Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

001 – General 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 (ECN and ECS respectively). 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 throughout 2020 to discuss matters concerning electronic communications network security. The group heard from experts in the field electronic communications security and held focussed discussions on the risks, challenges and best practices associated with electronic communications security. The series of ECSM documents have been developed by the NCSC informed by those meetings.

3 Scope

The ECSMs are applicable to all providers of public Electronic Communications Networks and publicly available Electronic Communications Services as defined in [Primary Legislation].

The security measures and guidance outlined in the series of ECSMs shall apply to operational electronic communications networks, rather than corporate/enterprise networks, except where the functions or data available in these networks could impact operational networks or where otherwise stated in the scope section of each ECSM.

The focus of the ECSMs is the protection of current and future networks and therefore the measures shall be applied to operator's current and future network deployments. Legacy networks or equipment which are expected to be decommissioned within the medium term (5 years / 2027) are not expected to have the same level of security as current and future network deployments. Operators should take a risk-based approach and apply a level of security appropriate to the risks posed during period between now and a legacy network's decommissioning. Transitionary arrangements are further elaborated upon in Section 9.3 of this document.

Whilst the reference architecture used in designing the ECSMs was that of a typical telecommunications operator, they have been written in such a way that they can be applied to a much broader set of ECNs and ECSs. However, not all security measures will be

directly applicable to all ECNs and ECSs. As an example, not all operators will include virtualisation as part of its operational network deployments, and in such cases, the security measures outlined in ECSM 007 – Virtualisation Security will be non-applicable.

4 References

Author	Title
Department of the Environment, Climate and Communications	National 5G Risk Assessment
NIS Cooperation Group	EU Coordinated Risk Assessment
NIS Cooperation Group	EU 5G Security Toolbox

5 Definitions, Symbols and Abbreviations

See Annex B for a combined list of Definitions, Symbols and Abbreviations used throughout the ECSM Series.

6 Context

6.1 EU Risk Assessment Process

In March 2019 the European Commission published its Recommendation 2335[1] which set out a process to allow Member States collectively assess cyber security risks to 5G networks in Europe and take a coordinated approach to the security of electronic communications networks. Under this EU process, Member States were asked to prepare national assessments and to forward these to the European Commission for collation and to jointly produce an EU-wide Risk Assessment.

The National Cyber Security Centre (NCSC) completed the National Risk Assessment for Ireland in collaboration and with input from ComReg, mobile network operators and various state agencies. This report was submitted to the European Commission on 15th July 2019 and formed part of a coordinated EU-wide Risk Assessment, which was published on 9th October 2019.[2].

6.2 National Risk Assessment and EU-wide Risk Assessment

Ireland's Risk Assessment analysed the Threats, Threat Actors, Assets, Vulnerabilities and potential risks of the future 5G infrastructure based on the inputs from MNOs, contributions from the NCSC, ComReg, the Irish State security agencies and international partner agencies. Ireland's Risk Assessment concluded that nation-state actors pose the greatest risk to networks, and that certain core network functions were highly sensitive, and required the highest levels of protection. The report also concluded that there are serious risks affecting 5G networks, in particular, risks arising from the move to software based and virtualised networks, poorly written or malicious code, supply chain risks, particularly those arising from high risk suppliers and the risk of third country or State interference.

The EU wide Risk Assessment came to broadly the same conclusions. In summary the EU Risk Assessment concluded that the attack surface of 5G networks would be greater, certain network functions would be more sensitive, and there would be an increased reliance on suppliers leading to dependency on these suppliers. This would leave MNOs open to the risk

[1] Cybersecurity of 5G networks | Shaping Europe's digital future (europa.eu)

[2] Report on EU coordinated risk assessment of 5G (europa.eu)

of interference from third countries. It concluded that the current legal and regulatory framework is insufficient to deal with the new risks presented by 5G networks.

Using the EU-wide Risk Assessment as a basis, the EU Member States, including Ireland, jointly authored a 5G Security Toolbox[3] of mitigation measures. The purpose of the toolbox is to identify a possible set of common measures that can be taken to mitigate the identified risks. It allows member states prioritise a set of measures that they can take based on its own risk assessment. The toolbox suggests 8 Strategic Measures, 12 Technical Measures & 10 Supporting Actions that can be taken to mitigate the risks. Some of these are measures to be taken at national level while others should be taken at EU level.

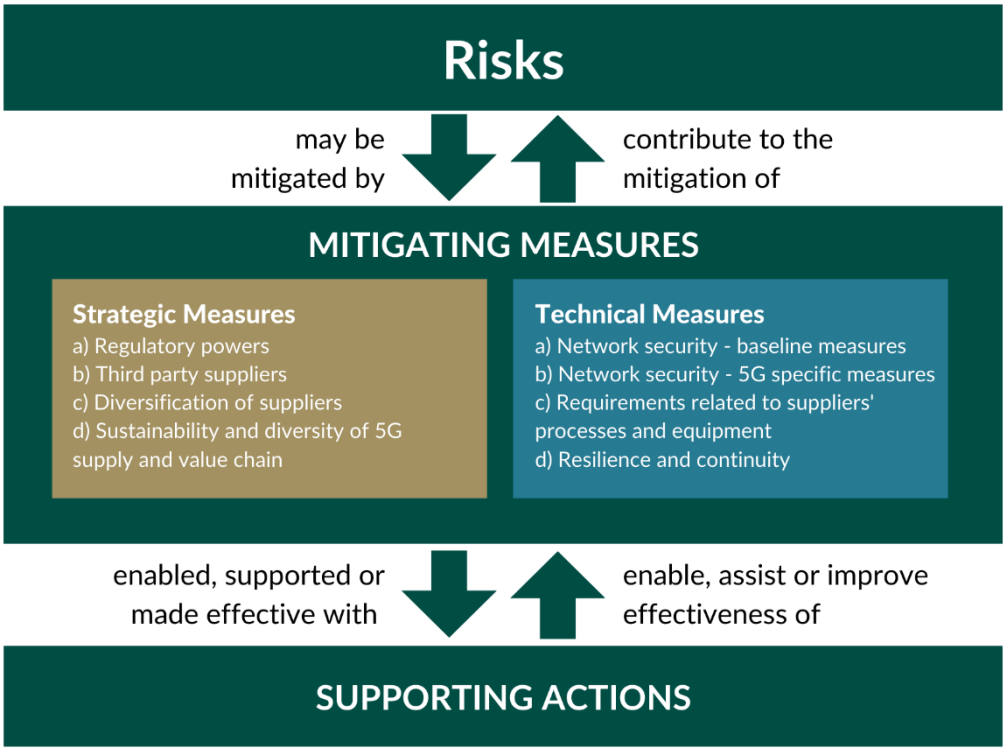

Figure 1 – Outline of EU 5G Security Toolbox

6.3 National Risk Assessment and EU-wide Risk Assessment

Ireland published the National Cyber Security Strategy[4] (2019 – 2024) in December 2019. Recognising the importance of electronic communications networks, the strategy stated:

[3] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures | (europa.eu)

[4] gov.ie - National Cyber Security Strategy (www.gov.ie)

> *"Critically, ongoing technological developments, including revolutions in telecommunications are likely to render this situation even more complex. In allowing for low latency and high bandwidth transmission of information, the deployment of 5G technologies will likely serve as a key enabling infrastructure for a series of other technologies and use cases. These potentially include customer facing services like autonomous vehicles, eHealth services and entertainment, and industry oriented services. On that basis, it seems likely that 5G networks will form the backbone of a new set of services critical to the operation of vital societal and economic functions. The nature of these networks and technology is relevant also; being software defined and virtualised means that* ***new types of security measures will likely be required in this sector to ensure the security of both the 5G network and of the services dependent on it****."*

Measure 7 of the National Cyber Security Strategy sets out how government will introduce a new and specific set of security requirements for the telecommunications sector, with detailed risk mitigation measures to be developed by the NCSC to assist ComReg in fulfilling its statutory functions under existing European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011, S.I. No. 333 of 2011 ("Framework Regulations"), and the European Electronic Communications Code (Directive 2018/1972). To realise this objective, the Electronic Communications Security Measures Working Group (ECSM WG) was established.

7 Electronic Communications Security Measures (ECSMs)

7.1 ECSM Working Group

Ireland The ECSM working group was established in March 2020 to design a set of security requirements for the electronic communications sector. The working group was co-chaired by the National Cyber Security Centre (NCSC) of the Department of the Environment, Climate and Communications and the Network Operations Unit (NOU) of the Commission for Communications Regulation (ComReg). The group also had membership from selected mobile and fixed line operators[5].

The group held a series of 6 thematic workshops throughout 2020, focussing on the areas identified as presenting the highest risk in the National and EU risk assessments. Each workshop included three sessions. The first session was dedicated to invited guest speakers from industry, academia and relevant public bodies which provided insights on the key risks, challenges, and best practices in the relevant security topics. During the second closed session the network operators discussed the issue in depth bringing practical industry insights to bear on the topics. Finally, the third session of each workshop consisted of a discussion on draft security requirements which could mitigate the main risks and ultimately informed the drafting of this series of documents. The six thematic workshops held covered:

- Risk Management;
- Physical and Environmental Security;
- Secure Network Design, Deployment and Operation;
- Supply Chain Security;
- Virtualisation Security; and
- Vendor Diversity & Open Networks.

The workshops resulted in the development by the NCSC of the series of documents known as the Electronic Communications Security Measures or ECSMs.

[5] A full list of members is included in Annex A to this document.

7.2 ECSM Structure

The goal of the ECSMs is to address the areas identified as the highest security risks, in the National Risk Assessment and EU-wide Risk Assessment, and to define Security Measures which are in line with the recommendations of the EU 5G Security Toolbox and other security best practices.

The approach taken is to summarise existing best practice for securing Electronic Communications Networks (ECNs) and Electronic Communications Services (ECSs) and to establish a baseline against which operators can design their own more detailed security policies, procedures, and processes, specific to their own organisational context. [The ECSMs provide detailed guidance to operators on the implementation of measures set out in regulations made by the Minister under Part X of the [Primary Legislation]. The ECSMs also act as guidance to ComReg who may use the ECSMs in determining any questions which arise in carrying out their functions. Further detail on the legislative basis of the ECSMs is provided in Section 8 of this document.]

Each ECSM contains four core sections - *Overview of Risk*, *Security Measures*, *Implementation Guidance* and *References*.

The *Overview of Risk* section outlines a short analysis of the main risks that the particular ECSM addresses. It is an answer to the question as to why the security measures need to be taken. The risks are derived from the national Risk Assessment, the EU Risk Assessment, as well as from the expert discussions that took place during the workshops of the ECSM WG. This section represents a brief overview, rather than a comprehensive analysis of the highest priority risks. Operators should conduct their own detailed risk assessments based on the principles outlined in ECSM 002 – Risk Management having regard to their own organisational context.

The *Security Measures* section is the core component of the ECSMs and provides a list of high-level outcomes that the operator must achieve in order to protect its network from the risks outlined in the previous section. These security measures are aligned with the measures set out by regulations made by the Minister under [Part X] of the [Primary Legislation]. It is mandatory for all public ECNs and ECSs to achieve the outcomes described. However, the capabilities and risk profiles of ECNs and ECSs vary greatly, and the Security Measures outlined in the ECSMs are intended to be high-level outcomes that can be used to shape the implementation of specific controls for each operator. The actual security policies, procedures, and processes that an operator implements should be

appropriate to the risks posed to the operator. Further guidance on proportionality is provided in Section 3.3

The *Implementation Guidance* section provides further detail on how operators could achieve the outcomes described in the Security Measures section. The implementation guidance has been based on various international standards, other publications such as the EU 5G Security Toolbox, as well as the detailed expert discussions during the meetings of the ECSM Working Group. Whilst the approach outlined in the implementation guidance shall not be considered as being mandatory, where an operator takes an alternative approach in achieving the security measures, it should be materially equivalent to the guidance and the operator should be able to justify its decision based on the outcome of a comprehensive risk assessment process.

Finally, the *Reference*s section provides links to relevant international standards and technical specification documentation which provide a further detail in order to assist operators in designing policies, procedures and processes that they can implement in order to achieve the outcomes outlined in the Security Measures section. The references listed are not necessarily endorsed by: DECC, NCSC. ComReg or the ECSM WG and are provided purely for information purposes. Where a standard is not publicly available; it is the responsibility of operators to purchase and will not be provided by the Minister or ComReg.

Ultimately, it will be for each operator to decide the appropriate policies to implement, based upon its risk assessment and particular circumstances, to achieve the outcomes outlined in the Security Measures section of each ECSM document.

