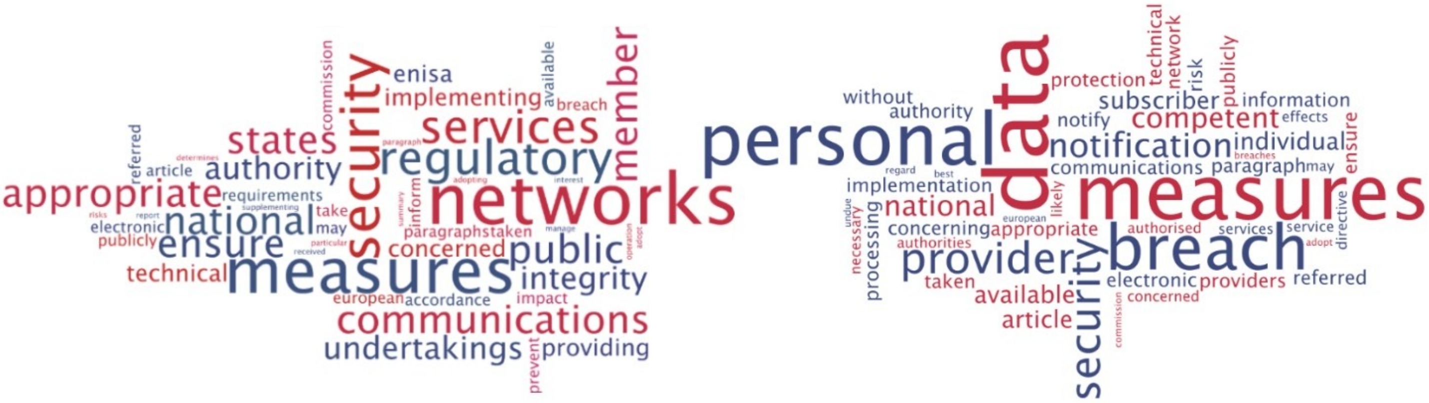


Security framework for Article 4 and 13a

Proposal for one security framework for Article 4 and 13a

Version 1.0, December 2013

European Union Agency for Network and Information Security   www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Dr. Marnix Dekker, Christoffer Karsberg, Konstantinos Moulinos

Contact

For contacting the authors, please use resilience@enisa.europa.eu.

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA received valuable input from a group of experts from 14 national authorities (national regulatory authorities and data protection authorities) from across the EU. Listing the participating organizations in no particular order: ADAE (Greece), UODOU (Czech Republic), CTU (Czech Republic), OCECPR (Cyprus), Danish business authority (Denmark), FICORA (Finland), BNetzA (Germany), NMHH (Hungary), TeleOff (Slovak Republic), PTS (Sweden), ICO (United Kingdom), BIPT (Belgium), GDPD (Italy). We are grateful for their valuable input and comments.

We also received valuable input and feedback from experts of the EC and experts from electronic communications providers.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

Executive summary

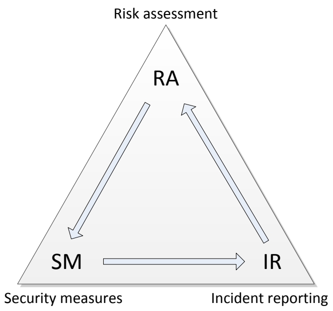
The 2009 reform of the EU legislative framework for electronic communications (or e-communications) introduces Article 13a into the Framework directive and it amends Article 4 of the e-privacy directive (2002/58/EC)[1]. The reform was transposed by most EU Member States halfway 2011[2]. We summarize both articles briefly.

Article 13a is entitled “Security and integrity” and requires authorities to ensure that:

- Providers take appropriate security measures to protect the security of networks and services, taking into account risks for users and connected networks.
- Providers report about incidents with significant impact on networks and services.

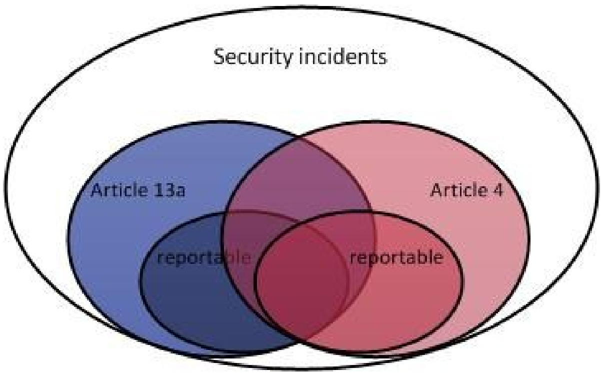
Article 4 is entitled “Security of processing” and requires authorities to ensure that:

- Providers protect the security of networks and services and that they take measures to ensure secure personal data processing.
- Providers notify about personal data breaches, and if needed communicate with the (ex-) subscribers affected.



Both articles are set-up in a similar way. Both articles regard three security processes which have to be supervised by authorities: 1) Risk assessment (RA), 2) Taking appropriate security measures (SM), and 3) Reporting about security incidents to authorities (IR). The three processes are depicted in the diagram above.

The main difference between the two articles is that Article 13a focuses on security breaches which could have an impact on the security of the networks and services, while Article 4 focuses on the security breaches which could have an impact on the personal data, processed in connection with the provision of networks and services. Basically both articles address two different and overlapping subsets of security incidents (see the Venn diagram on the right).



ENISA believes important efficiency gains can be made both for authorities and the providers in the sector if a single framework is used for supervising the security measures mandated by these two articles. It would seem to be also feasible and useful; Experts from authorities have argued there is roughly an 80% overlap in the security measures.

[1] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf

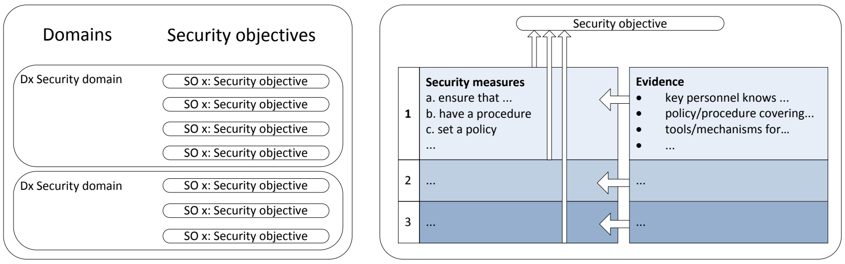
[2] Note that mid 2013 the EC issued a regulation for Article 4 (Regulation EC/611/2013), detailing how a number of technical issues around breach reporting should be implemented by EU member states (reporting template, reporting deadlines, et cetera). In the rest of this document we will simply refer to Article 13a and Article 4 (both the directive and the recent implementing regulation).

- For providers a single security framework (one terminology, similar concepts and structures, etc.) would reduce the costs of compliance for providers.
- From the perspective of the authorities (NRAs and DPAs), a single framework would make it easier to perform joint audits (in countries where responsibility for Article 13a and Article 4 is shared), and also to collaborate easier across borders (exchange audit/compliance reports for example) with NRAs and DPAs abroad, and to discuss about common issues, common root causes, for security incidents relevant for Article 13a and/or Article 4.

Proposal for a security framework for Article 4 and 13a

This document contains a proposal for such a security framework which covers security measures for both Article 4 and Article 13a. It exploits the large overlap between the articles. This proposal is based on input from a group of experts from competent national authorities (NRAs and DPAs), as well as earlier experience and discussions with authorities on Article 4 and Article 13a.

The core of the framework is a list of 26 high-level security objectives grouped in 7 domains (HR security, governance and risk management, et cetera). For each security objective we list a number of specific, more detailed, security measures. These measures are grouped in 3 sophistication levels. Per security measure we also list the kind of evidence which could be used to show that these measures are in place. The full structure is depicted in the diagram on the right.



This security framework is intended as a tool and guide *for authorities* supervising the sector, to be used as a structure for creating guidance or recommendations for providers, to be used for creating self-assessment forms, or as a structure for interviews or audits. It does *not* aim to replace the large body of existing literature on how to implement security measures and does not cover topics in detail. For example, the topic Business Continuity Management (BCM) is discussed here briefly (in 1-2 pages), while there are hundreds of documents with useful information about implementing BCM.

We would like to clarify that the detailed security measures should not be seen as a recommendation about which are the appropriate security measures individual providers should take. The electronic communications sector is diverse, including large and small providers, providers offering a full range of services or just black fibres. In each case the risks are different and what could be appropriate in one setting could be inappropriate in another setting.

Outlook and next steps

This is a proposal for a single framework for the security measures in Article 13a and Article 4, which is based on fruitful but short discussions with experts from 14 competent national authorities. We believe it is worth wile to take this security framework further and develop and validate it, involving all the competent national authorities (NRAs and DPAs) involved in Article 13a and Article 4.

Table of Contents

1 Introduction

In this document, we provide guidance to Electronic Communications National Regulatory Authorities (NRAs) and Data Protection Authorities (DPAs) about the technical issue of supervising the security measures mentioned in paragraph 1 of Article 4 of the e-Privacy directive as well as paragraphs 1 and 2 of Article 13a of the Framework directive (Directive 2002/21/EC).

Target audience

This document is addressed to experts from competent national authorities (ministries, DPAs, and NRAs) in European Member States who are tasked with the implementation of Article 4 and/or Article 13a.

This document may be useful also for experts working in the EU's electronic communications sector and for experts working in the network and information security (NIS) field.

Goal

This document is intended as guidance for competent national authorities about the security measures described in paragraph 1 of Article 4 of the e-Privacy directive, and paragraphs 1 and 2 of Article 13a of the Framework directive.

Structure of this document

In Section 2 we provide the background to this work and we discuss the policy context, as well as the role and objectives of ENISA. In Section 3 we introduce the two articles and terminology and abbreviations used in this document. Section 4 contains a list of 26 security objectives grouped in 7 domains. In Section 5 we describe how national competent authorities could supervise providers with respect to taking the appropriate security measures.

2 Background

This document concerns Article 13a of the Framework directive (Directive 2002/21/EC) and Article 4 of the e-Privacy directive (Directive 2002/58/EC), as amended in the 2009 reform of the EU's legal framework for electronic communications (Directive 2009/140/EC and Directive 2009/136/EC).

The full text of the Framework directive and the e-Privacy directive, incorporating the changes of the 2009 reform, is available online at the European Commission's website[3]. The 2009 reform was transposed in national legislation in 2011.

Mid 2013 the EC issued a regulation for Article 4 (Regulation EC/611/2013), detailing how a number of technical issues around breach reporting should be implemented by EU member states (reporting template, reporting deadlines, et cetera). In the rest of this document we will simply refer to Article 13a and Article 4 (both the directive and the recently adopted implementing regulation).

Related EU legislation

Both Article13a and Article 4 regard network and information security (NIS). Below we discuss other EU policy and legislation on NIS.

CIIP and e-Communications

There are a number of policy initiatives (legal or otherwise) addressing CIIP in general, including the security of public electronic communications networks and services in particular.

- In 2006, the EC issued a strategy for a secure information society – dialogue, partnership and empowerment (COM (2006) 251), which was endorsed the next year by the European Council (Council Resolution 2007/068/01). One of the main actions of the strategy is a multi-stakeholder dialogue on the security and resilience of network and information systems: the European Programme for Critical Infrastructure Protection (EPCIP).
- In 2009, the EC adopted a communication and action plan on Critical Information Infrastructure Protection (CIIP), called *Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience* (COM (2009) 149). This communication focuses on *"prevention, preparedness, and awareness"* and defines an immediate action plan to strengthen the security and resilience of CIIs.
- The Council Conclusion on CIIP issued in May 2011, taking stock of the results achieved since the adoption of the CIIP action plan in 2009, was launched to strengthen the security and resilience of vital Information and Communication Technology Infrastructures.

Electronic identification and trust services

The European Commission recently proposed a new regulation on electronic identification and trust services[4] for electronic transactions in the internal market.. Article 15 in this proposal introduces obligations concerning security measures and incident reporting:

- Trust service providers must implement appropriate technical and organisational measures for the security of their activities.

[3] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf

[4] *Trust service means any electronic service consisting in the creation, verification, validation, handling and preservation of electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic delivery services, website authentication, and electronic certificates, including certificates for electronic signature and for electronic seals.*

- Trust service providers must notify competent supervisory bodies and other relevant authorities of any security breaches and where appropriate, national supervisory bodies must inform supervisory bodies in other EU countries and ENISA about security breaches.
- The supervisory body may, directly or via the service provider concerned, inform the public.
- The supervisory body sends a summary of breaches to ENISA and the EC.

Article 15 is based on Article 13a of the Framework directive.

Data protection reform

The European Commission has proposed to reform the current European data protection framework (Directive 95/46/EC), and has proposed an EU regulation on data protection. The regulation regards organisations that are processing personal data, regardless of the business sector the organisation is in. Security measures and personal data breach notifications are addressed in Articles 30, 31 and 32:

- Organisations processing personal data must take appropriate technical and organisational security measures to ensure security appropriate to the risks presented by the processing.
- For all business sectors the obligation to notify personal data breaches becomes mandatory[5].
- Personal data breaches must be notified to a competent national authority without undue delay and, where feasible, within 24 hours, or else a justification should be provided.
- Personal data breaches must be notified to individuals if it is likely there will be an impact on their privacy. If the breached data was unintelligible[6], notification is not required.

Network and information security (NIS) directive

The European Commission also published a European Cyber Security Strategy and proposed a directive on network and information security (NIS). The strategy and the directive explicit refer to Article 13a as an example, and the proposed directive basically extends Article 13a to other critical sectors. In particular Article 14 of the proposed NIS directive has the following provisions:

- Market operators and public administrations should take appropriate security measures to protect their core services.
- Market operators and public administrations should report incidents to competent national authorities.
- Competent authorities should collaborate and share summaries of incident reports in a cooperation network of competent authorities.

In the preambles of the NIS directive ENISA is asked to act as a bridge between the different types of authorities, including data protection authorities, national telecommunications regulators, and others, and develop a single reporting template.

Connected continent regulation

The European Commission recently proposed a regulation to further improve competition in the EU's telecom market and achieve a single connected continent. The regulation does not explicitly address security of networks, services or personal data processing, but it does state that electronic

[5] This provision extends personal data breach notifications beyond the electronic communications sector.

[6] In the recommendation for the technical implementation of Article 4, unintelligible data is described as data that has either been encrypted (asymmetric or symmetric), or hashed.

communications providers should have a right to receive equal treatment (in similar circumstances) from different authorities across the EU, and that it will be enough for providers to obtain authorization in one country, to be considered electronic communications provider across the EU.

ENISA's role and objectives

We summarize the relevant passages in the telecom reform which describes explicit tasks and responsibilities for ENISA.

ENISA tasks in the EU directives

ENISA is mentioned in the preambles of Directive 2009/140/EC – the reform of the Framework directive:

- Preamble 44 asks ENISA to contribute to enhancing the level of security of electronic communications by, among other things, *"providing expertise and advice, and promoting the exchange of best practice"*.
- Preamble 44 mentions that ENISA should have the means to carry out the relevant duties and the powers "*to obtain sufficient information to assess the level of security of networks and services*".
- Preamble 46 asks ENISA to contribute to the "*harmonisation of appropriate technical and organisational security measures by providing expert advice*".

ENISA is mentioned in Article 13a of the Framework directive:

- Paragraph 3 of Article 13a requires NRAs to, when appropriate, inform NRAs in other Member States and ENISA about security incidents.
- Paragraph 3 of Article 13a requires NRAs to submit annual summary reports on the received security notifications to both the European commission and ENISA.
- Article 13a mentions that the European commission may decide to adopt technical implementing measures with a view to harmonisation of the implementation of paragraphs 1, 2, and 3 of Article 13a. Article 13a mentions that in this case the European commission will take into account the opinion of ENISA.

ENISA is mentioned in the preambles of Directive 2009/136/EC – reforming the e-Privacy directive:

- Preamble 74 asks the EC to consult ENISA, EDPS and the Article 19 Working Party, as well as other relevant stakeholders, when adopting implementing measures on security of processing (of personal data), particularly in order to be informed of the best available technical and economic means of improving the implementation of the e-Privacy directive.

ENISA is mentioned in Article 4 of the e-Privacy directive:

- Paragraph 5 says that the EC may adopt implementing measures adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements, taking into account the opinion of ENISA, as well as the Article 29 Working Party, and EDPS.

The EU regulation 611/2013 was adopted in mid-2013 and contains implementing measures for Article 4 of the e-Privacy directive, specifying a number of technical details around the process of breach reporting by providers.

- Paragraph 3 of Article 4 of that regulation says that the EC nay adopt an indicative 'list of appropriate technological protection measures', referring to an exemption for an obligation to notify victims, if the breached data was rendered 'unintelligible' (using encryption, hashing, et cetera).

ENISA's objectives

ENISA's first objective is to help competent national authorities to implement the security breach reporting mandated by Article 13a and Article 4, i.e. to agree and discuss with experts from Member States about an efficient and effective implementation of national and pan-European incident reporting, including the processes of notification reporting in case of cross-border incidents. This addresses what is asked of ENISA in Article 4 and Article 13a.

Secondly, ENISA aims to support competent national authorities with the supervision of security measures and the other supervision activities in general, such as following up on incidents, analysing and mitigating common root causes, providing guidance to the electronic communications sector, and so on. This addresses what is asked of ENISA mentioned in the preambles of the e-Privacy directive and the Framework directive.

Thirdly, our goal is to support national authorities (NRAs and DPAs) in achieving an implementation which is (as much as possible) *harmonized* across the EU. This addresses what is asked of ENISA in the preambles of the e-Privacy directive and the Framework directive. Harmonized implementation of legislation is important to reduce costs for providers, to create a level playing field across the EU, to make it easier for providers to operate across EU countries in the single digital market, and to make it easier for authorities to collaborate, both nationally and across borders.

Related ENISA work

We briefly discuss some related ENISA work:

- In 2009 ENISA published an overview of the status quo of the implementation of breach notification across the EU. That paper focusses on data protection authorities and privacy breaches specifically[7].
- In 2011 ENISA published an overview of existing best practices regarding security incident reporting. It provides summarizes the state-of-play in 2011 regarding the incident reporting, and exaplain the vision of several MS on this topic[8].
- In 2011 ENISA published, in collaboration with experts form DPAs and industry a technical guideline for providers for the implementation of Article 4. In that paper a more general approach (not specific for the electronic communications sector) is taken, looking forward to the databreach notification obligations in the proposed data protection regulation. Also, that paper focuses more on how providers can manage risks, rather than on the issue of supervision of Article 4 by authorities[9].
- In 2011 ENISA published two technical guidelines for authorities on the implementation of Article 13a, drafted in collaboration and consensus with experts from NRAs from across the EU, and EFTA and EU candidate countries[10].
- In 2012 ENISA published a paper on different security articles in EU legislation and it provides some first ideas for a possible harmonized implementation of the different articles[11].

