Technical Guideline for Minimum Security Measures

Guidance on the security measures in Article 13a

Version 1.0, December 2011

enisa
European Network and Information Security Agency

Authors

• Dr. Marnix Dekker, ENISA
• Dimitra Liveri, ENISA
• Daniele Catteddu, ENISA
• Lionel Dupré, ENISA

Acknowledgements

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

PTS (SE), Ministry of Economic Affairs (NL), FICORA (FI), Ofcom (UK), ANACOM (PT), ComReg (IE), EETT (GR), ITST (DK), CPNI (UK), RTR (AT), ANCOM (RO), EA “ECNIS” (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 Development (IT), OCECPR (CY).

We are grateful for their valuable input and comments.

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.**

Contact details

For contacting ENISA or for general enquiries on Article 13a, please use the following details:
- E-mail: resilience@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

For questions related to Article 13a, please use the following details:
- E-mail: resilience@enisa.europa.eu

Legal notice

Executive Summary

EU Directive 2009/140/EC amends existing directives on electronic communications networks and associated facilities (2002/19/EC, 2002/20/EC, 2002/21/EC). The directive, which had to be transposed to national legislation by the EU member states in May 2011, introduces Article13a on security and integrity of public communication networks.

Paragraphs 1 and 2 of Article 13a says that providers of public communications networks should take measures to guarantee the security and integrity of these networks and to ensure continuity of services provided over these networks. Paragraph 3 of Article 13a says that providers should report significant security breaches and losses of integrity and that, annually, summary reports about significant incidents should be sent to ENISA and the European Commission (EC).

In 2010, ENISA, the EC, Ministries and Telecommunication National Regulatory Authorities (NRAs), initiated a series of meetings (workshops, conference calls) to achieve a harmonised implementation of Article 13a. In these meetings, a working group of experts from NRAs reached a consensus on two non-binding technical documents providing guidance to the NRAs in the member states: Technical guideline for incident reporting and Technical guideline for minimum security measures (this document).

In this document we give guidance to NRAs about the implementation of Article 13a and in particular about the security measures that providers of public communications networks must take to ensure security and integrity of these networks. It lists the minimum security measures NRAs should take into account when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

The security measures in this document are categorized in different domains; Governance and risk management, Human resources security, Security of systems and facilities, Operations management, Incident management, Business continuity management, Monitoring, auditing and testing. Implementation and enforcement of the security measures (Article 13b) is beyond the scope of this document, but the different technical approaches NRAs could take are briefly discussed.

The meetings of the working group will continue beyond the publication of the documents, to further support harmonised implementation of Article13a across the EU.

Contents

1 Introduction

This document provides technical guidance to NRAs on paragraph 1 and 2 of Article 13a of Directive 2009/140/EC. It lists the minimum security measures that NRAs should take into account when evaluating the compliance of public communications network providers with paragraph 1 and 2 of Article 13a.

This document is drafted by a working group comprising NRAs and representatives of the EC, supported by ENISA (see Executive summary). This document is not binding.

1.1 Target audience

This document is targeted at national ministries and NRAs and provides guidance for NRAs on the technical aspects of implementing Article 13a. It is not a recommendation to NRAs.

1.2 Goal

The goal of this document is to provide guidance to NRA's on implementing paragraph 1 and 2 of Article 13a.
Additionally, this document aims to provide a baseline implementation, to support a harmonized implementation across the EU. A harmonized implementation is important for the many telecommunications providers who provide services across the EU.

1.3 Structure of this document

In Section 2 we introduce Article 13a and some terminology used in this document. Section 3 lists the minimum security measures and defines their scope. In Section 4 we briefly discuss technical approaches NRAs could take to ensure that network providers take appropriate measures and we give an example mapping to existing standards.

2 Article 13a terminology

In this section we introduce Article 13a and the terminology used in this document. As a reference, we reproduce below the text of paragraphs 1 and 2 of Article 13a.

"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. […]"

2.1 Abbreviations

In the interest 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 competent "national regulatory authority" as mentioned in Article 13a.
- The term networks and communications services is used to refer to "public communications networks or publicly available electronic communications services" as mentioned in Article 13a.

2.2 Security and integrity

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

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

  In this document we address both security (paragraph 1) and integrity (paragraph 2) by providing a single set of minimum security measures.

