The Public Telecoms 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 Public Telecoms Provider and third party suppliers.	7(1) 7(4)(a) 9(1) 9(2)(c)(ii),(iv),(vi)
M10.04	The Public Telecoms 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	Public Telecoms 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 Public Telecoms Provider shall define what information is made accessible to any third party supplier, ensuring that it is the minimum necessary to fulfil their function. Public Telecoms 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 Public Telecoms Provider's environment that is used to hold and make the network and user data available to the third party shall be	3(3)(a),(d) 3(5) 4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(iii)

	secure and segregated from the Public Telecoms Provider's wider systems and data.	7(4)(b)
M10.08	Public Telecoms 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
M10.09	Where network or user data leaves a Public Telecoms Provider's control, Public Telecoms Providers 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 Public Telecoms 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, Public Telecoms 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
M11.11	Public Telecoms Providers shall contractually oblige third party suppliers to notify the Public Telecoms 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 occurring. 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	Public Telecoms Providers shall contractually require third party suppliers to support the Public Telecoms Provider in investigations of incidents which cause or contribute to the occurrence of a security compromise in relation to the primary Public Telecoms 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	Public Telecoms 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 British Islands 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 Public Telecoms Providers 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 Public Telecoms Provider shall have a break clause with the third party supplier to allow exit from the contract without penalty.	7(4)(c)
M10.16	Public Telecoms Providers shall contractually require third party suppliers to support, as far as appropriate, any security audits, assessments or testing required by the Public Telecoms Providers in relation to the security of the Public Telecoms 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	Public Telecoms Providers shall flow down appropriate security measures to the third party administrator. Public Telecoms Providers shall ensure that the third party administrator applies controls that are at least as rigorous as the Public Telecoms Provider's when the third party administrator has access to the Public Telecoms Provider's network or service or to sensitive data.	7(3)(a) 7(3)(b) 7(4)(a)(i),(ii)
M10.18	The Public Telecoms Providers 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	Public Telecoms 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	Public Telecoms 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	Public Telecoms 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	Public Telecoms 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 Public Telecoms 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	Public Telecoms Providers shall implement and enforce security enforcing functions at the boundary between the third party administrator network and the Public Telecoms Providers network.	3(1)(a),(b),(c) 4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 7(4)(b)
M10.24	Public Telecoms Providers shall contractually require that the third party administrators implement technical controls to prevent one provider or their network from adversely affecting any other Public Telecoms Providers or their network.	4(1) 4(2) 7(1) 7(4)(a)(i),(ii) 7(4)(b) 9(2)(c)(iii),(v)
M10.25	Public Telecoms 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)
M10.26	Public Telecoms Providers shall contractually require that the third party administrators implement separation between third party administrator management environments used for different Public Telecoms Providers networks.	4(1)(a),(b) 4(2)(a),(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)

M10.27	Public Telecoms 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 Public Telecoms Provider's network.	4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
M10.28	Public Telecoms 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 Public Telecoms Provider.	4(1)(a),(b) 4(2)(a),(b) 4(4)(b) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
M10.29	Public Telecoms Providers shall contractually require that the third party administrators implement logically-independent privileged access workstations per Public Telecoms Provider.	4(4)(a) 7(1) 7(4)(a)(i),(ii) 7(4)(b)
M10.30	Public Telecoms Providers shall contractually require that the third party administrators implement independent administrative domains and accounts per Public Telecoms Provider.	7(1) 7(4)(a)(i),(ii)
M10.31	Public Telecoms Providers shall ensure that the elements of the Public Telecoms Provider's 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	Public Telecoms 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 Public Telecoms Provider shall contractually require the third party administrator to monitor and audit the activities of the third party administrator's staff when accessing the Public Telecoms 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 Public Telecoms Provider shall contractually require from the third party administrator all logs relating to the security of third party administrator's network to the extent that such logs relate to access into	6(1) 6(2)(a),(b) 6(3)(a) 7(4)(a)(iii),(iv) 8(5)(d)(i),(ii)

	the Public Telecoms Provider's network.	9(1) 9(2)(c)(iv),(v)
M10.35	Public Telecoms Providers shall require that the third party administrator networks that could impact the Public Telecoms Provider undergo the same level of testing as the Public Telecoms Provider applies to themselves (as set for the Public Telecoms Provider by JCRA from time to time).	7(4)(a)(i),(iii) 14(1) 14(2)
M10.36	Public Telecoms 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), and Public Telecoms 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	Public Telecoms 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), Public Telecoms 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	Public Telecoms 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	Public Telecoms Providers shall contractually require network equipment	3(3)(a),(b) 3(4)

