Technical Guideline on Security Measures

Technical guidance on the security measures in Article 13a

DRAFT, Version 1.93, April 2013

TLP GREEN (community wide)

About ENISA

The European Network and Information Security Agency (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 this version – in particular the practices and evidence in Sections 3 and 5.

For the completion of this guideline ENISA has worked closely with a working group of experts from national regulatory authorities and ministries from across Europe:

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.

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 working group now comprises experts from NRAs of most EU countries, and several EFTA and EU candidate countries. Meetings (telephonic or physical) are organized and chaired by technical experts from ENISA. The European Commission acts as an observer in these meetings.

The Article 13a Working Group reached consensus on 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 implementation of paragraphs 1 and 2 of Article 13a: how to ensure that providers take appropriate security measures. This document contains a list of 25 security measures divided in 7 domains (Governance and risk management, Human resources security, et cetera).Per security measure we provide guidance on how providers could implement the security measures (practices) and how auditors or supervisors could check the implementation (evidence). We also provide guidance for NRAs about some common regulatory activities, like assessing compliance across the sector, auditing, et cetera.

Table of Contents

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).

This document is drafted by a working group comprising experts from NRAs and representatives of the EC, supported by technical experts from ENISA (see Preface): the Article 13a Working Group.

1.1 Target audience

This document is addressed to national ministries and NRAs in European Member States, the authorities 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 information security field.

1.2 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.

1.3 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. What did not change is the 25 high-level security objectives (except for a minor change, see below) and the grouping of objectives in 7 domains.

List of changes:

- Environmental security in objective SO9 was moved to SO19 Disaster recovery. Environmental security in objective SO9 was moved to SO19 Disaster recovery.
- Removed quotes and snippets from examples of standards.
- Renamed security measures to security objectives
- Per security objective descriptions of security measures which could be implemented by providers to reach the security objectives and evidence auditors could take into account when assessing whether to assert the objective is reached.
- Guidance on different methods NRAs could use in their supervision of the security measures taken by providers to replace the short section on implementation in version 1.0.

1.4 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 Article 13a. In Section 6 we provide a mapping from the security measures in this guideline to some well-known international standards.

2 EU policy context and ENISA's role and objectives

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

2.1 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 business sectors.

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.

2.2 ENISA's role and objectives

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 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.

Secondly, ENISA aims to support NRAs with the task of ensuring that providers take appropriate security measures and in this way also support an efficient and harmonized implementation 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 Security Measures in Article 13a

In this section we introduce Article 13a and the terminology 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 Abbreviations

In the interest of brevity, we use the following abbreviations:

- The term "provider" is used to refer to an *"undertaking providing public communications networks or publicly available electronic communications services"*.
- 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.
- The term "networks and communication services" is used to refer to *"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.

3.3 Appropriate security measures

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

- Paragraph 1 requires Providers to *"take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services*", and to take measures "*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"*.

The use of the term integrity (of networks) in the article text may be confusing to some readers. We refer the reader to the definition in technical literature about networks and network inter-connections[1], which defines integrity *"as the ability of the system to retain its specified attributes in*

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

terms of performance and functionality". Integrity of networks would be called availability or continuity in most information security literature.

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.

3.4 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 for Incident Reporting'[2].

[2] *Note that only a subset of these incidents have to be reported to ENISA and the EC, that is, those incidents that have had a significant impact on the continuity of services.*

4 Security objectives and measures

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

We stress that this guideline is intended as guidance for NRAs. It is at the discretion of NRAs as to whether they mandate or recommend different security measures (for example, based on a national or international standard), only some of the security measures, or additional security measures. Note also that some security measures may not be fully applicable in all settings, depending on the type of network, service, or provider involved[3].

4.1 Scope and risk assessment

The scope of the security measures is defined as follows.

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. This guideline does *not* address risk assessment in detail. There are several standard methodologies providers could use for this (see References).

A risk assessment should be conducted to understand the risks, and this assessment should be used as the basis for choosing an appropriate implementation of security measures. Risk assessments need updating, to address changes and past incidents, because risks change over time.

4.2 Structure and terminology

The security objectives and measures have been derived from a set of international and national standards that are commonly used by providers (see References). We used an intermediate mapping which maps the security requirements in the most common standards to a single list of common security objectives and measures.

4.2.1 Security objectives

In the next section we list 25 security objectives[4] for providers. These security objectives should be taken into account when evaluating the compliance of providers with paragraphs 1 and 2 of Article 13a.

4.2.2 Security measures

Per security objective, we list security measures that could be taken by the provider, to reach the security objective.

