Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

010 – Diversity, Resilience and Continuity v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services. They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

The ECSM Working Group convened on the, 3rd, 4th and 5th November 2020 to discuss matters concerning vendor diversity including Open RAN. The group heard presentations from experts and held focussed discussions on the risks, challenges and best practices associated with vendor diversity and Open RAN. This workshop was followed by a call for inputs to participating operators. ECSM 010 – Diversity, Resilience and Continuity has been developed by the NCSC informed by those meetings and the responses to the call for inputs

3 Scope

The ECSMs are applicable to all undertakings providing public Electronic Communications Networks and publicly available Electronic Communications Services.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
ENISA	Supplement to the technical guideline on Security Measures under the EECC
ENISA	Technical Guideline on Security Measures under the EECC
ISO/IEC 22301:2019	Security and Resilience - Business Continuity Management Systems – Requirements
ISO/IEC 22313:2020	Security and resilience — Business continuity management systems — Guidance on the use of ISO

	22301
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27002:2013	Information technology — Security techniques — Code of practice for information security controls
NIST SP 800-34	Contingency Planning Guide for Federal Information Systems
NIST SP 800-53 R4	Security and Privacy Controls for Federal Information Systems and Organizations

5 Definitions, Symbols and Abbreviations

5.1 Definitions

Term	Meaning
Access Network	A collection of network entities and interfaces that provide the underlying transport connectivity between end user devices and the core network.
Business Continuity plan	The documentation of a predetermined set of instructions or procedures that describe how an organisation's business processes will be sustained during and after a significant disruption.
Core Network	The central element of an Electronic Communications Network that provides services to customers who are connected via the access network.
Critical or Sensitive Location	A network site that is critical to the integrity and security of a significant proportion or the complete network or hosts sensitive data. Such sites may be identified by a site or site category risk assessment.

Critical Remote Installations	Important sites that need to be protected - transmission nodes (mobile), exchange (fixed). Such sites may be identified by a site or site category risk assessment
Critical Security Vulnerability	A vulnerability that could allow remote code execution without user interaction or where code executes without warnings or prompts
Diversification Strategy	The documentation outlining the operator's plans and mitigating actions to address the risks associated with a dependency on a single supplier.
EU Risk Assessment	EU coordinated risk assessment of the cybersecurity of 5G networks report published jointly by the EU Member States on 09th October 2019
Important Security Vulnerability	Vulnerabilities where the client is compromised with warnings or prompts and whose exploitation could result in compromise of data
Interoperability	The ability of two or more networks, systems, devices, applications, or components to communicate and effectively function.
Managed Service Provider (MSP)	A third-party that helps to run or administrate a network.
Network equipment	Software or hardware component of the operator's network that transmits or receives data or provides supporting services to components of the operator's network that transmit or receive data. Includes both virtual machines and physical hardware.
Operator	An undertaking providing or authorised to provide a public electronic communications network or an associated facility;

Operator of Essential Services	A person designated as an operator of essential services under Regulation 12 of European Union (Measures for a High Common Level of Security of Network and Information Systems) Regulations 2018
Resilience	The ability of a network to continue to operate, possibly at reduces capability, while under attack or in the case of network element failure, and to rapidly recover full operational capabilities for essential functions after the event.
Security Incident	An event having an actual adverse effect on the security of electronic communications networks or services.
Supplier Monoculture	A supplier monoculture occurs when a large fraction of the operator's network equipment is sourced from the same supplier creating a critical dependency on that supplier.
Undertaking	A person engaged or intending to engage in the provision of electronic communications networks or services or associated facilities.

33 ## 5.2 Symbols

34 Nil

35 ## 5.3 Abbreviations

Term	Meaning
3GPP	Third Generation Partnership Project
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
ComReg	The Commission for Communications Regulation

DECC	The Department of Environment, Climate and Communications
ECSM	Electronic Communications Security Measure
EEA	European Economic Area
EECC	European Electronics Communications Code.
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDPR	General Data protection Regulation
MNO	Mobile Network Operator
MSP	Managed Service provider
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
RAN	Radio Access Network

6 Overview of Risk

Increasingly modern economic and societal functions are dependent on the resilience & availability of electronic communications networks and services. The continuous availability of electronic communications networks and services is a complex task and requires the management of risks associated with severe climatic events, physical security, cyber security, power supply security, hardware failure, hardware interoperability, human error, loss of skilled staff, supply chain assurance, life cycle management etc.

