Improving recognition of ICT security standards

Recommendations for the Member States for the conformance to NIS Directive

VERSION: 1.0

DECEMBER 2017

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists 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 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

For queries in relation to this paper, please use isdp@functional.mailbox
For media enquires about this paper, please use press@enisa.europa.eu.

ISBN: 978-92-9204-249-3, DOI 10.2824/176720

Table of Contents

Executive Summary

This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs.

This document provides the results of an assessment of the maturity of the implementation of the European Cyber Security Standardisation activities in the EU Member States with respect to the NIS Directive concerning measures for a high common level of security of network and information systems across the Union. The main assertions this report makes include the following:

- Standardisation for compliance with the NIS Directive is essential;
- Recognition of standardisation in policy is low;
- Utilisation of standards give value to Member States and their infrastructure;
- Utilisation of standards raises Cyber Security levels;
- Utilisation of standards provides sustainability and interoperability at European level.

The current market research has clearly shown that the information security/cyber security standard development ecosystem is healthy and fast moving. Few gaps actually exist and to implement the NIS Directive choosing the rights ones and implementing them is of paramount importance.

In the scope of this survey a questionnaire was sent to the Member States representatives and used as the basis of data gathering either in the form of interviews, or by directly completing it and sending responses to the authors. A summary of the responses given have been collated and summarised.

The content of these responses does not allow to identify whether Member States perceive the existence of a gap in current available standardisation. However, the content, and general limitations in the cohesion amongst Member States suggests that there is insufficient guidance from the specialists in the field (e.g. national normalization institutes, European institutions etc.), on which of the many standards available are to be used.

It is reasonably straightforward and it follows on the current rate on transposition, to suggest that all Member States are aware of the NIS Directive and their responsibilities in implementing it. What is less clear is the role that standards have in the NIS Directive implementation.

There is insufficient information with regard to the responses to conclude that a lack of knowledge of standards exists. This suggests however that if an appropriate standard is available, it will be adopted. For example, even though the ISO27000 series of standards are in the form of broad guidance, there is a well-established eco-system that addresses their implementation.

A major concern is that the NIS Directive domain, and compliance with the NIS Directive requirements, is often perceived as a purely national prerogative. Where international, cross-border, information sharing is required, this has been perceived as in the domain of existing CSIRT relationships used for reporting security incidents and not directly as an element of NIS Directive compliance.

At the operational level there is very little specified for standards-based NIS Directive compliance and this is one area where ETSI, for example, has made some contributions. However, there are no mandates at either national or European level to guide this activity at the implementation level.

In light of the above, the following solutions are recommended to mitigate the lack of overall awareness and trainings on the role of standards in NIS Directive compliance and to encourage wide deployment of common security platforms in the OES and PDS entities:

- Training initiatives by the European Commission and ENISA through workshops for Member States' relevant agencies
- Promotion of new work items in the European SDOs for some areas (e.g. criteria for defining OES / DSP) or the adoption of appropriate standards in Europe where existing (for example information exchange, where several mature efforts already are in place, like STIX)
- Repeat the information gathering as performed within the elaboration of this study after an adequate interval of time

1. Introduction

This report is an extension of previous ENISA work on approaches to the Directive on security of network and information systems ("NIS Directive")[1] by Member States, which:

- have made recommendations on standardisation (i.e. "Gaps in NIS standardisation - Recommendations for improving NIS in EU standardisation policy"[2])
- have outlined the use and management of CSIRTs, which is directly referred to in Article 12 of the NIS Directive that seeks to establish a CSIRTs network "*in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation*".

ENISA provides the secretariat of the CSIRTs Network and actively supports the cooperation among the CSIRTs. An up to date inventory of CSIRTs is also maintained by ENISA[3].

There are several assertions to take into account when discussing standardisation and EU policies:

- Standardisation for compliance with the intentions of the NIS Directive is essential;
- Recognition of standardisation in policy is generally low;
- Utilisation of standards give value to Member States and their infrastructure;
- Utilisation of standards raises Cyber Security levels;
- Utilisation of standards provides sustainability and interoperability at European level.

The role of standards in general is described in section 4 of this report, where also the structure of the European Standards process and a review of the core bodies involved is given.

