Technical guidelines for Minimum Security Measures

g the security measures in Article 13a

About ENISA

The European Network and Information Security Agency (ENISA) is a European Union (EU) agency which acts as a centre of expertise for the EU Member States and European institutions. It gives advice and recommendations on good practices, and acts as a "switchboard" for exchanging knowledge and information. The agency also facilitates contacts between the European institutions, the Member States, and private business and industry.

Contact details

Authors: Dr. Marnix Dekker, Lionel Dupré, Dimitra Liveri

For contacting ENISA, for enquiries about this document or about ENISA's activities regarding Article 13a, please email: resilience@enisa.europa.eu

Credits

This document is the result of close collaboration between ENISA and various stakeholders from across the EU: PTS (SE), MINEZ (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ITST (DK), CPNI (UK), RTR (AT), ANCOM (RO), ESMIS (BG), ANSSI (FR), Bundesnetzagentur (DE), BIPT (BE), MITYC (ES), MPO (CZ), CERT LT (LT), MFSR(SK), ILR (LU), APEK (SI), MCA (MT), Ministry of Economic and Development (IT), OCECPR (CY). We are grateful for their valuable input and comments.

Contents

Preface

Directive 2009/140/EC of the European Parliament and of the Council amends Directive 2002/19/EC, on access to, and interconnection of, electronic communications networks and associated facilities, Directive 2002/20/EC on the authorization of electronic communications networks and services, and Directive 2002/21/EC, on a common regulatory framework for electronic communications networks and services. The directive asks ENISA to contribute to the security of electronic communications and to contribute to the harmonization of technical and organizational security measures taken by the member states.

Paragraph 1 and 2 of Article 13a state that member states should ensure that providers of public communication networks take measures to guarantee security and integrity of these networks and to ensure continuity of services provided over these networks (in technical jargon this would be referred to as network availability). Paragraph 3 of Article 13a says that the member states should report about significant security breaches and losses of integrity to the EC and ENISA.

In 2010, ENISA, the European Commission (EC), Ministries and Telecommunication National Regulatory Authorities (NRAs), initiated a series of meetings (workshops, conference calls) to achieve a harmonized implementation of Article 13a. In these meetings, a working group of representatives of NRA's and EC reached consensus about two technical non-binding documents.

- Technical guidelines for incident reporting: Guidelines to support Member States in implementing paragraph 3 of Article 13a. Paragraph 3 concerns the notification of NRAs in case of a significant security breach or loss of integrity of networks, and it concerns annual reporting of these incidents to the EC and ENISA.
- Minimal Security Measures (this document): A list of minimum security measures that NRAs have to take into account when evaluating compliance of electronic communications providers to paragraph 1 and 2 of Article 13a.

The working group will continue beyond the publication of these documents to further support a harmonized implementation of Article13a across the EU.

1. Introduction

This document provides technical guidance for NRA's concerning paragraph 1 and 2 of Article 13a of Directive 2009/140/EC. This document contains a list of minimum security measures that NRA's should take into account when evaluating compliance of public communications network providers to paragraph 1 and 2 of Article 13a.

This document is drafted by a working group including NRA's and EC, supported by ENISA (see preface). This document is non-binding, it is targeted at national ministries and NRA's and provides guidance for NRA's concerning technical aspects of implementing Article 13a. It is not a recommendation to NRA's.

For the sake of reference, we include 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."*

In the remainder of this section we introduce abbreviations and terminology used in this document. In Section 2 we list the minimum security measures.

Abbreviations

In this document, for the sake of brevity, we use the following abbreviations:

- Telco is used to refer to an *"undertaking providing public communications networks or publicly available electronic communications services".*
- NRA is used to refer to a *"national regulatory authority".*
- Network is used to refer to *"public communications networks or publicly available electronic communication services".*

Security and integrity

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

- Paragraph 1 requires Telco's 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 Telco's to *"take all appropriate steps to guarantee integrity of their networks, and thus ensure the continuity of supply of services".*

This document addresses both security (paragraph 1) and integrity (paragraph 2) at once, by providing a single set of minimum security measures for both.

The integrity of networks (paragraph 2) would be called availability or continuity in technical jargon. In this document we use the word integrity like it is used in paragraph 2.

Incidents: Breaches of security and losses of integrity

Article 13a addresses two types of incidents: security breaches and losses of integrity.

In this document, in line with the text in Article 13a, incident is defined as follows.

An incident is an event which can cause a breach of security or a loss of integrity of electronic telecommunication networks and services.

Note that the same definition is used in the Technical guidelines for incident reporting document.

Networks and services

The paragraphs 1 and 2 in Article 13a address both networks and services and state that the goal of the security measures is to ensure security of the networks and continuity of the services (by other parties possibly) provided over the networks. The text clearly distinguishes between networks and services over these networks. In this document we, for the sake of simplicity, simply refer to networks and services.

We would like to remark that this scenario – of one or more (incumbent) service providers using networks of an (established) network operator - is addressed in various other parts of the Directive 2009/140/EC.

2. Minimum security measures

In this section we provide a list of minimum security measures that NRA's should take into account when evaluating compliance of public communications network providers to paragraph 1 and 2 of Article 13a.

We stress that the security measures are intended as guidance for NRA's. It is at the discretion of NRA's to adopt different security measures (for example, based on a national or international standard), part of the minimum security measures, or additional security

measures. To give an example, an NRA could differentiate for small Telco's and forego certain security measures.

Before providing the list of minimum security measures, we define the scope of the security measures. At the end of the section we map the security measures to international standards and we discuss possible technical approaches NRA's could take to ensure Telco's take these security measures.

Scope

The scope of the security measures is defined as follows.

The security measures apply to all assets which, when breached and or failing, can have a negative impact on the security or continuity of the electronic communication networks.

Telco's should therefore perform risk assessments to determine the assets that must be protected.

A non-exhaustive list of assets relevant in this context, provided as an example, follows.

- Information: Databases and data files, contracts and agreements, documentation and manuals, operational procedures and plans, audit trails, logs, archives.
- Software assets: Network and information systems software, application software, software for subscribers, development tools, operational tools, operational software.
- Physical assets: Facilities, switches, cables, terminal equipment, network and information systems hardware, network equipment, removable media.
- Services: Computing and network services, general utilities such as power supply.
- People: Telecommunication engineers, customer-service staff, IT support staff and users at service providers.

Minimum security measures

The minimum security measures are grouped in domains (D1, D2 …) and subdomains (SD1.1, SD1.2 …).

Note that, in the list of security measures below, we use the shorthand "the Telco should take measure X" to say that NRA's must take measure X into account when evaluating compliance of Telco's to paragraphs 1 and 2 of Article 13a.

Note also that, in the list of security measures below, we give examples and quotes from texts about technical security measures in existing international standards. These measures (in technical papers also called controls, or security controls) are provided as a pointer to similar or related security measures in existing standards. We stress that the examples are not exhaustive and that they do not indicate a complete or a preferred implementation of the security measure.

D1: Governance and risk management

This domain covers the security measures related to (network and information security) governance and risk management.

SD1.1 Information security policy

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

- Example: [from ISO27002 Ch 5] "*Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.*"

SD1.2 Governance and risk management framework

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

- Example: [from ISO27002 Ch 4] "*Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.*"

SD1.3 Security roles and responsibilities

The Telco should establish and maintain an appropriate structure of security roles and responsibilities.

- Example: [from ISO27011 Ch 8.1.1] "*Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy.*"

SD1.4 Managing third party networks or services

The Telco 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, et cetera.

- Example: [from ISO27002 Ch 6.2] "*The security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services.*"

D2: Human resources security

This domain covers the security measures taken to enhance the security of personnel such as employees, contractors and third-party users.

SD2.1 Background checks

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

- Example: [from ISO27002 Ch 8.1.2] "*Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.*"

SD2.2 Security knowledge and training

The Telco should ensure personnel has sufficient security knowledge and are provided with regular security training.

- Example: [from Cobit] "*Provide employees with appropriate orientation when hired and on-going training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals.*"
- *Example: [from ISO27002 Ch 8.2.2] "All employees of the organization and, where relevant, contractors and third-party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function."*

SD2.3 Personnel changes

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

- Example: [from ISO27002 Ch 8.3] "*Responsibilities should be in place to ensure an employee's, contractor's or third-party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.*"

SD2.4 Handling violations

The Telco should establish and maintain a disciplinary process for employees who have committed a security breach.

- Example: [from ISO27002 Ch 8.2.3] *"There should be a formal disciplinary process for employees who have committed a security breach."*

D3: Security of systems and facilities

This domain covers security of network and information systems and facilities where they are located

SD3.1 Physical and environmental security of facilities.

The Telco should establish and maintain appropriate physical security of facilities and network and service infrastructure. The Telco should establish and maintain appropriate environmental controls to protect against fire, flood, earth quakes and other forms of disasters that may affect the facilities.

- *Example: [from ISO27002 Ch 9.1] "Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference. The protection provided should be commensurate with the identified risks."*
- Example: [from ISO27002 Ch 9.1.4] *"Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied."*

SD3.2 Security of supplies

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

- Example: [from ISO27002 Ch 9.2.2] "*Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities."*

SD3.3 Access control to network and information systems

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

- Example: [from ISO27002 Ch 11] "*Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements."*

D4: Operations management

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

SD4.1 Operational procedures and responsibilities

The Telco should establish and maintain operational procedure and responsibilities.

- Example: [from ISO27011 Ch 10.1] *"Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures."*

SD4.2 Change management procedures.
The Telco should establish change management procedures in order to minimise the likelihood of disruptions and errors due to changes.

- Example: [from ISO27011 Ch 10.1.2] "*Operational systems and application software should be subject to strict change management control."*

SD4.3 Asset management
The Telco should adopt configuration controls and assets management procedures in order to verify asset availability and status.

- Example: [from ISO27011 Ch 7.1] *"All assets should be clearly identified and an inventory of important assets should be drawn up and maintained. (…)When developing and maintaining the inventory of assets, clear responsibilities between the telecommunications facilities of the organization and those of other connected or related telecommunications organizations should be specified and clearly documented."*
- *Example: [from CobiT] "Organisational management should be ensured that a baseline of configuration items is kept as a checkpoint to return to after changes."*

D5: Incident management

This domain covers incident detection, response, and communication.

SD5.1 Standards and procedures for incidents
The Telco should establish and maintain standards and procedures for managing incidents. Incidents should be investigated regardless.

- Example: [from ITU1056 Ch 6.1] *"Telecommunications organizations need to have processes in place to not only handle security incidents that do occur but to prevent incidents from occurring or re-occurring. These include processes to: plan and implement a security incident management capability; to secure and harden the organization's infrastructure to help prevent security incidents from occurring or to mitigate an on-going incident; to detect, triage, and respond to security incidents and events when they occur."*

SD5.2 Incident detection capability

The Telco should establish and maintain an incident detection capability that detects incidents, and forwards them to the appropriate people or processes.

- Example: [from ISO27001 Ch 4.2.3] *"Execute monitoring and reviewing procedures and other controls to promptly identify attempted and successful security breaches and incidents."*

SD5.3 Incident response and escalation processes

The Telco should establish, maintain and adopt a process for incident response and escalation, including roles and responsibilities. Incidents should be assessed (triage) and if needed escalated.

- Example: [from ISO27002 Ch 13.1] *"Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact."*
- Example: [from ITU1056 Ch 6.1] *"The Respond process, which includes sub-processes to: analyse the event; plan a response strategy; coordinate and provide technical, management, and legal response, which can involve actions to contain, resolve, or mitigate incidents and actions to repair and recover affected systems; communicate with external parties;"*

SD5.4 Incident reporting and communication plans

The Telco should establish, maintain and follow appropriate incident reporting and communication plans, which should include reporting certain incidents as described in the Technical guidelines for incident reporting.

- Example: [from ISO27002 Ch 13.1] *"all employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services."*
- Example: [from ITU1056 Ch 5.3.6] *"the security incident management scheme should have provisions for controlling the communication of the incident to external parties, including the media, business partners, customers, law enforcement, and the general public."*

D6: Business continuity management

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

SD6.1 Service continuity strategy and contingency plan

The TELCO should establish and maintain a strategy for maintaining continuity of networks and communication services and establish and maintain a contingency plan.

- Example: [from ISO27002 Ch 14.1.3] *"Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical processes."*

SD6.2 Disaster recovery capability

The Telco should establish and maintain an appropriate disaster recovery capability, to restore network and communication services after disasters.

- Example: [from ISO27011 Ch 14.1.3] *"In developing and implementing the business continuity plan, telecommunications organizations should consider the inclusion of emergency rehabilitation plan of telecommunications services and ensuring essential communications of telecommunications service customers. If adjacent buildings or site are damaged or requested for evacuation, telecommunications service facilities may become virtually out of control, even if the facilities themselves are. Telecommunications organizations should consider how to cope with such situations."*

D7: Monitoring, auditing and testing

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

SD7.1 Monitoring and logging policies

The Telco should establish and maintain monitoring and logging policies.

- *Example: [from CobiT] "Establish and maintain standards and procedures for collecting and interpreting logs."*
- Example: [from ISO27001 Ch 10.10] "*Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified."*

SD7.2 Exercise contingency plans

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

- Example: [from BS25999 Ch 8.3] *"An exercise program should be consistent with the objectives of the organization and the regulatory regimes to which it is subject. Exercises may include tests which anticipate a predetermined outcome, table tops, simulations, and full operational exercises."*

SD7.3 Network and information system testing
The Telco should establish and maintain policies for testing network and information systems, particularly when connecting to new networks or systems.

- Example: [from ISO27011 Ch 12.4.1] "*c) applications and operating system software should only be implemented after extensive and successful testing; the tests should include tests on usability, security, effects on other systems and user-friendliness, and should be carried out on separate systems (see also 10.1.4);"*

SD7.4 Security assessment and security testing
The Telco should establish and maintain an appropriate policy for performing security assessments and security testing of all assets.

- Example: [from ISO27002 Ch 15.2] *"Compliance checking also covers, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose."*

SD7.5 Compliance monitoring and audit policy
The Telco should establish and maintain a policy for compliance monitoring and auditing and have a process for compliance reporting and addressing audit deficiencies.

- Example: [CobiT] *"Obtain and report assurance of compliance and adherence to all internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any compliance gaps have been taken by the responsible process owner in a timely manner."*

Mapping example

Here we provide an example showing how the minimal security measures can be mapped to international standards. We would like to stress that this example does not indicate a preferred implementation or a preference for a particular set of standards.

In this example we assume a Telco uses ISO27001/2 for information security management, ISO27K5 for risk management, and BS25999 (or ISO22399) for continuity management. The minimal security measures can be mapped to the standards used by the Telco as follows.

MSM	TELCO	Compliance details
D1: Governance and risk management	ISO27001	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	ISO27001 and BS25999	ISO27001/2 Ch 8, and ISO 22399 Ch 7 in lesser detail, cover security clearances, security roles and responsibilities, security knowledge and training, and personnel changes.
D3: Security of systems and facilities	ISO27001	ISO27001 Ch 9 covers physical security of facilities, of IT equipment and environmental controls
D4: Operations management	ISO27001	ISO27001 Ch 10 covers operational procedures, operational roles, classification, access control and change controls.
D5: Incident management	ISO27001	ISO27002 Ch 13 covers incident management.
D6: Business continuity management	BS25999	BS25999 (or ISO22399), and in lesser detail ISO27001/2 Ch 14 cover business continuity.
D7: Monitoring and security testing	ISO27001	Monitoring is covered in ISO27001/2 Ch 10, security testing and compliance monitoring and reporting are covered in ISO27001/2 Ch 15.

Implementation

Here we outline different (technical) approaches NRA's could take to ensure that Telco's take appropriate security measures.

- Random: Compliance of Telco's is randomly checked by the NRA.
- Ad-hoc: Compliance of Telco's is checked on an ad-hoc basis by the NRA, taking into consideration for example the size or importance of a Telco or past incidents at a Telco.
- Periodic audit requirement: Telco's are required to pass periodic audits by competent independent parties.
- Guidance and post-incident: The NRA gives guidance to Telco's and checks compliance post-incident.
- Active collection: The NRA actively collects compliance documentation from all Telco's.

Note that implementation and enforcement of Article 13a by the MSs is specifically addressed in Article 13b and out of scope of this document.

References

For the sake of reference, we provide a non-exhaustive list of common information security standards, which were used as input for earlier drafts of this document.

International 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 (or ISO22399) Guide to Business Continuity Management
- ITU-T X.1056 (01/2009)
- ITU-T X.800 (1991)
- ITU-T X.805 (10/2003)
- ITU-T Recommendation X.1051 (02/2008)
- ISF Standard 2007
- CobiT Control Objectives for Information and related Technology
- ITIL Service Support
- ITIL Security Management
- UCF Guidance

National standards and good practices - EU

- IT Baseline Protection Manual Germany
- KATAKRI (FI)

National standards and good practices – Extra EU

- NIST 800 34
- NIST 800 61
- FIPS 200
- NICC ND 1643

Commercial standards and good practice

- PCI DSS 1.2

(this page is intentionally left blank)

3.