The interconnection and interdependence of networks can lead to incidents in one network impacting operations in other networks both within the same country and crossing borders to other countries. During the 5-year period 2016 to 2020 there were 8.87 bn user hours lost in 808 major incidents in electronic communications networks throughout Europe. The charts below taken from the ENISA CIRAS tool[1] presents an analysis of these incidents.

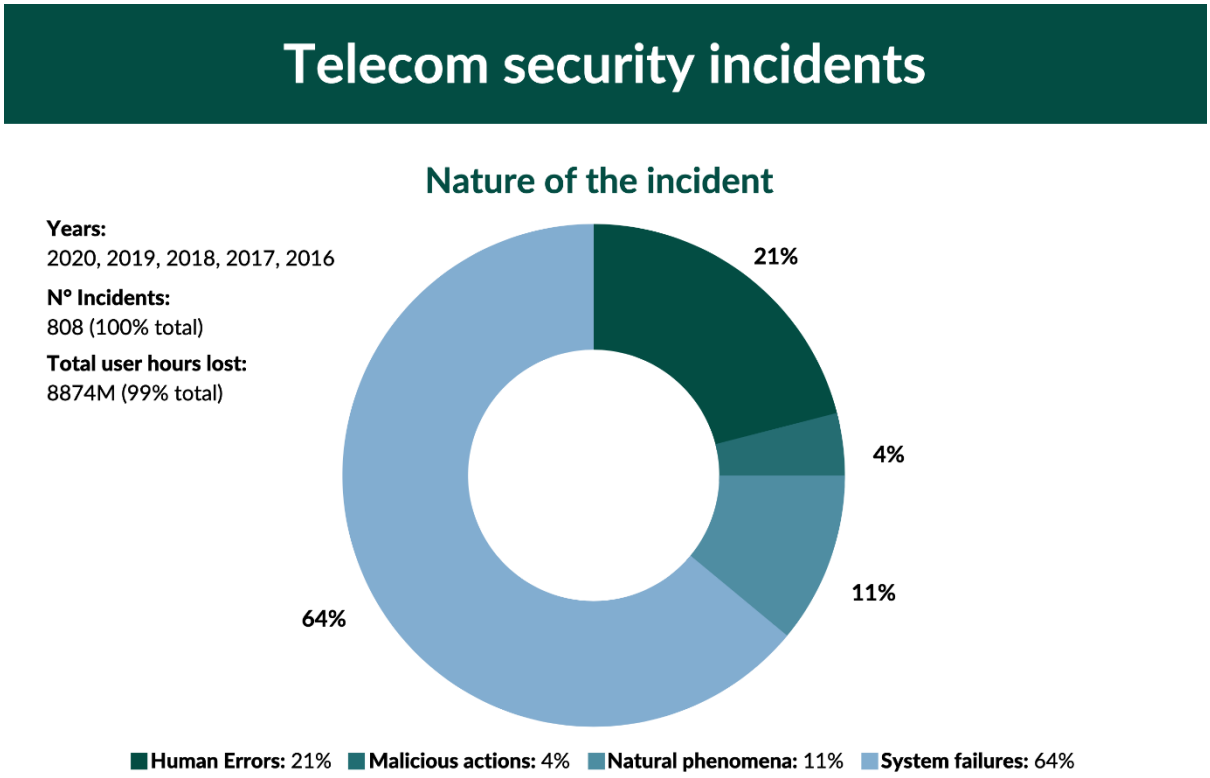


Figure 1 - Nature of incident causing the outage

[1] https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

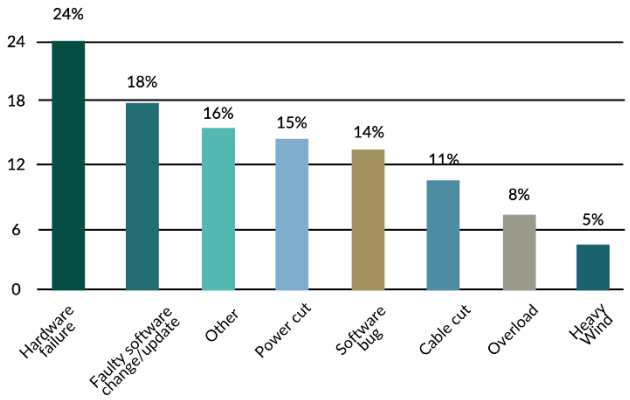
Telecom security incidents

Technical Causes

Years:
2020, 2019, 2018, 2017, 2016

N° Incidents:
808 (100% total)