The prevailing practice in European Standardisation is that standards are voluntary and are not cited by policy. With a few exceptions for standards that have a direct impact on regulated resources (e.g. radio bandwidth) or on safety there are very few domains where standards are harmonised across the EU and again in most cases voluntary adherence to common standards is the common practice. Only when it is shown that no effective standards exist is it expected that the EU will become directly involved by provision of a standard and its enforcement.

Specific recommendations made in the report "Gaps in NIS Standardisation" include the need to reach consensus among Member States and major partners on:

- Architectures, interfaces, and information exchange expressions
- Standards and specifications

It is also strongly recommended that given the strong similarities of the NIS Directive and USA Cybersecurity Act, that these two implementations be implemented after taking consideration of each other's features to the extent possible, including common architectures, interfaces, structured information expressions and privacy filters including taking the following actions:

[1] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[2] https://www.enisa.europa.eu/publications/gaps-eu-standardisation
[3] https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory

- Develop a means for Information Sharing and Analysis Centres (ISACs) and Information Sharing and Analysis Organizations (ISAOs) to fit into the NIS Directive model and architecture
- Develop a means for Public Electronic Communication Networks or Publicly Available Electronic Communication Service Providers under EU Directive 2002/21/EC and Trust Providers to fit into the NIS Directive model and architecture
- Develop additional border gateway defence and threat exchange standards for one Essential Service (Digital Infrastructure Internet Exchange Points)
- Develop a means for NFV, SDN, MEC and other virtualised infrastructures and services to fit into the NIS Directive model and architecture

when considering the role of CSIRTs, ISAOs and ISACs in the context of NISD it has been previously reported that there are no globally cited standards for interoperability of CSIRTS in support of the NIS Directive. The concern implicit in the NIS Directive is that there are insufficient measures for a high common level of security of network and information systems across the Union. The recommendations in this document taken along with those in the report are intended to provide a means to close the gap and to highlight those areas of standardisation that the authors of this report believe should be promoted by Member States.

2. Scope

This report provides the results of an assessment of the maturity of the implementation of the European Cyber Security Standardisation activities in the EU Member States with respect to the NIS Directive concerning measures for a high common level of security of network and information systems across the Union.

This report is the outcome of work undertaken under ENISA Work Programme 2017, Strategic Objective 1, part of Work Package 1.3. - Research & Development, Innovation. The objective of this report is therefore to provide a concise assessment of the maturity of the implementation of the European Security Standardisation activities in the EU Member States. The document includes the results of a fact gathering by series of interviews with selected Member States to ascertain the level of knowledge in the Member States of the deployment of NIS related standards that have been cited as being publicly available, or in the course of open development, to meet specific needs for IT products, systems and services.

In undertaking the analysis an assessment of the factors that are limiting or reducing the adoption of standards in NIS is given. This complements the previously published work from ENISA in identifying any potential gaps in NIS standardisation in terms of content or process and in this report provides recommendations for the future development of standards in the area of the NIS directive.

This report provides for identification of standards related to the NIS Directive and their uptake at the Member States level. A dedicated section contains the questions used as the basis of data gathering; a summary of the responses given have been collated and are summarised in the next section of this report.

3. Definitions

Formally speaking, the output of a Standards Development Organisation (SDO) may be considered as a standard. However, within that broad definition there is a large number of types of standards that are available. The following table has been taken from the working practices of each of CEN and ETSI (two of the three SDOs officially recognized as competent in the area of voluntary technical standardization in Europe[4] – ESOs, and those with a specific duty to address ICT standardisation).

ESO	DOCUMENT TYPE	APPROVAL PROCESS
ETSI	EN, European Norm Normative provisions	National standards bodies through national consultation and vote
	hEN, harmonised European Norme Normative provisions	National standards bodies through national consultation and vote
	TS, Technical Specification Normative provisions	Members of the ETSI Technical Committee that drafted the document
	ES, ETSI Standard Normative provisions	ETSI members by weighted vote
	TR, Technical Report Not normative	Members of the ETSI Technical Committee that drafted the document
	EG, ETSI Guide Not Normative	ETSI members by weighted vote
	SR, Special Report	The ETSI Board

[4] Regulation (EU) 1025/2012 on European standardisation, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF

	Not normative	
	White Paper	The ETSI Marketing division
ETSI ISG	GS, Group Specification Normative provisions	The ETSI ISG that drafted the document
	GR, Group Report Not normative	The ETSI ISG that drafted the document
CEN CENELEC	EN, European Norm Normative provisions	CEN and CENELEC are recognized as European Standardization CEN and CENELEC BT • Implemented as national standard in 34 countries • Conflicting national standards are withdrawn Vote by Member States : one country one voice 34 countries and 42 national standardisation bodies
	CWA, CEN Workshop Agreement May contain normative provisions but for a time limited period (2 years)	Not much used
	Technical specification	• No immediate need/enough consensus for EN or subject under technical development • May act as pre-standard • No obligation to withdraw conflicting national standards
	TR, Technical Report Not normative	• Informative nature • No obligation to withdraw conflicting national standards

	Vienna agreement (CEN)	Two modes of collaborative development: • ISO Lead: most common and preferred • CEN Lead: mostly when EU standardization requests/legislation exists Useful tool to recognize mutuality of international Standards (i.e. EU Regional standard is textually identical to International standards)
	Frankfurt agreement	Common planning of new work • CENELEC offers to IEC all its NWIs (i.e. future projects of European origin) • Parallel voting on draft International Standards • CDV and FDIS circulated in IEC are automatically submitted to parallel voting procedure within CENELEC • Conversion of European Standards into International Standards • CENELEC deliverables of European origin ('homegrown standards') • European common modifications to IEC based standards

The purpose of standards is primarily to achieve interoperability or comparability between two or more implementations or users.

It has to be noted that at the international level there are three globally recognised Standardisation bodies (also by the EU Regulation 1025/2012) – ISO, IEC, and ITU. These organisations also develop relevant standards to NIS. Thus an ISO standard can be cited and may be cross-published under the provisions of the Vienna and Frankfurt agreements. In some domains, particularly in the work of ISO/IEC JTC1 SC27, "IT security", is a joint committee developing standards in management systems, evaluation certification, application security and privacy.

In the technical domain standards can be broadly seen to support aspects of the CIA paradigm as it is understood in information security, i.e. to address requirements for Confidentiality, Integrity and Availability of a system.

4. Standards related to the Network and Information Security Directive

This section identifies standards having relation to the NIS Directive.

4.1 International Standards

4.1.1 ISO

In ISO/IEC JTC1 SC 27 a large number of standards may be applicable when putting NIS Directive into force. The key documents are listed below.

Information systems management systems to provide guidance and best practices for IT management:

- ISO/IEC 27000 Information security management systems - Overview and Vocabulary.
- ISO/IEC 27001 Information security management systems – Requirements
- ISO/IEC 27002 Code of practice for information security controls.
- ISO/IEC 27005 Information security risk management
- ISO/IEC 27007 Information security management systems - auditor guidelines
- ISO/IEC 27008 Guidelines for auditors on ISMS controls
- ISO/IEC 27009 Sector-specific application of ISO/IEC 27001 – Requirements
- ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Evaluation techniques and methods to provide assurance:

- ISO/IEC 15408 Common criteria
- ISO/IEC 15446 Guide for the production of Protection Profiles and Security Targets
- ISO/IEC 17825 Side channels attacks characterization
- ISO/IEC 18045 Common criteria evaluation method
- ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing
- ISO/IEC 19608 Guidance for developing security and privacy functional requirements based on ISO/IEC 15408
- ISO/IEC 19790 Security requirements for cryptographic modules
- ISO/IEC 19896 Competence requirements for information security testers and evaluators
    - Part 1 Introduction, concepts and general requirements
    - Part 2 Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers
    - Part 3 Knowledge skills and effectiveness requirements for ISO/IEC 15408 evaluators
- ISO/IEC 19989 Security evaluation of presentation attack detection for biometrics
    - Part 1 Framework
    - Part 2 Biometric recognition performance
    - Part 3 Presentation attack detection

Application security management:

- ISO/IEC 27032 Guidelines for cyber security
- ISO/IEC 27034 Application security
    - Part 1 Concepts and overview

