EUROPEAN UNION AGENCY
FOR CYBERSECURITY

GUIDELINE ON SECURITY MEASURES UNDER THE EECC

3rd Edition

DECEMBER 2020

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure.. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Goran Milenkovic, Dr. Marnix Dekker, European Union Agency for Cybersecurity.

ACKNOWLEDGEMENTS

For the completion of this guideline ENISA has worked closely with a working group of experts from national authorities, the ECASEC Expert Group (formerly known as the Article 13a Expert Group). We are grateful for their valuable input, comments and support in the process of developing of this document.

National authorities also organized a review of this document by providers in their countries. We are grateful for the many useful comments and suggestions we received from experts in the sector.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-457-2 - DOI: 10.2824/44013

TABLE OF CONTENTS

PREFACE

The **2009** reform of the EU legislative framework for electronic communications introduced **Article 13a** and **Article 13b** as part of the **Framework directive** (Directive 2009/140/EC). This reform was transposed into national legislation by EU Member States in 2011. Article 13a requires MS to ensure that providers of electronic communications manage security risks and take appropriate security measures to guarantee the security (paragraph 1) and integrity (paragraph 2) of these networks and services. Article 13a (paragraph 3) requires providers to notify significant security incidents to competent national authorities, who should report about these incidents to ENISA and the European Commission (EC) annually. Article 13b outlines how authorities can supervise and enforce compliance with these security requirements.

In **2010**, ENISA, the European Commission, and experts from ministries and telecom regulators in the EU Member States initiated a series of meetings to achieve an efficient and harmonised implementation of Article 13a across the EU, forming the **Article 13a Expert Group**[1]. This group is now chaired by an expert from a national competent authority in the EU and comprises experts from competent authorities from all EU countries as well as from some EFTA and EU candidate countries. The Article 13a Expert Group reached consensus about two non-binding technical guidelines for implementing Article 13a: the "Technical Guideline on Incident Reporting" and the "Technical Guideline on Security Measures".

In December **2018**, a new set of telecom rules called the **European Electronic Communications Code** (abbreviated as EECC) was adopted. The EECC updates the EU telecom package of 2009 and paves the way for the roll out of fibre, very high capacity networks and next generation mobile networks (5G), which will create jobs and growth, enable new application scenarios like internet of things (IoT) and new business models. An important part of the EECC is consumer protection[2] and security of electronic communications. EU countries have to transpose this EU directive into national law by 21 December 2020.

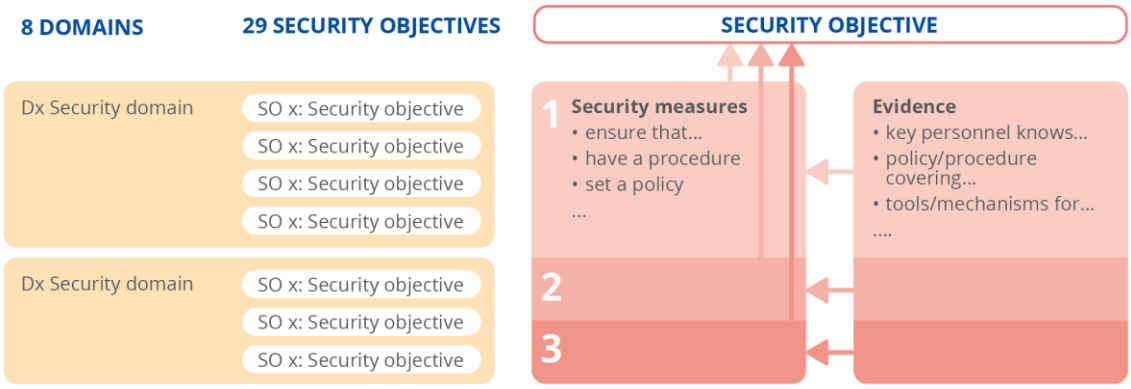
Article 40 of the EECC, which replaces the above-mentioned Article 13a, contains detailed security requirements for electronic communication providers. Article 41 of the EECC, which replaces Article 13b, outlines how competent authority can enforce these security requirements. Although the security requirements under the EECC are similar to the security requirements under the Framework directive, there are important differences. An overview of the main differences can be found in an ENISA policy paper about the EECC. As with Article 13a, ENISA will support the EU Member States with the implementation of Article 40 of the EECC, to ensure there is an effective, efficient, and harmonized approach to security supervision across the EU. To reflect this legislative change the Article 13a group has changed its name to ECASEC, European Competent Authorities for Secure Electronic Communications.

This document, the **Guideline on Security Measures under the EECC**, provides guidance to competent authorities about the technical details of implementing Articles 40 and 41 of the EECC: how to ensure that providers assess risks and take appropriate security measures.

[1] Now known as *ECASEC Expert Group*
[2] In addition to protection of *consumers*, EECC actually promotes interest of EU *citizens*. For example, one of the objectives listed in the Article 3, paragraphs (d), is to "promote the interests of the citizens of the Union, by ensuring connectivity and the widespread availability and take-up of very high capacity networks, including fixed, mobile and wireless networks, and of electronic communications services".

The **structure** of this guideline is as follows: The guideline lists 29 high-level security objectives, which are grouped in 8 security domains. For each security objective we list specific detailed security measures which could be taken by providers to reach the security objective. These security measures are grouped in 3 levels of increasing sophistication. We also give examples of evidence, which could be taken into account by an auditor, for example, when assessing if these security measures are actually in place. The overall structure is depicted in the diagram below.

Figure 1: Overall structure of the security objectives and security measures

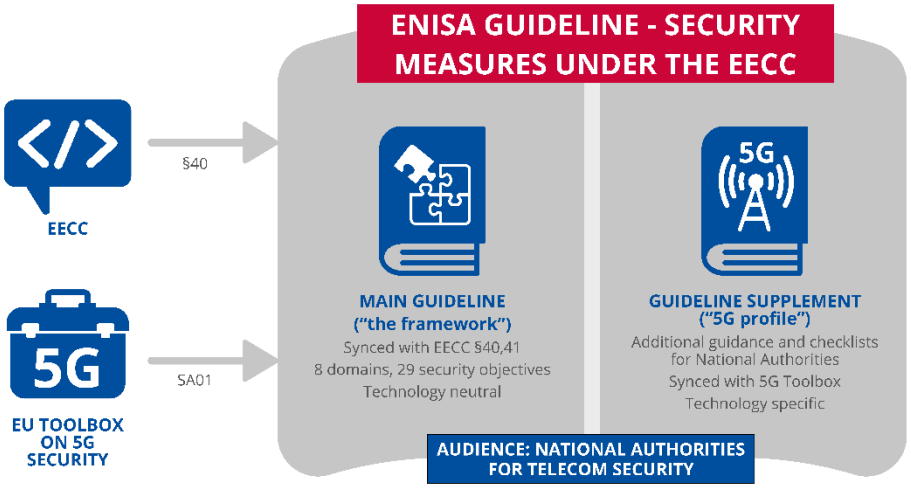


One size does not fit all: Neither the high-level security objectives nor the detailed security measures should be seen as binding recommendations about which are appropriate security measures for providers to take. The reason is that the electronic communications sector is very diverse; large incumbents, small service providers, black fibre operators, virtual mobile network operators, ISPs offering only DSL, etc. In each setting the risks are different and it is up to the providers to assess the risks and decide which are appropriate security measures to take. This document is intended as a tool for competent authorities supervising the sector. It could be used as a structure for self-assessments, audits and audit reports, guidance for providers, or as a mapping to international network and information security standards used in the electronic communications sector.

General security guideline supplemented by specific security profiles: The security measures in this guideline are technology-neutral. They should be applicable to a wide range of different types of technologies. As a supplement to this guideline we are developing more detailed guidance for specific networks and technology, such as 5G, for example. This security guideline, together with the 5G supplement[3], addresses the relevant technical measures in the EU toolbox of risk mitigating measures for 5G networks.

[3] https://www.enisa.europa.eu/publications/security-measures-under-the-eecc-technical-guidelines

Figure 2: Structure of the ENISA Guideline on Security Measures under the EECC



1. INTRODUCTION

This document provides technical guidance to the national authorities tasked with supervising the security of electronic communication networks and services (hereinafter Competent Authorities), and in particular the security measures mentioned in Article 40 the European Electronic Communications Code[4] (hereinafter EECC).

1.1 TARGET AUDIENCE

This guideline is for experts from competent authorities in the EU Member States tasked with the implementation of Article 40 of the EECC.

This guideline may be useful also for experts working in the EU's electronic communications sector and experts working in cyber security.

1.2 GOAL

This document aims to give guidance to competent authorities about the security measures described in Article 40 of the EECC and the enforcement described in Article 41 of the EECC.

1.3 VERSIONS AND CHANGES

ENISA updates this guideline periodically, when necessary, in agreement with the competent authorities.

This version is an update of the guideline used so far for Article 13a (version 2.0). The overall structure has remained largely unchanged.

List of main changes in version 3.0:

- Updated definitions of security and security incidents and made further alignment of the text and terminology used with the provisions of the EECC
- Added new security objective SO13: Use of encryption
- Added new security objective SO14: Protection of encryption data
- Added new security domain D8: Threat awareness
- Added new security objective SO28: Threat intelligence
- Added new security objective SO29: Informing users about threats
- Added additional measures in security objectives SO4, SO9, SO11, SO12, SO19 and SO21 for the purpose of reinforcement of baseline measures, as per the technical measures in the EU Toolbox on 5G cybersecurity
- Added clarification on supervision regime for NI-ICS service providers

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=EN

- Introduced the concept of technology profile, for development of supplements to the guideline for specific types of networks/service providers (e.g. 5G MNOs, NI-ICS providers)

Structure of this document

In Section 2 we summarize the role and objectives of ENISA related to the implementation of Article 40 of the EECC. In Section 3 we introduce Article 40, the scope and the terminology used in this document. In Section 4 we list 29 security objectives, divided in 9 domains, and we provide details about security measures and evidence. In Section 5 we give guidance on potential regulatory activities competent authorities could deploy to assess compliance to the security measures required by Article 40 of the EECC. In Section 6 we provide a mapping from the security measures in this guideline to some well-known international standards.

2. BACKGROUND

In this section we summarize the EU policy context and we explain ENISA's role and objectives.

2.1 EU POLICY CONTEXT

The European Electronic Communications Code, the EECC, is an EU directive, meaning that EU countries will have to transpose the new rules into national legislation. The deadline for this transposition is 21 December 2020. The new EECC replaces four EU directives. In this paper, we refer to these directives as the "old rules", although they are of course currently still in place.

- The Framework Directive, which is based on the Framework Directive 2002/21/EC as amended by Directive 2009/140/EC.
- The Access Directive, which is based on the Access Directive 2002/19/EC and amended by Directive 2009/140/EC.
- The Authorisation Directive is based on the Authorisation Directive 2002/20/EC and amended by Directive 2009/140/EC.
- The Universal Service Directive is based on the Universal Service Directive 2002/22/EC and the Citizens' Rights Directive 2009/136/EC.

These rules were last modified in 2009 as part of a wider EU telecom reform, which included also the ePrivacy directive[5], addressing confidentiality and privacy in electronic communications and the BEREC regulation[6], establishing the Body of European telecom regulators.

2.2 ENISA'S ROLE

Article 40 of the EECC asks ENISA to facilitate harmonization on the security aspects.

The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council ([7]), the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.

[5] https://eur-lex.europa.eu/eli/dir/2002/58
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R1211&from=EN
[7] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (OJ L 165, 18.6.2013, p. 41).

3. EECC DEFINITIONS AND TERMINOLOGY

3.1 EECC DEFINITIONS AND TERMINOLOGY

In this section we introduce the relevant parts of the EECC and the related terms used in this document.

3.1.1 EECC: Articles 40 and 41 and relevant recitals

Most of the security requirements are contained in Article 40 and Article 41 of the EECC.

For the sake of reference we quote Article 40 and Article 41 in full below.

Article 40 Security of networks and services

1. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.

The European Union Agency for Network and Information Security ('ENISA') shall facilitate, in accordance with Regulation (EU) No 526/2013 of the European Parliament and of the Council (45), the coordination of Member States to avoid diverging national requirements that may create security risks and barriers to the internal market.

2. Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.

In order to determine the significance of the impact of a security incident, where available the following parameters shall, in particular, be taken into account:

(a) the number of users affected by the security incident;

(b) the duration of the security incident;

(c) the geographical spread of the area affected by the security incident;

(d) the extent to which the functioning of the network or service is affected;

(e) the extent of impact on economic and societal activities.

Where appropriate, the competent authority concerned shall inform the competent authorities in other Member States and ENISA. The competent authority concerned may inform the public or require the providers to do so, where it determines that disclosure of the security incident is in the public interest.

Once a year, the competent authority concerned shall submit a summary report to the Commission and to ENISA on the notifications received and the action taken in accordance with this paragraph.

3. Member States shall ensure that in the case of a particular and significant threat of a security incident in public electronic communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers shall also inform their users of the threat itself.

4. This Article is without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC.

5. The Commission, taking utmost account of ENISA's opinion, may adopt implementing acts detailing the technical and organisational measures referred to in paragraph 1, as well as the circumstances, format and procedures applicable to notification requirements pursuant to paragraph 2. They shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 118(4).

Article 41 Implementation and enforcement

1. Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to issue binding instructions, including those regarding the measures required to remedy a security incident or prevent one from occurring when a significant threat has been identified and time-limits for implementation, to providers of public electronic communications networks or publicly available electronic communications services.

2. Member States shall ensure that competent authorities have the power to require providers of public electronic communications networks or publicly available electronic communications services to:

(a) provide information needed to assess the security of their networks and services, including documented security policies; and

(b) submit to a security audit carried out by a qualified independent body or a competent authority and make the results thereof available to the competent authority; the cost of the audit shall be paid by the provider.

3. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance and the effects thereof on the security of the networks and services.

4. Member States shall ensure that, in order to implement Article 40, the competent authorities have the power to obtain the assistance of a Computer Security Incident Response Team ('CSIRT') designated pursuant to Article 9 of Directive (EU) 2016/1148 in relation to issues falling within the tasks of the CSIRTs pursuant to point 2 of Annex I to that Directive.

5. The competent authorities shall, where appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities, the competent authorities within the meaning of Article 8(1) of Directive (EU) 2016/1148 and the national data protection authorities.

In addition, we include full or partial text of several recitals that are of direct or indirect relevance for ensuring security of networks and services:

(17) Interpersonal communications services are services that enable interpersonal and interactive exchange of information, covering services like traditional voice calls between two individuals but also all types of emails, messaging services, or group chats. Interpersonal communications services only cover communications between a finite, that is to say not potentially unlimited, number of natural persons, which is determined by the sender of the communication.

(18) […] The mere use of a number as an identifier should not be considered to be equivalent to the use of a number to connect with publicly assigned numbers and should therefore, in itself, not be considered to be sufficient to qualify a service as a number-based interpersonal communications service.

(94) […] Security measures should take into account, as a minimum, all the relevant aspects of the following elements: as regards security of networks and facilities: physical and environmental security, security of supply, access control to networks and integrity of networks; as regards handling of security incidents: handling procedures, security incident detection capability, security incident reporting and communication; as regards business continuity management: service continuity strategy and contingency plans, disaster recovery capabilities; as regards monitoring, auditing and testing: monitoring and logging policies, exercise contingency plans, network and service testing, security assessments and compliance monitoring; and compliance with international standards.

(95) […] independent inter personal communications services, […] are also subject to appropriate security requirements in accordance with their specific nature and economic importance. Providers of such services should thus also ensure a level of security appropriate to the risk posed. Given that providers of number -independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. Therefore, where justified on the basis of the actual assessment of the security risks involved, the measures taken by providers of number-independent interpersonal communications services should be lighter. […]

(96) Providers […] should inform users of particular and significant security threats and of measures they can take to protect the security of their communications, for instance by using specific types of software or encryption technologies. […]

(97) In order to safeguard security of networks and services, and without prejudice to the Member States' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences, the use of encryption for example, end-to-end where appropriate, should be promoted and, where necessary, encryption should be mandatory in accordance with the principles of security and privacy by default and by design.

(98) Competent authorities should ensure that the integrity and availability of public electronic communications networks are maintained. The European Union Agency for

Network and Information Security ('ENISA') should contribute to an enhanced level of security of electronic communications by, inter alia, providing expertise and advice, and promoting the exchange of best practices. The competent authorities should have the necessary means to perform their duties, including powers to request the information necessary to assess the level of security of networks or services. They should also have the power to request comprehensive and reliable data about actual security incidents that have had a significant impact on the operation of networks or services. They should, where necessary, be assisted by Computer Security Incident Response Teams ('CSIRTs') established by Directive (EU) 2016/ 1148 of the European Parliament and of the Council[8]. In particular, CSIRTs may be required to provide competent authorities with information about risks and security incidents affecting public electronic communications networks and publicly available electronic communications services, and recommend ways to address them.

3.2 TERMINOLOGY

We reiterate some of the definitions and terms used extensively in this document.

3.2.1 Security of networks and services

Article 2 (21) of the EECC defines '*security of networks and services*' as the ability of electronic communications networks and services to resist, at a given level of confidence, any action that compromises the availability[9], authenticity[10], integrity[11] or confidentiality[12] 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.

3.2.2 Security incidents

Article 2 (42) of the EECC defines '*security incident'* as an event having an actual adverse effect on the security of electronic communications networks or services.

3.2.3 Competent authorities

The term *'competent authorities'* is used in this document in line with the terminology used in Article 41 of the EECC, meaning those national authorities with competences to supervise Article 40, the implementation of security measures in the national telecom sector[13]. In practice these competences may be split or shared between multiple national authorities.

3.2.4 Security measures

Article 40 of the EECC defines *'security measures'* as *technical and organisational measures* for managing the risks posed to the security of networks and services.

3.2.5 NI-ICS

Article 2 (7) of the EECC defines a *'number-independent interpersonal communications service'* as an interpersonal communications service, which does not connect with "publicly assigned numbering resources", meaning (national or international) telephone numbers, or which does not enable communication with these (national or international) telephone numbers. In this document we use the acronym NI ICS for the sake of brevity.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).
[9] Availability is typically defined as a *property of being accessible and usable on demand by an authorized entity* (ISO/IEC 27000:2018)
[10] Authenticity is typically defined as a *property that an entity is what it claims to be* (ISO/IEC 27000:2018)
[11] Integrity is typically defined as a *property of accuracy and completeness* (ISO/IEC 27000:2018)
[12] Confidentiality is typically defined as a *property that information is not made available or disclosed to unauthorized individuals, entities, or processes* (ISO/IEC 27000:2018)
[13] Previous versions of this guideline used the abbreviation NRA, National Regulatory Authority.

4. SECURITY MEASURES

In this section we provide a list of 29 security objectives which competent authorities should take into account when assessing compliance of providers to Article 40 of the EECC.

We stress that this is only a guideline for competent authorities and that it is at the discretion of competent authorities to mandate or recommend different or additional security objectives, or different security measures.

Note that some of the security objectives or security measures may not be relevant or appropriate in all settings for all types of providers, depending on the type of networks or services offered[14].

4.1 ASSETS IN SCOPE AND RISK ASSESSMENT

The scope of the security measures is defined as follows.

Assets in scope: All assets[15] of the provider (including relevant third party assets) which, when compromised and/or failing, can have a negative impact on the security of networks and services.

Providers should perform analysis, specific for their particular setting, to determine which assets are in scope and should subsequently conduct risk assessment to determine which security measures are appropriate. Risk assessments need updating, to address changes and past incidents, because risks change over time. Note that this guideline does *not* address risk assessment in detail. There are several standard methodologies providers could use for this (see References).

Remark on classical information security risk management: *It is good to mention here that there is a lot of information security literature which focusses on how an organization can manage the information security risks related to the use of network and information security, for example through the establishment of an information security management system. A well-known example of a related standard is ISO 27001. Article 40 of the EECC, however, focuses primarily on risks for the users who rely on the networks and communications services provided by the provider, and not the risks for the provider. This means in practice that, while enterprise risk management methodologies are very helpful, they may not be fully suitable to be used for the EECC without adaptation.*

4.1.1 Primary and secondary assets

In some literature there is a distinction between primary assets and secondary (supporting) assets. In this context (Article 40 of the EECC) the primary assets are the electronic communication networks and services provided by the provider.

In this document when we speak about assets we mean the *secondary* assets i.e. the systems and processes supporting the provision of electronic communications networks and services (such as base stations, routers, registers, power supply, etc.).

[14] For example, in the case of dark fibre providers certain security measures may not be applicable because these providers do not directly deal with subscribers and do not have much staff.
[15] A widely used generic definition of an asset is “something that has value”. We provide more details about assets in sections 4.1.1 and 4.1.2.

4.2 CRITICAL ASSETS

In the remainder of this document, we use the term *critical assets* for assets (network and information systems, processes, data, etc.) which, when compromised and/or fail, there would be a *severe* impact on the security of networks and services. When determining *severity* of the impact, factors like *type* (e.g. whether the materialisation of a threat leads to compromised confidentiality, integrity and/or availability of the network) and *scale* of impact (e.g. in terms of affected users, duration, sensitivity of information altered or accessed) could be considered[16]. Parameters related to determination of significance of the impact of a security incident as listed in EECC Article 40 (2) and reproduced in section 3.1 should also be taken into account.

Critical assets should (obviously) be protected with priority.

4.2.1 Personnel and key personnel

In this document the term "personnel" refers to employees, contractors, and third-party users. We use the term "key personnel" to refer to the key roles in the organization with respect to security of networks and services. Now providers are not all the same and organizations and job profiles are different, but typically this would include roles like the CEO, the CIO, the CISO, the business continuity manager and system administrators of critical systems.

4.2.2 Third parties and outsourcing

In this document we use the term "third parties" to refer to parties (organizations, individuals) the provider works with to deliver the services, i.e. vendors the provider buys products from, suppliers, consultants who advise the provider, auditors auditing the provider, companies the provider outsources work to, and so on[17].