[7] http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/library/deliverables/dbn
[8] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting
[9] http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech
[10] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting
[11] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

- In 2012 and 2013 ENISA worked together with the Article 29 Working party on a data breach severity assessment methodology. A first version of a severity assessment methodology was included in the 2011 guideline for Article 4 (see above). ENISA continued this work based on the input received from some European DPAs in a series of reviews, discussions and meetings.
- In 2012 ENISA implemented an online reporting tool (accessible for authorities only) and updated the Article 13a incident reporting guideline to version 2.0 – adding more detailed fields to the reporting template and simplifying the reporting thresholds.
- In 2013 ENISA worked on an updated version of the Article 13a security measures guideline – adding more detail and more guidance on supervision. Drafts are available at the portal of the Article 13a expert group[12].
- In 2012 and 2013 ENISA published two Article 13a annual incidents reports, summarizing the major incidents from across the EU[13]. ENISA publishes these annual reports to provide the sector and the wider public with some insight into the major security incidents in the electronic communications sector (currently only outages are reported by national authorities).
- In 2014 ENISA will also work together with the EC to provide an indicative list of algorithms for encryption, hashing, and secure deletion which could render data unintelligible, which addresses the exemption mentioned in Article 4 which says that authorities might exempt providers from notifying victims of personal data breaches, if the data was rendered ‘unintelligible’ by encryption, hashing, or secure deletion, for instance.

[12] https://resilience.enisa.europa.eu/article-13

[13] www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports

3 Article 13a, Article 4 and terminology

In this section we introduce the parts of Article 4 and Article 13a relevant for this document and the terminology (abbreviations and simplifications) used in this document.

Both Article 13a and Article 4 are amendments to existing directives (the Framework directive and the e-privacy directive). As a source we use the consolidated version of the texts of the directives as published by the EC[14].

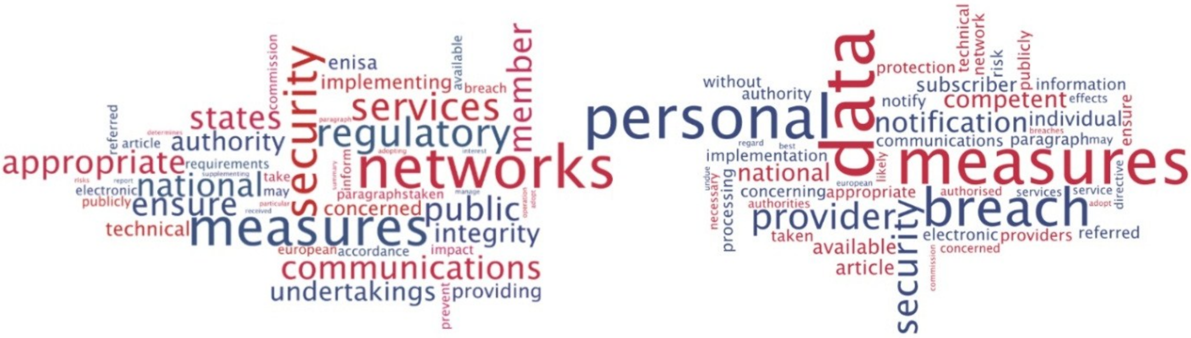


Figure 1: Word clouds of Article 13a (left) and Article 4 (right), showing the 50 most frequently used words.

3.1 Paragraph 1 of Article 4

For ease of reference, we reproduce the text of paragraph 1 of Article 4 here:

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

- *ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,*
- *protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,*
- *ensure the implementation of a security policy with respect to the processing of personal data,*

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

The rest of Article 4 focusses on notifying and reporting about personal data breaches[15] but the second part of paragraph 4 mentions another specific security measure:

[14] https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf

[15] Note that the term 'measures' is also used in another context. Paragraph 3 mentions an exemption to the reporting obligation if providers applied 'protection measures' to the breached data, rendering it

> *Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.*

3.2 Paragraph 1 and 2 of Article 13a

For ease of reference, we reproduce the text of paragraphs 1 and 2 of Article 13a here:

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

2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. […]"

3.3 Terminology

In the interest of brevity and readability, we use the following abbreviations in this document:

3.3.1 Provider

The term "provider" is used to refer to an *"undertaking providing public communications networks or publicly available electronic communications services"* as mentioned in the directives.

3.3.2 Authorities

The term authorities, or CNA, is used to refer to the "competent national authority" as mentioned in the directives. The CNA could be a national regulatory authority (NRA), a data protection authority (DPA), a ministry or another government agency, depending on the country.

3.3.3 Networks and services

The term "networks and services" is used to abbreviate the term *"public communications networks or publicly available electronic communications services*" as mentioned in the directives.

Across the EU there are different national interpretations of what constitutes a public communications network or publicly available communications service. In this document we simplify and focus just on the following services and networks:

- Fixed telephony (PSTN, VOIP)
- Mobile telephony (GSM, UMTS, LTE) and messaging (SMS)
- Fixed internet access (DSL, cable, fibre)
- Mobile internet access (GSM, UMTS, LTE)

'unintelligible'. From the context it is clear this does not refer to security measures providers have to take to prevent breaches, but rather to situation where data breached was treated with cryptographic algorithms (encryption, hashing, et cetera) decreasing the impact for the (ex-) subscribers. In this document we do not discuss incident reporting in detail.

This is not an exhaustive list of electronic communication services defined in the EU directives, nor an exhaustive list of electronic communication networks and services that are being regulated by authorities (CNAs) under national laws. Other networks and services (like email, television broadcasting, et cetera) might be in scope of national legislation, but they are not discussed explicitly in this document[16].

3.3.4 Security of networks, services and personal data processing

The first paragraphs of articles 13a and 4 contain security requirements:

- Paragraph 1 of Article 13a requires authorities to ensure that providers *"take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services*", and that they take measures "*to prevent and minimise the impact of security incidents on users and interconnected networks".*
- Paragraph 1 of Article 4 requires providers to take *"appropriate technical and organisational measures to safeguard security of its services*".
- Paragraph 2 of Article 13a uses another term: integrity. It requires authorities to ensure that providers *"take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services"*.

The use of the term integrity in the text of article 13a may be confusing to some readers. In technical literature about networks and network inter-connections, the term integrity is defined as "the ability of the system to retain its specified attributes in terms of performance and functionality". The term integrity in the article text might be called "resilience" or "continuity" in other information security literature. In this document, to be more in line with the terminology used in most literature on network and information security (NIS), we use the term "security" because in most information security literature continuity is seen as an integral aspect of network and information security.

- Paragraph 1a of Article 4 says that these measures should include at least measures to protect personal data from unauthorized access, accidental/unlawful destruction, accidental loss/modification, and a security policy on personal data processing.
- Paragraph 4 of Article 4 also says that providers should keep an inventory of personal data breaches.

In the rest of this document we refer to all these security requirements with a single term: security measures. We can now abbreviate the requirements of the two articles to:

Paragraph 1 of Article 4 and Paragraph 1, 2 of Article 13a: Competent national authorities must ensure that providers take appropriate security measures to protect the security of networks, services, and personal data processing.

From here onward, for the sake of clarity, we will use an underlined font to highlight these terms. So when we write security of networks, services, and personal data processing we mean the requirements in Article 13a and Article 4.

3.3.5 Security incidents

In the e-privacy directive the term 'personal data breach' is defined as follows.

- *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise*

[16] We do expect that many concepts can be applied also to these other types of networks and services.

processed in connection with the provision of a publicly available electronic communications service in the Community.

This means that a subset of security breaches is relevant for Article 4: the security breaches which have an impact on personal data.

Article 13a mentions both 'security breaches', 'security incidents' and 'integrity losses':

- Paragraph 1 requires *"that measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks"*
- Paragraph 2 requires providers to *"take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services"*.
- Paragraph 3 requires *"to notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services"*

This means that a subset of security breaches is relevant for Article 13a: the security breaches which have an impact on networks and services.

In this guideline we use the term[17] "security incident" for both types of security breaches:

Security incident: A single or a series of unwanted or unexpected events which could have an impact on the security of networks, services and/or the processing of personal data.

The definition we use here can be illustrated in the Venn diagram below. The blue indicates the subset of security incidents which are relevant for Article 13a, and the red area denoted the subset relevant for Article 4. They overlap. Only a subset of these security incidents must be notified or reported to authorities (CNAs): those with an impact on personal data and/or a 'significant' impact on the operation of the networks and services. Incident reporting (thresholds, templates, etc) is not described in detail in this document.

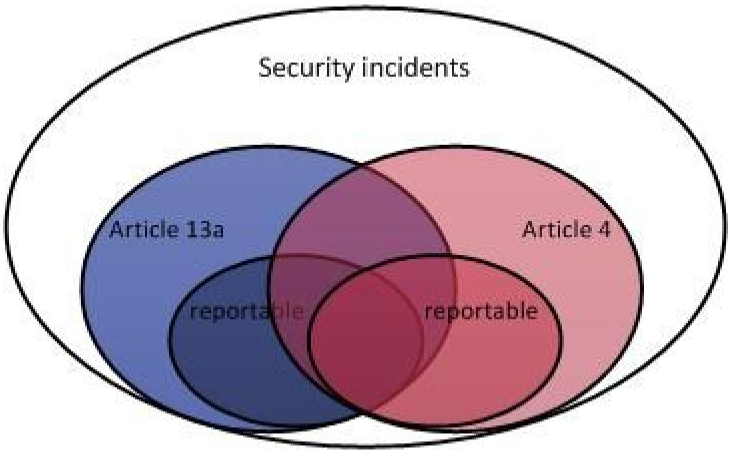


Figure 2: Security incidents in scope of Article 13a and Article 4

We give some examples of security incidents for the sake of explanation, and show where they fit in the Venn diagram above.

Example: We give some examples of security incidents in scope and/or reportable under Article 13a and/or Article 4 explaining in this way the different areas in the Venn diagram above.

[17] We use the term incident because it is more commonly used in technical network and information security literature and in the industry.

- *White area: A bug in the billing system means that certain customers get free calls. It is a security incident for the provider. The security incident is not in scope of Article 4 or 13a.*
- *Light-blue area: One of two redundant submarine cables is cut. There was no impact on end-users so the security incident is not reportable under Article 13a.*
- *Dark-blue area: Software-update of HLR goes wrong, keeping most of the customer base offline for hours. The security incident is not reportable under Article 13a.*
- *Dark-blue-dark-red area: HLR is hacked and taken offline, customers suffered downtime and communications-metadata was stolen, breaching severly the privacy of subscribers. The security incident is reportable under Article 13a and 4.*
- *Light-blue-light-red area: HLR was not patched by mistake, but there are no traces of exploits. The security incident is in scope of Article 13a and 4 but not reportable.*
- *Dark-red area: A telephone contract is sent to the wrong address.The security incident is reportable under Article 4.*
- *Light-Red area: A PC of an employee is infected, but there was no personal data of subscribers on the PC. The security incident is in scope of Article 4, because there could (eventually) be an impact on personal data (an attacker might use the PC to attack other systems), but this incident is not reportable because there was no impact.*

3.3.6 Threats and causes

In this document we often speak about threats. Threats are defined as follows[18].

Threat: A threat is an event or a circumstance which could cause a security incident.

After a threat caused a security incident we usually refer to it as a cause or a root cause.

[18] This definition is similar to the definition in ISO27K5, which describes threat as events which could cause an incident.

4 Security measures

In this section we address the security requirements in both articles (4 and 13a) by providing a single set of "security measures", which includes the "*technical and organisational measures"* mentioned in the first paragraphs of Article 4 and Article 13a, and the *steps* mentioned in the second paragraph of Article 13a.

The detailed security measures should not be seen as recommendations about which are the appropriate security measures individual providers should take. The electronic communications sector is diverse, including large and small providers, providers offering a full range of services or just black fibres. In each case the risks are different and what could be appropriate in one setting could be inappropriate in another setting.

Some of the security objectives or security measures, for example, may not be relevant or inappropriate in some settings, depending on the type of networks or services offered[19].

4.1 Assets in scope

This document contains a list of security objectives and security measures for protecting the assets[20] of the provider. The scope of the security measures is defined as follows.

Assets in scope: All assets of the provider which, when breached and/or failing, can have a negative impact on the security of networks, services and/or the processing of personal data.

Providers should perform risk assessments, specific for their particular setting, to determine which assets are in scope and 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). Also the ENISA technical guideline on Article 4 provides a risk management method – based on ISO27001.

Remark on enterprise 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: the field is called enterprise risk management. A well-known example is ISO27001. Article 4 and Article 13a, however, only mention 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 cannot be used for Article 4 and Article 13a without adaptation.*

4.1.1 Primary and secondary assets

Often in network and information security literature there is a distinction between primary assets and secondary assets. Secondary assets are (only) supporting primary assets. In the context of Article 4 and Article 13a we are concerned with two primary assets: the networks and services provided, and the personal data processed in connection with the provision of networks and services (see Figure 3 below). Secondary assets in scope are in principle all assets that directly support the primary assets. In this document when we say "assets" we usually mean the secondary assets and we refer

[19] For example, in the case of black fibre providers certain security measures may not be applicable because these providers do not directly deal with subscribers and do not have much staff.

[20] Most generally an asset is anything of value. Assets can be abstract (like processes or reputation), virtual (data for instance), physical (cables, a piece of equipment), human resources, et cetera.

to the primary assets more specifically with the terms networks, services and personal data processing.

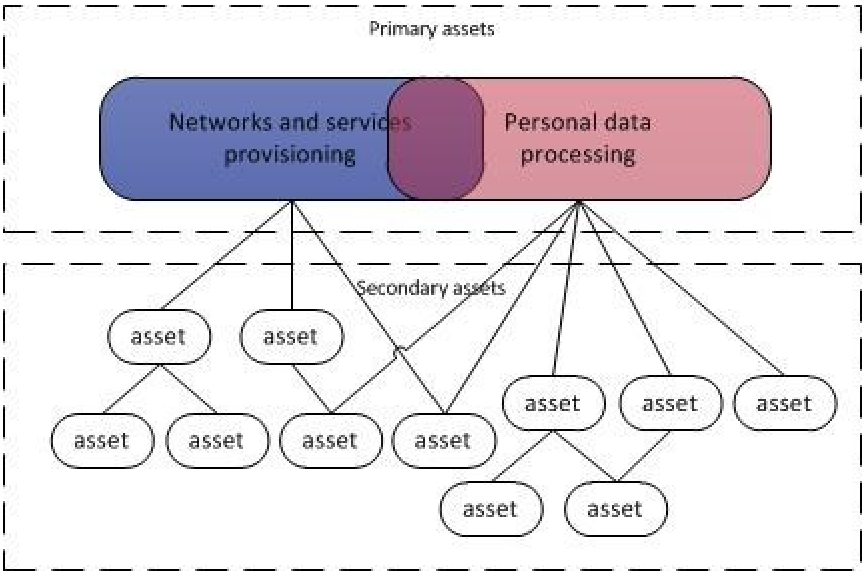


Figure 3: Primary and secondary assets in scope

4.1.2 Provision of networks and services and personal data processing

The primary assets are the provision of networks, services and personal data processing

The personal data processing which is in scope is the processing done “in connection with” the *provision* of the service. The type of personal data in question is typically:

1. Communications content; i.e. the content of communications of subscribers, such as the content of messages, voice conversations, voice mails, payload, internet traffic, etc. ,
2. Communications metadata; i.e. data *about* the communications, traffic data, numbers dialled, IP connection log, location data, etc. ,
3. Data about subscribers: contracts, bills, contract terms, billing addresses, billing/payment account details, detailed bills, home address, age, passport data, social security number, etc.

The networks and services which are in scope here are those networks and services regulated by the national legislation on electronic communications. The scope of national telecom legislation is not the same in all EU member states. As discussed in Section 3.3, in this document we simplify and focus only on:

- Fixed telephony (PSTN, VOIP)
- Mobile telephony (GSM, UMTS, LTE) and messaging (SMS)
- Fixed internet access (DSL, cable, fibre)
- Mobile internet access (GSM, UMTS, LTE)

This list is certainly not an exhaustive list of networks and services regulated under national laws implementing these directives.

4.1.3 Systems

It is not feasible to exhaustively list all systems which could be in scope, because this depends on the specific setting. We provide a list as an example of the type of systems which are often supporting, directly or indirectly, the provision of networks and services or the personal data processing:

- Base stations and controllers (e.g. BTS, NodeB, RNC)
- Mobile switching (e.g. MSC, VLR, SGSN, GGSN)
- Switches and routers (e.g. local exchanges, routers, DSLAM)
- Transmission nodes (e.g. SDH, WDM)
- Area network (fibre, cables, e.g.)
- Street cabinets
- Switching centre (MSC, VLR, e.g.)
- Addressing servers (DHCP, DNS)
- User and location registers (e.g. HLR, HSS, AuC)
- Databases, data storage, servers
- Messaging centres
- Core network (e.g. fibre-core, cable-aggregation)
- Interconnections (e.g. IXPs, IP transit)
- International backbone (submarine cables, international interconnections, e.g.)
- Operator backbone (fibre, cables, e.g.)
- PCs (laptops, desktops, e.g.)
- Removable media (USB sticks, CDROMs, external drives, e.g.)
- Power supply systems (e.g. transformers, power grid)
- Backup power supply (e.g. diesel generators, batteries)
- Cooling systems

Additionally in scope are the following systems:

- Provider web sites for customers, billing portals, et cetera, if they contain personal data which was collected and processed in connection with the provision of networks or services (see above for primary assets, see remark below about additional services).
- Customer premises equipment (CPE), if under the control of the operator (such as VOIP boxes, e.g.).
- Other systems used for storing or processing of personal data collected in connection with the provision of networks or services. This could involve procedures involving paperwork like paper-printed letters, contracts or bills.

Remark about additional services: *Additional services offered by the provider, which are not electronic communication networks and services, are out of scope, unless they contain personal data which had been processed in connection with the provision of these networks and services. Suppose, for example, that a provider offers also a cloud computing platform*[21] *- it is a separate product and customers can buy it separately. This means that the cloud computing service and the underlying assets are out of scope, unless (of course), they are used for storing/processing any of the personal data in connection with the provision of networks and services.*

Remark about scope difference between Article 4 and Article 13a: *By looking more closely at the (secondary) assets it is easy to see overlap and differences between Article 13a and Article 4. For example, an HLR (Home Location Register) or a core router would be in scope of Article 13a and Article 4. The helpdesk systems and the billing systems, for example, would be only in scope of Article 4. Backup power generators, for example, would be only in scope of Article 13a.*

[21] Many traditional EU telecom providers are now offering also cloud computing services.

4.1.4 Personnel

The personnel in scope are all employees, contractors, and third-party users which could have a negative impact on the security of networks, services and personal data processing.

In this document we use the term “key personnel” to refer to the key roles in the organization with respect to security of networks, services and personal data processing. 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 DPO, the business continuity manager, and the system administrators of critical systems.

4.1.5 Third parties and outsourcing

In this document we use the term “third parties” to refer to parties (organizations, individuals) the provider works with, for the provisioning of networks and services or the processing of personal data, i.e. vendors, suppliers, consultants, auditors, outsourcing partners, and so on. So in this document the term third-party does *not* refer to the customers, the public, or government authorities.

Third party assets are in scope just as if they were assets of the provider. In other words, even if certain processes are outsourced, the provider still remains responsible for ensuring that appropriate security measures are being taken. Risks related to third party assets need to be treated differently (using contracts and SLAs instead of using internal policies or processes).

4.1.6 Critical assets

We define critical assets as follows.

Critical assets: Assets are critical when if they fail there would likely be a *direct* and *significant* impact on the security of networks and services or a *direct* impact on personal data processing.

For example, the PC of an employee, which does not contain personal data (processed in connection with the provision of networks or services) nor directly supports the provision of networks or services, is not critical. If it is breached there is no direct impact on the security of networks and services or a *direct* impact on personal data processing. Of course the PC is still an asset in scope, as eventually there could be an impact, for example, an attacker might use the PC to gain further access and target a database with personal data. An HLR (home location register), for example, would be a critical asset, because if it is breached there is a direct impact *direct* and *severe* impact on the security of networks and services and a *direct* impact on personal data.

4.2 Threats in scope

All threats are in scope which could affect these assets and in this way cause a security incident. We give some examples of different types of threats.

Example: We give examples of threats which could affect the assets in scope.

- *Cable cut: A cable is cut, by accident, by a third party, for example by an excavation machine or by ship anchorage.*
- *Flood: Water floods an area which damages/obstructs physical infrastructure.*
- *Fire: A fire destroys a site, causing an outage and destroying paperwork stored there.*
- *Physical attack: Someone physically damages/obstructs physical infrastructure (cables, servers, et cetera).*

- *Mailing error: By mistake a paper-printed contract is put in the wrong envelope and sent to the wrong person.*
- *Cyber attack: Attackers tamper with the billing portal (using SQL injection) extracting sensitive and personal data.*
- *Phishing: Attackers use social engineering to obtain from someone of the provider's personal critical security data (a password e.g.).*
- *Fake basestation attack: Attackers set up a fake basestation and use it to intercept phone calls from a specific user.*
- *DDoS attack: Attackers flood a provider's DNS server using a DDoS attack causing large-scale outages.*
- *VOIP scam: Attackers exploit vulnerabilities in customer premise VOIP boxes (delivered and controlled by the provider) and subsequently commit dialiling fraud and wiretap the customer's communications.*
- *Wire tapping: Attackers place wiretaps on underground optical cables to eavesdrop on electronic communications.*
- *Theft: Someone steals equipment e.g. cables, storage media, laptops, et cetera.*
- *Third party failure: A road worker, by mistake, digs up an optical cable.*
- *Loss: Someone loses equipment, e.g, storage media, laptops, et cetera.*
- *Bad change: Someone executes (by mistake, by error) a bad change, for example, when installing a new piece of equipment or new piece of software.*
- *Software bug: A software bug causes network or information systems to function erratically.*

Most threats listed here are relevant for both Article 4 and Article 13a, some threats are only relevant for Article 4, some only for Article 13a.

Remark about risk assessment and risk management: *Assets and threats are the main ingredients in most risk assessment methodology. Usually the goal of a risk assessment is to look at the assets, see which threats could have an impact, and calculate the product of the likely hood of the threat occurring and the impact of the threat. The product is a measure of risk. This measure can be used to prioritize security measures.*

Depending on the setting, high risks often need to be mitigated with security measures. Low risks might be accepted and left unaddressed. Governance and risk management regards the practice of assessing risks periodically and controlling them, managing them, either by taking measures, or by accepting them.

Note that this guideline does not address in detail the issue of how providers should do their risk assessment and risk management. There are many different methodologies and standards, for different settings and different types of organizations.

4.3 Structure of the security measures

This document lists 26 security objectives[22] which have been derived from a set of international and national standards that are commonly used by providers in the EU's electronic communication

[22] In information security governance literature these are also sometimes referred to as control objectives.

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.

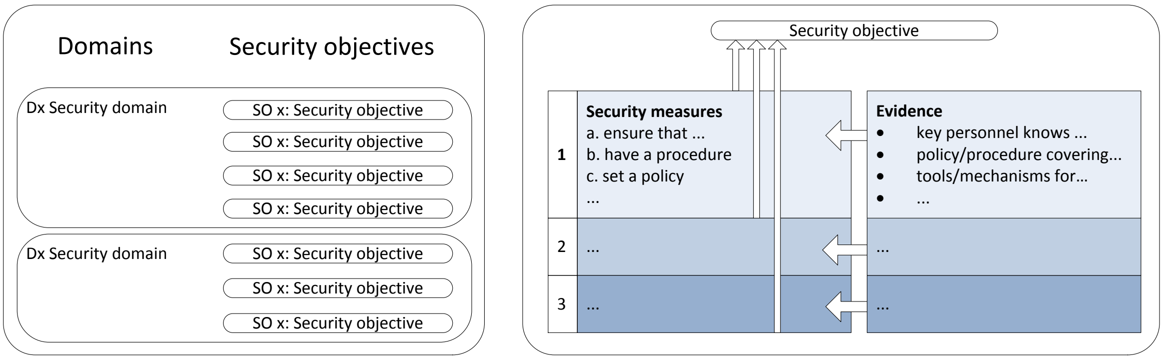


Figure 4: Structure of the security objectives and security measures.

Per security objective we also list detailed evidence which could indicate that these 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 overall structure of the security objectives and security measures is depicted in Figure 4.

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

Description of sophistication levels

Sophistication level 1 (basic):

- Basic security measures that could be implemented to reach the security objective.
- Evidence that basic measures are in place.

Sophistication level 2 (industry standard):

- Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents.
- Evidence of industry standard measures and evidence of reviews of the implementation reacting to changes and/or incidents.

Sophistication level 3 (state of the art):

- State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures.
- Evidence of state of the art (advanced) implementation, evidence of a structural review process, and evidence of pro-active steps to improve the implementation of 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.

Remark about profiles: *The levels of sophistication can be used to create profiles of providers, showing the sophistication of security measures across the board. Such profiles could be used by* *authorities, for example when evaluating the implementation of security measures across the sector. We elaborate on supervision methods in Section 5 and we give an example of two profiles there.*

Remark about 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. Note that in the first version of the Article 13a technical guideline on security measures carried the title "Minimum Security Measures".*

Remark about separate measures*: We list security measures separately per security objective, but this should not be seen as a recommendation to split activities into separate parts, or to keep separate documents or files. For example, a single inventory of assets could be used for risk assessment, but also to support change management and asset management procedures. For example, a policy about recruitment could well be a section or a paragraph in a wider security policy document.*

4.4 Security objectives and security measures

Below we list 26 high-level security objectives grouped in 7 domains (D1, D2, …). Per security objective we describe the kind of security measures that could be implemented by the provider to achieve the security objective, and the type of evidence that could be taken into consideration by a supervisor or an auditor when assessing if the security measures are in place (the structure is explained in Section 4.2).

Per security objective we indicate if it is particularly relevant for Article 13a or Article 4 using the notation [13a], [4], [4, 13a] in the title of the security objective. Note that the scope of Article 13a and Article 4 is subject to national interpretation, so this annotation should not be interpreted as a recommendation to CNAs about the scope of their (national) supervision. For example, by annotating a security objective as relevant for Article 4 it does not mean that the security objective should not be considered by an authority when assessing compliance with Article 13a.

D1: Governance and risk management

The domain "Governance and risk management" includes the security objectives related to governance and management of risks for the security of networks, services and personal data processing.

SO 1 [4, 13a] Information security policy

Establish and maintain an appropriate information security policy addressing the security of networks, services and personal data processing.

	Security measures	Evidence
1	a) Set a high level security policy addressing the security of the networks and services provided and the security of personal data processing. b) Make key personnel aware of the security policy.	• Documented security policy, including networks and services in scope, and personal data processing in scope, the critical assets, the security objectives (confidentiality of communications, protection of personal data, data-minimization etc.), applicable law and

		regulations. • Key personnel are aware of the security policy and its objectives (interview).
2	c) Set detailed information security policies for critical (secondary) assets. d) Provide access and make all personnel aware of the relevant security policies and what these imply for their work. e) Review the security policies following incidents.	• Documented information security policies for critical assets. • Personnel can access and are aware of the information security policies and what it implies for their work (interview). • 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.	• Information security policies are up to date and approved by senior management. • Logs of policy exceptions, approved by the relevant roles. • Documentation of review process, taking into account changes and past incidents.

Note that Article 4 explicitly mentions that providers need to have a security policy regarding personal data processing: *"ensure the implementation of a security policy with respect to the processing of personal data"*.

SO 2 [4, 13a] Governance and risk management

Establish and maintain an appropriate governance and risk management framework, to identify and address risks for networks, services and personal data processing.

	Security measures	Evidence
1	a) Make a list of the main risks for security of the networks, services or the personal data processing. b) Make key personnel aware of the main risks and how they are mitigated.	• List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security of networks, services or the personal data processing. • Key personnel know the main risks (interview).
2	c) Set up a risk management methodology and/or tools based on industry standards. d) Ensure that key personnel use the risk management methodology and tools. e) Review the risk assessments following changes or incidents. f) Ensure residual risks are accepted by key personnel, and/or management.	• Documented risk management methodology and/or tools. • Guidance for personnel on assessing risks. • List of risks and evidence of updates/reviews. • Review comments or change logs for risk assessments. • Sign-off on assessments of residual risks.

3	g) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.	• Documentation of the review process and updates of the risk management methodology and/or tools.

SO 3 [4, 13a] 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 (e.g. setting security policy, incident response, checking compliance, granting exceptions). b) Make sure the security roles are reachable in case of security incidents.	• List of security roles (CISO, DPO, business continuity manager, etc), who occupies them and their contact information.
2	c) Personnel is formally appointed in security roles. d) Make personnel aware of the security roles and when they should be contacted.	• List of appointments (CISO, DPO, business continuity manager, etc), and description of responsibilities and tasks for security roles (CISO, DPO, etc). • 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.	• Up-to-date documentation of the structure of security role assignments and responsibilities • Documentation of review process, taking into account changes and past incidents.

SO 4 [4, 13a] Security of third party assets

Establish and maintain a policy of security requirements for contracts with third parties (see Section 4.1.5),to ensure that dependencies on third parties do not negatively affect the security of networks, services or personal data processing.

	Security measures	Evidence
1	a) Include security requirements in contracts with third-parties, to ensure security of networks, services or personal data processing	• Explicit security requirements in the contracts with third parties supplying IT products, IT services, outsourced business processes, helpdesks, call centres, interconnections, shared facilities, et cetera. • Explicit security requirements for third parties processing personal data, taking into account personal data protection

		legislation, country/union borders, foreign jurisdictions, et cetera.
2	b) Set a security policy for contracts with third-parties. c) Ensure that all procurement of services or products from third-parties is done according to the policy. d) Review security policy for third parties, following incidents or changes. e) Mitigate residual risks that are not addressed by the third party.	• Documented security policy for contracts with third parties. • List of contracts with third-parties, and list of third parties processing personal data. • Contracts for third party services contain security requirements, in line with the security policy for procurement. • Review comments or change logs of the policy. • Residual risks resulting from dependencies on third parties are listed and mitigated.
3	f) Keep track of security incidents related to or caused by third-parties. g) Periodically review and update security policy for third parties at regular intervals, taking into account past incidents, changes, etc.	• List of security incidents related to or caused by engagement with third-parties. • Documentation of review process of the policy.

D2: Human resources security

The domain “Human resources security” covers the risks related to personnel.

SO 5 [4, 13a] Background checks

Perform appropriate background checks on personnel (employees, contractors, and third-party users) if required for their duties and responsibilities.

	Security measures	Evidence
1	a) Check professional references of key personnel.	• 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.	• Policy and procedure for background checks/screenings. • 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.	• Review comments or change logs of the policy/procedures.

SO 6 [4, 13a] 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 about security. b) Provide key personnel with relevant training about personal data and data protection legislation.	• Key personnel have followed security trainings and have sufficient security knowledge (interview). • Key personnel know which data is personal data, which data is sensitive personal data, and which are the main principles of personal data protection laws.
2	c) Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. d) Organise trainings and awareness sessions for personnel on network and information security, personal data and data protection legislation.	• Documented program for training on security skills, including, objectives for different roles and how to reach it (by e.g. training, awareness raising, etc). • Personnel have participated in awareness sessions on network and information security, personal data and personal data protection legislation.
3	e) Review and update the training program periodically, taking into account changes and past incidents. f) Test the security knowledge of personnel. Test the knowledge of personal about personal data.	• Updated awareness and training program • Results of tests of personnel. • Review comments or change logs for the program.

SO 7 [4, 13a] 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, et cetera, if no longer necessary or permitted. b) Brief and educate new personnel on the policies and procedures in place.	• Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, et cetera • 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 access rights, badges, equipment. d) Implement policy/procedures for education and training for personnel in new roles.	• 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. • Evidence that personnel changes have been carried according to the process and that access rights have been updated timely (checklists e.g.).
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.	• Evidence of checks of access rights etc. • Up to date policy/procedures for managing personnel changes. • Review comments or change logs.

SO 8 [4, 13a] Handling violations

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

	Security measures	**Evidence**
1	a) Hold personnel accountable for violating security policies, for example via employment contracts, third party contracts, etc.	• Rules and contracts for personnel which describes responsibilities for violations, as part of employment contracts, third party contracts.
2	b) Set up procedures for violations of security policies by personnel.	• Documentation of procedure, 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.	• Review comments or change logs

D3: Security of systems and facilities

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

SO 9 [4, 13a] Physical and environmental security of facilities

Establish and maintain the appropriate physical and environmental security of facilities.

	Security measures	**Evidence**

1	a) Set up physical controls to protect network and information systems and facilities from unauthorized physical access and burglary. b) Set up environmental controls, to protect against fire, flooding, et cetera.	• Basic implementation of physical security measures such as door and cabinet locks, burglar alarm, etc. • Basic implementation of environmental controls, such as fire alarms, fire extinguishers, etc.
2	c) Implement a policy for physical security measures and environmental controls. d) Industry standard implementation of physical and environmental controls.	• Documented policy for physical security measures and environmental controls, including description of network and information systems and facilities in scope. • Industry standard physical controls like electronic control of entrance, audit trail, segmentation of spaces according to authorization levels, etc. • Industry standard environmental controls lik automated fire extinguishers with halocarbon gases, etc.
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.	• Up to date policy for physical security measures and environmental controls • Documentation about evaluation of environmental control, review comments or change logs.

SO 10 [13a] Security of supplies

Establish and maintain appropriate security of supplies (electricity, fuel, cooling, etc) to the facilities.

	Security measures	**Evidence**
1	a) Ensure security of supplies, such as electric power, fuel or cooling.	• Security of 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, such as electrical power, fuel, etc. c) Implement industry standard security measures to protect supplies and supporting facilities.	• Documented policy to protect critical supplies such as electrical power, fuel, etc, describing different types of supplies, and the security measures protecting the supplies. • Evidence of industry standard measures to protect the security of supplies, such as for example, passive cooling, automatic restart after power interruption, battery backup power, diesel generators, backup fuel, etc.

3	d) Implement state of the art security measures to protect supplies. e) Review and update policy and procedures to secure supplies regularly, taking into account changes and past incidents.	• Evidence of state of the art measures to protect security of supplies, such as active cooling, UPS, hot standby power generators, sufficient fuel delivery SLA, SLAs with fuel delivery companies, redundant cooling and power backup systems. • Updated policy for securing supplies and supporting facilities, review comments and/or change logs.

SO 11 [4, 13a] Access control to network and information systems

Establish and maintain appropriate (logical) access controls for the network and information systems, to prevent unauthorized access, modification, or deletion of data on these systems.

	Security measures	Evidence
1	a) Users and systems have unique ID's and are authenticated before accessing systems. b) Implement (logical) access control mechanism for network and information systems to allow only authorized use. c) Encrypt security critical data (like passwords, shared secrets, private keys) and personal data, before storing it on removable media without proper access control mechanisms (for example, CDROMs, USB sticks, laptops etc), to prevent unauthorized access.	• Access logs show unique identifiers for users and systems when granted or denied access. • Overview of authentication and access control methods for systems and users. • Overview of encryption methods for storing security critical data and personal data on removable media.
2	d) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. e) Choose appropriate authentication mechanisms, depending on the type of access. f) Monitor access to network and information systems, have a process for approving exceptions and registering access violations.	• Access control policy including description of roles, groups, access rights, procedures for granting and revoking access. • Different types of authentication mechanisms for different types of access. • Log of access control policy violations and exceptions, approved by the CISO and/or the DPO, when relevant.
3	f) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. g) Access control policy and access control mechanisms are reviewed and when needed revised.	• Reports of security tests of access control mechanisms. • Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). • Logs of intrusion detection and anomaly detection systems.

		• Updates of access control policy, review comments or change logs.

SO 12 [4,13a] Integrity of network and information systems

Establish and maintain integrity of network and information systems, to protect from trojans, code injections, and other malware which could alter their functionality.

	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) Make sure security critical data (like passwords, shared secrets, private keys, etc) are not disclosed or tampered with. d) Check for malware on (internal) network and information systems.	• Software and data in network and information systems is protected using input controls, firewalls, encryption and signing. • Security critical data is protected using protection mechanisms like separate storage, encryption, hashing, etc. • Malware detection systems are present, and up to date.
2	e) Implement industry standard security measures, providing defence-in-depth against tampering and altering of systems.	• Documentation about how the protection of software and data in network and information system is implemented. • Tools for detection of anomalous usage of systems or anomalous behaviour of systems (such as intrusion detection and anomaly detection systems). • Logs of intrusion detection and anomaly detection systems.
3	f) Set up state of the art controls to protect integrity of systems. g) Evaluate and review the effectiveness of measures to protect integrity of systems.	• State of the art controls to protect integrity of systems, such as code signing, tripwire, et cetera. • Documentation of process for checking logs of anomaly and intrusion detection systems.

SO 13 [4] Confidentiality of communications

Establish and maintain an appropriate policy on confidentiality and integrity of communications content and communications metadata.

	Security measures	Evidence
1	a) Make sure communications content and metadata is kept confidential. b) Implement appropriate authentication mechanisms for customers of the networks and services.	• Overview of networks and services in scope, and the methods to protect confidentiality of communications content and metadata, such as protocols and encryption methods used to encrypt traffic, authentication methods for

	c) Protect security critical data for customers, such as SIM cards, IMEI number, passwords, et cetera.	customers of networks and services, et cetera.
2	d) Implement a policy for protecting confidentiality and integrity of communications content and metadata. e) Monitor usage of networks and services by customers and detect anomalous usage.	• Documented policy addressing confidentiality of communications content and metadata, including networks and services in scope, the objectives of the policy, the methods used for protecting confidentiality, encryption methods used when there is no access control (over the air e.g.).
3	e) Evaluate the effectiveness of methods to protect confidentiality of communications and communications metadata by performing cross-checks and tests. f) Review and update the policy on confidentiality of communications when needed, taking into account changes and/or past incidents.	• Tools showing anomalous usage by customers, logs of anomaly detection systems, et cetera. • Updates of policy on confidentiality of communications, review comments or change logs.

D4: Operations management

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

SO 14 [4, 13a] 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.	• 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.	• 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.	• Updated policy/procedures for critical systems, review comments and/or change logs.

SO 15 [4, 13a] Change management

Establish change management procedures for critical network and information systems, to mitigate incidents caused by changes.

	Security measures	Evidence
1	a) Follow predefined procedures when making changes to critical systems.	• Documentation of change management procedures for 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.	• Documentation of change management policy/procedures including, systems subject to the policy, objectives, roll back procedures, etc. • 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.	• Up to date change management procedures, review comments and/or change logs.

SO 16 [4, 13a] Asset management

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

	Security measures	Evidence
1	a) Manage critical assets and configurations of critical systems.	• List of critical assets and critical systems, i.e. list of assets which directly support networks or services, or which store or process personal data.
2	b) Implement policy/procedures for asset management and configuration control. c) Dispose of assets securely, using paper shredders, algorithms for the secure deletion of data, et cetera.	• Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, and the objectives of asset management. • An asset inventory or inventories, containing critical assets and the dependency between assets. • A configuration control inventory or inventories, containing configurations of critical systems.

		- Documented procedures for disposal and decommissioning of assets.
3	d) Review and update the asset management policy regularly, based on changes and past incidents.	- Up to date asset management policy/procedures, review comments and/or change logs.

D5: Incident management

The domain "Incident management" covers detection of, response to, incident reporting, and communication about incidents[23].

SO 17 [4, 13a] Incident management procedures

Establish and maintain procedures for managing security incidents, and forwarding them to the right 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 c) Keep an inventory of security incidents with an impact on personal data.	- Personnel are aware of how to deal with incidents and when to escalate. - Inventory of incidents with a significant impact on networks or services, and per incident, impact, cause, actions taken, and lessons learnt. - Inventory of security incidents with an impact on personal data, including a description of the incident, the impact, and the actions taken by the provider to mitigate the incident[24].
2	c) Implement policy/procedures for managing incidents.	- 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 CISO, DPO, CEO, et cetera.

[23] For the definition of 'incident' used in this document, see Section 2.

[24] According to Article 4 this inventory should have the information necessary for authorities to verify compliance to the incident reporting obligations of Article 4 – but not more. This document does not go into detail about the incident reporting obligations in Article 4 and Article 13a.

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.	• Individual reports about the handling of major incidents. • Up to date incident management policy/procedures, review comments and/or change logs.

Note that Article 4 explicitly requires providers to keep an inventory of all personal data breaches.

SO 18 [4, 13a] Incident detection capability

Establish and maintain an appropriate incident detection capability for detecting security incidents.

	Security measures	Evidence
1	a) Set up processes or systems for incident detection.	• Past incidents were detected and timely forwarded to key personnel if needed.
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.	• 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, et cetera.
3	d) Review systems and processes for incident detection regularly and update them taking into account changes and past incidents. .	• Up to date documentation of incident detection systems and processes. • Documentation of reviews of the incident detection process, review comments, and/or change logs.

SO 19 [4, 13a] Incident reporting and communication

Establish and maintain appropriate incident reporting and communication procedures, taking into account national legislation on incident reporting to government authorities[25].

	Security measures	Evidence
1	a) Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary. b) Notify individuals about personal data	• Evidence of past communications and incident reporting. • Evidence of past notifications to individuals.

[25] For example, Article 13a and Article 4 (both transposed by EU member states to national legislation) requires electronic communications providers to report personal data breaches (article 4) and significant security incidents (article 13a) to the competent national authorities. This document does not go into detail about the incident reporting obligations in Article 4 and Article 13a.

	breaches which affect them.	
2	c) Implement policy and procedures for communicating and reporting about incidents.	• 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. • Templates for incident reporting and communication
3	d) Evaluate past communications and reporting about incidents. e) Review and update the reporting and communication plans, based on changes or past incidents.	• List of incident reports and past communications about incidents • Up to date incident response and communication policy, review comments, and/or change logs.

D6: Business continuity management

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

SO 20 [13a] Service continuity strategy and contingency plans

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

	Security measures	**Evidence**
1	a) Implement a service continuity strategy for the networks and services.	• Documented service continuity strategy, including recovery time objectives for networks and services.
2	b) Implement contingency plans for critical systems. c) Monitor activation and execution of contingency plans, registering successful and failed recovery times.	• Contingency plans for critical systems, including clear steps and procedures for common threats, triggers for activation, steps and recovery time objectives • Decision process for activating contingency plans. • Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time.

3	d) Review and revise service continuity strategy periodically. e) Review and revise contingency plans, based on past incidents and changes.	- Up to date continuity strategy and contingency plans, review comments, and/or change logs.

SO 21 [13a] Disaster recovery capabilities

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

	Security measures	**Evidence**
1	a) Prepare for recovery and restoration of networks or services following disasters.	- Measures are in place for dealing with disasters, such as failover sites in other regions, backups of critical data to remote locations, et cetera.
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).	- Documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the networks or services, and a list of disaster recovery capabilities (either those available internally or provided by third parties). - Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, et cetera.
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.	- State of the art disaster recovery capabilities, such as full redundancy and failover mechanisms to handle natural and/or major disasters. - Updated documentation of disaster recovery capabilities in place, review comments and/or change logs.

D7: Monitoring, auditing and testing

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

SO 22 [4, 13a] Monitoring and logging policies

Establish and maintain systems and functions for monitoring and logging of critical network and communication systems.

	Security measures	**Evidence**

1	a) Implement monitoring and logging of critical systems.	- 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 critical systems.	- Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and the overall objectives of storing monitoring data and logs. - Tools for monitoring systems and collecting logs. - 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.	- Tools to facilitate structural recording and analysis of monitoring and logs. - Updated documentation of monitoring and logging policy/procedures, review comments, and/or change logs. .

SO 23 [4, 13a] 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.	- 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 times. 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.	- 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. - Reports about exercises and drills showing the execution of contingency plans, including lessons learnt from the exercises. - Issues and lessons learnt from past exercises have been addressed by the responsible people.

3	d) Review and update the exercises plans, taking into account changes and past incidents and contingencies which were not covered by the exercises program. e) Involve suppliers, and other 3rd parties, like business partners or customers in exercises.	- Updated exercises plans, review comments, and/or change logs. - Input from suppliers and other 3rd parties involved about how to improve exercise scenarios.

It is important to stress here that contingency exercises should not have an impact on security of networks, services and personal data processing, and that, as a general rule, personal data should not be used in exercises.

Certain personal data breaches are so severe that they trigger a contingency plan. The ENISA technical guideline for the implementation of Article 4 recommends creating contingency plans for dealing with personal data breaches as well as scenarios for exercising such plans.

SO 24 [4, 13a] Network and information systems testing

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

	Security measures	Evidence
1	a) Test network and information systems before using them or connecting them to existing systems.	- 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	- Policy/procedures for testing network 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.	- List of test reports. - Updated policy/procedures for testing network and information systems, review comments, and/or change log.

It is important to stress here that testing should not have an impact on security of networks, services and personal data processing, and that, as a general rule, personal data should not be used in tests.

SO 25 [4, 13a] Security assessments

Establish and maintain an appropriate policy for performing security assessments and tests 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. .	- Reports from past security scans and security tests.
2	b) Implement policy/procedures for security assessments, scanning and testing.	- Documented policy/procedures for security assessments, scanning, 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 .
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.	• List of reports about security assessment and security tests • Reports of follow up actions on assessment and test results • Up to date policy/procedures for security assessments and security testing, review comments, and/or change log.

SO 26 [4, 13a] 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.	• Reports describing the result of compliance monitoring.
2	b) Implement policy/procedures for compliance monitoring and auditing.	• 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. • 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..	• List of all compliance and audit reports • Updated policy/procedures for compliance and auditing, review comments, and/or change logs.

5 Technical supervision of security measures

Paragraphs 1 of Article 4 and paragraphs 1, 2 of Article 13a require authorities (CNAs) to ensure that providers take appropriate security measures. Both Article 4 and Article 13a give a mandate to authorities to 'audit' providers in this regard.

In this section we discuss the technical details of supervising the security measures[26]. Common activities regarding supervision of the security measures are:

- 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 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 would allow providers to indicate, per security objective, what kind of security measures are in place. Used in this way the sophistication levels would yield a profile of a provider, allowing for a quick comparison between providers across the sector.

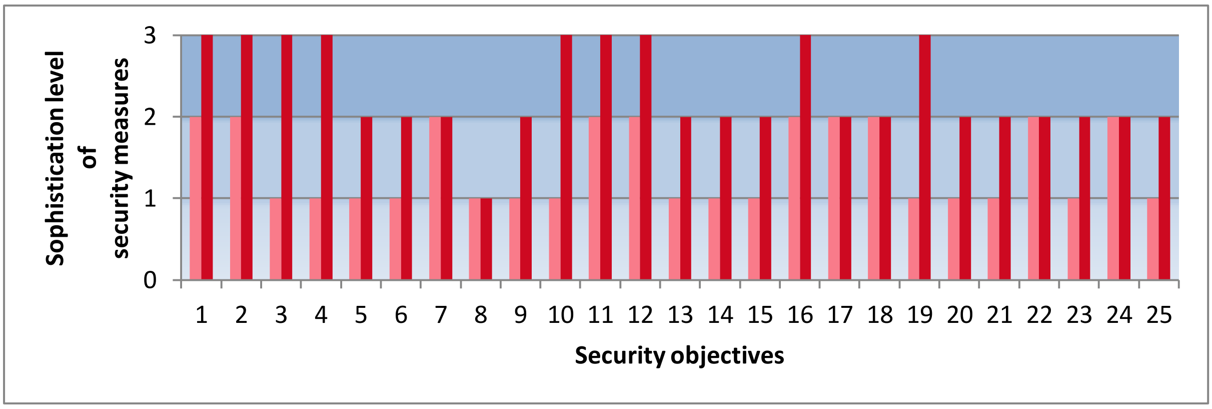


Figure 5: Two different profiles with different sophistication of measures for each security objective.

In figure 2 we show two example profiles in one diagram. The vertical axis spans the sophistication levels and the horizontal axis spans the security objectives. Dark red indicates a provider with more sophisticated security measures. The light red indicates a provider with less sophisticated security measures. The difference in sophistication could be explained, for example, by a difference in the type of communication services or networks being offered by the two providers.

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

[26] Supervision of security measures is not an easy task, because network and information technology changes rapidly, because capabilities of attackers change rapidly, and because the effectiveness of security measures often depends on technical implementation details. In addition, supervision by the NRA is further complicated by the fact that in most EU countries the electronic communications sector consists of a wide range of different types of providers, including very small providers, incumbents, black fibre operators, et cetera.

Authorities (CNAs) 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 CNA could set up a self-assessment form. In the first example, the CNA assesses security measures across all providers in the sector, but with a focus on a subset of the security objectives.

Example: The CNA of country D has organized a self-assessment focussed 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 CNA focusses on a subset of security measures and a subset of providers:

Example: The CNA 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 CNA 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), SO19 (Service continuity strategy and contingency plans), SO20 (Disaster recovery capabilities), SO22 (Exercise contingency plans), indicate the level of sophistication, on a scale from 0 to 4 (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 CNA 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.*

5.2 Taking a staged approach

Depending on the national circumstances, authorities might want to adopt a staged approach in supervising (and enforcing) compliance to the security requirements in Article 4 or Article 13a. For example, in case some providers do not (yet) have appropriate security measures in place (or if they cannot provide evidence of this), authorities might want to give providers some time to comply, in stages. This guideline supports a staged approach. We discuss some possible options for staging:

- **Subset of networks and services or subset of assets:** Authorities could first focus on a subset of services (for example mobile networks) or a subset of assets (for example, core network, or large facilities), and deal with the rest later.

  Example: The CNA in country A wants to focus first on the mobile networks, because they are (nationally) the most critical. The CNA starts with a self-assessment across providers of mobile networks. The scope of the assessment is 'assets supporting mobile networks'. Other providers are out of scope initially.

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

  Example: The CNA in country B wants to focus first on the providers with large market share, because here a lot of users are at stake. The CNA 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 CNA will start a separate supervision program for smaller providers (focussed more on guidance).

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

  Example: The CNA 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 CNA focusses first on the measures SO9, SO10, SO19, SO20, and SO22. The CNA will address other security measures at a later stage.

- **Sophistication levels and baselines:** Authorities could first focus on ensuring that all providers have taken certain basic security measures, a baseline. For example, level 1 as defined in this guideline, or another baseline. We should stress here that such an approach would have limitations: particularly when the sector has both large and small providers, it will be difficult to find a baseline of measures which suits both categories. To take the differences across the sector into account it is necessary to define several different baselines for different types of providers.

  Example: The CNA 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, …, D7)– it is the baseline for large providers (>10% of market share).

  At a later stage the CNA 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.).

5.3 Auditing providers

Depending on the setting, authorities (CNAs) 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 a 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: *CNAs 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. CNAs 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, CNAs should take into account that providers may keep certain relevant documentation (manuals, policies, procedures, et cetera) in the English language for efficiency reasons, because the provider operates in several countries or because the operator employs personnel from abroad.*

5.3.1 Assessment types

An audit involves different types of assessments, for example a review of security policies, an interview with the DPO, 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 simply 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), Data protection officer (DPO), 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, interviews, an ultimate check to see if the network & information systems are secure is by inspecting or testing these systems directly. This kind of system review may be needed in certain settings, for example to understand

how a security incident could have happened. System evaluation should be focused at critical systems because it can be time-consuming.

5.3.2 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 authorities (CNAs). An advantage of self-assessments is that self-assessments are relatively cheap for providers. Earlier in this chapter (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.
- **CNA as auditor:** The CNA could carry out an audit of a provider, by using internal staff 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 ISO27001 certified. Certification is often refreshed yearly, following a yearly re-audit. Authorities (CNAs) could require certification, and ask providers to submit their certificates as a way to show compliance.
- **Specialist auditor:** In special cases the CNA may want to designate a specific auditor, for a specific purpose or following a specific incident. For example, a CNA could mandate providers to undergo a security scan of systems by a security scanning specialist.
- **Pool of auditors:** The CNA 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 scores. For example, authorities (CNAs) could start with a list of licensed auditors27 and offer them a yearly training which focusses on the Article 13a and Article 4, in this way creating and educating a pool of auditors.

[27] In most countries, for example, there are organizations that license auditors to carry out IT audits.

5.3.3 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, but it is good practice to set-up preventive audits according to a multi-year plan and focus on certain (important) issues first 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 CNA of country H mandates providers to undergo yearly (preventive) audits by 3rd party auditors. To simplify matters and to reduce the burden for providers, the NRA 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, SM19, SM20, SM22). 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 a CNA 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 assets affected by the incident, the assets affected) and regards specific security measures (measures failing during the incident, or measures which could prevent re-occurrence).

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

- ENISA published two annual reports about major incidents in the EU electronic communications sector. The two reports, concerning the 2011 incidents and the 2012 incidents, are available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports
- The ENISA guidelines on the implementation of Article 13a are available at: https://resilience.enisa.europa.eu/article-13
- The ENISA guideline on the implementation of Article 4 is available at: http://www.enisa.europa.eu/act/it/risks-and-data breaches/dbn/art4_tech/at_download/fullReport
- ENISA's whitepaper on cyber incident reporting in the EU shows Article 13a and how it compares to some other security articles mandating incident reporting and security measures:

  http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
- For the interested reader, ENISA's 2009 paper on incident reporting shows an overview of the situation in the EU 3 years ago: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/good-practice-guide-on-incident-reporting/good-practice-guide-on-incident-reporting-1

Relevant EU Legislation

- The electronic communications regulatory framework (incorporating the telecom reform of 2009), including the reform of 2009, including the Framework directive, the e-Privacy directive and more specifically Article 13a and Article 4: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Copy%20of%20Regulatory%20Framework%20for%20Electonic%20Communications%202013%20NO%20CROPS.pdf
- An overview of the main elements of the 2009 reform: http://ec.europa.eu/information_society/policy/ecomm/tomorrow/reform/index_en.htm
- In 2013 the European commission proposed a cyber security strategy and a cyber security directive: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
- The regulation on implementing measures for Article 4, issued in 2013, which focuses on the notification of personal data breaches under Article 4: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:EN:PDF

Security standards and security best practices

- ISOIEC 27001/ISOIEC 27002 "Information security management"
- ISOIEC 24762 "Guidelines for information and communications technology disaster recovery services"

- ISO 27005 “Information security risk management”
- ISO 27011 “Information security management guidelines for telecommunications”
- BS 25999-1 “Guide to Business Continuity Management”
- BS 25999-2 “Business Continuity Management Specification”
- 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”
- ISF Standard 2007 “The Standard of Good Practice for Information Security”
- CobiT “Control Objectives for Information and related Technology”
- ITIL Service Support
- ITIL Security Management
- PCI DSS 1.2 Data Security Standard

National standards and good practices

- IT Baseline Protection Manual Germany
- KATAKRI, National security auditing criteria, Finland
- NIST 800 34 “Contingency Planning Guide for Federal Information Systems”
- NIST 800 61 “Computer Security Incident Handling Guide”
- FIPS 200 “Minimum Security Requirements for Federal Information and Information Systems”
- NICC ND 1643 “Minimum security standards for interconnecting communication providers”

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu