

Technical Guideline on Security Measures

TLP:Green, Version 1.98, November 2013





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

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 worked with TNO, the Netherlands, (in the context of ENISA tender P/28/11/TCD) to develop the practices and evidence in Section 3 and the supervision activities in Section 5. For the completion of this guideline ENISA has worked closely with a working group of experts from national regulatory authorities and ministries in the EU (the Article 13a Expert Group):

PTS (SE), Agentschap Telecom (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), Ministry of Defence (DK), RTR (AT), ANCOM (RO), EA "ECNIS" (BG), CCED (FR), Bundesnetzagentur (DE), ADAE (GR), BIPT (BE), MINETUR (ES), MPO (CZ), CTO (CZ), CERT LT (LT), MFSR(SK), ILR (LU), APEK (SI), MCA (MT), Ministry of Economic Development (IT), OCECPR (CY), PT (NO).

We are grateful for their valuable input and comments.

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

© European Union Agency for Network and Information Security (ENISA), 2013

Reproduction is authorised provided the source is acknowledged.

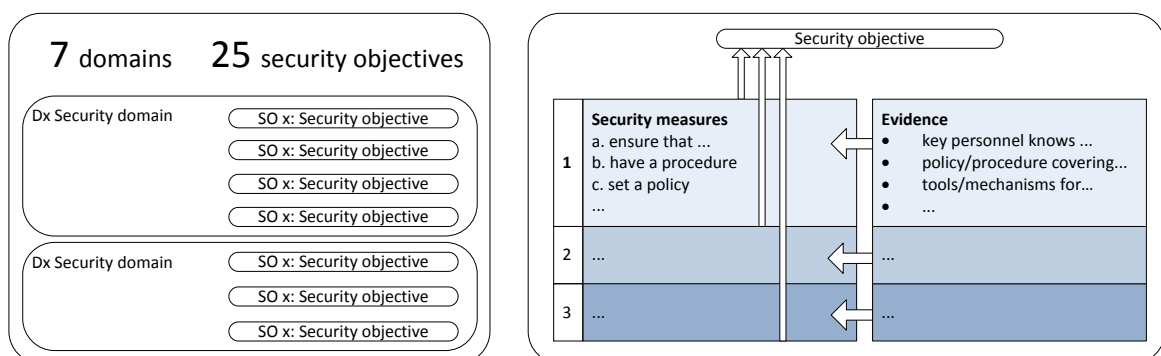
Preface

The 2009 reform of the EU legislative framework for electronic communications (EU Directive 2009/140/EC) introduces Article 13a into the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). The reform was transposed by most EU Member States halfway 2011.

Article 13a concerns security and integrity of electronic communications networks and services. The first part of Article 13a requires that providers of networks and services manage security risks and take appropriate security measures to guarantee the security (paragraph 1) and integrity (paragraph 2) of these networks and services. The second part of Article 13a (paragraph 3) requires providers to report about significant security breaches and losses of integrity to competent national authorities, who should report about these security incidents to ENISA and the European Commission (EC) annually.

In 2010, ENISA, the European Commission (EC), Ministries and Electronic Communications National Regulatory Authorities (NRAs), initiated a series of meetings (workshops, conference calls) to achieve an efficient and harmonised implementation of Article 13a across the EU. The Article 13a Expert Group now comprises experts from NRAs from all EU countries and some EFTA and EU candidate countries. Meetings (telephonic or physical) are organized and chaired by technical experts from ENISA. The European Commission participates as an observer in these meetings. The Article 13a Expert Group reached consensus about two non-binding technical guidelines for NRAs: the "Technical Guideline on Incident Reporting" and the "Technical Guideline on Security Measures" (this document).

This document, the Technical Guideline for Security Measures, provides guidance to NRAs about the technical details of implementing paragraphs 1 and 2 of Article 13a: how to ensure that providers assess risks and take appropriate security measures. This document contains a list of 25 high-level security objectives, divided in 7 domains (Governance and risk management, Human resources security, et cetera). Per security objective we list the security measures that could be taken by providers to reach the objective, grouped in 3 levels of sophistication. We also list evidence which could indicate that measures are in place. The overall structure is depicted in the diagram below.



Neither the high-level security objectives nor the detailed security measures should be seen as binding recommendations about which are appropriate security measures for providers to take. The electronic communications sector is diverse with large and small providers, providers offering a full stack of services or just black fibres, offering mobile networks or just DSL, and so on. Risks are different in each case. This document is intended as a tool for NRAs supervising the sector, to be used for creating guidance for providers, self-assessment forms, or as a structure for audits and audit reports.

Table of Contents

Preface	iii
1 Introduction	1
2 Background	2
3 Article 13a and terminology	4
3.1 Paragraph 1 and 2 of Article 13a	4
3.2 Terminology	4
4 Security measures	6
4.1 Assets in scope and risk assessment	6
4.2 Structure of the security measures	7
4.3 Security objectives and security measures	9
5 Technical supervision of security measures	25
5.1 Mandating or recommending a security standard	25
5.2 Assessing compliance across the market	27
5.3 Taking a staged approach	28
5.4 Auditing providers	29
6 Mapping to international standards	33
7 References	34

1 Introduction

In this document, we provide guidance to Electronic Communications National Regulatory Authorities (NRAs) about the security measures mentioned in paragraphs 1 and 2 of Article 13a of the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). The main content of this document is a list of high-level security objectives NRAs should take into account when assessing compliance of providers to Article 13a.