4.2.3 Evidence

Per security objective, we also provide guidance about what type of evidence could be taken into consideration by an (internal or external) auditor to be assured that the objective is reached.

---

[3] *For example, in the case of black fibre providers certain security measures may not be applicable.*

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

4.2.4 Sophistication levels

Per security objective we describe security measures and evidence, in 3 different levels of sophistication, as follows.

Description of sophistication levels
Sophistication level 1 (basic): • Basic security measures that could be implemented to reach the security objective. • Evidence that basic measures are in place and/or evidence that the security objective is reached to some extent.
Sophistication level 2 (industry standard): • **I**ndustry standard security measures to reach the objective and a 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): • 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.

It is important to note that at level 2 we do not repeat the security measures and the evidence for level 1, but they are understood to be included (accumulated). And similarly for level 3.

The levels of sophistication can be used to derive profiles of providers, showing the sophistication of security measures across the board. Such profiles can 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 in that section.

4.3 Security objectives

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 to be assured that the objective is being reached.

D1: Governance and risk management

D1 includes the security measures related to (network and information security) governance and risk management.

SO 1: Information security policy

The provider should establish and maintain an appropriate information security policy.

	Security measures	Evidence
1	a) Set a high level security policy addressing the key business processes of the organisation. b) Make key personnel aware of the security policy.	• Policy document exists, and describes primary assets in scope and security objectives. • Key personnel aware of the policy and its objectives (interview).
2	c) Set detailed security policies for key assets and business processes. d) Make all personnel aware of the existence and what it implies for their work. e) Review the policy following incidents.	• Documented policies, approved by management, including applicable law and regulations, accessible to personnel. • Personnel are aware of the security risks affecting their job and how the policy applies to their job (interview).
3	f) Review the information security policies periodically, and take into account past incidents, past tests/exercises, and incidents affecting other (similar) providers.	• Security policies are up to date and approved by senior management. • Logs of policy exceptions, approved by the relevant security roles. • Documentation of review process, taking into account changes and past incidents.

SO 2: Governance and risk management framework

The provider should establish and maintain an appropriate governance and risk management framework, to identify and address risks for the communications networks and services.

	Security measures	Evidence
1	a) Do a high level assessment of the main risks for security and integrity (continuity) of networks or services b) Make key personnel are aware of the main	• Main risks are listed, and described in high level, including impact, probability, and mitigation.

	risks and how they are mitigated.	
2	c) Set up an industry standard risk management methodology and tools d) Ensure that security roles use the risk management methodology and tools. e) Review the risk assessments following changes or incidents f) Ensure residual risks are accepted by management.	• Documented risk management methodology and/or tooling. • Guidance for personnel on assessing risks, impact, probability, and mitigation. • Guidance for mitigation and treatment of residual risks • Risk register exists and there is evidence of reviews. • Management approval of residual risks
3	g) Review the implementation of the risk management methodology periodically, taking into account changes and past incidents.	• Results of recent risk assessments • Documentation of the review process for the RM methodology. • Documentation of review process, taking into account changes and past incidents.

203

204 **SO 3: Security roles and responsibilities**

205 The provider should establish and maintain an appropriate structure of security roles and
206 responsibilities.

	Security measures	**Evidence**
1	a) Assign security roles and responsibilities b) Make sure key security roles are reachable and contacted in case of security incidents.	• List of persons dealing with security, their role, and contact information. • Personnel knows how to contact security roles
2	c) Personnel are formally appointed in security roles and are aware of their tasks and responsibilities.	• List of responsibilities and tasks for key security roles (CIO, CISO, DPO, etc). • Personnel are aware of the key security roles, their responsibilities, and when they should be contacted.
3	d) Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	• Updated structure of security roles and responsibilities • Documentation of review process, taking into account changes and past incidents.

207

SO 4: Managing third party networks or services

The provider should establish and maintain a policy, with security requirements, for procuring and managing third-party networks or services, such as IT services, software, call centres, interconnections, shared facilities, etc. in such a way that consultancy, outsourcing, or other third party service, do not affect the security of the provider (negatively).

	Security measures	Evidence
1	a) Include security requirements in procurement of third-party services, systems and networks.	• Contracts with key third party vendors and service providers contain security requirements .
2	b) Set security policy and procedures for procurement of third-party services c) Ensure that all procurement of third-party services follows the security policy	• Documented security policy for procurement • List of contracts with third-party service providers • All contracts with third party vendors and service providers contain security requirements, in accordance with the security policy for procurement
3	d) Keep track of security incidents at third-party service providers. e) Review and update the security policy for procurement at regular intervals, based on changes and past incidents.	• List of security incidents related to third-party service providers • Documentation of review process, taking into account changes and past incidents.