  - Part 2 Organisation normative framework
  - Part 3 Application security management process
  - Part 4 Application security validation
  - Part 5 Protocols and application security controls data structure
  - Part 6 Security guidance for specific applications
  - Part 7 Application security assurance prediction model »
- ISO/IEC 27035 Information security incident management
  - Part 1 Principles on incident management
  - Part 2 Guidelines to plan and prepare for incident response
  - Part 3 Guidelines for incident response operations
- ISO/IEC 27036 Information Security for Supplier Relationships
  - Part 1 Overview and Concepts.
  - Part 2 Requirements.
  - Part 3 Guidelines for ICT supply chain security.
  - Part 4 Guidelines for security of cloud services

4.2 European Standards

4.2.1 CEN and CENELEC

In 2017 CEN and CENELEC established a new joint Technical committee, TC 13 on "Cybersecurity and data protection", which intends to develop standards and guidelines in support of EU policies. As of writing of this report, no deliverables have been published by TC13, nor has any publicly information been made available.

4.2.2 ETSI

There is a broad set of technologies being addressed across ETSI's Technical Bodies including CYBER[5], NFV[6] that prepare standardisation related documents that may be used in support of NISD compliance. The following is a selection of the publications from ETSI TC CYBER that apply:

- TR 103 303, Protection measures for ICT in the context of CI
- TR 103 309, Secure by Default adoption – Platform Security Technology
- TS 103 487, Security baseline requirements for sensitive functions for NFV and related platforms
- TR 103 305, Security Assurance by Default; Critical Security Controls for Effective Cyber Defence
- TR 103 331, CYBER Structured threat information sharing
- TR 103 456, NIS Directive Implementation

NOTE: The above provides guidance on the available technical specifications and those in development by major cyber security communities

The work performed by the Industry Specification Group (ISG)[7] Information Security Indicators (ISI)[8] is also of interest for application in the NISD domain. The following ETSI publication is of specific interest in the NISD domain for reporting and classifying security events:

[5] http://www.etsi.org/technologies-clusters/technologies/cyber-security
[6] http://www.etsi.org/technologies-clusters/technologies/nfv
[7] http://www.etsi.org/about/how-we-work/how-we-organize-our-work/industry-specification-groups-isgs
[8] http://www.etsi.org/technologies-clusters/technologies/information-security-indicators

- ETSI GS ISI Information Security Indicators (ISI); Key Performance Security Indicators (KPSIs) to evaluate the maturity of security event detection

4.2.3 Other bodies

At the European level the work already carried out by the European Network for Critical Infrastructure Protection (ERNCIP)[9] should be taken into consideration, even if not strictly part of standardization activities.

4.3 Conclusions

The current market research has clearly shown that the information security/cyber security standard development ecosystem is healthy and fast moving. Few gaps actually exist and to implement the NIS Directive choosing the rights ones and implementing them is of paramount importance. For that to happen, however, the organizations tasked with the actual, technical compliance with NIS Directive need to be aware of the multiplicity of standards and guidelines available and also that - if possible - all EU Member States adopt the same ones. In the next chapter the questionnaire that the expert group developed to assess recognition of standards across the EU will be presented.

[9] https://erncip-project.jrc.ec.europa.eu/

5. Questionnaire

This section of the report contains the questions used as the basis of data gathering either in the form of interviews with representatives of the Member States, or by the Member State directly completing the questionnaire and sending their responses to the authors. A summary of the responses given have been collated and are summarised in the next section of this report.

A significant observation of the data gathering exercise has been to recognise that many Member States have reserved the right to not directly participate in this work and optional interviews necessary to complete the questionnaires. One reason is that in undertaking activity to allow national NIS Directive compliance a number of concurrent work items has been in progress. Such work in progress related to the national implementation and understanding of the NIS Directive, and of the impact of the NIS Directive on existing intra- and inter-Member State activities in the cyber-security domain, has been stated as significantly limiting the time to address the questionnaire. However, in most cases the Member States have made public some or all of their cyber-security plans, including those relating to the NIS Directive, and the content of the present report has been compiled from examination of such sources.

However, with respect to the role of standards, it has been noted that most of the responders to the questionnaire (either by analysis of MS publications or by direct response) are not familiar with either existing standards or with current work in progress. It may be reasonably noted that at the policy level a statement of intent to interwork with other Member States, and to ensure that NIS Directive obligations to interwork may be seen to imply a requirement for standardisation without having to directly being able to cite the standards to be used at that policy level.