	suppliers to supply up-to-date guidance on how the equipment should be securely deployed.	7(1) 7(3)(a),(b) 7(4)(a)(i),(iv) 7(4)(c) 12(a) 13(2)(d)(i),(ii)
M10.42	Public Telecoms 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)
M10.43	Public Telecoms 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 Public Telecoms Provider's particular usage of equipment, Public Telecoms Providers shall contractually require third party suppliers to remediate all security issues that pose a security risk to a Public Telecoms 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	Public Telecoms Providers shall record where third party suppliers fail to meet these security obligations.	7(4)(iii)(iv)
M10.46	Public Telecoms 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	Public Telecoms Providers shall	3(3)(a),(b)

	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(4) 7(1) 7(4)(a)(i) 7(4)(c) 12(a) 12(c)(i),(ii)
M10.48	Public Telecoms 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	Public Telecoms 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	Public Telecoms 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	Public Telecoms 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
M10.52	Public Telecoms 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 Figure 9). 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, Public Telecoms 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	Public Telecoms Providers shall ensure that network equipment continues to meet the requirements in 9.05, 9.06, 9.07, 10.14 and 14.13 throughout its lifecycle including after an upgrade or patch.	7(4)(c) 7(5) 12
M10.54	The Public Telecoms Provider shall verify	4(4)(c)

	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.	7(4)(a)(i) 12

The following measures should be completed by 31 March 2029		
Measure number	**Description**	**Relevant Article(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 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	8(4) 8(5)(a),(e)

	once privileged access is no longer required.	
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 Public Telecoms Provider's risk management processes.	8(5)(a),(b),(e) 8(6)(a),(b)
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	3(3)(d)

	shall be via a centralised element manager or equivalent config deployment system. For example, privileged users shall not be provided with direct access to any management terminal, except where network connectivity is not available (e.g. break-glass situations).	3(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 12.24.	3(3)(d) 3(5) 6(3)(d) 8(2)(f) 8(4) 8(5)(a),(e)
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 their administrative functions and their 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 Public Telecoms 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 Public Telecoms Provider's 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
M11.28	Security critical patches shall be applied to PAWs within 14 days.[62] 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 British	3(3)(c) 8(6)

[62] Unlike the patching of network equipment, patching of PAWs is a standard enterprise function which does not require additional time as described in Figure 9.

	Islands.	
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)
M12.04	Public Telecoms 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	3(3)(a)(iv) 3(3)(c),(d),(e)

	data provided over an external signalling interface (This applies to all equipment which this measure applies to, including existing equipment). The Public Telecoms 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)(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.[63]	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)
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)

[63] 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 by Figure 9.

M13.05	Modification of databases and systems that define the operation of the network shall require two authorised-person sign-off.	3(1)(a),(b),(c) 3(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 Public Telecoms 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.[64]	3(1)(a),(b),(c) 3(3)(d),(e) 4(1)(a),(b) 4(2)(a),(b) 4(5)
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	3(3)(d) 3(5)

[64] *Using TLS to protect data* (NCSC, 2021)

	signed prior to use. The specific trust domain shall be based on the risks associated with the workload.	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, Public Telecoms 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)

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 Public Telecoms 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 Public Telecoms 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 Public Telecoms 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)

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, Public Telecoms 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 Public Telecoms 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 Figure 9). 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 a network oversight functions shall be rebuilt from an up-to-date known-good software	3(3)(a),(d),(e) 4(1)(b) 4(2)(b)

	state every 24 months. This includes the operating system and application software. This can be performed in line with a system upgrade.	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 Public Telecoms 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)
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	3(3)(a),(d),(e)

	network oversight functions shall be isolated from other internal and external networks, including the management plane used by other equipment.	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)
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	Public Telecoms 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	8(2)(a) 13(2)(a),(b),(c) 14(1)