This document is drafted by an expert group of experts from NRAs and representatives of the EC, supported by technical experts from ENISA (see [Preface](#)): the [Article 13a Expert Group](#).

Target audience

This document is addressed to experts from national ministries and NRAs in European Member States tasked with the implementation of Article 13a.

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

Goal

This document is published by ENISA to provide guidance to NRAs about the security measures described in paragraph 1 and 2 of Article 13a.

Versions and changes

ENISA updates this guideline periodically, when necessary, and in agreement with the NRAs.

This version is an update of Version 1.0 of the Guideline on Minimum Security Measures. With respect to Version 1.0 the security domains did not change, and also the structure of the high-level security objectives remained the same (except for minor changes, see below).

List of main changes:

- SD5.3 Incident response and escalation processes was combined with SD5.2 Incident detection capability (now SO17). Hence v2.0 has 25 security objectives, instead of 26 in v1.0.
- Removed quotes and snippets from standards which served as examples.
- Renamed security measures to security objectives (SO).
- Added, per security objective, detailed security measures which could be taken by providers to reach the security objective and also descriptions of evidence which auditors/supervisors could take into account when assessing if the security measures are in place.
- Added guidance on different methods NRAs could use in their supervision of the security measures. This replaces the short section on implementation in Version 1.0.

Structure of this document

In [Section 2](#) we summarize the role and objectives of ENISA related to the implementation of Article 13a. In [Section 3](#) we introduce Article 13a, the scope and the terminology used in this document. In [Section 4](#) we list 25 security objectives, divided in 7 domains, and we provide details about security measures and evidence. In [Section 5](#) we give guidance for a number of regulatory activities NRAs could deploy to assess compliance to the security measures required by Article 13a. In [Section 6](#) we provide a mapping from the security measures in this guideline to some well-known international standards.

2 Background

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

EU policy context

This guideline concerns Article 13a of the Framework directive (Directive 2002/21/EC as amended by Directive 2009/140/EC). There are a number of other initiatives (legal or otherwise) addressing the security of public electronic communications networks and services.

- 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 networks and information systems: the [European Programme for Critical Infrastructure Protection](#) (EPCIP).
- In 2009, the EC adopted, in March 2009, a communications 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.

The European Commission has also [published](#) a European Cyber Security Strategy and a proposed directive on network and information security (NIS). The strategy, the directive and speeches from the EC contain explicit references to Article 13a and they mention the possibility of extending Article 13a to other sectors of the society.

For an overview of several security articles, which address security measures and incident reporting, we refer to the ENISA paper [Cyber incident reporting in the EU](#) which summarizes and compares Article 13a of the Framework directive, Article 4 of the e-Privacy directive, Article 15 of the proposed e-Trust/e-ID regulation and the reporting requirements in the proposed data protection reform.

ENISA's role

We briefly describe ENISA's role and objectives in the implementation of the Framework directive (2002/21/EC as amended by 2009/140/EC) and Article 13a in particular.

ENISA is mentioned in the preambles of the Framework directive:

- Preamble 44 of the Framework directive 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 of the Framework directive 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 of the Framework directive asks ENISA to contribute to the “*harmonisation of security measures by providing expert advice*”.

ENISA is also 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's objectives

ENISA's first objective is to implement the incident reporting mandated in Article 13a, i.e. to agree with the Member States on an efficient implementation of pan-European incident reporting, including the processes of ad-hoc reporting about cross-border incidents as well as the annual summary reporting.

Secondly, ENISA aims to support NRAs with the task of ensuring that providers take appropriate security measures and the supervision activities in general, including collecting incident reports nationally, following up on incidents, analysing and mitigating common root causes, providing guidance to the providers, and so on.

In this way ENISA supports an efficient and harmonized implementation of Article 13a across the EU. Harmonized implementation of legislation is important to create a level playing field and makes it easier for providers and users to operate across different EU countries.

3 Article 13a and terminology

In this section we introduce the relevant parts of Article 13a and the related terms used in this document.

3.1 Paragraph 1 and 2 of Article 13a

For the sake 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. [...]"

3.2 Terminology

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

- Provider: The term "provider" is used to refer to an *"undertaking providing public communications networks or publicly available electronic communications services"*.
- NRA: The term "NRA" is used to refer to the competent authority on Article 13a i.e. the *"national regulatory authority"* as mentioned in Article 13a, which could be a ministry, or a government agency, depending on the national situation.
- Networks and communications services: The term "networks and communications services" is used to abbreviate the term *"public communications networks or publicly available electronic communications services"* as mentioned in Article 13a. This includes telecom operators, mobile network operators, internet service providers, et cetera.

3.2.1 Security and integrity

Paragraphs 1 and 2 of Article 13a contain two different requirements:

- Paragraph 1 requires NRAs 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 2 requires NRAs 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 (of networks¹) in the article text may be confusing to some readers. In technical literature about networks and network inter-connections², 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.

¹ And not integrity of data.

² Ward, K, 1995, 'The Impact of Network Interconnection on Network Integrity'. British Telecommunications Engineering, 13:296–303.

In this document we address both security (paragraph 1) and integrity (paragraph 2) by providing a single set of ‘security measures’, which include the *“technical and organisational measures”* in the first paragraph and the *steps* mentioned in the second paragraph of the article.

In this document, to be more in line with the majority of literature on network and information security, we use the terms “security” and “continuity” to cover these requirements, or simply “security” (because in most information security literature continuity is seen as an aspect of security).