D2: Human resources security

D2 covers the security measures regarding the security of personnel, such as employees, contractors and third-party users.

SO 5: Background checks

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

	Security measures	Evidence
1	a) Perform background checks for key personnel (system administrators, security officers, guards, et cetera).	• Documentation of performed background checks for key personnel.
2	b) Set a policy for background checks. c) Check references of personnel in important roles.	• Procedure for background checks • Guidance for personnel about when/how to perform background checks

		• Documentation of reference checks for important roles.
3	d) Review and update the policy for background checks and reference checks at regular intervals, based on changes and past incidents.	• Review comments or change logs.

219

220 **SO 6: Security knowledge and training**

221 The provider should ensure that personnel have sufficient security knowledge and are provided with
222 regular security training.

	Security measures	**Evidence**
1	a) Provide personnel in important roles with relevant training and material on security issues.	• Personnel in important roles have followed security trainings and have sufficient security knowledge.
2	b) Implement a program for training, making sure that all personnel have sufficient security skills for their daily jobs. c) Organise trainings and awareness raising sessions on security topics specific to your organisation.	• Documented program for training of personnel on security skills, including – Objectives, for different roles – Approach to reach the goal, by e.g. training, awareness actions etc. • List of roles in the organisation, indicating the type of security training each role should take • List of employees that have taken a security training
3	d) Review and update the training program periodically, taking into account changes and past incidents. e) Evaluate the security knowledge of personnel by carrying out inspections, tests and exercises.	• Updated, approved and actual security awareness and training program • Results of inspections, test, exercises, or security awareness checks. Review comments or change logs.

223 **SO 7: Personnel changes**

224 The provider should establish and maintain an appropriate process for managing changes in personnel
225 (employees, contractors, third-party users) or changes in their roles and responsibilities. New
226 personnel should be briefed and educated on the policies and procedures in place. Accounts, rights,
227 possession of equipment or data should be reviewed upon personnel changes.

	Security measures	Evidence
1	a) Following changes in personnel revoke access rights, badges, equipment, et cetera, if no longer necessary or permitted.	• Evidence that personnel changes have been followed up with revocation of access rights, badges, equipment, et cetera
2	b) Implement policy/procedures for personnel changes, taking into account timely revocation access rights, badges, equipment. c) Implement policy/procedures for education and training for personnel in new roles.	• Documentation of process for personnel changes, including, responsibilities for managing changes, description of rights of access and possession of assets per role, procedures for briefing and training personnel in new roles. • Evidence that personnel changes have been carried according to the process and that access rights have been updated timely.
3	d) Periodically review and evaluate the process for personnel changes, based on changes or past incidents.	• Up to date policy/procedures for managing personnel changes. • Review comments or change logs.

228

229 **SO 8: Handling violations**

230 The provider should establish and maintain a disciplinary process for employees who have committed
231 a security breach, or have a broader process that covers security breaches.

	Security measures	Evidence
1	a) Establish procedures for holding personnel accountable for security breaches caused by violations of policies, and consider disciplinary measures where needed.	• Rules for personnel, including responsibilities, code of conduct, violations of policies, et cetera.
2	b) Implement policy/procedures for violations of policies by personnel.	• Documentation of policy/procedure, including types of security breaches 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.	• Up to date policy/procedures for violations. • Documentation of review of the process.

D3: Security of systems and facilities

This domain covers the security of network and information systems and facilities.

SO 9: Physical security of facilities

The provider should establish and maintain the appropriate physical security of facilities and network and service infrastructure.

	Security measures	Evidence
1	a) Prevent unauthorized physical access to facilities and infrastructure and set up environmental controls.	• Basic implementation of physical security measures and environmental controls, , such as door and cabinet locks, burglar alarm, et cetera.
2	b) Implement a policy for physical security measures and environmental controls. c) Industry standard implementation of physical and environmental controls, such as electronic control of entrance and audit trail, segmentation of the building spaces according to authorization levels, et cetera.	• Documented policy for physical security measures and environmental controls, including the minimum physical security measures required for facilities and infrastructure. • Overview of infrastructure and facilities that are subject to the policy
3	d) Evaluate the effectiveness of physical and environmental controls e) Review and update the policy for physical security measures and environmental controls regularly taking into account changes and past incidents.	• Up to date policy for physical security measures and environmental controls • Documentation about evaluation and updates, meeting minutes of review sessions • Review comments or change logs.

SO 10: Security of supplies

The provider should establish and maintain appropriate security of supplies and supporting facilities, such as electric power, fuel or cooling.