	supplier.	
M16.02	Public Telecoms 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	Public Telecoms 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)
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	Physical and logical interfaces between networks that operate at different trust levels shall be monitored, and between groups of network functions (e.g. core networks and access networks).	3(3)(a) 4(1)(b) 4(2)(b) 5(2) 5(3) 6(2)(a),(b) 6(3)(a),(b),(c),(d),(e),(f) 6(4) 9(1) 9(2)(c)(i),(v)
M16.07	Systems that collect and process logging and monitoring data shall be treated as	3(3)(a),(d) 3(5)

	network oversight functions.	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)
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 Public Telecoms Providers' network as well as other pertinent data needed for understanding log entries.	6(1) 6(2)(a),(b) 6(3)(e) 9(2)(c)(i),(iv)
M16.16	Network equipment configurations shall be	3(3)(e)

	regularly and automatically collected and audited to detect unexpected changes.	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 5 minutes) and generate security relevant events.	4(4)(b) 5(1)(a) 6(1) 6(2)(a),(b) 6(3)(c),(d),(e) 9(2)(c)(i),(iv) 11(a)
M16.19	The Public Telecoms 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	Public Telecoms 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 2030		
Measure number	**Description**	**Relevant Article(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 Public Telecoms 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)
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 Public Telecoms 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)

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 2 of the Order.	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 Public Telecoms Provider under Article 3(3)(f) of the Order should normally include ensuring, so far as is reasonably practicable, that the equipment performing Public Telecoms Provider's network oversight functions is located within the British Islands, and operated using British Islands-based staff.	3(3)(f)(i)
M21.03	The Public Telecoms Provider shall retain a British Islands-based technical capability to provide subject matter expertise on the	3(3) 13(1)

	operation of the Public Telecoms Provider's Jersey networks and the risks to the Public Telecoms Provider's Jersey networks.	
M21.04	Where data is stored offshore, the Public Telecoms 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 Public Telecoms 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 British Islands data relating to more than 1000 Jersey 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)
M21.06	If it should become necessary to do so, the Public Telecoms Provider shall have the ability to maintain (as relevant, where it provides such a form of connectivity prior to the event) the following Jersey network connectivity for a period of one month in the event of loss of off-Island connections: fixed and mobile data connectivity to Jersey peering points; on-Island mobile voice; and on-Island text-based mobile messaging.	3(3)(f)(iii) 5(2)
M2.07	If it should become necessary to do so, the Public Telecoms Provider shall be able to transfer into Jersey functions required by Jersey networks to maintain an operational service, should off-Island bearers fail.	3(3)(f)(iii) 5(2)

Annex - Glossary of terms

The terms listed below are used throughout this 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, and Passive Optical Network (PON) .
Asset	Anything of value, financial or otherwise, that is required to enable the operations of an organisation.
Authentication, Authorisation, and Accounting (AAA)	A security framework used to control and track user access to computer networks and resources. **Authentication - v**erifies the identity of a user or device attempting to access a network or resource, typically through a username and password. **Authorisation - d**etermines what resources or actions a user or device is allowed to access after successful authentication. **Accounting** - tracks and logs user activity, including resource consumption and access times, for auditing and billing purposes. Common AAA protocols include RADIUS, TACACS+, and Kerberos
Bare Metal Hypervisor	Another name for a Type 1 hypervisor, so called as it does not run on top of a hosts operating system but on the “bare metal” of the hosts hardware.
Break Glass	A method of bypassing normal access controls to gain access to a system or service in an emergency. Break-glass accounts are often a type of high-risk access, granting full access to critical systems, for example, administrator accounts for identity providers or root accounts for cloud services. Root accounts for individual devices are not generally

	considered break-glass accounts
British Islands	"British Islands" is defined in the UK's Interpretation Act 1978 and Interpretation (Jersey) Law 1954 as "the United Kingdom, the Channel Islands and the Isle of Man".
Business Continuity and Disaster Recovery Planning	The process of creating systems of prevention and recovery to deal with potential threats.
Container	Software that packages up code and all its dependencies so the application runs efficiently and reliably from one computing environment to another.
Containerisation	The running of multiple containers on a single system. The host system is providing the separation between these containers. As a hypervisor is not used, a container is not a security boundary.
Core nodes	The main network elements that processes data and store information
Corporate Security Domain	A system or group of systems that all have the same level of security which protects the Public Telecoms 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)	The Customer Premises Equipment provided and managed by the Public Telecoms Provider to the customer. This excludes consumer electronic devices such as mobile phones and tablets, but does include devices such as edge firewalls, SD-WAN equipment, and fixed wireless access kit.
Cyber Assessment Framework (CAF)	The CAF provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible. NCSC CAF guidance - NCSC.GOV.UK
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.