Total user hours lost:
8874M (99% total)



53 **Figure 2 - Technical causes of outages**

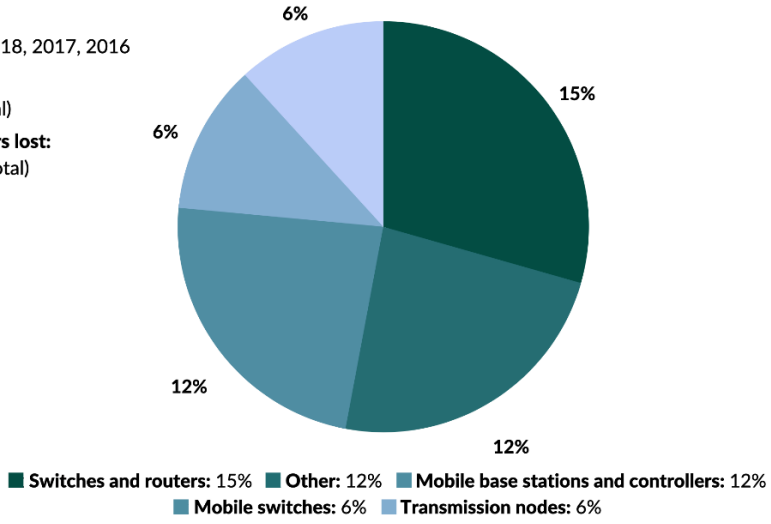
Telecom security incidents

Technical assets affected

Years:
2020, 2019, 2018, 2017, 2016

N° Incidents:
808 (100% total)

Total user hours lost:
8874M (99% total)



54

55 **Figure 3 - Technical Assets affected by outages**

56

Operators need to be aware of these risks to the availability of their networks and services and take appropriate steps to ensure insofar as possible the resilience and continuity of their networks.

Dependency on a single supplier within an individual network was highlighted as one of the risks in both the EU coordinated risk assessment[2] and the national risk assessment. It exposes an operator to systemic risk if there is a specific vulnerability with that vendor's equipment which exposes the entire network to attack.

If the vendor ceases supply of equipment due to economic factors or for any other reason such as losing access to key technology due to international trade sanctions, an operator may not be able to procure additional hardware, software, spares or software updates and security patches. Commercial risks can also arise from over dependence on a single vendor where it becomes very difficult to switch to another vendor, the incumbent vendor can leverage this dependence to increase costs to the operator.

The location and ownership of Managed Service Providers also needs to be considered as a potential risk, MSPs are extensively used by networks operators at all levels including specialised support and the nature of the work carried out by these entities means that they have extensive access to network assets.

Operators need to take these factors into account when selecting suppliers and take measures to avoid dependency on a single supplier, particularly in the case of suppliers considered high risk using the criteria outlined in ECSM 009 – Supply Chain Security.

[2] EU coordinated risk assessment of the cybersecurity of 5G networks

7 Security Measures

The operator should implement the Diversity, Resilience and Continuity Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
DR.01	The operator shall have an appropriate Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) in place. The BCP and DRP should be tested on a regular basis, at least annually.
DR.02	The operator should avoid supplier monocultures or developing a critical dependency on a single supplier.
DR.03	The operator shall produce a diversification strategy which outlines their procurement plans and measures which mitigate the risks associated with dependency on a single supplier
DR.04	The operator shall ensure that network capacity is provided in the core network sufficient to handle all traffic in the event of the failure of a single network element or transmission path.
DR.05	The operator shall ensure that network equipment, buildings and external plant are protected from climate extremes insofar as possible in line with ECSM 003.
DR.06	The operator shall source network equipment and management software from reputable vendors in terms of quality of equipment and future evolution and support in line with ECSM 009.
DR.07	The operator shall ensure that equipment used within its operational network is maintained up to date with latest versions, wherever technically feasible. Critical and important security vulnerabilities shall be patched in a timely manner.
DR.08	The operator shall manage its network elements using either its own resources or an EU/EEA registered company or a company operating in a manner compliant with European electronic communications, security and data protection legislation.