3.2.2 Security incidents

Article 13a mentions ‘security incidents’, ‘security breaches’ 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”*

In this guideline we only use the term “security incidents” with the following definition:

Security incident: A breach of security or a loss of integrity that could have an impact on the operation of electronic telecommunications networks and services.

This is the same definition as the one used in the ‘Technical Guidelines on Incident Reporting’³.

³ Note that only a subset of these incidents have to be reported to ENISA and the EC, namely those incidents that actually had a significant impact on the operation of services.

4 Security measures

In this section we provide a list of 25 security objectives NRAs should take into account when assessing compliance of providers to Article 13a with paragraphs 1 and 2 of Article 13a.

We stress that this guideline is a guideline for NRAs and that it is at the discretion of NRAs as to whether they mandate or recommend different security objectives, or different security measures, only some of the security measures and/or additional security measures.

Note that some of the security objectives or security measures may not be relevant or appropriate in all settings for all types of providers, depending on the type of networks or services offered⁴.

4.1 Assets in scope and risk assessment

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 or continuity of electronic communications networks or services.

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](#)).

***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 13a, however, only mentions 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 13a without adaptation.*

4.1.1 Critical assets

We call assets (network and information systems, processes, data, et cetera) critical when if they fail there would be a severe impact on the security or continuity of networks and services. Critical assets should be protected with priority. In the remainder of this document, for the sake of clarity, we call these assets “critical assets”, or “critical systems”.

In some literature there is a distinction between primary assets and secondary (supporting) assets. In this context (Article 13a) the primary assets are the electronic communication networks and services provided by the provider. In this document when we speak about assets we usually mean the secondary assets i.e. the systems and processes supporting the provision of electronic communications networks and services (such as base stations, routers, registers, power supply, etc.).

4.1.2 Key personnel

In this document we use the term “key personnel” to refer to the key roles in the organization with respect to security and continuity. Now providers are not all the same and organizations and job profiles are different, but typically this would include roles like the CEO, the CIO, the CISO, the business continuity manager and system administrators of critical systems.

⁴ 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.

4.1.3 Third parties and outsourcing

In this document we use the term “third parties” to refer to parties (organizations, individuals) the provider works with to deliver the services, i.e. vendors the provider buys products from, suppliers, consultants who advise the provider, auditors auditing the provider, companies the provider outsources work to, and so on⁵.

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

4.2 Structure of the security measures

This document lists 25 security objectives⁶ which have been derived from a set of international and national standards that are commonly used by providers in the EU’s electronic communication sector (see [References](#)). For each of the security objectives we list more detailed security measures which could be implemented by providers to reach the security objective. Per security objective we also list detailed evidence which could indicate that the measure is in place. Note that the security measures or the evidence should not be seen as a baseline or list of minimum requirements for providers (see the remark below).

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

Description of sophistication levels
Sophistication level 1 (basic): <ul style="list-style-type: none"> • Basic security measures that could be implemented to reach the security objective. • Evidence that basic measures are in place.
Sophistication level 2 (industry standard): <ul style="list-style-type: none"> • 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 following changes or incidents.
Sophistication level 3 (state of the art): <ul style="list-style-type: none"> • 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. If

⁵ So in this document the term third parties does not refer to customers, the public, or government or regulatory authorities.

⁶ In information security governance literature these are also sometimes referred to as control objectives

the measures at level 1 are not (fully) implemented than this could be called level 0, but we do not explicitly mention level 0 in this document.

The overall structure of the security objectives and security measures is depicted in Figure 1.

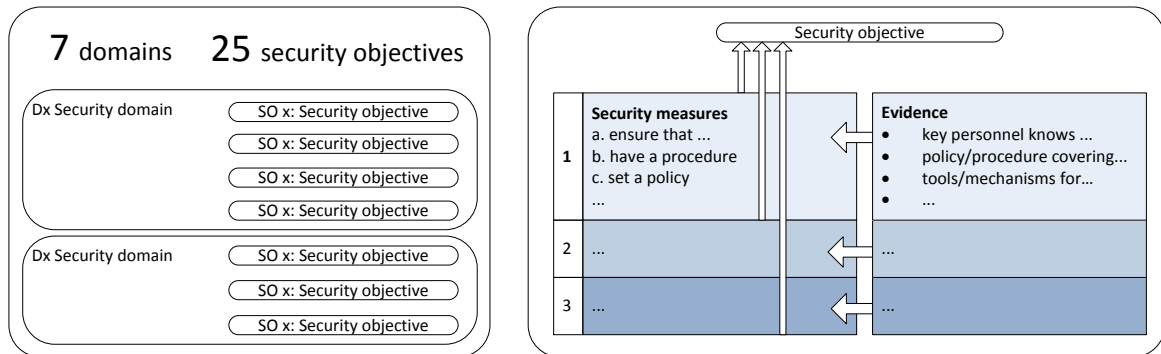


Figure 1 Structure of the security objectives and security measures.

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 NRAs, for example when evaluating the state of 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.

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.

4.3 Security objectives and security measures

Below we list 25 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 measures are in place (the structure is explained in [Section 4.2](#)).

D1: Governance and risk management

The domain “Governance and risk management” includes the security objectives related to governance and management of network and information security risks.

SO 1: Information security policy

Establish and maintain an appropriate information security policy.