7.3 How to use the ECSMs

As previously outlined, the ECSMs are not intended to act as a comprehensive security standard; rather they address the areas of highest risk identified during the National and EU risk assessment process and through the work of the ECSM WG. As such, operators are encouraged, in the first instance to base their overall security policies, process and procedures, on recognised international standards or guidance, produced by recognised international standards bodies or security organisations, such as the European Union Agency for Cybersecurity (ENISA), the National Institute of Standards and Technology (NIST), the International Standards Organisation (ISO), the European Telecommunications Standards Institute (ETSI), the Centre for Internet Security (CIS), the GSM Association (GSMA) etc. Each of the published ECSMs contain a non-exhaustive list of standards, which operators can reference in order to design their security policies, processes and procedures to meet the outcomes described in the *Security Measures* section.

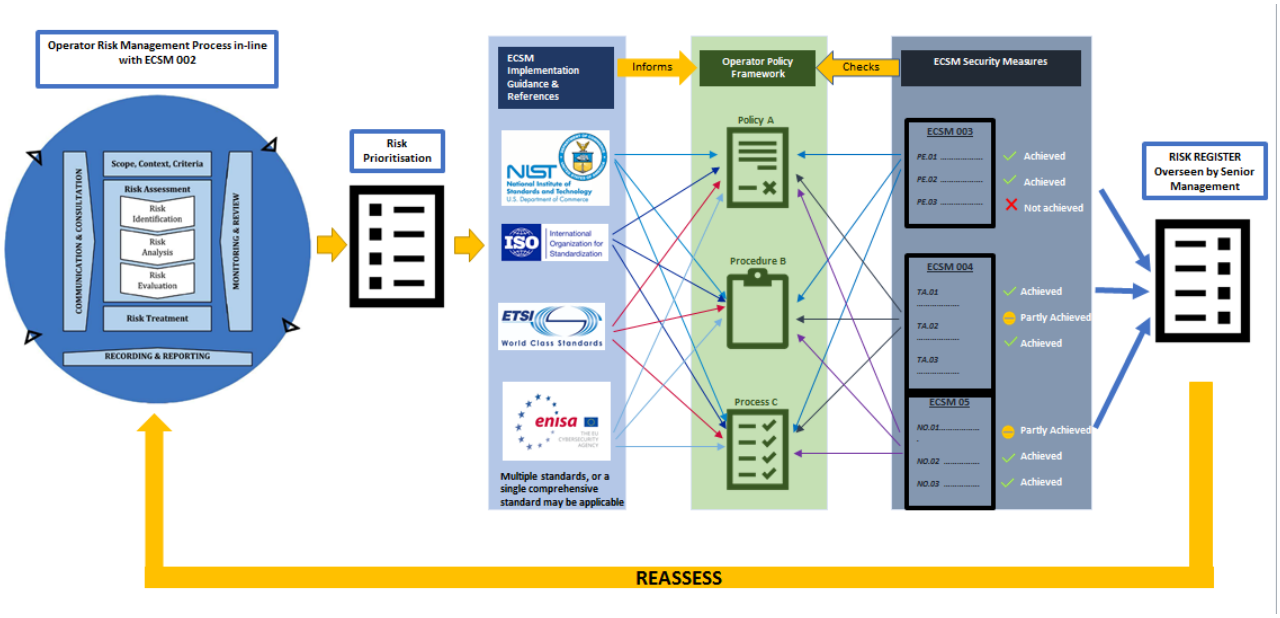

Figure 2 – The role of risk management and standards in ECSM implementation

The *Security Measures* in the ECSMs are written in a high-level way to be compatible with international standards and network operators own security policies. As such, the ECSMs should act as the minimum baseline of security. Network operators should use the outcomes described in the *Security Measures* section of the ECSMs to examine and confirm the effectiveness of their own security policies, processes and procedures.

The ECSMs do not represent a complete or exhaustive list of security measures that an operator must take in order to fully secure their network, and implementing the full set of ECSMs does not discharge operators from their general legal obligation to take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services – i.e. risks not addressed in the ECSMs remain the responsibility of the operator to take appropriate and proportionate measures to address.

7.4 Future areas of focus

The ECSMs are not a comprehensive overview of all areas of security, and instead focus on the areas identified as being of the highest risk, during the risk assessment process, representing a point in time. To maintain their relevance, the ECSMs should be considered as *"living documents"* and should be updated on a regular basis and as required.

Additional ECSMs may be developed which focus on other areas of security relevance as the networks and technology they are based upon develops and evolves, for example the use of eSIMs, over-the-air (OTA) provisioning, multi-access edge computing (MEC), network slicing or any other topics of significance to the security of networks and services.

8 Regulatory Framework

NOTE: The regulatory framework which will underpin the ECSMs is currently under development. The following is provided for information and is without prejudice.

DECC held an information session for industry on the current status of this proposed legislation in July 2021. A copy of the presentation can be found on the Department's website. [6]

The Department's policy is that the security provisions of the EECC (Articles 40 & 41) would be transposed by primary legislation. Additionally, the Minister would be provided with the power to make regulations further specifying the measures to be taken by providers to meet the general obligation to take appropriate and proportionate security measures. The Minister would also have the power to make guidelines which would provide practical guidance to operators on the implementation of measures specified by regulation. It is also proposed that enhanced powers would be provided to ComReg in order to supervise and enforce operator's compliance with the specified security measures.

[6] gov.ie - European Electronic Communications Code (EECC) (www.gov.ie)

9 Implementation

9.1 Prioritisation

It is acknowledged that due to the existing investments and practices by operators, electronic communications networks and services have proven to be very resilient, with overall network uptime exceeding 99%[7]. This represents a strong base for operators to continue to increase the bar of security and ensure the next generation of networks are secure, resilient, and future-proofed.

Wherever possible, existing policies, processes and procedures should be adapted to ensure compliance with the ECSMs. However, in some instances, it may require operators to design and implement an entirely new approach. The implementation of the entirety of the ECSMs will be a complex process and will require a period of time, in some cases. However, measures will have to be prioritised by operators, working towards full compliance over time. Ultimately, deciding on the priority of implementation will be the responsibility of each operator, who will have the clearest understanding of their current security posture, operational context and risk profile. However, this does not preclude ComReg from directing an operator to take certain security measures, or interim steps, particularly in the case where a significant threat to the security of networks and services has been identified.

9.2 Technology Neutrality

The principle of *technology neutrality* applies to the ECSMs and operators shall not be bound to any choice of technology in meeting their statutory obligations under the security measures regulations. Operators shall be free to design and manage their networks using the most appropriate technologies, provided, that they meet the equivalent level of security and are substantively equivalent to the methods described in the ECSMs.

9.3 Legacy Networks

The focus of the ECSMs is the protection of current and future networks and therefore the measures shall be applied to operator's current and future network deployments. Legacy networks or equipment which is expected to be decommissioned within the medium term (5 years / 2027) are not expected to have the same level of security as current and future network deployments. Operators should take a risk-based approach and apply a level of

[7] Based on the total amount user-hours lost during significant incidents reported to ComReg in 2020. User-hours lost through minor incidents which are not reported to ComReg are not reflected in this figure.

security appropriate to the risks posed during period between now and a legacy network's decommissioning.

Operators may plan to continue to use certain legacy network equipment or nodes, which may not support certain technical requirements of the ECSMs, for example Multi Factor Authentication (MFA). Where it is infeasible to comply with an ECSM requirement, operators should document the exception, the reasoning, perform a risk assessment and implement alternative mitigations where possible. The ongoing use of such network equipment, without an appropriate alternative mitigation for periods longer than 5 years / 2027 shall not be compliant.

Likewise, when it comes to the physical security of assets, certain legacy sites and older buildings may not comply with the measures set out in ECSM 003 or planning restrictions may not allow for the optimal level of physical reinforcements. In such cases, providers are expected to make best efforts and implement alternative mitigations where possible.

9.4 Proportionality

The security measures taken should be appropriate and proportionate to address the risks posed. For this reason, a one-size-fits all approach to security for all public ECNs and publicly available ECSs is not possible. The outcomes in the *Security Measures* section are written in such a way, that they can be applied by various organisations – how those outcomes are achieved, and the level of security applied will depend on the risk profile of the individual ECN or ECS, and the specific asset being protected.

Each ECN or ECS will have to conduct their own risk assessments (based on the principles outlined in ECSM 002 – Risk Management) in order to determine the level of controls they will need to put in place in order to meet the outcomes described.

9.4.1 Operator Risk Profiles

Cognisant of the requirement of operators to take a risk-based approach to the security of networks, it is expected that operators with varying risk profiles will implement different but appropriate levels of security ranging from basic security controls up to the state of the art.

The individual risk profile of each operator varies based on a number of factors, including but not limited to:

- subscriber numbers;
- subscriber type;

- coverage area;
- level of infrastructure, including if the operator is a wholesale provider to other operators;
- provision of services to critical infrastructure providers (such as operator of essential services (OES) and digital service providers (DSPs)[8], government departments and public service bodies) and,
- Experience of previous security incidents.

The following exemplars of operators aim to illustrate the varying types of operators there are and the type of implementation that may apply. However, it is not a definitive guide and ComReg reserves the right to judge each case on its merits, as part of its statutory supervision of obligations pursuant to [Primary Legislation].

Example 1

Company A is a Wireless Internet Service Provider (WISP) with a subscriber base of 5,000 users restricted to a small regional coverage area. The subscriber base consists of mainly residential customers and does not support any critical infrastructure providers. The provider has a relatively small infrastructure and relies heavily on larger Electronic Communications Security Measure operators for national connectivity.

It would be expected that this operator could achieve the outcomes described in the *Security Measures* section with a basic level of security controls.

Example 2

Company B is a fixed access Fibre to the Premises (FTTP) provider with a subscriber base of 20,000 users with a large coverage area in a number of different regions of the country. The subscriber base consists of a mix of residential and commercial customers. The provider does not support critical national infrastructure but does support a number of smaller healthcare centres and manufacturers. The provider has a modest infrastructure but relies mostly on other providers for nationwide connectivity.

[8] As defined in SI 360 of 2018 - http://www.irishstatutebook.ie/eli/2018/si/360/made/en/pdf

It would be expected that this operator could achieve the outcomes described in the *Security Measures* section using an industry-standard level of security controls.

Example 3

Company C is a large telecommunications operator providing both mobile and fixed line services to 300,000 users with a national coverage area. The subscriber base is a mix of residential and commercial customers. The provider supports a number of critical infrastructure providers including large hospitals and energy suppliers. The operator provides the Emergency Call Answering Service (ECAS) to the state. The provider owns a large infrastructure and provides connectivity for other smaller Electronic Communications Security Measure operators. The operator is a provider to a number of government agencies involved in the security and defence of the Irish State.

It would be expected that this operator could achieve the outcomes described in the *Security Measures* section implementing a state-of-the-art level of security controls.

Example 4

Company D is a number independent interpersonal communications service with a subscriber base of 3 million users within the State. It is not provided on a not-for-profit basis, receiving remuneration for the service through user's provision of personal and other data. The service is used in all regions throughout the state. The subscriber base consists mainly of private citizens; however, it is also extensively used by businesses to communicate with their customers. The service is provided on an over-the-top basis meaning it relies on providers of electronic communications networks for connectivity, however, it owns and operates much of the infrastructure that is used to operate the service.

It would be expected that this operator could achieve the outcomes described in the *Security Measures* section using a state-of-the-art level of security controls.

9.5 Costs

The Whilst many of the security measures outlined in this series of ECSM documents reflect policies, processes, and procedures already in place for many operators, others will require

significant changes to daily operations. Implementation of the ECSMs will be a complex programme that will in some cases require significant investments in time, financial and human resources. The implementation of certain ECSMs may necessitate operators investing in training of staff or hiring entirely new expertise. In other cases, compliance may necessitate entire network redesigns or equipment upgrades. There are likely to also be costs associated with the supervision of and demonstrating compliance with the ECSMs, at least initially and depending on the existing security standard of operators.

Ultimately these costs may place pressure on the financial position of operators who in turn may need to increase prices, which may likely influence the price paid by the consumer. However, the costs of recovering from an attack can often dwarf the cost of preventative security measures both directly and indirectly having regard to the reputational risks and damage that such attacks can cause to operators, customers and consumers. Electronic communications networks and services are vital to the functioning of society and the economy and providing connectivity to the essential services upon which citizens rely. The value associated with ensuring the security and resilience of our electronic communications networks and services is deemed to be worth the cost. It is now accepted it is an investment well made.

ANNEX A: Electronic Communications Security Measures Working Group (ECSM WG)

Representatives from the following organisations made up the membership of the ECSM working group, having been selected to provide practical industry input on the implementation of security measures:

- The Department of the Environment, Climate and Communications
- The Commission for Communications Regulation
- BT Ireland
- DenseAir
- Eir
- Imagine
- SIRO
- Three Ireland
- Virgin Media
- Vodafone

A public consultation shall be held prior to the formal adoption of the ECSMs in order to receive the views of interested parties, in particular third parties which are directly affected, including end-users and consumers, manufacturers and undertakings that provide electronic communications networks or services.

408 ANNEX B: Definitions, Symbols, Abbreviations

409 B.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.
Board	A group of individuals appointed to represent shareholders in the governance of an organisation.
Border Gateway protocol	A standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.
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.
Component	Part of a system that has operational and/or management significance
Control Plane	The control plane has a layered structure and performs the connection control functions; it deals with the signalling necessary to set up, supervise and release connections
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	Important sites that need to be protected - transmission nodes

Installations	(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
Diameter	An authentication, authorization, and accounting protocol for computer networks. It evolved from the earlier RADIUS protocol. It belongs to the application layer protocols in the internet protocol suite
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 5G Security Toolbox	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' document published jointly by member states on 31st of January 2020
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
Fuzz Testing	Negative testing technique for automatically generating and injecting into a target system anomalous invalid message sequences, broken data structures or invalid data, in order to find the inputs that result in failures or degradation of service
Hardening	The process of securing a system by reducing its surface of vulnerability, reducing available means of attack. This typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, and the disabling or removal of unnecessary service.
Host	A computer or other device that communicates with other hosts on a network. Hosts on a network include clients and

	servers that send or receive data, services or applications.
Hyperjacking	An attack in which a hacker takes malicious control over the hypervisor that creates the virtual environment within a virtual machine host
Important Security Vulnerability	Vulnerabilities where the client is compromised with warnings or prompts and whose exploitation could result in compromise of data
Incident Handling	Actions of detecting, reporting, assessing, responding to, dealing with, and learning from security incidents
Incident Response	Actions taken to mitigate or resolve a security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.
Incident Response Function	A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Security Incident Response Team (CSIRT), a Computer Emergency Response Team (CERT) or Computer Incident Response Capability (CIRC)
Indicator of Compromise	An artefact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.
Interface	Common boundary between two associated systems.
Interoperability	The ability of two or more networks, systems, devices, applications or components to communicate and effectively function.
Jump Server	A jump server is a hardened remote access server. It acts as a stepping point for administrators accessing critical systems with all administrative actions performed via a jump server.

Kernel	A computer program at the core of a computer's operating system that has complete control over everything in the system.
Managed Service Provider (MSP)	A third-party that helps to run or administrate a network.
Management Plane	Performs management functions for the User and Control Plane, and the system as a whole. It also provides coordination between all the planes. Performance, fault, configuration, accounting, and security management are performed in the Management Plane.
Multi Factor Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
National Risk Assessment	Risk assessment carried out by the National Cyber Security Centre and forwarded to the European Commission on 15 July 2019.
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.
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.
Noisy neighbour problem	When a VM accessing shared resources uses more than it should. This causes other VMs accessing those resources to

	suffer from reduced or erratic performance
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
Orchestration	A set of processes that collectively automate the management and control of digital information systems.
Personnel	The people who work for an organisation.
Playbook	A documented planned course of action in response to anticipated events.
Privileged Access Workstation	A dedicated computing environment for sensitive tasks that is protected from Internet attacks and other threat vectors.
Privileged user / Administrator	A person who is granted Privileged Access, through their role, access and credentials, or through any other means.
Privileged/Administrative Access	An access to network equipment where greater capabilities are granted than a regular user. Accounts granted privileged access can be used to perform elevated security relevant functions including modifying configurations, changing security controls, creating new accounts with equal or greater privilege or allowing full control of network equipment. .
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.
Risk Appetite	The amount and type of risk that an organisation is prepared

	to take.
Risk Assessment	The process of identifying, estimating and prioritising risks.
Risk Management	The programme and supporting processes to manage risk.
Risk Mitigation	The process of developing options and actions to reduce threats of a risk event occurring.
Risk Rating	An assessment of risk based on the likelihood of an event occurring (from most unlikely to most likely) and the severity of the impact if the event does occur (from trivial impact to major impact).
Scaling	The ability to dynamically extend/reduce resources granted to virtual elements as needed
Scaling out/in	The ability to scale by add/remove resource instances
Scaling up/down	The ability to scale by changing allocated resource, e.g. increase/decrease memory, CPU capacity or storage size
Security Awareness Program	An set of policies the organisation implements in order to create a culture of security for its staff.
Security Event	Any observable occurrence in a network or system that poses a risk to the security of networks and services.
Security Incident	An event having an actual adverse effect on the security of electronic communications networks or services.
Security of Networks and Services	The ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of those networks and services, of stored or transmitted or processed data, or of the related services offered by, or accessible via, those electronic communications

	networks or services
Senior Management	A group of individuals responsible for making the management and executive decisions of an organisations.
Signalling System No. 7	A set of telephony common channel signalling protocols developed by the ITU-T and standardised in the ITU-T Q .700 Series Recommendations.
SIGTRAN	A signalling protocol that supports the same application and call management paradigms as SS7 using Internet Protocol (IP) .
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.
Supply chain	A system of organisations, people, technology, activities, information and resources involved in moving a product or service from supplier to customer
Threat Intelligence	Data that is collected, processed, and analysed to understand threat actors' motives, targets and attack behaviours.
Trust Domain	A collection of entities that share a set of security policies
Trusted Platform Module	Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure crypto processor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys.
Undertaking	A person engaged or intending to engage in the provision of electronic communications networks or services or associated facilities.
User Plane	Plane that has a layered structure and provides user information transfer, along with associated controls

Virtual Machine	Virtualised computation environment that behaves very much like a physical computer/server
Virtualisation	The process of abstracting a resource beyond its physical form. Many types of technologies can be virtualised, including servers, storage devices, networks, network functions and applications.
Virtualisation Infrastructure	The totality of all hardware and software components that build up the environment in which virtualised elements are deployed

410

411 B.2 Symbols

412 Nil

413 B.3 Abbreviations

414

Abbreviation	Meaning
2FA	Two Factor Authentication
3GPP	Third Generation Partnership Project
3PA	Third Party Administrators
AV	Anti-Virus
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BMC	Baseboard Manager Controller

BTS	Base Transceiver Station
C2	Command and Control
CAMEL	Customised Applications for Mobile networks Enhanced Logic
CNI	Critical National Infrastructure
ComReg	The Commission for Communications Regulation
COTS	Commercial off the shelf
CSIRT	Computer Security Incident Response Team
DECC	The Department of Environment, Climate and Communications
DMZ	De-Militarised Zone
ECN	Electronic Communications Network
ECS	Electronic Communications Service
ECSM	Electronic Communications Security Measures
EEA	European Economic Area
EECC	European Electronics Communications Code.
ENISA	European Union Agency for Cyber Security
EPC	Evolved Packet Core
EU	European Union
GDPR	General Data protection Regulation

GSM	Global Systems Mobile
GSMA	GSM Association
GT	Global Title
HLR	Home Location Register
IDS	Intrusion Detection Systems
ILO	Integrated Lights Out
IMSI	International Mobile Subscriber Identity
IOC	Indicator of Compromise
ISAC	Information Sharing and Analysis Centre
JML	Joiners, Movers, Leavers
JSON	Java Script Object Notation
LTE	Long Term Evolution
MANO	Management and Orchestration
MAP	Mobile Application Part
MFA	Multi Factor Authentication
MISP	Malware Information Sharing Platform
MNO	Mobile Network Operator
MSC	Message Switching Centre

MSP	Managed Service Providers
NAT	Network Address Translation
NCSC	National Cyber Security Centre
NESAS	Network Equipment Security Assurance Scheme
NF	Network Function
NFV	Network Function Virtualisation
NIST	National Institute of Standards and Technology
NOC	Network Operations Centre
ODPC	Office of the Data Protection Commissioner
OS	Operating System
PAW	Privileged Access Workstation
PLMN	Public Land Mobile Network
RAN	Radio Access Network
RAS	Reliability, Availability, Serviceability
SIEM	Security Information and Event Management
SIM	Subscriber Identification Module
SMS	Short Messaging Service
SMSC	Short Message Service Centre

SOC	Security Operations Centre
SS7	Signalling System No. 7
TI	Threat Intelligence
TMSI	Temporary Mobile Subscriber Identity
TPM	Trust Platform Module
VLAN	Virtual Local Area Network
VLR	Visitor Location Register
VM	Virtual Machine
VNF	Virtual Network Function

415

416