The use of the term integrity in the article text may be confusing to some readers. We refer the reader to the definition in technical literature about networks and network

interconnections[1], which defines integrity "as the ability of the system to retain its specified attributes in terms of performance and functionality". Integrity of networks would be called availability or continuity in most information security literature[2].

2.3 Incidents: Breaches of security and losses of integrity

In this document, 'incident' is used to refer to events which can cause a breach of security or a loss of integrity that would have an impact on the operation of electronic telecommunications networks and services. This is in line with the definition used in the document 'Technical Guidelines for Incident Reporting'[3].

2.4 Networks and services

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 service (possibly by other parties) provided over the networks.

The text distinguishes between networks and services provided over these networks. In this document, for the sake of simplicity, we simply refer to networks and services. This scenario – of one or more (newcomer) service providers using networks of an (incumbent) network operator – is addressed in various other parts of Directive 2009/140/EC.

[1] Ward, K, 1995, 'The Impact of Network Interconnection on Network Integrity'. British Telecommunications Engineering, 13:296–303.
[2] In information security literature the term 'integrity' usually refers to the property that data or communications cannot be altered or tampered with.
[3] A subset of these incidents have to be reported, i.e. incidents that have a significant impact on users and services.

3 Minimum security measures

In this section we list the minimum security measures and we define their scope.

We stress that the minimum security measures are intended as guidance for NRAs. It is at the discretion of NRAs as to whether they adopt different security measures (for example, based on a national or international standard), just some of the minimum security measures, or additional security measures. To give an example, an NRA could decide to differentiate between Telcos and, for example, forego certain security measures for the latter. It should be noted also that it may be the case that some of these measures may not be fully applicable in all settings, depending on the type of network or service provider involved[4].

3.1 Scope

The scope of the security measures (the assets to which they should be applied) is defined as follows:

All assets which, when breached and or failing, can have a negative impact on the security or continuity of electronic communications networks.

Telcos should perform risk assessments, specific for their particular setting, to determine which assets fall under this scope.

A number of standard methodologies exist for performing risk assessments, such as, for example, the ISO 27005 standard. We provide a non-exhaustive list of assets as an example:

- Information: Databases and data files, configuration setups, 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 services, network services, general utilities such as power supply, temperature and humidity control.
- People: Telecommunications engineers, customer service staff, IT support staff and users of service providers.

3.2 Minimum security measures

The minimum security measures have been derived from a set of international and national standards that are commonly used by Telcos (see References). We used a survey, to determine which standards are used most often by Telcos, and we used an intermedi-

[4] For example, in the case of black fibre providers it may be the case that certain security measures are not applicable.

ate mapping which maps the security requirements in the most common Below we quote from texts about technical security measures in existing international standards (often called 'controls' in technical papers). These quotes are provided as pointers to similar or related security measures in existing security standards. We wouldl like to stress here that these examples are not exhaustive and that they do not indicate a complete or a preferred implementation of the security measure.

In the list below we say "the Telco should take measure X" to indicate that NRAs must take into account measure X when evaluating the compliance of Telcos with paragraphs 1 and 2 of Article 13a.

The minimum security measures are grouped in domains (D1, D2 …) and in sub-domains (SD1.1, SD1.2, et cetera.

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 organisation."

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 communications networks and services.

Example: [from ISO27002 Ch 4] "Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organisation. 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, etc.

Example: [from ISO27002 Ch 6.2] "The security of the organisation'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) if 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 its personnel have 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 organisation and, where relevant, contractors and third-party users, should receive appropriate awareness training and regular updates in organisational 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 organisation 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 (or have a broader process that covers security breaches).

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 the security of network and information systems and facilities.

SD3.1 Physical and environmental security of facilities

The Telco should establish and maintain the appropriate physical security of facilities and network and service infrastructure. The Telco should establish and maintain appropriate environmental controls to protect against fire, flood, earthquakes 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 unauthorised 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 Control of access 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."

SD3.4 Information security of network and information systems

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

Example: [from ISO27002 Ch 10] "Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code. Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. (…) Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code."

D4: Operations management

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

SD4.1 Operational procedures and responsibilities

The Telco should establish and maintain operational procedures 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 resulting from 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 asset 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 organisation and those of other connected or related telecommunications organisations should be specified and clearly documented."

Example: [from CobiT] "Organisational management should be ensured so that a baseline of configuration items is kept as a checkpoint to return to after changes."

D5: Incident management

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

SD5.1 Standards and procedures for incidents

The Telco should establish and maintain standards and procedures for managing incidents.

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

Example: [from ITU1056 Ch 6.1] "Telecommunications organisations 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 organisation'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 departments or processes, within an appropriate time frame.

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, where necessary, 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 organisational 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. These plans should include reporting incidents to the NRA, 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 for protecting communications 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 ensuring continuity of networks and communication services and it should establish and maintain a contingency plan.

Example: [from BS 25599-2 Ch 4] "The organization shall establish:

the requirements for business continuity, taking account of the organization's objectives, obligations and legal duties;

business continuity objectives and plans;

the scope of business continuity, in terms of its products and services."

SD6.2 Disaster recovery capability

The Telco should establish and maintain an appropriate disaster recovery capability for restoring network and communication services after disasters.

Example: [from BS 25599 Ch 5] "The organization shall define how it will provide for the recovery of its critical activities for which business continuity is the chosen risk treatment and take account of those activities not defined as critical."

D7: Monitoring, auditing and testing

This domain covers monitoring, testing and auditing of 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 in collaboration with relevant third parties, such as network operators, where appropriate.

Example: [from BS 25999 Ch 5] "The organization shall ensure that its BCM arrangements are validated by exercise and review and are kept up-to-date (…). The organization shall evaluate the competence and capability of its BCM with a view to continual improvement."

SD7.3 Network and information systems 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 reporting compliance 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."

4 Technical approaches to implementation

In this section we discuss different technical approaches NRAs could take to ensuring that Telcos take appropriate security measures.

4.1 Implementation

Implementation and enforcement of Article 13a by MSs are addressed in Article 13b. Although this part of the directive is outside the scope of this document, we briefly discuss different technical approaches NRAs could take to ensure that Telcos are taking appropriate security measures. The following examples, which are not mutually exclusive, are based on input from NRAs, who have compliance schemes in place:

- Random or ad-hoc checking: Compliance of Telcos is randomly checked, or 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. This approach is similar to the approach sometimes taken by insurance companies when checking insurance claims. In this approach the NRA may supply guidance to Telcos up front and additionally may require the Telcos to undergo periodic audits by competent independent parties. The NRA checks compliance documentation or audit reports at random.
- Periodic audit requirement: Telcos are required to pass periodic audits by competent independent parties. In this setting the NRA may supply guidance to Telcos up front. The NRA collects only the periodic audit reports, but not the underlying compliance documentation.
- Guidance and post-incident: The NRA gives guidance to Telcos upfront. The NRA may require the Telcos to undergo yearly audits by competent independent parties. Compliance is checked by the NRA only post-incident, to see if the Telco complied to the regulation.
- Active collection: The NRA actively collects compliance documentation from all Telcos. The format of the compliance documentation is standardized by the NRA, by means of a template. In this approach the NRA collects detailed compliance documentation. In this setting the NRA could still require Telcos to undergo periodic audits by a competent independent party.

Whichever approach is taken, it is important to provide guidance to Telcos. Guidance could take the form of a simple list of national or international standards as a reference, or give technical details describing specific technical requirements. The advantage of re-using existing standards is that this would allow Telcos to take advantage of existing compliance and certification schemes.

4.2 Example mapping to existing standards

It is important to stress that the minimum security measures are not intended to replace existing national or international standards that may be in use in member states already. We show by giving an example how the minimal security measures could be mapped to existing standards. We stress that this example does not indicate a preferred implementation.

As an example, we assume a Telco uses ISO27001/2 for information security management, ISO27005 for risk management and BS25999-1/2 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	ISO 27001/2 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	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	ISO27001 Ch 9 covers the physical security of facilities, IT equipment and environmental controls
D4: Operations management	ISO 27001/2	ISO27001 Ch 10 covers operational procedures, operational roles, classification, access control and change controls.
D5: Incident management	ISO 27001/2	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	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 here as an 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.

5 References

As references, we provide a non-exhaustive list of common information security standards used as input to earlier drafts of this document.

5.1 International standards and good practice

- 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

5.2 National standards and good practice - EU

- IT Baseline Protection Manual Germany
- KATAKRI, National security auditing criteria, Finland

5.3 National standards and good practice – extra EU

- 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”

5.4 Commercial standards and good practice

- PCI DSS 1.2 Data Security Standard

enisa

European Network and Information Security Agency