In response it is considered that further communication effort has to be launched by ENISA and partner agencies in Member States in order to further promote and get support on standardisation work. For example, whilst the ISO 270xx family is often cited, the other work done or in progress is clearly not well known.

5.1 Overview

The questions are grouped as follows:

- Standardisation awareness
  - The aim here is to directly address article 14(2) and article 16(2) and to drive the answers towards the intent of article 19 to support standardisation and the deployment/acceptance of open international standards at the core of the NIS Directive implementation
- Organisation and authority
  - These questions are intended to ensure that Member States have the relevant structures in place in order to manage the NIS requirements and to distinguish the implementation phase from the operational phase
- Computer Security Incident Response Team (CSIRT)
  - These questions address how CSIRTs interoperate (ideally focussing the answers on common standards)

5.2 Standardisation awareness questions

NUMBER	QUESTION	PRO-FORMA ANSWER FOR GUIDANCE
1	How does the MS ensure that operators of essential services have taken measures to prevent and minimise the impact of incidents affecting the security of their network and information systems?	
1a	Using International standards and guidelines published by a recognised European Standards Body (i.e. CEN/CENELEC/ETSI)	Please identify the list of standards
1b	Using recognised standards from other standards development organisations and publishers (e.g. ITU-T, IETF, ISO, IEC	Please identify the list of standards, e.g. ISO 27001, ISO 27018
1c	Using industry standards agreed by specific industrial sectors	Please identify the list of standards
1d	Independent OES assessment by market regulator	Provide details of MS assessment scheme
1e	Guidance and recommendations provided by the Member State	Provide copies of MS guidance
1f	Other	Freeform text expected
2	How does the MS ensure that providers of digital services (as defined in Annex III of NISD) have taken measures to prevent and minimise the impact of incidents affecting the security of their network and information systems?	
2a	Using International standards and guidelines published by a recognised European Standards Body (i.e. CEN/CENELEC/ETSI)	Please identify the list of standards
2b	Using recognised standards from other standards development organisations and publishers (e.g. ITU-T, IETF, ISO, IEC	Please identify the list of standards, e.g. ISO 27001, ISO 27018
2c	Using industry standards agreed by specific industrial sectors	Please identify the list of standards

2d	Independent OES assessment by market regulator	Provide details of MS assessment scheme
2e	Guidance and recommendations provided by the Member State	Provide copies of MS guidance
2f	Other	Freeform text expected

5.3 Organisation and Authority questions

NUMBER	QUESTION	PRO-FORMA ANSWER FOR GUIDANCE
3	Do you have a nominated single point of contact for the implementation of the NISD?	YES/NO If yes, identify how it can be contacted, else indicate when this will be provided Establishment phase
4	Have you identified a single point of contact for the management of the NISD once it is established in national law and practice?	YES/NO If yes, identify how this is contacted, else indicate when this will be provided Operational phase
5	Please identify for your MS the national competent authorities for matters falling under the remit of the NISD For both establishment and operational phases	List of contact points for each DSP under Annex III of NISD, and OES under Annex II of NISD
6	How does the MS ensure notification of OES or DSP status under the NISD?	Freeform text Official notification in some MS
7	What criteria are used to determine OES or DSP status?	Metrics under national or EU agreement Implementing act will do this for the DSP case
10	Is the relevant entity of the MS aware of and registered to the co-operation group for NIS?	YES/NO

		Identify the coordinates of the co-operation group (e.g. the secretary of the group)
10a	If yes, are you an active participant in the cooperation group, and please provide a link to those responsible for that participation.	
11	In addition to the aforementioned co-operation group does the MS participate in any bilateral international cooperation activities within the scope of NISD?	YES/NO
11a	If yes please identify the scope and partners of each relevant cooperation activity	
12	Is there any implementation policy control and what are the sanctions that may be applied by the MS ?	There is a requirement for MS to provide means to manage NISD failures. MS should identify the means for policing the system. Financial sanctions? Withdraw authorisation to operate and removal of means to access the service?

5.4 CSIRT questions

NUMBER	QUESTION	PRO-FORMA ANSWER FOR GUIDANCE
13	Can you (the MS) identify the means by which CSIRTs share data?	Suggestion is that should be by use of a standard Examples include ETSI ISG ISI specifications, STIX, OASIS
14	Can you (the MS) identify the means by which OESs and DSPs share data with CSIRTs?	Suggestion is that should be by use of a standard Examples include ETSI ISG ISI specifications, STIX, OASIS

5.5 Summary of existing security standards in support of NISD

5.5.1 ETSI specifications

STANDARD	AREA
Doc. Nb. TR 103 331 Ver. 1.1.1 Ref. DTR/CYBER-0009 Technical Body: CYBER	CYBER; Structured threat information sharing
Doc. Nb. TR 103 306 Ver. 1.2.1 Ref. RTR/CYBER-0026 Technical Body: CYBER	CYBER; Global Cyber Security Ecosystem
Doc. Nb. TR 103 305-4 Ver. 1.1.1 Ref. DTR/CYBER-0012-4 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms CSC Facilitation Mechanisms
Doc. Nb. TR 103 305-3 Ver. 1.1.1 Ref. DTR/CYBER-0012-3 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations CSC Service Sector Implementations
Doc. Nb. TR 103 305-2 Ver. 1.1.1 Ref. DTR/CYBER-0012-2 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing CSC Measurement and auditing
Doc. Nb. TR 103 305-1 Ver. 2.1.1 Ref. RTR/CYBER-0012-1 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls Critical Security Controls for Effective Cyber Defence
Doc. Nb. TR 103 303 Ver. 1.1.1 Ref. DTR/CYBER-0001 Technical Body: CYBER	CYBER; Protection measures for ICT in the context of Critical Infrastructure Security of ICT in CI

5.5.2 ISO Specifications

STANDARD	AREA
ISO/IEC 27000	Information security management systems - Overview and Vocabulary
ISO/IEC 27001	Information security management systems – Requirements
ISO/IEC 27002	Code of practice for information security controls.

ISO/IEC 27005	Information security risk management
ISO/IEC 27007	Information security management systems - auditor guidelines
ISO/IEC 27008	Guidelines for auditors on ISMS controls
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements
ISO/IEC 27033	Network security
ISO/IEC 27034	Application security
ISO/IEC 27035	Information security incident management
ISO/IEC 27044	Guidelines for Security Information and Event Management SIEM

6. Analysis of results

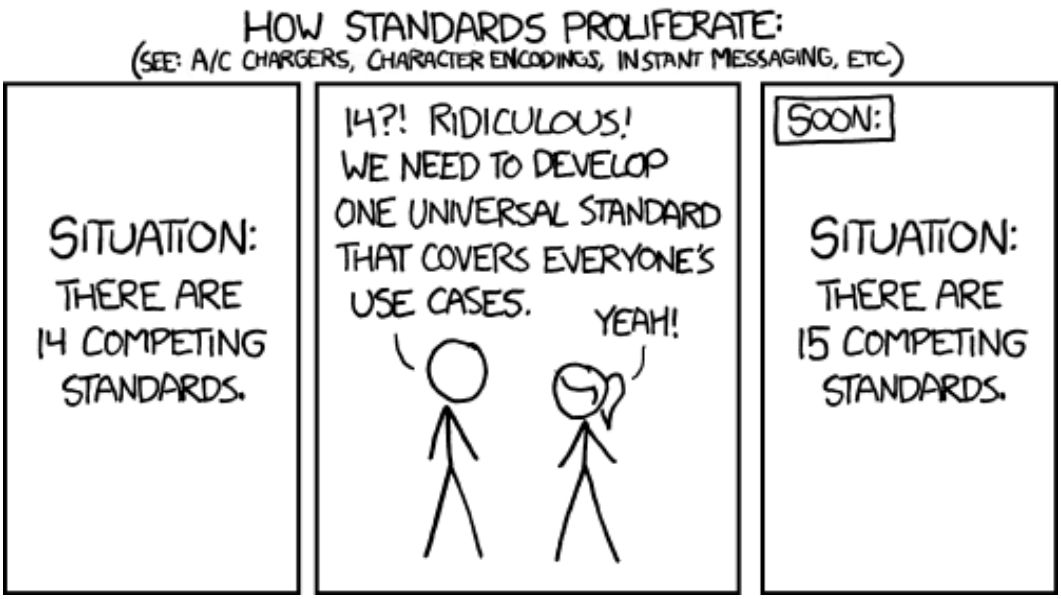
As noted in section 5 a series of questions have been raised the aim of which has been to directly address article 14(2) and article 16(2) and to drive the answers towards the intent of article 19 to support standardisation and the deployment/acceptance of open international standards at the core of the NISD implementation. The results, however, of the questionnaire are not conclusive.

6.1 General observations

The content of the responses to the questionnaire does not allow to identify if the Member States perceive the existence of a gap in available standardisation. However, the content, and general lack of cohesion amongst Member States suggests that there is insufficient guidance from the specialists in the field (e.g. national normalization institutes, European institutions etc.), on which of the many standards available are to be used.

NOTE: For the purposes of this report the SDOs are not considered as experts in the field as their primary purpose is to prepare standards. As a direct consequence of their business model standards will overlap and compete. For example, in the world of security there are a large number of 128-bit block cipher algorithms, all of which perform essentially the same function of maintaining confidentiality of data, but cannot interoperate. Which is the correct one to choose? If the policy level **standard** is to use 128-bit encryption additional guidance is required to select algorithm and mode of operation. This is a secondary level of standardisation and may in turn require a tertiary level to be invoked and specified.

An impression of the standards gap identified in the responses is typified in the cartoon:



Drawing courtesy of XKCD[10]

In layman's terms it is clear that there are lots of standards but it is not clear which to use. Adding a new standard for a perceived gap results in another standard, whereas an impression of the lack of simple

[10] https://xkcd.com/

answers to this part of the questionnaire may rather be that an authority should state which standard to use for which part of NIS Directive compliance. It is noted that this is the direction taken by ETSI in TR 103 465[11].

6.2 Observations related to ESOs

6.2.1 ETSI

The following set of observations have been noted and published by ETSI in TR 103 456:

- There is basically no cyber security standards gap
  - There are several standards available, perhaps one could note, even too many, and many are not actionable or particularly useful
  - The real need is to converge toward useful, practical, actionable, interoperable sets of standards
  - Standards that are not freely available on-line, constantly evolving, and well-versioned have diminished value and represent cyber security impediments
  - TC CYBER sought to discover the ecosystem and focus on identifying the most effective platforms and specifications and that have the broadest industry support
- There are no simple or easy cyber security solutions
  - Cybersecurity as such is not achievable given the enormity of constantly evolving vulnerabilities
  - What you can do is implement sets of defence measures (Critical Security Controls), and threat exchange measures (STIX ensemble or equivalent) that can reduce the risks
  - Whilst encryption has positive benefits, there are adverse effects of end-to-end encryption which need urgent attention
  - Rapidly evolving new industry platforms such as NFV-SDN/5G and quantum computing need urgent attention to control the cyber security risks

The suite of recommendations made in TR 103 456 are the following:

- Operators of essential services
  - The operators of Essential Services should be encouraged to adopt common interoperable platforms such as STIX or equivalent for cyber threat intelligence sharing and the Critical Security Controls for Effective Cyber Defence, as well as critical capabilities such as the Middlebox Security Protocol to deal with the mounting challenges of encrypted traffic
- Digital service providers
  - Digital Service Provider should be encouraged to adopt common interoperable platforms such as STIX or equivalent for cyber threat intelligence sharing and the Critical Security Controls for Effective Cyber Defence, as well as critical capabilities such as the Middlebox Security Protocol to deal with the mounting challenges of encrypted traffic
- Facilitative mechanisms for network and information security
  - In general, the use of the facilitative mechanisms described in Part 4 of TR 103 305, “CYBER; Critical Security Controls for Effective Cyber Defence,” including privacy impact assessments, mappings to national cyber security frameworks, cyber hygiene programmes, and governance strategies, can significantly enhance network and information security.

[11] ETSI Technical Report: Implementation of the Network and Information Security (NIS) Directive
http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

6.2.2 CEN and ISO

- Operators of essential services
  - ISO/IEC 2700x family offers security requirements in order to achieve good practice level and provide information system management evaluation
- Digital service providers
  - ISO/IEC 2700x can be recommended in order to achieve good practice level and provide information system management evaluation
- Facilitative mechanisms for network and information security
  - ISO/IEC 27044 offers standards on security event format standard consistent with the one developed by ISI group in ETSI

7. Conclusions

7.1 General summary and review

It is reasonably straightforward to see that all Member States have a high degree of understanding of the NIS Directive and their responsibilities in implementing it; this can be evidenced through the degree of transposition of the directive across the Member States and the ensuing preparations at Member State level. What is less clear is what role standards can further have in the NIS Directive implementation process.

Most Member States have a clear understanding of their role at national and regional level. Those Member States with a well-established security agency that functions within their public administration, appear to have integrated the responsibilities emanating from the NIS Directive (and similar EU initiatives) with their existing agencies competences and have done so with only minor updates in the legal framework and operating procedures. As there are already well established paths for cross border co-operation in security, the obligations of the NIS Directive typically take advantage of them.

What may be the most apparent is the absence of a specific standard to define each Operator of Essential Services (OES) and Digital Service Provider (DSP) but even without such a standard, or at least a standard for the metrics to allow their identification, each Member State has developed a method to identify them. However at a later stage and as the internal market integration progresses, further consolidation in this area is foreseeable.

7.2 How to enhance the uptake of standards at MS?

There is insufficient information in the responses to conclude that there is a lack of knowledge of standards. This suggests however that if an appropriate standard is available, it will be adopted. For example, even though the ISO27000 series of standards are in the form of broad guidance, there is a well-established eco-system that addresses their implementation. The preconditions for uptake of a standard are well known:

- Existence of the standard that is seen as essential by their stakeholders
- A support infrastructure to oversee the implementation and maintenance of the standard on behalf of the stakeholders

In the context of the NIS Directive there has been no clear requirement expressed by the stakeholders to define additional standards. It may be that in time to come such requirements may be expressed and the support infrastructure be built. A shortcut that may be envisaged is to provide a specific support infrastructure. Such an infrastructure should be able to specify exactly which standards Member States need to implement in support of the NIS Directive and for them to task the ESOs to develop specific standards.

7.3 What are the limiting factors and how to mitigate them?

A major concern is that the NIS Directive domain, and compliance to the NIS Directive requirements, is often perceived as a purely national prerogative. Where international, cross-border, information sharing is required, this has been perceived as in the domain of existing CSIRT relationships used for reporting security incidents and not directly as an element of NIS Directive compliance.

With regards to understanding of the role of standards, as they apply to NIS Directive compliance, there is somewhat limited awareness. In part this is implied from the responses indicating that from a Member

State point of view NIS Directive is mostly a policy issue dealing with requirements that are placed on Operators of Essential Services (OES) and Providers of Digital Services (PDS). Once the policy is established, and under active management, the Member States may make a reasonable claim that they have complied to NIS Directive. However, at this point the OES and PDS entities may be trans-national and their best interests in complying to the delegated elements of NIS Directive may be met by very specific standards. In the first part of this process, where policy and process management functions apply, it is the set of security management standards that are both most deployed and for which there is most awareness, i.e. the ISO 27000 series of standards and guidelines.

At the operational level there is very little specified for standards-based NIS Directive compliance and this is one area where ETSI, for example, has made some contributions. However, there are no mandates at either national or European level to guide this activity at the implementation level. Given the importance standards however it is important to aim at specific technical levels of knowledge and understanding that can be attained through proper training.

In light of the above, the following solutions are recommended to mitigate the lack of overall awareness and trainings on the role of standards in NIS Directive compliance and to encourage wide deployment of common security platforms in the OES and PDS entities:

- Training initiatives by the European Commission and ENISA through workshops for Member States' relevant agencies
- Promotion of new work items in the European SDOs for some areas (e.g. criteria for defining OES / DSP) or the adoption of appropriate standards in Europe where existing (for example information exchange, where several mature efforts already are in place, like STIX[12])
- Repeat the information gathering as performed within the elaboration of this study after an adequate interval of time

7.4 Additional considerations

A set of standardization requests identifying those standards which may be used to state NIS Directive compliance (when conformed with) should be drafted. To this aim, the expertise pool of the European Standardization Organizations could be used, when needed.

[12] https://stixproject.github.io/

ENISA

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

Athens Office

1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

TP-02-18-011-EN-N

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

ISBN: 978-92-9204-249-3,
DOI 10.2824/176720