DR.09	The operator shall retain sufficient expertise to adequately monitor and supervise suppliers accessing their network and should avoid building up a long-term dependence on an individual supplier in line with ECSM 009
DR.10	The operator shall ensure that standby power systems are in place to ensure that service is maintained, in the event of a mains power failure, for a time appropriate to the criticality of a site.
DR.11	The operator shall ensure that there is an adequate stock of spares available to the organisation, to support critical network equipment.

82

83

8 Implementation Guidance

The implementation guidance in the following subsections is applicable to the security measures in section 7 as shown in **Error! Reference source not found.** below.

Table 1 - Correlation of implementation Guidance to Security Measures

	DR. 01	DR. 02	DR. 03	DR. 04	DR. 05	DR. 06	DR. 07	DR. 08	DR. 09	DR. 10	DR. 11
8.1		✓	✓			✓					
8.2		✓	✓			✓			✓		✓
8.3	✓			✓	✓		✓			✓	

8.1 Diversification Strategy

Applicable Security Measures: DR.02, DR.03, DR.06

Strategic Measure 05 of the EU 5G Security Toolbox recommends that each MNO has an appropriate multi-vendor strategy taking into account technical constraints and interoperability issues. The objective of this measure is to avoid a major dependency on a single supplier or suppliers considered as high risk.

Security Measure **DR.03** requires that operators produce a Diversification Strategy whereby they describe their approach to network development and procurement for their critical suppliers of network equipment. This document should contain a risk assessment, in line with ECSM 002, on the risks associated with their chosen supplier strategy. It should in particular examine if the operator is susceptible to the risks associated with dependency on an individual supplier. It should also outline the mitigation measures the operator has implemented to manage the identified risks. It should also describe how the strategy will be implemented in practice, taking into account interoperability of equipment and changes to the existing network. This document should be available for review by ComReg.

The size of the Irish market and the limited number of vendors of network equipment pose challenges to the implementation of a diversification strategy. This is especially the case where operators are not part of a larger multinational group with the ability to leverage international buying power, expertise, and experience. Introducing equipment from multiple vendors into a single network carries increased overheads for an operator in terms of skills, management tools, responsibility for interoperability between vendors, etc. However, these

challenges can be offset to some extent by operators' avoidance of vendor lock in and the cost reductions brought about through sustaining a more competitive and diverse vendor eco-system.

There are a number of approaches that operators can take in order to mitigate the risks associated with dependency on a single supplier. Some of the potential solutions are outlined below. Operators may choose to implement one, or a combination of the below strategies in order to mitigate the risks associated with dependency on a single supplier. Ultimately, the approach each operator takes will be dependent on their own operational context; however, their Diversification Strategy should clearly outline their analysis of the risks associated with dependency on individual suppliers and their proposed mitigation actions.

Network operators should assess any critical suppliers against a range of technical and non-technical criteria as part of their procurement processes and ongoing supplier management. These assessments should determine whether a supplier is used in critical parts of the operator's networks, as well as the ongoing level of security oversight and supervision the supplier is subject to.

8.2 Diversification Strategy Options

Applicable Security Measures: DR.02, DR.03, DR.06, DR.09, DR.11

8.2.1 Multi-vendor Strategy

A multi-vendor strategy involves having multiple suppliers for an operator's network equipment. There are various approaches that an operator can take towards a multi-vendor strategy, which are briefly outlined.

8.2.1.1 Horizontal and Vertical Diversity

Horizontal diversity refers to the selection of multiple vendors **within** a specific layer of the network. For example, a telecommunications operator could choose to deploy at least 2 network equipment vendors in the RAN, core, aggregation, and transport layers. This approach would ensure that the operator is not dependent on an individual supplier for any layer of the network. From a technical perspective, such a strategy is likely more feasible in certain layers, such as the RAN and less feasible in other areas, such the core.

Vertical diversity refers to the selection of different vendors **between** specific layers of the network. For example, a telecommunications operator could choose to deploy different network equipment vendors in each layer of the network, such as a different vendor for the RAN, core, aggregation, and transport layers. This approach means that an operator has a

relationship with multiple vendors reducing some of the risks associated with dependency on a single supplier; however, the operator may still be dependent on a single supplier for particular layers of the network and would need to take further measures to mitigate this risk. Standards, such as those produced by 3GPP, generally ensure that interoperability between network layers is technically feasible.