	Security measures	Evidence
1	a) Set a high level security policy addressing the security and continuity of the communication networks and/or services provided. b) Make key personnel aware of the security policy.	<ul style="list-style-type: none"> Documented security policy, including networks and services in scope, critical assets supporting them, and the security objectives. Key personnel are aware of the security policy and its objectives (interview).
2	c) Set detailed information security policies for critical assets and business processes. d) Make all personnel aware of the security policy and what it implies for their work. e) Review the security policy following incidents.	<ul style="list-style-type: none"> Documented information security policies, approved by management, including applicable law and regulations, accessible to personnel. Personnel are aware of the information security policy 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.	<ul style="list-style-type: none"> 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.

SO 2: Governance and risk management

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

Security measures	Evidence
-------------------	----------

1	<p>a) Make a list of the main risks for security and continuity of the provided communication networks or services, taking into account main threats for the critical assets.</p> <p>b) Make key personnel aware of the main risks and how they are mitigated.</p>	<ul style="list-style-type: none"> List of main risks described at a high level, including the underlying threat(s) and their potential impact on the security and continuity of networks and services. Key personnel know the main risks (interview).
2	<p>c) Set up a risk management methodology and/or tools based on industry standards.</p> <p>d) Ensure that key personnel use the risk management methodology and tools.</p> <p>e) Review the risk assessments following changes or incidents.</p> <p>f) Ensure residual risks are accepted by management.</p>	<ul style="list-style-type: none"> 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. Management approval of residual risks.
3	<p>g) Review the risk management methodology and/or tools, periodically, taking into account changes and past incidents.</p>	<ul style="list-style-type: none"> Documentation of the review process and updates of the risk management methodology and/or tools.

SO 3: Security roles and responsibilities

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

	Security measures	Evidence
1	<p>a) Assign security roles and responsibilities to personnel.</p> <p>b) Make sure the security roles are reachable in case of security incidents.</p>	<ul style="list-style-type: none"> List of security roles (CISO, DPO, business continuity manager, etc), who occupies them and contact information.
2	<p>c) Personnel is formally appointed in security roles.</p> <p>d) Make personnel aware of the security roles in your organisation and when they should be contacted.</p>	<ul style="list-style-type: none"> List of appointments (CISO, DPO, 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	<p>e) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.</p>	<ul style="list-style-type: none"> 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: Security of third party assets

Establish and maintain a policy, with security requirements for contracts with third parties (see Section 4.1.3), to ensure that dependencies on third parties do not negatively affect security of networks and/or services.

	Security measures	Evidence
1	a) Include security requirements in contracts with third-parties.	<ul style="list-style-type: none"> 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.
2	b) Set a security policy for contracts with third-parties. c) Ensure that all procurement of services/products from third-parties follows the policy. d) Review security policy for third parties, following incidents or changes. e) Mitigate residual risks that are not addressed by the third party.	<ul style="list-style-type: none"> Documented security policy for contracts with third parties. List of contracts with third-parties. 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.	<ul style="list-style-type: none"> 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 security risks related to the personnel.

SO 5: 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 (system administrators, security officers, guards, et cetera).	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Policy and procedure for background checks/screenings. Guidance for personnel about when/how to perform background checks/screenings.

	background checks.	
3	d) Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents.	<ul style="list-style-type: none"> Review comments or change logs of the policy/procedures.

SO 6: Security knowledge and training

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

	Security measures	Evidence
1	a) Provide key personnel with relevant training and material on security issues.	<ul style="list-style-type: none"> Key personnel have followed security trainings and have sufficient security knowledge (interview).
2	b) Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge. c) Organise trainings and awareness sessions for personnel on security topics important for your organisation.	<ul style="list-style-type: none"> Personnel have participated in awareness sessions on security topics. Documented program for training on security skills, including, objectives for different roles and how to reach it (by e.g. training, awareness raising, etc).
3	d) Review and update the training program periodically, taking into account changes and past incidents. e) Test the security knowledge of personnel.	<ul style="list-style-type: none"> Updated security awareness and training program Results of tests of the security knowledge of personnel. Review comments or change logs for the program.

SO 7: 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.	<ul style="list-style-type: none"> 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	<p>c) Implement policy/procedures for personnel changes, taking into account timely revocation access rights, badges, equipment.</p> <p>d) Implement policy/procedures for education and training for personnel in new roles.</p>	<ul style="list-style-type: none"> • 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	<p>e) Periodically check that the policy/procedures are effective.</p> <p>f) Review and evaluate policy/procedures for personnel changes, taking into account changes or past incidents.</p>	<ul style="list-style-type: none"> • Evidence of checks of access rights etc. • Up to date policy/procedures for managing personnel changes. • Review comments or change logs.

SO 8: 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 security breaches caused by violations of policies, for example via the labour contract. .	<ul style="list-style-type: none"> • Rules for personnel, including responsibilities, code of conduct, violations of policies, et cetera, possibly as part of employment contracts.
2	b) Set up procedures for violations of policies by personnel.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Review comments or change logs

D3: Security of systems and facilities

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

SO 9: Physical and environmental security

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

	Security measures	Evidence
1	a) Prevent unauthorized physical access to facilities and infrastructure and set up environmental controls, to protect against unauthorized access, burglary, fire, flooding, et cetera..	<ul style="list-style-type: none"> Basic implementation of physical security measures and environmental controls, , such as door and cabinet locks, burglar alarm, fire alarms, fire extinguishers, et cetera.
2	b) Implement a policy for physical security measures and environmental controls. c) Industry standard implementation of physical and environmental controls. .	<ul style="list-style-type: none"> Documented policy for physical security measures and environmental controls, including description of facilities and systems in scope. Physical and environmental controls, like electronic control of entrance and audit trail, segmentation of spaces according to authorization levels, automated fire extinguishers with halocarbon gases, et cetera.
3	d) Evaluate the effectiveness of physical and environmental controls periodically. e) Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents.	<ul style="list-style-type: none"> Up to date policy for physical security measures and environmental controls Documentation about evaluation of environmental control , review comments or change logs.