	Security measures	Evidence
1	a) Ensure security of supplies, such as electric power, fuel or cooling.	• Security of supplies is protected in a basic way, for example, backup power and/or backup fuel is available.
2	b) Implement a policy or procedures to protect important supplies and supporting facilities, such as power and cooling. c) Implement industry standard security measures to protect supplies and supporting facilities.	• Documented policy or procedure to protect important supplies such as power and cooling, containing minimum security measures that must be applied for each type of supply and supporting facility, lists of supplies and supporting facilities covered

		by the policy • 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.
3	d) Implement state of the art security measures to protect supplies, such as for example, active cooling, UPS with battery and power generators (hot standby), sufficient fuel to allow fuel delivery to start up (e.g. 24 hours), SLAs with fuel delivery companies, redundant cooling and power backup systems. e) Review and update policy and procedures to secure supplies regularly, taking into account changes and past incidents. .	• Evidence of state of the art measures to protect security of supplies. • Updated, policy for securing supplies and supporting facilities • Review comments or change logs.

241

242 **SO 11: Control of access to network and information systems**

243 The provider should establish and maintain appropriate (logical) access controls for access to network
244 and information systems.

	Security measures	**Evidence**
1	a) Users and systems have unique ID's and are authenticated accordingly. b) Implement access control to network and information systems, granting access to users and systems only when needed, for instance using roles.	• Access logs show unique identifiers for users and systems when granted or denied access. • Overview of authentication and access control methods for network and information systems and user group.
2	c) Implement policy and procedures for protecting access to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. c) Choose appropriate authentication mechanisms, depending on the type of access. d) Monitor access to network and information systems, have a process for approving exceptions and register access violations.	• Access control policy document including roles, user groups and access rights, procedures for granting and revoking access. • Log of access control policy exceptions, approved by the security officer. • Log of access violations, checked by the security officer.
3	e) Evaluate the effectiveness of access control policies and procedures. f) Implement cross checks on access control	• Reports of tests of access control mechanisms. • Review comments or change logs.

	mechanisms, such as anomaly detection. g) Access control policy and access control mechanisms are reviewed and when needed revised.	

SO 12: Information security of network and information systems

The provider should establish and maintain appropriate information security of network and information systems, to provide protection against malware, viruses and other common threats.

	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, for instance by using encryption. c) Check for malware on (internal) network and information systems.	• Software and data in network and information systems is protected using input controls, firewalls, encryption and signing. • Malware detection systems are present, and up to date, to detect malware on network and information systems.
2	d) Implement industry standard security measures, providing defense-in-depth against tampering and altering of network and information systems, such as anomaly detection systems and intrusion detection systems to monitor abnormal activities.	• Documentation about how the protection of software and data in network and information system is implemented. • Logs of anomaly detection systems, intrusion detection systems, et cetera. • Evidence of additional measures protecting from tampering and altering network and information systems.
3	e) Set up state of the art controls to prevent tampering and altering of network and information systems (code signing, tripwire, et cetera). f) Evaluate and review the effectiveness of policies and measures to protect network and information systems from tampering or altering.	• Reports recording results of regular review of access control and authorization processes • Up to date access control policy and authorization process • Review comments or change logs.

D4: Operations management

This domain covers the security of operation and management of network and information systems.

SO 13: Operational procedures and responsibilities

The provider should establish and maintain operational procedures and responsibilities.

	Security measures	Evidence
1	a) Set up operational procedures and assign responsibilities for the operation and management of network and information systems.	• Documentation of operational procedures and responsibilities for key network and information systems.
2	b) Implement a policy/procedures for operation and management of network and information systems, to make sure these systems are operated and managed correctly.	• Documented policy/procedures for operation and management of network and information systems, including an overview of network and information systems subject to the policy,
3	c) Review and update the policy/procedures for operation and management of systems is procedures and responsibilities is regularly reviewed and revised, based on the review, new insights, changing regulations and effectiveness of the policy.	• Up to date operational procedures for network and information systems. • Review comments or change logs.

SO 14: Change management procedures

The provider should establish change management procedures in order to minimise the likelihood of disruptions and errors resulting from changes.

	Security measures	Evidence
1	a) Follow predefined procedures when making changes to important network or information systems.	• Reports about important changes, showing procedures followed and detailed steps. • Documentation of change management procedures for important network and information systems.
2	b) Implement policy/procedures for change management, to make sure that changes are always carried out in a controlled way. c) Document change management procedures, and record for each changes the steps of the followed procedure.	• Documentation of change management policy/procedures including, operational systems and application software subject to the policy, and objectives and high level approach of change management, roll back procedures.