There are various combinations of vertical and horizontal diversity that operators can choose, ranging from a *"1+1"* approach, representing one supplier in the core and a different supplier in the RAN, to a *"1+2"* approach, representing one supplier in the core and two different suppliers in the RAN, all the way up to having multiple vendors within and between each layer.

8.2.1.2 Geographic Diversity

This refers to the selection of different vendors for deployment in different geographic areas. For example, an operator could choose one vendor for certain regions, whilst selecting a different vendor in other regions. This strategy reduces some of the risks associated with a single vendor; however, it still means that certain parts of the network will be reliant on an individual supplier, somewhat negating the benefit. The geographic and population distribution in Ireland make the feasibility of implementing this strategy somewhat challenging.

8.2.1.3 Generational Diversity

This refers to the selection of different vendors for different generations of technology. For example, an operator could select different vendors between generations of networks such as 2G, 3G, 4G and 5G. This scenario offers the advantage of having a "fall-back" should a systemic vulnerability affect a supplier of one of the generations of equipment. However, certain services may cease to function due to the reduced capabilities of previous generations. This approach may face certain interoperability challenges, such as between 4G and 5G RAN equipment, but may be feasible in other areas.

8.2.2 Open Network initiatives

Increased network interoperability has become an important topic within the electronic communications industry and is seen as an important aspect of an effective diversification of electronic communications networks. Increased interoperability has the potential to counter vendor lock-in by reducing the risk and cost associated with adding new suppliers' equipment to networks.

Currently, most network equipment within specific network layers is based on proprietary specifications which can lead to considerable supplier lock-in. Interoperability has the potential to increase network diversification by enabling operators to select multiple vendors within network layers with the assurance that doing so would not negatively affect performance, efficiency, and the end user experience.

Open RAN is the movement to disaggregate hardware and software of the Radio Access Network and to create open interfaces between them. This would mean that suppliers could develop interoperable products and components allowing operators to deploy equipment from multiple suppliers in the Radio Access Network. This may allow operators to choose the best equipment suppliers for a particular component of the RAN to suit their particular deployment requirements or needs, potentially reducing vendor lock in and increasing competition and market diversity.

At present. the concept of Open RAN is being promoted by various groups such as the Telecom Infra Project[3] and the O-RAN Alliance[4]. The project is still in its infancy, requiring further research and performance testing.. Through Science Foundation Ireland's 'Research Infrastructure Programme', the Irish State funds research into open network initiatives. In September 2020, the SFI funded CONNECT launched "Open Ireland"[5] open networking testbed to conduct research into open networking technologies including Open RAN.

There are likely a number of risks associated with the deployment of OpenRAN. The EU NIS Cooperation Group on 5G Security is conducting an analysis of the risks and benefits associated with OpenRAN which is due to be published in Q4 2021. The analysis may have recommendations around the secure deployment of OpenRAN, and future ECSMs may be published which focus on security measures associated with Open Network Initiatives.

Open Network Initiatives may in the future offer some opportunities for operators pursuing diversity within their network and may form part of an operator's overall Diversification Strategy, however there is no obligation on any operator to do so.

8.2.3 Additional Mitigation Measures

It may not be entirely possible to avoid dependency on an individual supplier through a multi-vendor strategy and such a strategy may not be appropriate given the size and scale of the Irish market. Equally concerns around the integration of multiple vendors within the network

[3] Telecom Infra Project | Global Community Connectivity collaboration

[4] O-RAN ALLIANCE (o-ran.org)

[5] CONNECT | Launch of "Open Ireland" - €2m open networking testbed - CONNECT (connectcentre.ie)

may be challenging to operators, particularly smaller operators. Where operators, based on a risk assessment, elect not to implement a multi-vendor strategy and depend on a single supplier for critical parts of their networks they should compensate with additional mitigation measures. Such measures should be documented in the operator's Diversification Strategy and could include, but are not limited to:

- Retaining sufficient expertise in-house to reduce the dependency on a supplier to maintain and operate the network
- Strictly implementing all measures outlined in ECSM 009, in particular conducting detailed vendor assessments during procurement and ongoing supplier management.
- Strong contractual arrangements with agreed SLAs and enforcement and remedy clauses in the event of underperformance by the supplier.
- Operators should maintain and appropriate stockpile spare parts and components to maintain the network in the event of a supplier failure.

8.3 Resilience and Continuity

Applicable Security Measures: DR.01, DR.04, DR.05, DR.07, DR.10

Resilience and continuity are key attributes of a electronic communications networks and services and are underpinned by Security Measures in section 7 above

8.3.1 Business Continuity Plan

The business continuity plan is a key measure towards achieving resilience in an organisation. It should contain a series of measures to sustain an organisation's activity during a disruption. The ability of an organisation to recover from a disaster is directly related to the degree of business continuity planning that has taken place before the disaster. Plans should be drawn up using guidance from relevant standards and put in place. Plans should also be communicated to all relevant personnel and should be tested in training exercises. Business continuity is applicable to all sizes and types of organisations.

While guidance on the creation of BCPs can be found in the international standards covered in *Section 9* below, a Business Continuity Management System (BCMS) should include the following:

- Full support at Board level for the BCMS by ensuring that it is compatible with the strategic direction of the organisation, integrated into business-as-usual processes and communicated effectively throughout the organisation.

- Clear identification of the scope and context of the BCMS taking into account the organisation's appetite for risk.
- Assignment of responsibility for the various elements and phases of a BCMS throughout the organisation.
- Staff trained appropriately to understand and implement the BCP measures and oversee the recovery to normal operation after the event.
- A clear view of the measurable objectives of the BCP, including the minimum level of service that the organisation expects the plan to deliver.
- Redundancy for elements that underpin each objective of the BCP taking into consideration that more than one element might fail in a given event.
- Documented procedures to restore and return to normal operation.

8.3.2 Core Network Resilience

The core network comprises of network routing equipment and / or voice switching equipment which is typically independent of the connection technology to the terminal equipment. This functionality requires a high level of resilience which can be achieved the design architecture of a network. The implementation of core network resilience should be done using a risk-based approach. Examples of how this could be achieved include but are not limited to:

- The use of multiple diverse transmission paths between various nodes in the core with sufficient capacity to carry all traffic in the event of a single path failing.
- Geographic resilience of network nodes as appropriate.
- The use of self-healing ring architecture in core network design.
- The use of network elements which have built in resilience e.g., Active / Standby

9 Relevant References

The following standards, guidelines and reports offer further detail and will assist operators in designing policies, procedures and processes that meet the *Security Measures* outlined in Section 7 of this document.

9.1 ISO/IEC 22301:2019 Security and resilience — Business continuity management systems — Requirements

https://www.iso.org/standard/75106.html

This is an international standard that supports organisations to put business continuity plans in place, it also helps to identify potential threats and build capacity to deal with unforeseen events. It specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events when they arise.

9.2 ISO/IEC 22313:2020 Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301

https://www.iso.org/standard/75107.html

This document explains the principles of a Business Continuity Management System, provides guidance intended to explain and clarify the requirements of ISO 22301 and assist in the interpretation of these requirements. It has the same clause headings as ISO 22301 to facilitate correlation between the two documents. It explains the Plan-Do-Check-Act process for the development, operation, maintenance, and improvement of BCPs.

9.3 NIST SP 800-34 Rev 1: Contingency Planning Guide for Federal Information Systems

https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final

This guide produced by NIST addresses specific contingency planning recommendations for three platform types and provides strategies and techniques common to all systems.

- Client/server systems.
- Telecommunications systems; and
- Mainframe systems.

It describes various types of contingency plans, the contingency planning process, contingency plan development and considerations for different types of systems.

It defines the following seven-step contingency planning process that an organisation may apply to develop and maintain a viable contingency planning program for their information systems. These seven progressive steps are designed to be integrated into each stage of the system development life cycle.

1. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.
2. Conduct the business impact analysis (BIA). The BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes. A template for developing the BIA is provided to assist the user.
3. Identify preventive controls. Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs.
4. Create contingency strategies. Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
5. Develop an information system contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
6. Ensure plan testing, training, and exercises. Testing validates recovery capabilities, whereas training prepares recovery personnel for plan activation and exercising the plan identifies planning gaps; combined, the activities improve plan effectiveness and overall organization preparedness.

Ensure plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.