SO 10: Security of supplies

Establish and maintain appropriate security of supplies (electricity, fuel, etc).

	Security measures	Evidence
1	a) Ensure security of supplies, such as electric power, fuel or cooling.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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	<p>d) Implement state of the art security measures to protect supplies. .</p> <p>e) Review and update policy and procedures to secure supplies regularly, taking into account changes and past incidents. .</p>	<ul style="list-style-type: none"> • Evidence of state of the art measures to protect security of supplies, such as active cooling, UP, 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: Access control to network and information systems

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

	Security measures	Evidence
1	<p>a) Users and systems have unique ID's and are authenticated before accessing services or systems.</p> <p>b) Implement (logical) access control mechanism for network and information systems to allow only authorized use.</p>	<ul style="list-style-type: none"> • 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.
2	<p>c) Implement policy for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights.</p> <p>d) Choose appropriate authentication mechanisms, depending on the type of access.</p> <p>e) Monitor access to network and information systems, have a process for approving exceptions and registering access violations.</p>	<ul style="list-style-type: none"> • 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 security officer.
3	<p>f) Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms.</p> <p>h) Access control policy and access control mechanisms are reviewed and when needed revised.</p>	<ul style="list-style-type: none"> • 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: Integrity of network and information systems

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

	Security measures	Evidence
1	a) Make sure software of network and information systems is not tampered with or altered, for instance by using input controls and firewalls. b) Make sure security critical data (like passwords, shared secrets, private keys, etc) are not disclosed or tampered with, c) Check for malware on (internal) network and information systems.	<ul style="list-style-type: none"> 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	d) Implement industry standard security measures, providing defense-in-depth against tampering and altering of systems.	<ul style="list-style-type: none"> 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	e) Set up state of the art controls to protect integrity of systems. f) Evaluate and review the effectiveness of measures to protect integrity of systems.	<ul style="list-style-type: none"> 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.

D4: Operations management

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

SO 13: 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Updated policy/procedures for critical systems, review comments and/or change logs.

SO 14: Change management

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

	Security measures	Evidence
1	a) Follow predefined procedures when making changes to critical systems.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> Up to date change management procedures, review comments and/or change logs.

SO 15: Asset management

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

	Security measures	Evidence
1	a) Manage critical assets and configurations of critical systems.	<ul style="list-style-type: none"> List of critical assets and critical systems.

2	b) Implement policy/procedures for asset management and configuration control.	<ul style="list-style-type: none"> • Documented policy/procedures for asset management, including roles and responsibilities, the assets and configurations that are subject to the policy, the objectives of asset management • An asset inventory or inventories, containing critical assets and the dependency between assets. • A configuration control inventory or inventories, containing configurations of critical systems.
3	c) Review and update the asset management policy regularly, based on changes and past incidents.	<ul style="list-style-type: none"> • 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 incidents⁷.

SO 16: Incident management procedures

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

	Security measures	Evidence
1	a) Make sure personnel is available and prepared to manage and handle incidents. b) Keep a record of all major incidents	<ul style="list-style-type: none"> • Personnel is aware of how to deal with incidents and when to escalate. • Inventory of major incidents and per incident, impact, cause, actions taken, lessons learnt.
2	c) Implement policy/procedures for managing incidents.	<ul style="list-style-type: none"> • Policy/procedures for incident management, including, types of incidents that could occur, objectives, roles and responsibilities, detailed description, per incident type, how to manage the incident, when to escalate to senior management (CISO e.g.), et cetera.
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	<ul style="list-style-type: none"> • Individual reports of the handling of major incidents. • Up to date incident management policy/procedures, review comments and/or change logs.

⁷ For the definition of ‘incident’ used in this document, see [Section 2](#).

	policy/procedures based on past incidents.	
--	--	--

SO 17: Incident detection capability

Establish and maintain an incident detection capability that detects incidents.

	Security measures	Evidence
1	a) Set up processes or systems for incident detection.	<ul style="list-style-type: none"> Past incidents were detected and timely forwarded to the appropriate people.
2	b) Implement industry standard systems and procedures for incident detection. c) Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	<ul style="list-style-type: none"> 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. .	<ul style="list-style-type: none"> Up to date documentation of incident detection systems and processes. Documentation of review of the incident detection process, review comments, and/or change logs.

SO 18: Incident reporting and communication

Establish and maintain appropriate incident reporting and communication procedures, taking into account national legislation on incident reporting to government authorities⁸.

	Security measures	Evidence
1	a) Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary.	<ul style="list-style-type: none"> Evidence of past communications and incident reporting.
2	b) Implement policy and procedures for communicating and reporting about incidents.	<ul style="list-style-type: none"> Documented policy and procedures for communicating and reporting about incidents, describing reasons/motivations

⁸ For example, Article 13a, which is now transposed by all EU member states to national legislation, requires electronic communications providers to report 'significant' incidents to the NRA. The thresholds for reporting are set nationally.

		<p>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.</p> <ul style="list-style-type: none"> • Templates for incident reporting and communication
3	<p>c) Evaluate past communications and reporting about incidents.</p> <p>d) Review and update the reporting and communication plans, based on changes or past incidents.</p>	<ul style="list-style-type: none"> • 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 19: Service continuity strategy and contingency plans

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

	Security measures	Evidence
1	a) Implement a service continuity strategy for the communications networks and/or services provided.	<ul style="list-style-type: none"> • Documented service continuity strategy, including recovery time objectives for key services and processes. •
2	<p>b) Implement contingency plans for critical systems. .</p> <p>c) Monitor activation and execution of contingency plans, registering successful and failed recovery times.</p>	<ul style="list-style-type: none"> • 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	<p>d) Review and revise service continuity strategy periodically.</p> <p>e) Review and revise contingency plans, based on past incidents and changes.</p>	<ul style="list-style-type: none"> • Up to date continuity strategy and contingency plans,,review comments, and/or change logs.

SO 20: Disaster recovery capabilities

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

	Security measures	Evidence
1	a) Prepare for recovery and restoration of services following disasters.	<ul style="list-style-type: none"> 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).	<ul style="list-style-type: none"> Documented policy/procedures for deploying disaster recovery capabilities, including list of natural and/or major disasters that could affect the services, and a list of disaster recovery capabilities (either those available internally or provided by third parties). Industry standard implementation of disaster capabilities, such as mobile equipment, mobile sites, failover sites, et cetera.
3	c) Set up state of the art disaster recovery capabilities to mitigate natural and/or major disasters. d) Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	<ul style="list-style-type: none"> 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 21: 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.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Documented policy for monitoring and logging, including minimum monitoring and logging requirements, retention period, and

	d) Set up tools to collect and store logs critical systems.	<p>the overall objectives of storing monitoring data and logs.</p> <ul style="list-style-type: none"> Tools for monitoring systems and collecting logs. List of monitoring data and log files, in line with the policy.
3	<p>e) Set up tools for automated collection and analysis of monitoring data and logs.</p> <p>f) Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.</p>	<ul style="list-style-type: none"> 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 22: 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.	<ul style="list-style-type: none"> Reports of past exercises of backup and contingency plans.
2	<p>b) Implement program for exercising backup and contingency plans regularly, using realistic scenarios covering a range of different scenarios over times.</p> <p>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.</p>	<ul style="list-style-type: none"> 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	<p>d) Review and update the exercises plans, taking into account changes and past incidents and contingencies which were not covered by the exercises program.</p> <p>e) Involve suppliers, and other 3rd parties, like business partners or customers in exercises.</p>	<ul style="list-style-type: none"> Updated exercises plans, review comments, and/or change logs. Input from suppliers and other 3rd parties involved about how to improve exercise scenarios.

SO 23: Network and information systems testing

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

	Security measures	Evidence
1	a) Test networks and information systems before using them or connecting them to existing systems.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates.
3	d) Review and update the policy/procedures for testing, taking into account changes and past incidents.	<ul style="list-style-type: none"> List of test reports. Updated policy/procedures for testing networks and information systems, review comments, and/or change log.

SO 24: Security assessments

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

	Security measures	Evidence
1	a) Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes. .	<ul style="list-style-type: none"> Reports from past security scans and security tests.
2	b) Implement policy/procedures for security assessments and security testing.	<ul style="list-style-type: none"> Documented policy/procedures for security assessments and security testing, including, which assets, in what circumstances, the type of security assessments and tests, frequency, approved parties (internal or external), confidentiality levels for assessment and test results and the objectives security assessments and tests .
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.	<ul style="list-style-type: none"> 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 25: 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.	<ul style="list-style-type: none"> • Reports describing the result of compliance monitoring.
2	b) Implement policy/procedures for compliance monitoring and auditing.	<ul style="list-style-type: none"> • 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..	<ul style="list-style-type: none"> • 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 and 2 of Article 13a requires NRAs to ensure that providers do appropriate risk management and that they take appropriate security measures. In this section we discuss the technical details of supervising the security measures⁹.

The most common regulatory activities of NRAs regarding supervision of security measures are¹⁰:

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

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

5.1 Mandating or recommending a security standard

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

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

Below we go into detail about the different options.

5.1.1 Mandating versus recommending a security standard

When discussing the supervision of security legislation by government authorities there is often a discussion about whether or not the government authority should mandate a specific list of security measures, strongly recommend them, or just recommend them as guidance. One could argue that mandating a standard would create clarity about what providers need to do to be compliant. On the other hand, one could also argue that in most settings the sector, the organizations involved, the technology used, is just too diverse to allow for a single checklist of minimum security measures for the entire sector. Often only very high-level security standards could be reasonably applied to a wider number of organizations. Inevitably such high-level standards leave a lot of important technical details unaddressed. So it is hard to capture all the security requirements of Article 13a *comprehensively* in one standard. At the same time for *specific* settings or specific issues the NRA could mandate *specific* security measures to be taken. For instance, an NRA could ask all providers to

⁹ 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.

¹⁰ We asked NRAs across the EU, via a survey, which are the activities they are deploying or planning to deploy.

provide the NRA with a contact point in case of contingencies, or ask all providers to have 4 hours of backup power for their base station controllers.

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

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

5.1.2 Using the ENISA guideline as a recommendation

NRAs could use this ENISA guideline to provide guidance to providers. The ENISA guideline consists of 25 high level security objectives derived from different standards (see [References](#)). To reach the security objectives, providers should choose appropriate technical security measures. This document lists detailed security measures which providers could take to reach the security objectives. The security measures are split in three (sophistication) levels ranging from 1) basic, to 2) industry standard, to 3) state of the art. Providers should assess the risks to their communications networks and services to understand which security measures are appropriate.

5.1.3 Using the ENISA guideline as a mapping

Many (especially larger) providers already have a security standard or a security governance framework in place, often based on international standards. This ENISA guideline could be used as a neutral mapping to different standards in use by the industry. Such a mapping would allow providers to continue use existing international standards, and it would avoid incurring unnecessary costs for providers when complying with the requirements of Article 13a.

In practice, for example, providers could show compliance to Article 13a by providing audit reports or certification against existing industry standards, combined with a mapping from these standards to this ENISA guideline. In [Section 6](#) we provide an example of such a mapping to two well-known existing international security standards: ISO27001 and ISO27002 for information security governance and BS 25999 for business continuity.

5.1.4 Using existing national or international standards or best practices

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

- NRAs should take into account that some (especially the large) providers may operate in several EU countries, and that it would be cumbersome for these providers to adopt different standards in different countries. In this respect it could be useful to allow providers to use international standards which are widely used across the EU and in this way reduce compliance costs for these providers.
- In most countries the electronic communications sector is large (hundreds of providers) and contains both large providers (>10% of market share) and very small ones (<1% of market

share)¹¹. NRAs should also take into account the differences between the providers in their country. What might work for large providers may well be overwhelming for smaller providers, and vice versa, what might work for one provider might be inappropriate for another provider.

- Finally, NRAs should take into account that best practices in network and information security are rapidly changing, because information technology changes rapidly and because the capability of attackers changes rapidly. This makes it hard to capture the high-level security requirement of Article 13a comprehensively in a list of detailed security measures. In this light, NRAs should focus first on supervising that providers assess risks and proactively take appropriate security measures, rather than on trying to cast detailed security measures in stone.

5.2 Assessing compliance across the market

Self-assessments could be used to get an overview of the kind of security measures taken by providers, across the sector. The security objectives and measures listed in Section 4 can be used directly in self-assessment forms. The sophistication levels (see Section 4) would allow providers to indicate, per security objective, what kind of security measures are in place. Used in this way the sophistication levels would yield a profile of a provider, allowing for a quick comparison between providers across the sector.

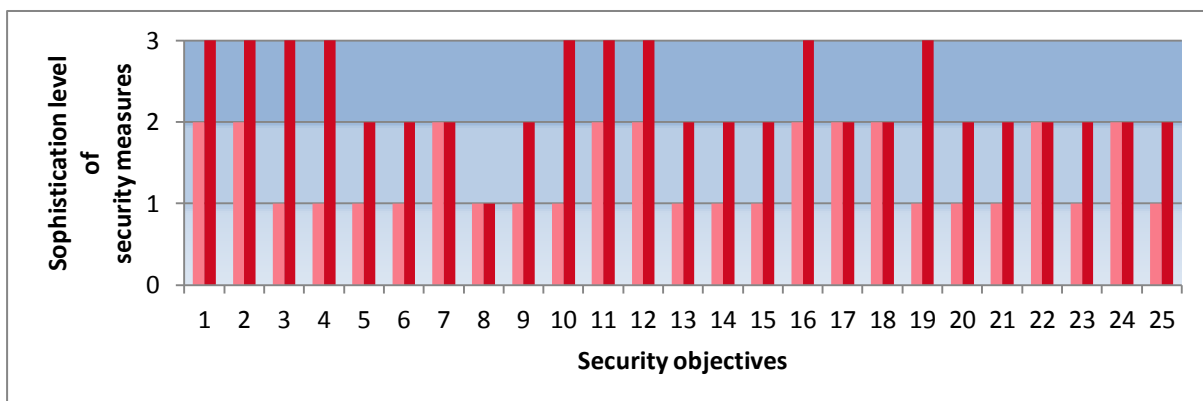


Figure 2: Two different profiles with different sophistication of measures for each security objective.

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 NRA could focus on a subset of security objectives. For example, an NRA could be interested in a domain like business continuity or specific security objectives around change management.

NRAs 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.).

¹¹ We asked NRAs across the EU, via a survey, about the type of providers in their sector, looking at market share.

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

Example: The NRA 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 NRA focusses on a subset of security measures and a subset of providers:

Example: The NRA 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 NRA 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 NRA which could substantiate that measures are in place: (0 none, 1 internal documentation, 2 audit report from external auditor)

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

5.3 Taking a staged approach

Depending on the national circumstances, NRAs might want to adopt a staged approach in supervising (and enforcing) compliance to the security requirements of 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), NRAs might want to give providers some time to comply, in stages. NRAs could use this guideline to adopt a staged approach. We discuss some possible options for staging:

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

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

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

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

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

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

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

Example: The NRA 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 NRA 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.).