3	d) Review and update change management procedures regularly, taking into account changes and past incidents.	• For each change, a report is available describing the result of the change • Up to date change management policy/procedures • Review comments or change logs.

256

257 **SO 15: Asset management**

258 The provider should adopt configuration controls and asset management procedures in order to verify
259 asset availability and status.

	Security measures	**Evidence**
1	a) Manage assets and system configurations.	• List of important assets and system configurations.
2	b) Implement policy/procedures for asset management and configuration control.	• Documented policy for asset management, including, the assets and configurations that are subject to the policy, the objectives asset management • Documented asset management process, including, roles and responsibilities, types of assets and system configurations that must be recorded.
3	c) Review and update the asset management policy regularly, based on changes and past incidents.	• An asset inventory or inventories, containing all assets, their classification and the dependency between assets • A configuration control inventory or inventories, containing all configuration controls • Up to date asset management policy/procedures • Review comments or change logs.

260 ## D5: Incident management

261 This domain covers detection of, response to, and communication about incidents[5].

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

262 **SO 16: Standards and procedures for incidents**

263 The provider should establish and maintain standards and procedures for managing incidents.

	Security measures	Evidence
1	a) Handle incidents with care and escalate to the appropriate management when needed (CISO e.g.) b) Keep a record of all incidents	• Personnel is aware of how to deal with incidents and when to escalate. • Documented list of incidents and their status.
2	b) Implement policy/procedures for managing incidents, including when incidents should be escalated.	• Policy/procedures for incident management, including, types of incidents that could occur, objectives and high level approach of incident management, roles and responsibilities, detailed description, per incident type, how to manage the incident, et cetera.
3	c) Investigate major incidents in detail and draft final incident reports, including actions taken and recommendations to address the type of incident that occurred. d) Evaluate incident procedures based on past incidents. e) Regularly review and update the incident management policy taking into account changes and past incidents.	• Individual reports of the handling of major incidents • Up to date incident management policy/procedures • Review comments or change logs.

264 **SO 17: Incident detection capability**

265 The provider should establish and maintain an incident detection capability that detects incidents, and
266 forwards them timely to the appropriate people.

	Security measures	Evidence
1	a) Set up processes or systems for incident detection.	• Past incidents were detected and timely forwarded to the appropriate people.
2	b) Implement systems and procedures for incident detection. c) Implement systems and procedures for registering and forwarding incidents timely to the appropriate people.	• Incident detection systems and procedures, such as Security Incident and Event Management (SIEM) tools, (network and application related incidents), security helpdesk for personnel, reports and advisories from Computer Emergency Response Teams (CERTs), malware analysts, security agencies, et cetera.

3	d) Review systems and processes for incident detection regularly and update them taking into account changes and past incidents. .	• Up to date documentation of incident detection systems and processes. • Reports recording results of regular review of the incident detection process • Review comments, or change logs.

267

268 **SO 18: Incident reporting and communication plans**

269 The provider should establish, maintain and follow appropriate incident reporting and communication
270 plans. These plans should include reporting incidents to government authorities, if necessary (see for
271 instance the Article 13a Technical Guideline on Incident Reporting).

	Security measures	**Evidence**
1	a) Communicate and report about on-going or past incidents to third parties, and/or regulatory authorities, if necessary.	• Evidence of communications and reporting to third parties about on-going or past incidents.
2	b) Implement policy and procedures for communicating and reporting about incidents.	• Documented policy for incident reporting and communication, including type of incidents that should be communicated or reported about, the content of communications and/or reports about incidents, objectives of incident reporting and communication • Documented incident reporting and communication process, including, roles and responsibilities, detailed description, per incident type, what to report and what to communicate, including the roles that carry out the reporting and communication • Inventory of past incident reports and communications about incidents
3	c) Evaluate past communications and reporting about incidents. d) Review and update the reporting and communication plans, based on changes or past incidents.	• List of incident reports and communications about incidents • Templates for incident reporting and communication • Up to date incident response and communication policy • Review comments, or change logs.

272

D6: Business continuity management

This domain covers the security measures for protecting communications services from the effects of major failures of information systems or disasters and to ensure their timely resumption.

SO 19: Service continuity strategy and contingency plan

The provider should establish and maintain a strategy for ensuring continuity of networks and communication services and it should establish and maintain a contingency plan.