Third parties and third party assets are in scope just as if they were assets of the providers. In other words, even if certain processes are outsourced, the provider remains responsible for ensuring that appropriate security measures are taken to protect the security of networks and services it is providing.

4.3 STRUCTURE OF THE SECURITY MEASURES

This document lists 29 security objectives[18] which have been derived from a set of international and national standards that are commonly used by providers in the EU's electronic communication sector (see References). For each of the security objectives we list more detailed security measures which could be implemented by providers to reach the security objective. For each security objective we also list detailed evidence which could indicate that the measures are in place. Note that the security measures or the evidence should not be seen as a baseline or list of minimum requirements for providers (see the remark below).

The security measures are grouped in 3 different sophistication levels, defined as follows.

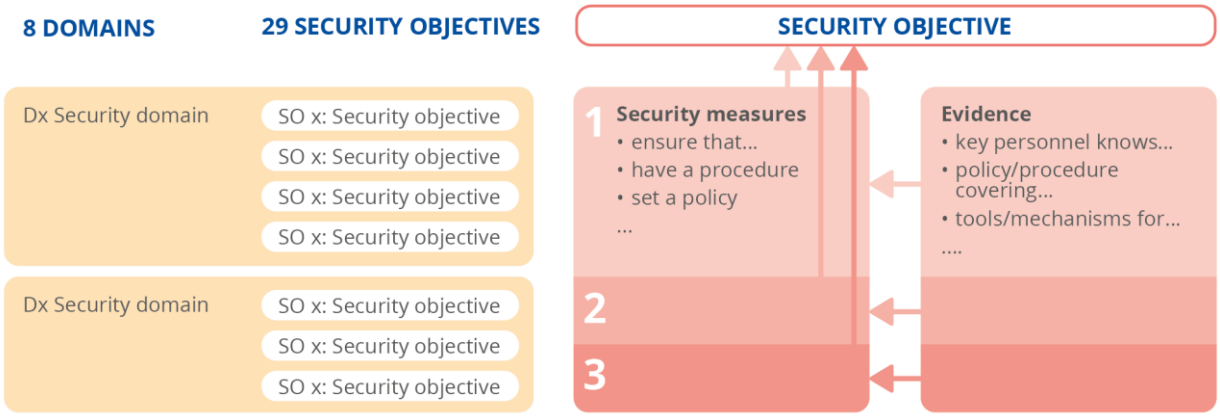
[16] This criteria is in line with the criteria used in the EU Coordinated risk assessment of the cybersecurity of 5G networks. Further guidance related to critical asset identification pertaining to 5G networks specifically is provided in the supplement of this document - security profile for 5G MNOs.
[17] So in this document the term third parties does not refer to customers, the public, or government or regulatory authorities.
[18] In information security governance literature these are also sometimes referred to as control objectives.

Figure 3: Structure of the security measures

The levels are cumulative. In other words, at level 2 we do not repeat the security measures and the evidence for level 1, for the sake of brevity, but they are understood to be included (accumulated). And similarly at level 3 the security measures are understood to include the ones of levels 1 and 2. If the measures at level 1 are not (fully) implemented than this could be called level 0, but we do not explicitly mention level 0 in this document.

The overall structure of the security objectives and security measures is depicted as following.

Figure 4: Overall structure of the security objectives and security measures



***Remark about baselines and minimum security measures**: Neither the high-level security objectives in this document nor the detailed security measures should be seen as binding recommendations about which are appropriate security measures for providers to take. So, for example, the security measures at level 1 are not to be considered "the minimum" for the sector. Risks are different for different providers and it depends on the specifics (the setting, the type of provider, the type of services offered, the assets in question, etc.) which security objectives are important and which measures are appropriate.*

***Remark about separate measures**: We list a number of individual security measures, one by one. But this should not be seen as a recommendation to split security activities into parts, or to keep separate standalone documents or files for each measure. For example, one could imagine using a single inventory of assets could be used for risk assessment, change management and asset management procedures.*

***Remark about technological limitations and implementation feasibility**: Some of the recommended measures may be more difficult (or not simply not feasible) to implement in an old or legacy systems with outdated equipment, using old technology and/or relying on old standards and network protocols. In such cases, it is advisable to have limitations and exclusions stated and documented and to consider including formal decommissioning plans for these old or legacy systems.*

4.4 SECURITY OBJECTIVES AND SECURITY MEASURES

Below we list 29 high-level security objectives (SO1, SO2, …), grouped in 8 domains (D1, D2, …). For each security objective we list detailed security measures, which could be implemented by the provider, as well as the type of evidence that could be taken into consideration by an auditor, for example, when assessing if measures are in place.

We list the 8 domains and the 29 security objectives below for the sake of reference:

D1: GOVERNANCE AND RISK MANAGEMENT

- SO1: Information security policy
- SO2: Governance and risk management
- SO3: Security roles and responsibilities
- SO4: Security of third party assets

D2: HUMAN RESOURCES SECURITY

- SO5: Background checks
- SO6: Security knowledge and training
- SO7: Personnel changes
- SO8: Handling violations

D3: SECURITY OF SYSTEMS AND FACILITIES

- SO9: Physical and environmental security
- SO10: Security of supplies
- SO11: Access control to network and information systems
- SO12: Integrity of network and information systems
- SO13: Use of encryption
- SO14: Protection of security critical data

D4: OPERATIONS MANAGEMENT

- SO15: Operational procedures
- SO16: Change management
- SO17: Asset management

D5: INCIDENT MANAGEMENT

- SO18: Incident management procedures
- SO19: Incident detection capability
- SO20: Incident reporting and communication

D6: BUSINESS CONTINUITY MANAGEMENT

- SO21: Service continuity strategy and contingency plans
- SO22: Disaster recovery capabilities

D7: MONITORING, AUDITING AND TESTING

- SO23: Monitoring and logging policies
- SO24: Exercise contingency plans
- SO25: Network and information systems testing
- SO26: Security assessments
- SO27: Compliance monitoring

D8: THREAT AWARENESS

- SO28: Threat intelligence
- SO29: Informing users about threats

4.4.1 D1: Governance and risk management

The domain "Governance and risk management" covers the security objectives related to governance and management of network and information security risks.

4.4.1.1 SO1: Information security policy

Establish and maintain an appropriate information security policy.

	Security measures	Evidence
1	a) Set a high level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. ii. Key personnel are aware of the security policy and its objectives (interview).
2	c) Set detailed information security policies for critical assets and business processes. d) Make all personnel aware of the security policy and what it implies for their work. e) Review the security policy following incidents.	iii. Documented information security policies, approved by management, including applicable law and regulations, accessible to personnel. iv. Personnel are aware of the information security policy and what it implies for their work (interview). v. Review comments or change logs for the policy.
3	f) Review the information security policies periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	vi. Information security policies are up to date and approved by senior management. vii. Logs of policy exceptions, approved by the relevant roles. viii. Documentation of review process, taking into account changes and past incidents.

4.4.1.2 SO2: Governance and risk management

Establish and maintain an appropriate governance and risk management framework, to identify and address risks for the communications networks and services.

	Security measures	Evidence
1	a) Set a high level security policy addressing the security of networks and services. b) Make key personnel aware of the security policy.	i. List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security of networks and services ii. Key personnel know the main risks (interview).

2	c) Set detailed information security policies for critical assets and business processes d) Set up a risk management methodology and/or tools based on industry standards. e) Ensure that key personnel use the risk management methodology and tools. f) Review the risk assessments following changes or incidents. g) Ensure residual risks are accepted by management.	iii. Documented risk management methodology and/or tools. iv. Guidance for personnel on assessing risks. v. List of risks and evidence of updates/reviews. vi. Review comments or change logs for risk assessments. vii. Management approval of residual risks.
3	h) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	viii. Information security policies are up to date and approved by senior management. ix. Logs of policy exceptions, approved by the relevant roles. x. Documentation of review process, taking into account changes and past incidents.

4.4.1.3 SO3: Security roles and responsibilities

Establish and maintain an appropriate structure of security roles and responsibilities.

	Security measures	Evidence
1	a) Assign security roles and responsibilities to personnel. b) Make sure the security roles are reachable in case of security incidents.	i. List of security roles (CISO, DPO, business continuity manager, etc.), who occupies them and contact information.
2	c) Personnel is formally appointed in security roles. d) Make personnel aware of the security roles in your organisation and when they should be contacted.	ii. List of appointments (CISO, DPO, etc.), and description of responsibilities and tasks for security roles (CISO, DPO, etc.). iii. Awareness/dissemination material for personnel explaining security roles and when/how they should be contacted.
3	e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	iv. Up-to-date documentation of the structure of security role assignments and responsibilities v. Documentation of review process, taking into account changes and past incidents.

4.4.1.4 SO4: Security of third party assets

Establish and maintain a policy, with security requirements for contracts with third parties (see Section 4.2.2), to ensure that dependencies on third parties do not negatively affect security of networks and/or services.

	Security measures	Evidence
1	a) Include security requirements in contracts with third-parties.	i. Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centres, interconnections, shared facilities, etc.
2	b) Set a security policy for contracts with third-parties. c) Ensure that all procurement of services/products from third-parties follows the policy. d) Review security policy for third parties, following incidents or changes. e) Demand specific security standards in third-party supplier's processes during procurement. f) Mitigate residual risks that are not addressed by the third party.	ii. Documented security policy for contracts with third parties. iii. List of contracts with third-parties. iv. Contracts for third party services contain security requirements, in line with the security policy for procurement. v. Review comments or change logs of the policy. vi. Contracts with equipment suppliers contain requirements for adhering to security best practices and industry standards[19]. vii. Residual risks resulting from dependencies on third parties are listed and mitigated.
3	g) Keep track of security incidents related to or caused by third-parties. h) Periodically review and update security policy for third parties at regular intervals, taking into account past incidents, changes, etc.	viii. List of security incidents related to or caused by engagement with third-parties. ix. Documentation of review process of the policy.

[19] This should include demonstrating quality levels of information security processes, security maintenance of products and equipment throughout its lifetime and built-in of security in the product development processes.

4.4.2 D2: Human resources security

The domain "Human resources security" covers the security objectives related to personnel.

4.4.2.1 SO5: Background checks

Perform appropriate background checks[20] on personnel if required for their duties and responsibilities.

	Security measures	Evidence
1	a) Check professional references of key personnel (system administrators, security officers, guards, etc.).	i. Documentation of checks of professional references for key personnel.
2	b) Perform background checks/screening for key personnel, when needed and legally permitted. c) Set up a policy and procedure for background checks.	ii. Policy and procedure for background checks/screenings. iii. Guidance for personnel about when/how to perform background checks/screenings.
3	d) Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	iv. Review comments or change logs of the policy/procedures.

4.4.2.2 SO6: Security knowledge and training

Ensure that personnel have sufficient security knowledge and that they are provided with regular security training.

	Security measures	Evidence
1	a) Provide key personnel with relevant training and material on security issues.	i. Key personnel have followed security trainings and have sufficient security knowledge (interview).
2	b) Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. c) Organise trainings and awareness sessions for personnel on security topics important for your organisation.	ii. Personnel have participated in awareness sessions on security topics. iii. Documented program for training on security skills, including, objectives for different roles and how to reach it (by e.g. training, awareness raising, etc.).
3	d) Review and update the training program periodically, taking into account changes and past incidents. e) Test the security knowledge of personnel.	iv. Updated security awareness and training program v. Results of tests of the security knowledge of personnel. vi. Review comments or change logs for the program.