5.4 Auditing providers

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

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

***Remark about audit costs:** NRAs 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. NRAs 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, NRAs 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.*

5.4.1 Assessment types

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

- **Document review:** Document review is essential in any audit. Relevant documents may include descriptions of policies, roles and responsibilities, descriptions of processes and procedures, systems architecture and design, test procedures and actual test results. [Chapter 4](#) of this guideline includes descriptions of evidence which could be considered when assessing the implementation of security measures.
- **Interviews:** In addition to document review, a lot of information may be collected by interviewing service provider employees. At small providers it may be enough to speak to one or two persons with commercial and technical responsibility. At large providers, typical roles to be interviewed are C-level managers (CIO), chief security officers (CSO or CISO), tactical/operational security officers, NOC managers, internal CERT team, product managers, and system administrators responsible for critical processes or systems.
- **System evaluation:** Besides documentation, certification, and interviews, the ultimate check to see if the networks and information systems are secure, and if policy/procedures are being applied in practice, is by inspecting or testing the systems itself. In some settings system review may be needed, for example to understand how a security incident could have happened. System evaluation should focus on critical systems because it can be time-consuming.

5.4.2 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 NRAs. An advantage of self-assessments is that self-assessments are relatively cheap for providers. Earlier in this document, in [Section 5.2](#), we discuss self-assessments in more detail.
- **Internal auditor:** In large organizations, a provider could ask an internal security role or internal audit department to do an audit of certain systems or parts of the organization. Compared to self-assessments, an internal auditor may be less biased. An advantage is that internal auditors often know the organization inside out. Also internal auditors could more easily leverage the deep knowledge about the network and information systems at the provider.
- **External auditor:** An audit report from an external auditor is even less biased. The only issue here may be that the external auditor may not know all the details about the organization and/or the network and information systems. This would make the entire audit more costly, because on the one hand the external auditor would need to dedicate a lot of time to study the setting and systems at the provider, and the provider would also need to dedicate a lot of time to providing the necessary information to the auditor.
- **NRA as auditor:** The NRA could carry out an audit of a provider, by using internal staff with auditing expertise, or by outsourcing the auditing to an auditing firm.
- **Certifying auditor:** In certification a licensed auditor checks compliance to a specific standard. The audit report results in a certificate of compliance issued by a certifying authority. For example it is quite common for large providers to be ISO270001 certified. Certification is often refreshed yearly, following a yearly re-audit. NRAs could require certification, and ask providers to submit their certificates as a way to show compliance. By requiring certification
- **Specialist auditor:** In special cases the NRA may want to designate a specific auditor, for a specific purpose or following a specific incident. For example, an NRA could mandate providers to undergo a security scan of systems by a security scanning specialist.
- **Pool of auditors:** The NRA could designate a pool of external auditors. Criteria for auditors could be based on past experience (a track record of audits, or security tests) or be based on examination criteria. For example, NRAs could start with a list of licensed auditors¹² and offer them a yearly training which focusses on Article 13a requirements for the sector, in this way creating a pool of auditors.

5.4.3 Audit timing and objectives

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

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

¹² In most countries, for example, there are organizations that license auditors to carry out IT audits.

Example: The NRA in country H mandates providers to undergo yearly (preventive) audits by 3rd party auditors. To simplify matters and to reduce the burden for providers, the 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 an NRA is usually done ad-hoc, depending on the type of incident and the setting. Post-incident audits have a specific focus – and usually they are aimed at assessing if security measures are in place to prevent the incident from re-occurring. The audit in this case has a specific scope (the services affected by the incident, the assets affected) and regards specific security measures (measures failing during the incident, or measures which could prevent re-occurrence).

6 Mapping to international standards

It is important to stress that the security measures described in this document have been derived from existing international network and information security standards. This guideline is not intended to replace existing international standards or other frameworks used by providers. In this section we provide a mapping from the security measures in this document to common international standards.

A number of providers use ISO27001/2 for information security management, ISO27005 for risk management and BS25999-1/2 for continuity management. As an example we map the security measures in this guideline to those two standards.

Security objectives	Addressed in	Details
D1: Governance and risk management	ISO 27001/2 Chapter 5 and ISO 27005	ISO27005 describes methods for setting the scope of information security risk management. ISO27002 Ch 5 covers information security policy, governance, risk management and controls for third parties (who deliver services, hardware or software), such as security requirements and procurement procedures for developed or acquired information systems.
D2: Human resources security	ISO 27001/2 Chapter 8	ISO27001/2 Ch 8 covers security clearances, security roles and responsibilities, security knowledge and training, and personnel changes.
D3: Security of systems and facilities	ISO 27001/2 Chapter 9	ISO27001 Ch 9 covers the physical security of facilities, IT equipment and environmental controls
D4: Operations management	ISO 27001/2 Chapter 10	ISO27001 Ch 10 covers operational procedures, operational roles, classification, access control and change controls.
D5: Incident management	ISO 27001/2 Chapter 13	ISO27002 Ch 13 covers incident management.
D6: Business continuity management	BS 25999-1/2	BS 25999 covers business continuity.
D7: Monitoring and security testing	ISO 27001/2 Chapters 10 and 15	Monitoring is covered in ISO27001/2 Ch 10; security testing and compliance monitoring and reporting are covered in ISO27001/2 Ch 15.

We have used ISO standards in this example, but a similar mapping could be made to other national or international standards. The mapping would look similar if we would take instead of ISO27001/2 and ISO27005, for example ITU X.1051 for information security management and ITU X. 1055 for risk management.

7 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>
- 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

- Article 13a of the Framework directive of the EU legislative framework on electronic communications:
http://ec.europa.eu/information_society/policy/ecomm/doc/140framework.pdf
- The electronic communications regulatory framework (incorporating the telecom reform):
http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.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>

Security standards and security best practices

- ISO/IEC 27001/ISO/IEC 27002 "Information security management"
- ISO/IEC 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