	Security measures	Evidence
1	a) Implement a service continuity strategy containing high-level objectives in terms of services or business processes.	• Documented business continuity strategy, including recovery time objectives for key services and processes. • Contingency plans for key services and processes, including clear steps and procedures for common threats.
2	b) Implement contingency plans for key services and business processes explaining triggers for activation, steps and recovery time objectives. c) Monitor activation and execution of contingency plans, plan and execute exercises, register successful and failed recovery times.	• Decision process for activating contingency plans. • Logs of activation and execution of contingency plans, including decisions taken, steps followed, final recovery time. • Reports about exercises and drills showing the execution of contingency plans
3	d) Review and revise business continuity strategy periodically. Review and revise continuity plans, based on past incidents and findings.	• Up to date documentation of service continuity strategy and contingency plans. • Meeting minutes, review comments, or change logs.

SO 20: Disaster recovery capability

The provider should establish and maintain an appropriate disaster recovery capability for restoring network and communication services after disasters. The provider should establish and maintain appropriate environmental controls to protect against fire, flood, earthquakes and other forms of disasters that may affect the facilities.

	Security measures	Evidence
1	a) Prepare for recovery and restoration of important services following natural disasters.	• Measures are in place for dealing with natural 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 capability for network and communication services, such as mobile equipment, mobile sites, failover sites, et cetera.	• Documented policy/procedures for deploying disaster recovery capabilties, including list of natural disasters that could affect network and communication services, list of assets and services which should be equipped with disaster recovery capabilities, and an overview of disaster recovery capabilities.
3	c) Set up state of the art disaster recovery capabilities, including full redundancy and failover mechanisms to handle natural disasters. d) Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	• Updated documentation of disaster recovery capabilities in place. • Meeting minutes, review comments, or change logs.

D7: Monitoring, auditing and testing

This domain covers monitoring, testing and auditing of network and information systems, facilities, and security measures.

SO 21: Monitoring and logging policies

The provider should establish and maintain monitoring and logging policies.

	Security measures	**Evidence**
1	a) Implement monitoring and logging in important network and information systems.	• Logs and monitoring reports for important network and information systems.
2	b) Implement policy and processes for logging and monitoring of network and information systems. c) Set up tools to collect and store logs of network and information systems. d) Set up tools for monitoring network and information systems.	• Documented policy and processes for monitoring and logging, including minimum monitoring and logging requirements, how long monitoring reports and logs should be retained, the objectives and high level approach of monitoring and logging • Monitoring reports and log files, in line with the policy
3	e) Review and update logging and monitoring processes, taking into account changes and past incidents.	• Central registry of all monitoring reports and log files • Tooling to facilitate structural recording of monitoring and logging and enforce the

		policy • Updated documentation of monitoring and logging policy and procedures. • Meeting minutes, review comments, or change logs. .

SO 22: Exercise contingency plans

The provider should establish and maintain policies for testing and exercising backup and contingency plans in collaboration with relevant third parties, such as network operators, where appropriate.

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

SO 23: Network and information systems testing

The provider should 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.	• Test reports of the network and information systems, including tests after big changes or the introduction of new systems.
2	b) Implement policy/procedures for testing network and information systems, c) Implement tools for automated testing	• Policy/procedures for testing 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.	• Inventory of test reports • Updated policy/procedures for testing networks and information systems • Review comments, change log.

298 **SO 24: Security scanning and testing**

299 The provider should establish and maintain an appropriate policy for performing security assessments
300 and security testing of all assets.

	Security measures	**Evidence**
1	a) Ensure security scans and security testing is regularly carried out, when introducing new systems and following changes	• Reports from past security scans and security tests.
2	b) Implement policy/procedures for frequent security assessments and security testing.	• Documented policy/procedures for security assessments and security testing, including, which assets, in what circumstances, the type of security assessments and tests available, frequency, requirements and modalities, approved parties (in or external), confidentiality levels for assessment and test results, the objectives and high level approach for 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.	• Inventory of all reports about security assessment and security tests • Documented procedures for security assessments and security, such as test cases. • Templates for reporting about security assessments and security tests. • Tools to carry out automatic security assessments 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, change log.

301

302 **SO 25: Compliance monitoring and audit policy**

303 The provider should establish and maintain a policy for compliance monitoring and auditing and have a
304 process for reporting compliance and addressing audit deficiencies.

	Security measures	Evidence
1	a) Monitor compliance and audit frequently	• Reports describing the result of compliance monitoring and auditing.
2	b) Implement policy/procedures for compliance monitoring and auditing.	• Documented policy/procedures for compliance monitoring 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..	• Central registry of all compliance monitoring and auditing reports • Updated policy/procedures for compliance and auditing. • Review comments, change log.

305

5 Technical supervision

In different countries NRAs take different approaches to ensure that appropriate security measures are taken. In some countries the NRA requires providers to be certified by licensed auditors, while in other countries the NRA only intervenes after large incidents. The most common[6] regulatory activities, with respect to supervising the security measures, are:

- Mandating or recommending a standard
- Assessing compliance across the market
- Taking a staged approach to enforcing compliance
- Auditing providers (periodic, ad-hoc, or post-incident)

Below we provide technical guidance to NRAs about how to implement these activities

5.1 Mandating or recommending a security standard

NRAs could mandate or recommend a standard of security measures for various reasons, for instance:

- 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. 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.

In this section we provide guidance about mandating or recommending a security standard.

5.1.1 Referring to the ENISA guideline directly

NRAs could refer providers to the ENISA guideline directly. The ENISA guideline is based on a number of high level security objectives. To reach the security objectives, providers should choose appropriate technical security measures to reach these objectives. The guideline also provides a list of detailed security measures, as guidance about how providers could reach the security objectives.

The guidance on security measures is 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 understand which security measures would be appropriate. Risks depend on the type of assets involved, or the type of provider, or the type of networks or communication services involved.

5.1.2 Using the ENISA guideline as a mapping:

Many (especially larger) providers already have a security standard or a security governance framework in place, sometimes based on an international standard. It is important to allow these

[6] *The most common activities were determined using a survey across the different NRAs in the EU.*

providers to show compliance to Article 13a (i.e. that appropriate security measures have been taken) without incurring unnecessary costs for providers. One solution would be to allow providers to show compliance by providing an audit report combined with a mapping from the audited security standard to the ENISA standard. In Section 6 we provide a mapping from this document to some well-known existing international standards.

5.1.3 Recommending national or international standards

NRAs could also mandate or recommend existing national or international standards or requirements. An overview of standards widely used in the industry is included in the section References. Note that the security measures in this guideline are a combination of security measures from different standards. This can be seen for example by looking at the mapping in Section 6.

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 internally, allowing these providers to show compliance by mapping their standards to standards mandated or recommended by the NRA.

NRAs should also take into account the differences between the different providers in a country. What might work for large providers may well be cumbersome for smaller providers, and vice versa. 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).

5.2 Organising self-assessments

NRAs could organise self-assessments to get an overview of the kind of security measures taken by providers, across the board. This guideline can be used as a framework for such self-assessments.

NRAs could 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.).

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.

The sophistication levels can be used by providers to indicate, per security objective, what kind of security measures are in place. The sophistication levels could be used to make a profile per provider, which would allow for a quick comparison between providers.

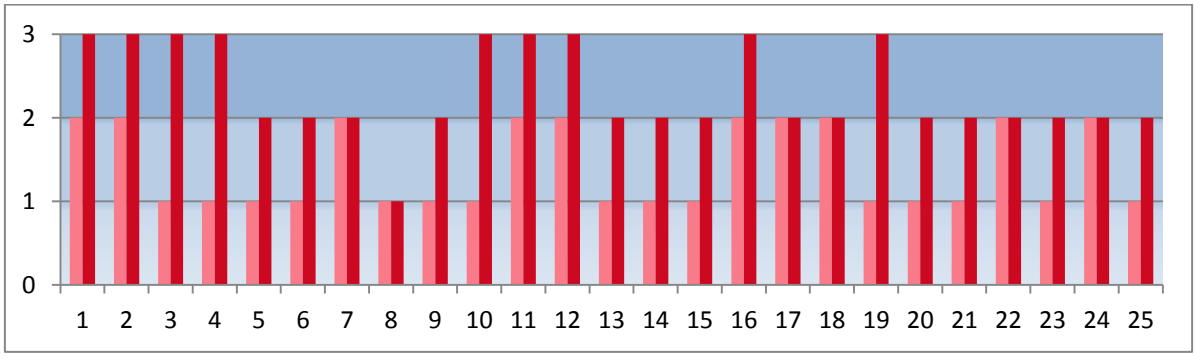

Figure 1: Two different profiles with varying sophistication for different security measures.

In figure 2 we show the profiles of two different providers. The vertical axis spans the sophistication levels and the horizontal axis spans the 25 security objectives. Dark red indicates a provider with more sophisticated security measures. The light red indicates a provider with less sophisticated security measures.

5.2.1 Examples

Below we provide two simplified examples of how an NRA could use the levels of sophistication in self-assessment forms.

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 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 measures SO9, SO10, SO19, SO20, SO22:

Indicate the level of sophistication: (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 that could substantiate your claim: (0 none, 1 internal documentation, 2 audit report from external auditor)

5.3 Staged approach

Depending on the national circumstances there may well be providers that do not have appropriate security measures, or who cannot provide evidence of such measures being in place. To allow providers the time to properly implement important security measures, NRAs could use this guideline to adopt a staged approach. Such stages could be defined in different ways. We show some options:

- **Services or assets in scope:** NRAs 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:** NRAs 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:** NRAs 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. Once these measures are implemented in a satisfactory way, the NRA will address other security measures.