[20] Background checks should be appropriate and proportionate to the risk assessed, in particular when they apply to personnel other than providers' own employees, e.g. for contractors and third-party users.

4.4.2.3 SO7: Personnel changes

Establish and maintain an appropriate process for managing changes in personnel or changes in their roles and responsibilities.

	Security measures	Evidence
1	a) Following changes in personnel revoke access rights, badges, equipment, etc., if no longer necessary or permitted. b) Brief and educate new personnel on the policies and procedures in place.	i. Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, etc. ii. Evidence that new personnel has been briefed and educated about policies and procedures in place.
2	c) Implement policy/procedures for personnel changes, taking into account timely revocation of access rights, badges and equipment. d) Implement policy/procedures for education and training for personnel in new roles.	iii. Documentation of process for personnel changes, including, responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles. iv. Evidence that personnel changes have been carried out according to the process and that access rights have been updated timely (e.g. checklists).
3	e) Periodically check that the policy/procedures are effective. f) Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents.	v. Evidence of checks of access rights etc. vi. Up to date policy/procedures for managing personnel changes. vii. Review comments or change logs.

4.4.2.4 SO8: Handling violations

Establish and maintain a disciplinary process for personnel who violate security policies and have a broader process that covers security incidents caused by violations by personnel.

	Security measures	Evidence
1	a) Hold personnel accountable for security incidents caused by violations of policies, for example via the employment contract.	i. Rules for personnel, including responsibilities, code of conduct, violations of policies, etc., possibly as part of employment contracts.
2	b) Set up procedures for violations of policies by personnel.	ii. Documentation of procedures, including types of violations which may be subject to disciplinary actions, and which disciplinary actions may be taken.
3	c) Periodically review and update the disciplinary process, based on changes and past incidents.	iii. Review comments or change logs

4.4.3 Security of systems and facilities

This domain "Security of systems and facilities" covers the physical and logical security of network and information systems and facilities.

4.4.3.1 SO9: Physical and environmental security

Establish and maintain the appropriate physical and environmental security of network and information systems and facilities.

	Security measures	Evidence
1	a) Prevent unauthorized physical access to facilities and infrastructure and set up adequate environmental controls, to protect provider assets[21] against unauthorized access, burglary, fire, flooding, etc.[22]	i. Basic implementation of physical security measures and environmental controls , such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, etc.
2	b) Implement a policy for physical security measures and environmental controls. c) Industry standard implementation of physical and environmental controls. d) Apply reinforced controls for physical access to critical assets[23].	ii. Documented policy for physical security measures and environmental controls, including description of facilities and systems in scope. iii. Physical and environmental controls, like electronic control of entrance and audit trail, segmentation of spaces according to authorization levels, automated fire extinguishers with halocarbon gases, etc. iv. The policy includes lists of critical assets and reinforced physical controls for accessing these assets.
3	e) Evaluate the effectiveness of physical and environmental controls periodically. f) Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents.	v. Up to date policy for physical security measures and environmental controls vi. Documentation about evaluation of environmental control, review comments or change logs.

[21] Including third party assets, where applicable.
[22] Security controls should be selected based on the risk assessment, which should also take in consideration current and forecasted environmental security risks – e.g. related to climate change.
[23] For example, physical access to such assets should only be granted to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored.

4.4.3.2 SO10: Security of supplies

Establish and maintain appropriate security of critical supplies (for example electric power, fuel, cooling etc.[24]).

	Security measures	Evidence
1	a) Ensure security of critical supplies.	i. Security of critical supplies is protected in a basic way, for example, backup power and/or backup fuel is available.
2	b) Implement a policy for security of critical supplies. c) Implement industry standard security measures to protect critical supplies and supporting facilities (e.g. passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.).	ii. Documented policy to protect critical supplies such as electrical power, fuel, etc., describing different types of supplies, and the security measures protecting the supplies. iii. Evidence of industry standard measures to protect the security of critical supplies
3	d) Implement state of the art security measures to protect critical supplies (such as active cooling, UP, hot standby power generators, SLAs with fuel delivery companies, redundant cooling and power backup systems). e) Review and update policy and procedures to secure critical supplies regularly, taking into account changes and past incidents.	iv. Evidence of state of the art measures to protect security of critical supplies. v. Updated policy for securing critical supplies and supporting facilities, review comments and/or change logs.

4.4.3.3 SO11: Access control to network and information systems

Establish and maintain appropriate (logical) access controls for access to network and information systems.

	Security measures	Evidence
1	a) Users and systems have unique ID's and are authenticated before accessing services or systems. b) b) Implement logical access control mechanism for network and information systems to allow only authorized use.	i. Access logs show unique identifiers for users and systems when granted or denied access. ii. Overview of authentication and access control methods for systems and users.

[24] Only examples are given, the list is not exhaustive. Critical supplies could be any other supplies that essential for providers to provide the service.

2	c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. d) Choose appropriate authentication mechanisms, depending on the type of access. e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations. f) Reinforce controls for remote access to critical assets of network and information systems by third parties.	iii. Access control policy including description of roles, groups, access rights, procedures for granting and revoking access. iv. Different types of authentication mechanisms for different types of access. v. Log of access control policy violations and exceptions, approved by the security officer. vi. Principles of least privilege and segregation of duties are documented and applied where appropriate. vii. Remote access to critical assets by third-parties is minimised and subjected to strict access controls, including state of the art authentication, authorization and auditing controls, especially for privileged accounts.
3	g) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. h) Access control policy and access control mechanisms are reviewed and when needed revised.	viii. Reports of (security) tests of access control mechanisms. ix. Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). x. Logs of intrusion detection and anomaly detection systems. xi. Updates of access control policy, review comments or change logs. xii. Documented risk analysis for the application of logging and retention xiii. Procedures to ensure that access controls are in effect all the time and that they evolve with the network.

4.4.3.4 SO12: Integrity of network and information systems

Establish and maintain integrity of network and information systems and protect from viruses, code injections, and other malware that can alter the functionality of systems.

	Security measures	Evidence
1	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls. b) Check for malware on (internal) network and information systems.	i. Software and data in network and information systems is protected using input controls, firewalls, encryption and signing. ii. Malware detection systems are present, and up to date.
2	c) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems. d) Apply reinforced software integrity, update and patch management controls for critical assets in virtualised networks.	iii. Documentation about how the protection of software and data in network and information system is implemented. iv. Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). v. Logs of intrusion detection and anomaly detection systems. vi. Adequate tools and processes to ensure software integrity[25] when performing software updates and applying security patches to critical assets in virtualised networks.
3	e) Set up state of the art controls to protect integrity of systems. f) Evaluate and review the effectiveness of measures to protect integrity of systems.	vii. State of the art controls to protect integrity of systems, such as code signing, tripwire, etc. viii. Documentation of process for checking logs of anomaly and intrusion detection systems.

4.4.3.5 SO13: Use of encryption

Ensure adequate use of encryption to prevent and/or minimise the impact of security incidents on users and on other networks and services.

	Security measures	Evidence
1	a) Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data[26] during its storage in and/or transmission via networks.	i. Description of main data flows, and the encryption protocols and algorithms used for each flow. ii. Description of justified exclusions and limitations[27] in implementing encryption.

[25] Including reliable identification, monitoring and tracking of changes and the status of patches.
[26] The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents.
[27] Ability to implement encryption may also be influenced by technological limitations, like in the case of legacy networks or when old equipment and network protocols are used.

2	b) Implement encryption policy. c) Use industry standard encryption algorithms and the corresponding recommended lengths of encryption keys.	iii. Documented encryption policy including details about the cryptographic algorithms and corresponding cryptographic keys, according to international best practices and standards. iv. Documented justified exclusions that provide rationale for when data is not encrypted, including the related impact assessment.
3	d) Review and update of encryption policy. e) Use state of the art encryption algorithms.	v. Updated encryption policy, review comments and/or change logs. vi. Encryption policy includes details about the state of the art cryptographic protocols used.

4.4.3.6 SO14: Protection of security critical data

Ensure that cryptographic key material and other security-critical data is adequately protected.

	Security measures	Evidence
1	a) Make sure that cryptographic key material, shared secrets and passwords and similar security-critical data is not disclosed or tampered with. b) Access to private keys is strictly controlled and monitored.	i. Security critical data is protected using security best practices and standards for protection mechanisms (like split knowledge and dual control, encryption, hashing, secure hardware etc.). ii. Description of mechanisms for controlling and monitoring access to private keys.
2	c) Implement policy for management of cryptographic keys. d) Implement policy for management of user passwords.	iii. Key management policy including roles, responsibilities and controls for the use, protection and lifetime of cryptographic keys throughout their life cycle including controls for access to and backup and recovery of private keys. iv. User password management policy including processes, methods and techniques for secure storing of user passwords using industry best practices[28].
3	e) Review and update of key management policy. f) Review and update of user password management policy.	v. Updated key management policy, review comments and/or change logs. vi. Updated user password management policy, review comments and/or change logs.

[28] E.g. hashing using appropriate hashing algorithms, salting etc.

4.4.4 D4: Operations management

The domain “Operations management” covers operational procedures, change management and asset management.

4.4.4.1 SO15: Operational procedures

Establish and maintain operational procedures for the operation of critical network and information systems by personnel.

	Security measures	Evidence
1	a) Set up operational procedures and assign responsibilities for operation of critical systems.	i. Documentation of operational procedures and responsibilities for key network and information systems.
2	b) Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures.	ii. Documented policy for operation of critical systems, including an overview of network and information systems in scope.
3	c) Review and update the policy/procedures for operation of critical systems, taking into account incidents and/or changes.	iii. Updated policy/procedures for critical systems, review comments and/or change logs.

4.4.4.2 SO16: Change management

Establish change management procedures for critical network and information systems in order to minimise the likelihood of incidents resulting from changes.

	Security measures	Evidence
1	a) Follow predefined methods or procedures when making changes to critical systems	i. Documentation describing predefined methods or procedures followed when making changes to critical systems.
2	b) Implement policy/procedures for change management, to make sure that changes of critical systems are always done following a predefined way. c) Document change management procedures, and record for each change the steps of the followed procedure.	ii. Documentation of change management policy/procedures including, systems subject to the policy, objectives, roll back procedures, etc. iii. For each change, a report is available describing the steps and the result of the change.
3	d) Review and update change management procedures regularly, taking into account changes and past incidents.	iv. Up to date change management procedures, review comments and/or change logs.

4.4.4.3 SO17: Asset management

Establish and maintain asset management procedures and configuration controls in order to manage availability of critical assets and configurations of critical network and information systems.

	Security measures	Evidence
1	a) Identify critical assets and configurations of critical systems.	i. List of critical assets and critical systems. The list should include all critical assets and critical systems for network or service, operational and security, including relevant third party assets.
2	b) Implement policy/procedures for asset management and configuration control.	ii. Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, the objectives of asset management. iii. An asset inventory or inventories, containing critical assets and the dependency between assets. iv. A configuration control inventory or inventories, containing configurations of critical systems.
3	c) Review and update the asset management policy regularly, based on changes and past incidents.	v. Up to date asset management policy/procedures, review comments and/or change logs.

4.4.5 D5: Incident management

The domain “Incident management” covers detection of, response to, incident reporting, and communication about incidents[29].

4.4.5.1 SO18: Incident management procedures

Establish and maintain procedures for managing incidents, and forwarding them to the appropriate personnel (triage).

	Security measures	Evidence
1	a) Make sure personnel is available and prepared to manage and handle incidents. b) Keep a record of all major incidents.	i. Personnel is aware of how to deal with incidents and when to escalate. ii. Inventory of major incidents and per incident, impact, cause, actions taken and lessons learnt.
2	c) Implement policy/procedures for managing incidents.	iii. Policy/procedures for incident management, including, types of incidents that could occur, objectives, roles and responsibilities, detailed description, per incident type, how to manage the incident, when to escalate to senior management (e.g. CISO) etc.
3	d) Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate future occurrence of this type of incident. e) Evaluate incident management policy/procedures based on past incidents.	iv. Individual reports of the handling of major incidents. v. Up to date incident management policy/procedures, review comments and/or change logs.

[29] For the definition of ‘incident’ used in this document, see Section 2.

4.4.5.2 SO19: Incident detection capability

Establish and maintain an incident detection capability that detects incidents[30].

	Security measures	Evidence
1	a) Set up processes or systems for incident detection.	i. Documented examples of past incidents that were detected and timely forwarded to the appropriate people.
2	b) Implement industry standard systems and procedures for incident detection. c) Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	ii. Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, security helpdesk for personnel, reports and advisories from Computer Emergency Response Teams (CERTs), tools to spot anomalies, etc. iii. Network Operation Centres (NOC) and/or Security Operation Centres (SOC)[31] for ensuring visibility and effective network monitoring and to detect anomalies and to identify and avoid threats.
3	d) Review systems and processes for incident detection regularly and update them taking into account changes and past incidents. e) Implement state of the art systems and procedures for incident detection.	iv. Up to date documentation of incident detection systems and processes. v. Documentation of review of the incident detection process, review comments, and/or change logs. vi. NOC/SOC solutions with state of the art capabilities are used - e.g. SOAR (Security Orchestration, Automation and Response), ensuring integration with threat and vulnerability management and incident response function, security operations automation etc.

[30] Measures to detect *incidents* described under this security objective should be understood in a broader sense as to be able to also detect serious events that may lead to incidents

[31] Where justified on the basis of the actual assessment of the security risks involved, operators should run their NOC and/or SOC on premise, inside the country and/or inside the EU.

4.4.5.3 SO20: Incident reporting and communication

Establish and maintain appropriate incident reporting and communication procedures, taking into account national legislation on incident reporting to government authorities[32].

	Security measures	Evidence
1	a) Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.	i. Evidence of past communications and incident reporting.
2	b) Implement policy and procedures for communicating and reporting about incidents.	ii. Documented policy and procedures for communicating and reporting about incidents, describing reasons/motivations for communicating or reporting (business reasons, legal reasons etc.), the type of incidents in scope, the required content of communications, notifications or reports, the channels to be used, and the roles responsible for communicating, notifying and reporting. iii. Templates for incident reporting and communication.
3	c) Evaluate past communications and reporting about incidents. d) Review and update the reporting and communication plans, based on changes or past incidents.	iv. List of incident reports and past communications about incidents. v. Up to date incident response and communication policy, review comments, and/or change logs.

[32] For example, Article 40 of the EECC, which is being transposed by all EU member states to national legislation, included requirement to report to a competent authority security incident that has had a significant impact on the operation of networks or services.

4.4.6 D6: Business continuity management

The domain "Business continuity management" covers continuity strategies and contingency plans to mitigate major failures and natural or man-made disasters.

4.4.6.1 SO21: Service continuity strategy and contingency plans

Establish and maintain contingency plans and a strategy for ensuring continuity of networks and communication services provided.

	Security measures	Evidence
1	a) Implement a service continuity strategy for the communications networks and/or services provided.	i. Documented service continuity strategy, including recovery time objectives for key services and processes
2	b) Implement contingency plans for critical systems. c) Monitor activation and execution of contingency plans, registering successful and failed recovery times. d) Implement contingency plans for dependent and inter-dependent critical sectors and services[33].	ii. Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives. iii. Decision process for activating contingency plans. iv. Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time. v. Map of critical sectors and services essential for and/or dependent on the continuity of the network and service operation and contingency plans for mitigating the impact related to dependent and interdependent sectors and services.
3	e) Review and revise service continuity strategy periodically. f) Review and revise contingency plans, based on past incidents and changes.	vi. Up to date continuity strategy and contingency plans, review comments, and/or change logs.

[33] When determining dependent critical sectors and services, providers may take into account those services that are dependent on the continuity of the network and service operation which are essential for the maintenance of critical societal and/or economic activities and for which an incident would have significant disruptive effects on the provision of that service. One possible way for identifying such dependent services may be to pass the obligation to service consumers to inform the providers if their service is considered critical.

4.4.6.2 SO22: Disaster recovery capabilities

Establish and maintain an appropriate disaster recovery capability for restoring network and communication services in case of natural and/or major disasters.

	Security measures	Evidence
1	a) Prepare for recovery and restoration of services following disasters.	i. Measures are in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, etc.[34]
2	b) Implement policy/procedures for deploying disaster recovery capabilities. c) Implement industry standard disaster recovery capabilities. or be assured they are available from third parties (such as national emergency networks).	ii. Documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third parties). iii. Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, etc.
3	d) Set up state of the art disaster recovery capabilities to mitigate natural and/major disasters. e) Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	iv. State of the art disaster recovery capabilities, such as full redundancy and failover mechanisms to handle natural and/or major disasters. v. Updated documentation of disaster recovery capabilities in place, review comments and/or change logs

[34] Not all of the listed evidence may be applicable in scenarios with large geographically extended national Telco networks, for assets offering direct connectivity to end users

4.4.7 D7: Monitoring, auditing and testing

The domain “Monitoring, auditing and testing” covers monitoring, testing and auditing of network and information systems and facilities.

4.4.7.1 SO23: Monitoring and logging policies

Establish and maintain systems and functions for monitoring and logging of relevant security events in critical network and communication systems.

	Security measures	Evidence
1	a) Implement monitoring and logging of critical systems.	i. Logs and monitoring reports of critical network and information systems.
2	b) Implement policy for logging and monitoring of critical systems. c) Set up tools for monitoring critical systems d) Set up tools to collect and store logs of critical systems.	ii. Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs. iii. Tools for monitoring systems and collecting logs. iv. List of monitoring data and log files, in line with the policy.
3	e) Set up tools for automated collection and analysis of monitoring data and logs. f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	v. Tools to facilitate structural recording and analysis of monitoring and logs. vi. Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs.

4.4.7.2 SO24: Exercise contingency plans

Establish and maintain policies for testing and exercising backup and contingency plans, where needed in collaboration with third parties.

	Security measures	Evidence
1	a) Exercise and test backup and contingency plans to make sure systems and processes work and personnel is prepared for large failures and contingencies.	i. Reports of past exercises of backup and contingency plans.
2	b) Implement program for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over time. c) Make sure that the issues and lessons learnt from exercises are addressed by the responsible people and that the relevant processes and systems are updated accordingly.	ii. Exercise program for backup and contingency plans, including types of contingencies, frequency, roles and responsibilities, templates and procedures for conducting exercises, templates for exercise reports. iii. Reports about exercises and drills showing the execution of contingency plans, including lessons learnt from the exercises. iv. Issues and lessons learnt from past exercises have been addressed by the responsible people
3	d) Review and update the exercise plans, taking into account changes and past incidents and contingencies which were not covered by the exercise program. e) Involve suppliers, and other 3rd parties, like business partners or customers in exercises.	v. Updated exercises plans, review comments, and/or change logs. vi. Input from suppliers and other 3rd parties involved about how to improve exercise scenarios.

4.4.7.3 SO25: Network and information systems testing

Establish and maintain policies for testing network and information systems[35], particularly when connecting to new networks or systems.

	Security measures	Evidence
1	a) Test networks and information systems before using them or connecting them to existing systems.	i. Test reports of the network and information systems, including tests after big changes or the introduction of new systems.
2	b) Implement policy/procedures for testing network and information systems, c) Implement tools for automated testing	ii. Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates.
3	d) Review and update the policy/procedures for testing, taking into account changes and past incidents.	iii. List of test reports. iv. Updated policy/procedures for testing networks and information systems, review comments, and/or change log.

4.4.7.4 SO26: Security assessments

Establish and maintain an appropriate policy for performing security assessments of network and information systems.

	Security measures	Evidence
1	a) Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes. .	i. Reports from past security scans and security tests.
2	b) Implement policy/procedures for security assessments and security testing.	ii. Documented policy/procedures for security assessments and security testing, including, which assets, in what circumstances, the type of security assessments and tests, frequency, approved parties (internal or external), confidentiality levels for assessment and test results and the objectives security assessments and tests.

[35] Testing in this context refers primarily to testing of security related functionality, rather than to general-purpose ICT functionality testing

3	c) Evaluate the effectiveness of policy/procedures for security assessments and security testing. d) Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents.	iii. List of reports about security assessment and security tests. iv. Reports of follow up actions on assessment and test results. v. Up to date policy/procedures for security assessments and security testing, review comments, and/or change log.

4.4.7.5 SO27: Compliance monitoring

Establish and maintain a policy for monitoring compliance to standards and legal requirements.

	Security measures	Evidence
1	a) Monitor compliance to standards and legal requirements.	i. Reports describing the result of compliance monitoring.
2	b) Implement policy/procedures for compliance monitoring and auditing.	ii. Documented policy/procedures for monitoring compliance and auditing, including what (assets, processes, infrastructure), frequency, guidelines who should carry out audits (in- or external), relevant security policies that are subject to compliance monitoring and auditing, the objectives and high level approach of compliance monitoring and auditing, templates for audit reports. iii. Detailed monitoring and audit plans, including long term high level objectives and planning
3	c) Evaluate the policy/procedures for compliance and auditing. d) Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents.	iv. List of all compliance and audit reports v. Updated policy/procedures for compliance and auditing, review comments, and/or change logs.

4.4.8 D8: Threat awareness

The domain "Threat awareness" covers security objectives related to threat intelligence and to outreach to end-users for the purpose of sharing the information about major threats to the security of networks and services.

4.4.8.1 SO28: Threat intelligence

Establish and maintain appropriate mechanisms for monitoring and collecting information about relevant threats to the security of networks and services.

	Security measures	Evidence
1	a) Perform regular threat monitoring.	i. Regular monitoring of external threat intelligence feeds (OSINT, commercial feeds, security researches etc.[36]) with a recorded log of relevant significant threat events. ii. Informal and ad-hoc sharing of relevant threat intelligence with relevant organisations on bi-lateral basis.
2	b) Implement threat intelligence program.	iii. Documented and implemented threat intelligence program that includes roles, responsibilities, procedures and mechanisms for collecting information related to significant threats and corresponding mitigation measures. iv. The program also includes mechanisms for systematic sharing of threat intelligence with relevant organisation on bi-lateral and multi-lateral basis using a dedicated threat intelligence sharing platform (e.g. MISP). v. Appropriate information marking scheme in place for facilitation of sharing of sensitive threat information (e.g. TLP).
3	c) Review and update the threat intelligence program. d) Threat intelligence program makes use of state of the art threat intelligence systems.	vi. Updated threat intelligence program, review comments and/or change logs. vii. Threat intelligence platform (TIP) with state of the art functionality is used (e.g. consolidation of threat intelligence feeds from various sources, automation, security analytics and integration with other security tools etc.)

[36] Information sources should be relevant, current and credible and may include known threat intelligence reports, such as ENISA Threat Landscape (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape) or various other threat reports by commercial entities, industry associations or academia.

4.4.8.2 SO29: Informing users about threats

Inform users of particular and significant security threats to network or service that may affect the end-user and of the measures they can take to protect the security of their communications.

	Security measures	Evidence
1	a) Inform end-users of communication networks and services about particular and significant security threats to network or service that may affect the end-user.	i. Security bulletin, a dedicated threat information web page or another documented and tested mechanisms for reaching out to end-users in the case of significant threats. ii. Documented lists of best practices and security recommendations for end-users to mitigate typical risks (e.g. encryption, strong authentication, updates, backups, user awareness etc.).
2	b) Implement policy/procedures for regular update of end-users about security threats to network or service that may affect the end-user	iii. Documented and implemented end-user outreach policy with defined roles and responsibilities, mechanisms and criteria for identifying significant threats and the procedures, tools and methods for timely and appropriate informing of end-users. iv. The policy includes mechanisms for identifying and sharing the recommendations and best practices for end-users to mitigate specific threats.
3	c) Review and update the policy/procedures for regular update of end-users about security threats to network or service that may affect the end-user.	v. Updated outreach policy, review comments and/or change logs.

5. TECHNICAL SUPERVISION OF SECURITY MEASURES

The principles of security supervision under the new rules (Article 40 and 41 of the EECC) are a continuation of the old rules (Article 13a and Article 13b of the Framework directive). Under the new rules, as with under the old rules:

- Communication providers have to assess risks, take appropriate security measures and report significant incidents to competent authorities (Article 13a of the Framework directive, Article 40 of the EECC).
- Competent authorities should have powers to supervise this, to enquire about measures in place, and to investigate cases of non-compliance by providers (Article 13b of the Framework directive, Article 41 of the EECC).

This means that for the new rules competent authorities can build on the experience and practice developed under the old rules.

The most common regulatory activities of competent authorities regarding supervision of security measures are [37]:

- Mandating or recommending a security standard
- Assessing compliance across the market
- Taking a staged approach to supervision
- Auditing providers (periodically, at random, and/or post-incident)

In the remainder of this section we discuss the technical aspects of each of these activities.

5.1 MANDATING OR RECOMMENDING A SECURITY STANDARD

There could be several reasons for mandating or recommending a standard of security measures:

- to provide **guidance** about what security measures should be implemented, for example by explaining high-level objectives or detailed security measures.
- to provide a **terminology** for discussing about security objectives or security measures.
- to provide a **structure** for supervision and auditing, by dividing security in different domains.
- to provide a **baseline**, i.e. a minimum set of security measures that must be in place, for example because without basic security measures it may be difficult to conduct an audit, because key evidence, like logs, records about incidents, etc. may be missing.
- to provide a **mapping** between different existing standards, for example, to be able to compare compliance and audit reports which are based on different standards.

Following we go into detail about the different options.

[37] This list is based on input from a survey, asking competent authorities across the EU, which are the activities they are deploying or planning to deploy.

5.1.1 Mandating versus recommending a security standard

When discussing the supervision of security legislation by government authorities there is often a discussion about whether or not the government authority should mandate a specific list of security measures, strongly recommend them, or just recommend them as guidance. One could argue that mandating a standard would create clarity about what providers need to do to be compliant. On the other hand, one could also argue that in most settings the sector, the organizations involved, the technology used, is just too diverse to allow for a single checklist of minimum security measures for the entire sector. Often only very high-level security standards could be reasonably applied to a wider number of organizations. Inevitably such high-level standards leave a lot of important technical details unaddressed. So it is hard to capture all the security requirements of Article 40 of the EECC *comprehensively* in one standard. At the same time for *specific* settings or specific issues the competent authority could mandate *specific* security measures to be taken. For instance, a competent authority could ask all providers to provide the competent authority with a contact point in case of contingencies, or ask all providers to have 4 hours of backup power for their base station controllers.

Note that when mandating security measures for specific aspects, it is important that competent authorities discuss with providers about effectiveness and feasibility beforehand. Such discussions could be triggered by large incidents or focus happened in the past period, frequent root causes, and/or other common issues (for example, about software vulnerabilities in common IT equipment).

Best practices in network and information security are rapidly changing, because information technology changes rapidly and because the capability of attackers changes rapidly. The competent authority is in a unique role to support and foster the exchange of and discussion about best practices between experts of different providers. In this way the competent authority supports that best practices are adopted across the sector. Especially providers with less experience and less expertise could benefit greatly from such discussions and exchanges.

5.1.2 Using the ENISA guideline as a recommendation

Competent authorities could use this ENISA guideline to provide guidance to providers. The ENISA guideline consists of 29 high level security objectives derived from different standards (see References). To reach the security objectives, providers should choose appropriate technical security measures. This document lists detailed security measures which providers could take to reach the security objectives. The security measures are split in three (sophistication) levels ranging from 1) basic, to 2) industry standard, to 3) state of the art. Providers should assess the risks to their communications networks and services to understand which security measures are appropriate.

5.1.3 Using the ENISA guideline as a mapping

Many (especially larger) providers already have a security standard or a security governance framework in place, often based on international standards. This ENISA guideline could be used as a neutral mapping to different standards in use by the industry. Such a mapping would allow providers to continue use existing international standards, and it would avoid incurring unnecessary costs for providers when complying with the requirements of Article 40 of the EECC.

In practice, for example, providers could show compliance to Article 40 of the EECC by providing audit reports or certification against existing industry standards, combined with a mapping from these standards to this ENISA guideline. In Section 6 we provide an example of such a mapping to some well-known international security standards.

5.1.4 Using existing national or international standards or best practices

Competent authorities could refer to existing national or international standards or requirements, either as a baseline requirement or as a recommendation. An overview of standards widely used in the industry is included in the section References. Competent authorities should take into account national circumstances when choosing an appropriate set of standards or best practices. We would like to make three remarks in this regard:

- Competent authorities should take into account that some (especially the large) providers may operate in several EU countries, and that it would be cumbersome for these providers to adopt different standards in different countries. In this respect it could be useful to allow providers to use international standards which are widely used across the EU and in this way reduce compliance costs for these providers.

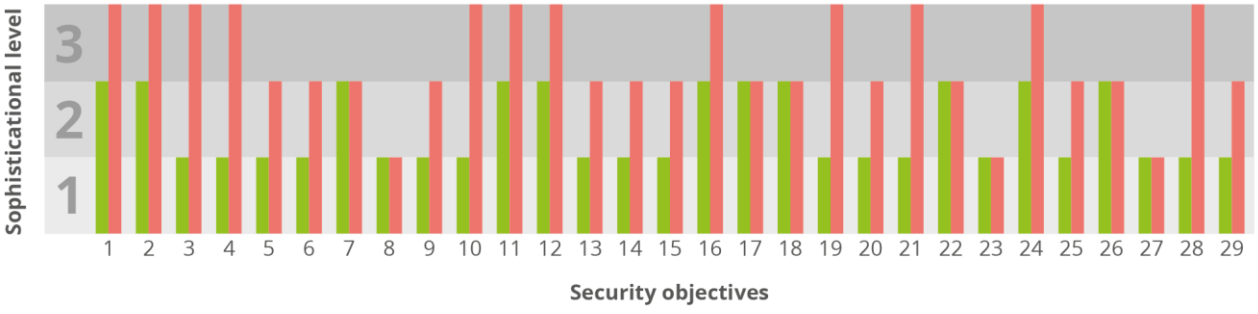
- In most countries the electronic communications sector is large (hundreds of providers) and contains both large providers (>10% of market share) and very small ones (<1% of market share). Competent authorities should also take into account the differences between the providers in their country. What might work for large providers may well be overwhelming for smaller providers, and vice versa, what might work for one provider might be inappropriate for another provider.

- Finally, competent authorities should take into account that best practices in network and information security are rapidly changing, because information technology changes rapidly and because the capability of attackers changes rapidly. This makes it hard to capture the high-level security requirement of Article 40 of the EECC comprehensively in a list of detailed security measures. In this light, competent authorities should focus first on supervising that providers assess risks and proactively take appropriate security measures, rather than on trying to cast detailed security measures in stone.

5.2 ASSESSING COMPLIANCE ACROSS THE MARKET

Self-assessments could be used to get an overview of the kind of security measures taken by providers, across the sector. The security objectives and measures listed in Section 4 can be used directly in self-assessment forms. The sophistication levels (see Section 4) would allow providers to indicate, per security objective, what kind of security measures are in place. Used in this way the sophistication levels would allow for a quick comparison between providers across the sector. We give an example in the diagram below. Here the red bars indicate the level of sophistication of the security measures taken by one provider, while the green bars show the levels for a provider with less sophisticated security measures. Such a difference in sophistication may be justified by a difference in the type of services or networks being offered by the two providers.

Figure 5: Example of two different providers (green and red), with security measures at different levels of sophistication.



Depending on the motivation behind the assessment the competent authority could focus on a subset of security objectives. For example, a competent authority could be interested in a domain like business continuity or specific security objectives around change management.

Competent authorities could also restrict self-assessments to a subset of the sector, for instance providers with a certain number of users (more than 10% market share e.g.), a certain service (mobile networks, e.g.), or providers offering certain critical services (communications for ports and airports e.g.).

We provide two simplified examples of how a competent authority could set up a self-assessment form. In the first example, the competent authority assesses security measures across all providers in the sector, but with a focus on a subset of the security objectives.

Example: The competent authority of country D has organized a self-assessment focused on governance and risk management (domain D1 in the ENISA guideline). Self-assessment forms are emailed to all providers:

Indicate your estimate market share: (choose from <1%, >10%, >10%)
Indicate which service you are offering: (fixed/mobile telephony, fixed/mobile internet)
Per security objective, indicate the level of sophistication and if you can produce evidence.

SO1: Information security policy
Sophistication level: (choose from 0, 1, 2, 3). Evidence exists: (choose from yes, no).

SO2: Governance and risk management framework
Sophistication level: (choose from 0, 1, 2, 3). Evidence exists: (choose from yes, no).

SO3: Security roles and responsibilities
Sophistication level: (choose from 0, 1, 2, 3). Evidence exists: (choose from yes, no).

SO4: Managing third party networks or services
Sophistication level: (choose from 0, 1, 2, 3). Evidence exists: (choose from yes, no).

In the second example the competent authority focuses on a subset of security measures and a subset of providers:

Example: The competent authority in country E wants to focus on the issues behind a number of large mobile network outages in the past year which are caused by power cuts, cable cuts, and natural disasters. The competent authority focusses on the security measures which are most relevant in this context. Self-assessment forms are sent only to mobile network operators with large market share (>10%). Questions are a combination of multiple choice and open questions for a description of security measures in place, and open questions for the type of evidence that the provider can produce to substantiate answers.

For each of the security objectives SO9 (Physical and environmental security), SO10 (Security of supplies), SO21 (Service continuity strategy and contingency plans), SO22 (Disaster recovery capabilities), SO24 (Exercise contingency plans), indicate the

level of sophistication, on a scale from 0 to 3 (0 none, 1 basic, 2 industry standard, 3 state of the art):

Describe the security measures in place to reach the objective: (max 200 words)

Describe the evidence you could provide to the competent authority which could substantiate that measures are in place: (0 none, 1 internal documentation, 2 audit report from external auditor)

Remark about confidentiality: *Self-assessment results or profiles could be sensitive and it is important to ensure confidentiality of results from other providers and/or the public. It is important to explain clearly the purpose of the assessment (for example, by explaining that there are no regulatory consequences) and to give explicit guarantees to providers about confidentiality of the results.*

5.3 SUPERVISION REGIME FOR NI-ICS PROVIDERS

In general, the security provisions in the EECC for NI-ICS are the same as for the number-based services. Both are subject to (normal) ex-ante, supervision, and are required to provide information, submit to security audits and be subjected to investigation of non-compliance by the competent authorities. However, because these providers of do not normally exercise actual control over the transmission networks, there may be different risks for these providers, and certain security measures may not be needed, if justified on the basis of a risk assessment[38]. See the recital 95:

> *(95) […] independent inter personal communications services, […] are also subject to appropriate security requirements in accordance with their specific nature and economic importance. Providers of such services should thus also ensure a level of security appropriate to the risk posed. Given that providers of number -independent interpersonal communications services normally do not exercise actual control over the transmission of signals over networks, the degree of risk for such services can be considered in some respects to be lower than for traditional electronic communications services. Therefore, where justified on the basis of the actual assessment of the security risks involved, the measures taken by providers of number-independent interpersonal communications services should be lighter. […]*

In practice this means that, depending on the setting, the type of network or service offered, the assets involved, etc., some of the security measures in this guideline may not be fully applicable to NI-ICS providers. When assessing the compliance of providers with Article 40, competent authorities should take into account the type of network or service offered, the assets involved, the threats and resulting risks for this network or service.

5.4 TECHNOLOGY PROFILES

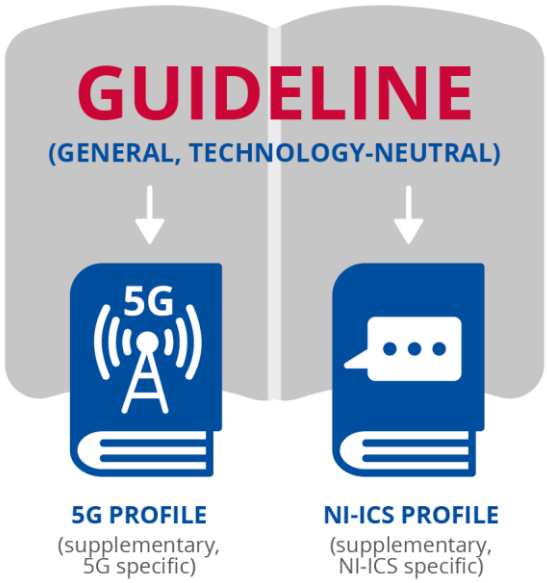
This guideline on security measures is technology neutral. To provide more specific guidance for specific types of network/service providers, we supplement this guideline with “security profiles”, for technologies like 5G or providers NI ICS. These security profiles supplement this

[38] Security Supervision under the EECC, ENISA, January 2020, https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc/

generic and technology-agnostic guideline. The following supplementary security profiles are under development and will be published separately:

- **Security profile for 5G MNOs,** containing supplementary guidance for technical supervision of security measures for 5G MNOs;
- **Security profile for NI-ICS providers**, containing supplementary guidance on number-independent interpersonal communication services (NI-ICS).

Figure 6: ENISA Guideline on Security Measures under the EECC – Technologies Supplements



5.5 TAKING A STAGED APPROACH

Depending on the national circumstances, competent authorities might want to adopt a staged approach in supervising (and enforcing) compliance to the security requirements of Article 40 of the EECC. In case some providers do not (yet) have appropriate security measures in place (or if they cannot provide evidence of this), competent authorities may want to give providers some time to comply, in stages. Competent authorities could use this guideline to adopt a staged approach. We discuss some possible options for staging:

- **Services or assets in scope:** One could first focus on a subset of services (for example mobile networks) or a subset of assets (for example, core network), and deal with other services later.

> **Example**: The competent authority in country A wants to focus first on the mobile networks, because they are (nationally) the most critical. The competent authority starts with a self-assessment across providers of mobile networks. The scope of the assessment is 'assets supporting mobile networks'. Other services are out of scope initially, as well as providers who do not offer mobile telephony networks.

- **Providers in scope:** One could first focus on a subset of providers, for example providers with a large market share, and look at other providers at a later stage.

  Example: The competent authority in country B wants to focus first on the providers with large market share, because here a lot of users are at stake. The competent authority starts with collecting self-assessment reports from the main providers (>10% of market share). The survey is followed up by a series of workshops where the main causes of incidents are discussed. Next year the competent authority will start a separate supervision program for smaller providers (focussed more on guidance).

- **Security domains:** One could first focus on a subset of security objectives, business continuity for example, and focus on other objectives at a later stage.

  Example: The competent authority in country C wants to focus first on the main incidents, taking into account the incidents reported by providers. Since last year in country A the incidents were mostly due to natural disasters, in the supervision the competent authority focusses first on the measures SO9, SO10, SO21, SO22, SO24. The competent authority will address other security measures at a later stage.

- **Sophistication levels and baselines:** Competent authorities could first focus on ensuring that all providers have taken the basic security measures, for example level 1 as defined in this guideline, and only later focus on ensuring that providers take more sophisticated security measures. We should stress here that such an approach would have limitations: particularly when the sector has both large and small providers: For large providers basic security measures may be insufficient, while for small providers they could be more than enough. It would be better to take differences across the sector into account and define different baselines for providers of different size.

  Example: The competent authority in country D defines two profiles as baselines.

  - The first profile contains the basic security measures for only the domains D1 Governance and risk management, D2 Human resource security, D3 Security of systems and facilities, – it is the baseline for small providers (<10% market share.

  - The second profile contains industry standard security measures for all domains (D1, … D8)– it is the baseline for large providers (>10% of market share).

  At a later stage the competent authority will review the profiles, and where needed raise the requirements in some areas or define different baselines for other types of providers **(IXPs e.g.).**

5.6 AUDITING PROVIDERS

Depending on the setting, competent authorities might want to require providers to undergo an audit. Depending on the setting and the goal of auditing different types of audits may be needed. In this section we discuss different options for auditing providers.

Note that auditing is not always easy because network and information systems are often complex. To understand if specific subsystems are working correctly, an auditor may need to have deep knowledge and expertise: in security the devil is in the details. To give one simple example: An auditor may find there is a firewall in place to protect certain systems, but the detailed firewall rules determine greatly the effectiveness of the firewall. One rule with one mistake may make the entire firewall useless.

Remark about audit costs: *Competent authorities should take into account the costs of third-party audits for providers, particularly the smaller providers. Self-assessments (see previous section) may be a more light-weight approach.*

Remark about efficiency of audits*: A frequent complaint from organizations subject to information security audits is that auditing often forces them to generate a lot of paper work, and that this is not only useless but that it also diverts resources from the actual task at hand: making the network and information systems secure. Competent authorities should take into account that some providers are already partaking in compliance or certification programs (voluntarily or in the context of different legislation) and are already undergoing (internal or external) audits. If auditing is needed, it is important to leverage where possible existing audit reports and compliance evidence.*

Remark about language and international operators: *When requesting documentation or evidence from providers, competent authorities should take into account that providers may keep certain relevant documentation (manuals, policies, procedures, etc.) in the English language for efficiency reasons, because the provider operates in several countries or because the operator employs personnel from abroad.*

5.6.1 Assessment types

An audit involves different types of assessments, for example a review of security policies or an interview with the CISO about contingency planning. Audits usually consist of a combination of different types of assessments. We discuss the different types below:

- **Document review:** Document review is essential in any audit. Relevant documents may include descriptions of policies, roles and responsibilities, descriptions of processes and procedures, systems architecture and design, test procedures and actual test results. Chapter 4 of this guideline includes descriptions of evidence which could be considered when assessing the implementation of security measures.
- **Interviews:** In addition to document review, a lot of information may be collected by interviewing service provider employees. At small providers it may be enough to speak to one or two persons with commercial and technical responsibility. At large providers, typical roles to be interviewed are C-level managers (CIO), chief security officers (CSO or CISO), tactical/operational security officers, NOC managers, internal CERT team, product managers, and system administrators responsible for critical processes or systems.

- **System evaluation:** Besides documentation, certification, and interviews, the ultimate check to see if the networks and information systems are secure, and if policy/procedures are being applied in practice, is by inspecting or testing the system itself. In some settings system review may be needed, for example to understand how a security incident could have happened. System evaluation should focus on critical systems because it can be time-consuming.

5.6.2 Auditor types

Auditing can be carried out by different parties.

- **Self-assessment:** In self-assessments there is really no auditor, but the personnel of the provider assesses and reports about compliance. Although self-assessment reports may be biased, they can provide useful information for providers and competent authorities. An advantage of self-assessments is that self-assessments are relatively cheap for providers. Earlier in this document, in Section 5.2, we discuss self-assessments in more detail.
- **Internal auditor:** In large organizations, a provider could ask an internal security role or internal audit department to do an audit of certain systems or parts of the organization. Compared to self-assessments, an internal auditor may be less biased. An advantage is that internal auditors often know the organization inside out. Also internal auditors could more easily leverage the deep knowledge about the network and information systems at the provider.
- **External auditor:** An audit report from an external auditor is even less biased. The only issue here may be that the external auditor may not know all the details about the organization and/or the network and information systems. This would make the entire audit more costly, because on the one hand the external auditor would need to dedicate a lot of time to study the setting and systems at the provider, and the provider would also need to dedicate a lot of time to providing the necessary information to the auditor.
- **Competent authority as auditor:** The competent authority could carry out an audit of an provider, by using internal staff with auditing expertise, or by outsourcing the auditing to an auditing firm.
- **Certifying auditor:** In certification a licensed auditor checks compliance to a specific standard. The audit report results in a certificate of compliance issued by a certifying authority. For example it is quite common for large providers to be ISO 27001 certified. Certification is often refreshed yearly, following a yearly re-audit. Competent authorities could require certification, and ask providers to submit their certificates as a way to show compliance[39].
- **Specialist auditor**: In special cases the competent authority may want to designate a specific auditor, for a specific purpose or following a specific incident. For example, an competent authority could mandate providers to undergo a security scan of systems by a security scanning specialist.
- **Pool of auditors:** The competent authority could designate a pool of external auditors. Criteria for auditors could be based on past experience (a track record of audits, or security tests) or be based on examination criteria. For example, competent authorities could start with a list of licensed auditors[40] and offer them a yearly training which focuses on Article 13a requirements for the sector, in this way creating a pool of auditors.

[39] This may also include a more detailed scope statement (or a Statement of Applicability for ISO 27001).
[40] In most countries, for example, there are organizations that license auditors to carry out IT audits.

5.6.3 Audit timing and objectives

The frequency and objectives of auditing varies. We distinguish two types of audits.

- **Preventive audits:** Preventive audits are usually done at fixed intervals, periodically. In the case of certification (see above) audits are carried out yearly or bi-yearly. Preventive audits often do not have a specific scope, however it is good practice to set-up preventive periodic audits according to a multi-year plan and focus first on certain (important) issues and only later on other issues in subsequent audits. The frequency of auditing should take into account that providers may need some time to address deficiencies found in previous audits.

  Example: The competent authority in country H mandates providers to undergo yearly (preventive) audits by 3rd party auditors. To simplify matters and to reduce the burden for providers, the competent authority works according to a 3 year supervision plan, focussing on urgent issues first: In the first year the scope of audits is restricted to business continuity, natural disasters and power cuts (measures SM9, SM10, SM21, SM22, SM24). In the second year the focus is on the storage and retention of customer data. In the third year all security measures will be audited.

- **Post-incident audits:** Post-incident auditing by an competent authority is usually done ad-hoc, depending on the type of incident and the setting. Post-incident audits have a specific focus – and usually they are aimed at assessing if security measures are in place to prevent the incident from re-occurring. The audit in this case has a specific scope (the services affected by the incident, the assets affected) and regards specific security measures (measures failing during the incident, or measures which could prevent re-occurrence).

5.7 AUTHORISATIONS CONDITIONS

5.7.1 Authorisations

Member States are allowed to attach general authorisation conditions concerning the security of public networks. This was already envisaged under the “old rules” (Directive 2009/140/EC) and is also included in the Annex I of the EECC.

For the sake of clarity, in the next section we highlight those conditions listed in the Annex I of the EECC that are of particular relevance for the security of networks and services.

5.7.2 Conditions

List of conditions which may be attached to general authorisations, rights of use for radio spectrum and rights of use for numbering resources are indicated in the Annex I of the EECC and are grouped in different categories, for general and specific conditions.

Of those conditions, some are specifically and directly related to assuring security of networks and services, such as:

- In Category A (General conditions which may be attached to a general authorisation):
  - **Condition 8:** Measures designed to ensure compliance with the standards or specifications referred to in Article 39 (when standards or specifications referred to are related to information security, e.g. ISO 27001)

- In Category B (Specific conditions which may be attached to a general authorisation for the provision of electronic communication networks):
    - **Condition 4:** Maintenance of the integrity of public electronic communications networks in accordance with this Directive including by conditions to prevent electromagnetic interference between electronic communications networks or services in accordance with Directive 2014/30/EU.
    - **Condition 5:** Security of public networks against unauthorised access in accordance with Directive 2002/58/EC

6 MAPPING TO INTERNATIONAL STANDARDS

The security measures described in this document (see Section 4) have been derived from existing international network and information security standards. This guideline is not intended to replace existing standards or frameworks that are used by providers. Providers could map the standards they use internally to the security measures in Section 4, and in this way show compliance with Article 40. In this section we give two examples of such a mapping.

5.8 MAPPING SECURITY DOMAINS

Below, as an example, we map the security domains of Section 4 to a number of international standards frequently used by providers. We map to the following standards:

- ISO 27001:2013, a standard for information security management,
- ISO 27002:2013, a catalogue of information security controls,
- ISO 27005:2018, a standard for information security risk management, and,
- ISO 22301:2019, a standard for business continuity management.

Security domains	Addressed in	Details
D1: Governance and risk management	ISO 27001, ISO 27002, and ISO 27005.	ISO 27001 provides a standard for governance of information security risks. ISO 27005 provides a standard for risk management. ISO 27001 Section A.4 (and ISO 27002 Chapter 5) covers Information security policies. ISO 27001 Section A.7 (and ISO 27002 Chapter 7) covers information security roles and responsibilities. ISO 27001 Section A.15 (and ISO 27002 Chapter 15) covers relationships with suppliers.
D2: Human resources security	ISO 27002	ISO 27001 Section A.7 (and ISO 27002 Chapter 7) covers background screening, information security roles and responsibilities, security knowledge and training, and personnel changes.
D3: Security of systems and facilities	ISO 27002	ISO 27001 Section A.11 (and ISO 27002 Chapter 11) covers physical and environmental security. ISO 27001 Section A.11 (and ISO 27002 Chapter 9) covers access control to information systems and facilities. ISO 27001 Section A.13 (and ISO 27002 Chapter 13) covers network security. ISO 27001 Section A.10 (and ISO 27002 Chapter 10) covers encryption (cryptography)

D4: Operations management	ISO 27002	ISO 27001 Section A.13 (and ISO 27002 Chapter 12) covers operational procedures and change management. ISO 27001 Section A.8 (and ISO 27002 Chapter 8) covers asset management.
D5: Incident management	ISO 27002	ISO 27001 Section A.16 (and ISO 27002 Chapter 16) covers management of information security incidents, as well as communications about security events.
D6: Business continuity management	ISO 22301	ISO 27001 Section A.11 (and ISO 27002 Chapter 17) covers security aspects of business continuity management. ISO 22301 covers Business Continuity Management[41].
D7: Monitoring and security testing	ISO 27002	Monitoring is covered in ISO 27001 Sections A.12 and A.15 (and in ISO 27002 Chapters 12 and 15). Security testing and compliance reviews are covered in ISO 27001 Sections A.14 and A.18 (and in ISO 27002 Chapters 14 and 18).
D8: Threat awareness	ISO 27002	User awareness is partially covered in ISO 27001 Section A.7 (and ISO 27002 Chapter 7) Management of technical vulnerabilities is covered in ISO 72001 Section A.12.6.1 (and ISO 27002 Chapter 12). Contact with special interest groups (e.g. for exchange of information about threats) is covered in ISO 27001 Section A.6.1.4 (and ISO 27002 Chapter 6)

We have used ISO standards in this example, but a similar mapping could be made to other national or international standards. For example, the mapping would look similar if, instead of ISO 27001 and ISO 27005, we would map to the ITU standards X.1051 (information security management) and X.1055 (risk management).

5.9 MAPPING SECURITY OBJECTIVES

One could also make a more detailed mapping. Below, as an example, we map the security objectives in Section 4 to individual control objectives in the annex of ISO 27001:2013.

Security objectives	Control objectives in ISO 27001:201
SO1 Information security policy	A.5.1 Management direction for information security
SO2 Governance and risk management	ISO 27001 for governance Sections 8.2 and 8.3 for risk management[42]
SO3 Security roles and responsibilities	A.6.1 Internal organization A.7.1 Prior to employment A.7.2 During employment
SO4 Security of third party assets	A.15.1: Information security in supplier relationships[43]

[41] In addition, ISO 22301 covers Business Continuity Management
[42] See also ISO 27005
[43] See also ISO 27026-3:2013 - Guidelines for ICT supply chain security

Security objectives	Control objectives in ISO 27001:201
SO5 Background checks	A.7.1 Prior to employment
SO6 Security knowledge and training	A.7.1 Prior to employment A.7.2 During employment A.7.3 Termination and change of employment
SO7 Personnel changes	
SO8 Handling violations	
SO9 Physical and environmental security	A.11.1 Secure areas A.11.2 Equipment
SO10 Security of supplies	A.11.2 Equipment
SO11 Access control to network and information systems	A.9.1 Business requirements of access control A.9.2 User access management A.9.3 User responsibilities A.9.4 System and application access control A.13.1 Network security management
SO12 Integrity of network and information systems	A.12.2 Protection from malware A.12.5 Control of operational software A.12.6 Technical vulnerability management A.13.1 Network security management
SO13 Use of encryption	A.10.1.1 Policy on the use of cryptographic controls
SO14 Protection of security critical data	A.10.1.2 Key management
SO15 Operational procedures	A.12.1 Operational procedures and responsibilities.
SO16 Change management	
SO17 Asset management	A.8.1 Responsibility for assets
SO18 Incident management procedures	A.16.1 Management of information security incidents and improvements
SO19 Incident detection capability	
SO20 Incident reporting and communication	
SO21 Service continuity strategy and contingency plans	A.17 Information security aspects of Business Continuity management[44]
SO22 Disaster recovery capabilities	

[44] In addition, ISO 22301 covers Business Continuity Management

Security objectives	Control objectives in ISO 27001:201
SO23 Monitoring and logging policies	A.12.4 Logging and monitoring
SO24 Exercise contingency plans	A.17 Information security aspects of Business Continuity management[45]
SO25 Network and information systems testing	A.14.2 Security in development and support processes A.18.2 Information security reviews
SO26 Security assessments	
SO27 Compliance monitoring	A.18.1 Compliance with legal and contractual requirements
SO28 Threat intelligence	A.12.6.1 Management of technical vulnerabilities A.6.1.4 Contact with Special Interest Groups
SO29 Informing users about threats	A.7.2.2 Information security awareness, education and training

[45] Ibid.

6. REFERENCES

In this section we provide references to related ENISA papers, and relevant EU legislation. We also provide a non-exhaustive list of common information security standards we used as input to earlier drafts of this document.

Related ENISA papers

Document	URL
Security Supervision under the EECC, 2020	https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc
Article 13a Technical Guideline on Security Measures v 2.0 2014	https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures/at_download/fullReport
Technical guideline on incident reporting	https://www.enisa.europa.eu/publications/technical-guideline-on-incident-reporting/at_download/fullReport
Indispensable baseline security requirements for the procurement of secure ICT products and services	https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services/at_download/fullReport
Security Guide for ICT Procurement for electronic communications service providers	https://www.enisa.europa.eu/publications/security-guide-for-ict-procurement

Relevant EU Legislation

Document	URL
European Electronic Communications Code	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972&from=E
ePrivacy Directive	https://eur-lex.europa.eu/eli/dir/2002/58
EU Cybersecurity Act	https://eur-lex.europa.eu/eli/reg/2019/881/oj
BEREC regulation	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R1211&from=EN

International standards and security best practices

- ISO 27001 “Information security management systems”
- ISO 27002 “Code of practice for information security controls”
- ISO 24762 “Guidelines for inf. and communications technology disaster recovery services”
- ISO 27005 “Information security risk management”
- ISO 27011 “Information security management guidelines for telecommunications”
- ISO 22301 “Business continuity management systems”
- ITU-T X.1056 (01/2009) “Security incident management guidelines for telecommunications organizations”
- ITU-T Recommendation X.1051 (02/2008) “Information security management guidelines for telecommunications organizations based on ISO/IEC 27002”
- ITU-T X.800 (1991) “Security architecture for Open Systems Interconnection for CCITT applications”
- ITU-T X.805 (10/2003) “Security architecture for systems providing end-to-end communications”

TP-04-20-722-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-457-2
DOI 10.2824/44013