Exposed Edge	Equipment that is either within customer premises, directly addressable from customer/user equipment, or is physically vulnerable. Physically vulnerable equipment includes mobile base sites, equipment in road-side cabinets or attached to street furniture.
Externally-Facing Interface	Any system interface which is accessible to people or systems outside of the Public Telecoms Provider's direct control.
Externally-Facing System or Service	Any system or service with an externally-facing interface.
Fixed-Profile SIM	A Subscriber Identity Module Card where the credentials used to authenticate access to the network cannot be modified.
Fuzzing	An automated software testing technique that involves providing invalid, unexpected, or random data as inputs to assess a system's vulnerability to them.
The Global System for Mobile Communications (GSM)	A digital mobile network that is widely used by mobile phone users in Europe and other parts of the world.
Hardening	The process of securing a system by reducing its attack surface
Home Location Register (HLR)	A database containing pertinent data regarding subscribers authorised to use a global system for mobile communications (GSM) network. Including their last known location and service they are allowed to use.
Host-based sensors	Piece of code installed in a computer or other devices to collect and forward information on system activity.
Hub signalling address	The parts of the network which need to communicate with other Public Telecoms Providers (e.g. for roaming or number portability).
Insecure Protocols	An insecure protocol should be considered to be any protocol that is unencrypted, deprecated or proprietary security protocols. 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 Public Telecoms Provider's direct control.
Jersey Cyber Security Centre	Jersey's technical authority for cyber threats.
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.
Major components	Assets that can have a material impact on the proper operation of the entire network or service, or a material part of it.
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'. A malformed signalling message would either not meet a recognised standard such as FS11 and FS19; be longer or shorter than it should be; could be an internal type message arriving at an external interface and/or would fail to meet FS11 and FS19.
Management Access	Access to control or modify the operation of a device or network.
Management Networks	A collective term for systems that are responsible for the network management
Management Plane	The interfaces and connectivity and supporting equipment that allows Network Equipment to be managed.
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.

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.
Multi Factor Authentication (MFA)	An authentication method that requires the user to provide two or more verification factors to gain access to a resource
Multi-Service Access Node (MSAN)	A device which connects customers' telephone lines to the core network, to provide telephone, ISDN, and broadband, all from a single platform.
Mobile Switching Centre (MSC)	The MSC connects calls between subscribers by switching the digital voice packets between network paths. It also provides information needed to support mobile subscribers services that the home location register has given access to.
National Cyber Security Centre (NCSC)	The UK's technical authority for cyber threats. It is part of the Government Communications Headquarters (GCHQ). The NCSC provides advice to the Crown Dependencies.
National Protective Security Authority (NPSA)	The UK's Technical Authority for physical and personnel security. As part of the Security Service, MI5, we make the UK more resilient to terrorism and state threats.
Negative Testing	The process of validating the application against invalid inputs. Invalid data is used in testing to compare the output against the given input and results monitored for potential vulnerabilities.
The GSMA's Network Equipment Security Assurance Scheme (NESAS)	An industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry.
Network and Information Systems Regulations (NIS Regulations)	These UK regulations provide legal measures to protect UK essential services and infrastructure by improving the security of their network and information systems and maturing their resilience.
Network-based sensors	A component installed in a network to collect and forward information on system activity.
Network Data	The network identifiers, logs, documents that help to describe the network and the

	equipment in the network
Network equipment	Includes hardware, software and firmware that is used to provide the network or service
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 Public Telecoms Provider to understand the network, secure the network, or to recover the network.
Network Function Virtualisation	A way to virtualize network services, such as routers, firewalls, and load balancers, that have traditionally been run on proprietary hardware.
Optical Line Terminal (OLT)	The endpoint hardware device in a passive optical network
Privileged Access / Administrative Access	An access to network equipment where greater capabilities are granted than a 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 which is able to make changes to security critical functions via a management plane.
Privileged User / Administrator	A person who is granted privileged access, through their role, access and credentials, or through any other means.
Profile-Modifiable SIM	A SIM card where the SIM profile credential used to authenticate access to the network can be modified or deleted, or where new SIM profiles and credentials may be added. 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.

Scanning the wider network	Only the appropriate ports should be available on any component. The Public Telecoms Provider should ensure that all other ports are closed. Similarly, all protocols should be unavailable except for those specifically required by the Public Telecoms Provider. Scanning should flag any of these which are available and unless specifically recorded as required, these must be shut down immediately as they are unnecessary and present a risk to security.
Software Defined – Wide Area Network (SD-WAN)	A virtual WAN architecture that allows enterprises to leverage any combination of transport services to securely connect users to applications.
Secure Channel	A communications flow which is encrypted using industry best practice such as TLS 1.2, SSHv2, or IPsec with industry best practice cipher suites. This is not an exhaustive list and is constantly evolving.
Security Analysis	Considering data or information with the intent of detecting a threat actor or understanding the behaviour of a threat actor. Used to determine mitigating actions.
Security Critical Function	A 'Security Critical Function' in relation to a telecoms provider 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. For clarity, services shall include, but are not limited to, encryption. For example, dependent upon network architecture, a small cell, could be considered a Security Critical Function if its failure has a material impact on network capacity or coverage. Automation functionality that has the ability to influence the confidentiality, integrity and/or availability of the network should be considered as a NOF and SCF.
Security failings	Security failings refer to instances where security measures fail to protect systems, data, or networks from unauthorised access, use, or attacks. These failings can

	result from various factors, including inadequate security controls, outdated software, or human error.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Sensitive Data	In relation to a public electronic communications network or a public electronic communications service, means (a) data which controls, or significantly contributes to, a security critical function, or (b) data which is the content of a signal.
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 Public Telecoms Provider-defined identity, credential, algorithms, parameters and applets stored on the SIM card.
Signalling System No7 (SS7 or CCITT #7)	A telecommunications signalling architecture traditionally used for the set up and clear down of telephone calls and services in fixed or mobile telecommunications networks.
Text-based mobile messaging	Messages sent using the Short Message Service (SMS) on mobile devices.
Third party administrators (3PA)	Managed service providers, Public

	Telecoms Provider group functions, or external support for third party supplier equipment (e.g. third-line support function).
Transport Layer Security (TLS)	A widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet.
Trusted Platform	A secure platform which has the characteristics defined in https://www.ncsc.gov.uk/information/secure-by-default-platforms - 22 September 2016
Trusted Platform / Trusted Computing Platform	A platform that uses roots of trust to provide reliable reporting of the characteristics that determine its trustworthiness.
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.
Trust levels	Where all the devices at the same level have the same standard of security, integrity and availability.
Trustworthy	Reliable and of good reputation. The Vendor Security Assessment outlines expected good practice and operators should also consider whether it is appropriate to source services or personnel from countries who regard the British Islands as an adversary
UICC	Any physical card SIM-like credential allowing network access, including permanently soldered-in UICCs in some

	handsets and IoT devices. (An eSIM does not require a UICC)
Up-to-date known-good software state	A piece of software that is proven to be current, supported and unmodified from the agreed standard
Third party supplier Equipment or Network Equipment	Either software or hardware component of the Public Telecoms Provider's network that transmits or receives data or provides supporting services to components of the Public Telecoms Provider's network that transmit or receive data. Includes both virtual machines and physical hardware.
Vendor's End-Of-Life Date	The end of the vendor's standard, global support for the equipment. The point at which no further security patches will be provided.
Virtualisation "Cut-Through" and Paravirtualization	Paravirtualization is when specific guest OS kernel modifications are made to replace non-virtualizable instructions with hypercalls that communicate directly with the virtualisation layer hypervisor. The hypervisor also provides hypercall interfaces for other critical kernel operations such as memory management, interrupt handling and time keeping). These are often referred to as "cut-throughs".
Virtualisation Administrators	Administrators who are granted privileged access to virtualisation infrastructure (NFVi), or the functions which manage virtualisation infrastructure.
Virtualisation Fabric	The physical servers and networking equipment used to provide the resources for virtualised workloads to run on.
Virtual LAN (VLAN)	Any broadcast domain that is partitioned and isolated in a computer network at the data link layer.
Virtual Extensible LAN (VXLAN)	A network virtualisation technology that attempts to address the scalability problems associated with large cloud computing deployments.
Wide Area Network (WAN)	A data network that extends over a large geographic area for the primary purpose of computer networking.