- **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 is composed (mostly) of basic implementation levels – it is the baseline for small providers (<10% market share. The other is composed of (mostly) industry standard) implementation levels – it is the baseline for large providers (>10% of market share). In this way the NRA takes into account the fact that for small providers with few users and few employees basic implementation of security processes could be sufficient.

5.4 Auditing

Auditing providers and auditing network and information systems is not easy because systems are often complex and specific (sub) systems may require deep knowledge and expertise. Depending on the scenario and the goal of auditing different types of audits may be needed. In this section we go over some key aspects of auditing.

5.4.1 Delegating audits

NRAs do not always have the required resources to carry out certain audits. This section addresses the delegation of auditing, to specialised auditors or other experts.

- **Self-assessment:** In self-assessments there is really no auditor. The audit is basically delegated to the personnel of the provider and it is up to them to assess and report about compliance. Although self-assessment reports may be biased, they can provide useful information for NRAs and they are relatively cheap for providers. In Section 5.2 we discuss how NRAs could set up self-assessments.
- **Internal audit:** Compared to self-assessments, an audit report from an internal security role or internal audit department may be less biased, because internal auditors are trained to be unbiased. An advantage is that internal auditors often know the organization inside out.
- **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.
- **Auditing by the NRA:** In some cases the NRA carries out an audit of a provider. The NRA could hire experts with auditing experience, or outsource the auditing to a specialized auditing firm.
- **Certification:** Certifications are basically audits, against a specific standard, carried out by licensed auditors from an auditing firm. A special certification body (accredited to issue certifications) then assesses the audit report and, based on this, issues a certificate of compliance. For example it is quite common for large providers to be ISO270001 certified. Certification is often refreshed yearly, following a yearly re-audit.
- **Designated auditor**: In special cases the NRA may want to designate a specific auditor, for a specific purpose. For example, an NRA could mandate providers to undergo tests by a certain security specialist.
- **Pool of auditors:** The NRA might want to designate a pool of auditors. Criteria for auditors could be based on past experience (a track record of audits, or security tests), be based on examination criteria, or alternatively the pool could be just a list of licensed auditors[7].

5.4.2 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-

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

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.

Post-incident audits: Post-incident auditing are often done ad-hoc, depending on the type of incident, and the setting. Sometimes post-incident audits are standard procedure, for example 3 weeks after a major incident. 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 (the ones failing during the incident).

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.

5.4.3 Audit types

Different settings require different types of audits. An audit can involve a review of high-level documents (policies, procedures) provided by the provider, interviews with C-level executives, or tests and checks of network and information systems. We list the different audit 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.

Certification: Certification is a process whereby a specific (licensed) auditor carries out an audit and the audit report is then submitted to a certification body which evaluates the audit report and issues a certificate of compliance. Certification often asserts that the organization has organized its processes and security in a certain structure way.

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 security officer (CSO or CISO), tactical/operational security officer, NOC managers or members of the internal CERT, product managers (middle-level management), and system administrators responsible for important platforms 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.

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 take for example ITU X.1051 for information security management (which is based on ISO27002) 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.

7.1 Related ENISA papers

- The first public annual report of incidents, concerning the 2011 incidents, is available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2011/
- 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

7.2 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

7.3 Standards and good practices

- ISOIEC 27001/ISOIEC 27002 "Information security management"
- ISOIEC 24762 "Guidelines for information and communications technology disaster recovery services"
- ISO 27005 "Information security risk management"
- ISO 27011 "Information security management guidelines for telecommunications"
- BS 25999-1 "Guide to Business Continuity Management"

- BS 25999-2 “Business Continuity Management Specification”
- ITU-T X.1056 (01/2009) “Security incident management guidelines for telecommunications organizations”
- ITU-T Recommendation X.1051 (02/2008) “Information security management guidelines for telecommunications organizations based on ISO/IEC 27002”
- ITU-T X.800 (1991) “Security architecture for Open Systems Interconnection for CCITT applications”
- ITU-T X.805 (10/2003) “Security architecture for systems providing end-to-end communications”
- ISF Standard 2007 “The Standard of Good Practice for Information Security”
- CobiT “Control Objectives for Information and related Technology”
- ITIL Service Support
- ITIL Security Management
- PCI DSS 1.2 Data Security Standard

7.4 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”

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu