ETSI TR 103 866 V1.1.1 (2023-02)

TECHNICAL REPORT

Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls

Reference

DTR/CYBER-0080

Keywords

critical infrastructure, cyber-defence,
cyber security, risk management

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The European Union Revised Network and Information Security (NIS2) Directive aims to minimize security risks and enhance resilience of identified public and private entities in Member countries through implementation of sets of horizontal best practice requirements to be applied to "essential and important entities" in scope of the Directive and supply chains, under the surveillance of responsible authorities in Member States [i.1]. The requirements consist of a combination of technical and organizational controls designed to instantiate a measurable level of security risk combined with the detection and structured exchange of threat information among Computer Security Incident Response Teams (CSIRT). The NIS2 Directive also gives specific responsibilities to Member States, notably in the preparation of national cybersecurity strategies and related policies.

The present document suggests that most of the technical objectives and provisions of NIS2 Directive can benefit from application of Critical Security Control Safeguards and Facilitation Mechanisms, including the Privacy Enhancements (Annex A) ETSI TR 103 305-1 [i.9], ETSI TR 103 305-3 [i.10], ETSI TR 103 305-4 [i.11] and ETSI TR 103 305-5 [i.12], and from other described specifications, combined with the MISP-Project tools and methods [i.18], [i.19]. The use of OSCAL, combined with the Control mapping mechanisms additionally provides accommodations for the different identified entities to meet definitive tailored implementations within their sectors or mandated by national authorities within the Union and worldwide. The Control Workbench mechanism can help with the complexity and enables each implementation to select relevant jurisdiction, sector/national, context and risk variables to obtain specific Control Safeguards that meet the Directive requirements. The NIS2 includes potential European cybersecurity certification schemes which are not addressed in the present document.

The use of OSCAL as an essential means for interoperability and openness among all the operational and regulatory standards faced by network service providers under requirements such as NIS2, as well as automated continuous compliance, was explored by the European Union's Horizon 2020 MEDINA Project [i.20] and [i.21]. Embracing the use of a Zero Trust Security Model by EU Members and affected entities is described [i.35] (see annex C, bibliography).

Introduction

In December 2015, the European Parliament and Council adopted a Directive "*concerning measures to ensure a high common level of network and information security across the Union*" (NIS1) [i.3]. That Directive advanced measures similar to those being pursued worldwide. ETSI responded by analysing the Directive, collaborating with ENISA, holding a Security Workshop session, and pursuing several related work items that were aggregated in ETSI TR 103 456 [i.8] recommending how best to implement the measures (see annex C, bibliography).

Five years later in 2020, the European Commission proposed a revision to the NIS Directive (NIS2). The co-legislators reached a provisional agreement on the text on 13 May 2022. The EU Parliament and the Council adopted the final text in November 2022. "*By 21 months after the date of entry into force of the Directive, Member States shall adopt and publish the measures necessary to comply with this Directive*" [i.1] and [i.7]. Those measures are applied the following day.

The present document responds to the NIS2 Directive, based on the previous ETSI TR 103 456 [i.8] contributed in support of the initial NIS Directive. The revised Directive is similar to NIS1, but Risk Management measures were made explicit and many changes instituted to have far-reaching global effects. The Essential and Important Entities were significantly expanded. Those entities are required to implement risk management measures and exchange incident and threat information. Supply chain and vulnerability exchange measures were added. For ICT, entities under the regime were significantly expanded to include cloud virtualization, encryption, 5G operators, among others. It is expected that the wider applicability of the new Directive will foster enhanced cooperation and experience sharing in implementing cybersecurity best practices across vertical industry sectors. Especially significantly, the jurisdiction and territorial reach of the Directive is significantly expanded under Art. 26 to an array of entities providing services in Europe and subject to the provisions of the Directive.

Certain sets of ETSI work undertaken over the past several years with related ETSI publications are highly relevant and applicable to NIS2. This work notably includes:

1) substantial significant evolution of the Critical Security Controls through global communities of users and tool vendors;

2) the creation of numerous facilitation mechanisms including risk management measures and coded hardened images for all major cloud data centre operating systems; and

3) the customized adaptation of the Controls to meet the specialized requirements of many different industry sectors and national authorities - for which definitive, structured mappings have become created.

The creation of the Controls Workbench as a means to deal with the complexity, enables each implementation to select all the relevant jurisdiction, sector/national, context, and risk variables to facilitate the Directive requirements and identify specific Control Safeguards. The Critical Security Controls also implement:

1) the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework which enables expression of any attack type as a set of attack techniques, known as attack patterns and more definitive risk management measures; and

2) the Open Security Controls Assessment Language (OSCAL) which facilitates interoperability among Control frameworks and Safeguards [i.11].

Notably, the ETSI Critical Security Controls are also acknowledged by the ITU-T in its basic global intergovernmental standard for cybersecurity information exchange a global technique "*to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks…reflect[ing] the combined knowledge of actual attacks and effective defences*" [i.14]. It is envisioned that the ETSI Critical Security Controls can be considered under Arts. 21 and 25 of the NIS2 Directive concerning international standards.

Given the regulatory nature of the Directive and wide applicability to providers, the on-line availability of continually evolved, on-line standards specifications, guidance, playbooks, structured information, and other materials widely used and developed by industry will be essential. The Critical Security Controls and associated materials meet this requirement. However, although the Controls can provide a foundation for compliance, additional mechanisms for the structured exchange of information, including vulnerability reporting, certification, and supply chain cyber resilience are needed.

The present document is structured to identify and articulate the security measures that are included in the NIS2 Directive in clause 4, below, and provides mappings to the Critical Security Controls and Facilitation Mechanisms which are applied to the various Directive Articles and Annexes in clause 5. References to relevant ETSI cybersecurity security standards are also provided.

The NIS2 Directive applies to trust services regulated under Regulation (EU) No. 910/2014 [i.2] (commonly referred to as eIDAS). Thus, the existing ETSI European Standards and Technical Specifications for Electronic Signatures and Infrastructures which apply to trust services under eIDAS need to take into account any requirements for NIS2, not already covered by eIDAS.

It should be noted that the proposed "*Directive of the European Parliament and of the Council on the Resilience of Critical Entities*" [i.6] is implemented in part by the NIS2 Directive, and the annexes identifying essential and important entities are aligned.

The NIS2 Directive omits treatment of the recent emergence of a Zero Trust (ZT) Security Model. The present document describes the introduction of a ZT Model in the context of the NIS2 Directive provisions by EU Members and affected entities.

1 Scope

The present document describes an ensemble of cyber security specifications and other materials, especially the ETSI Critical Security Controls in ETSI TR 103 305-1 [i.9] that can be applied to support NIS2 Directive [i.1] requirements by EU Member States and affected essential and important entities.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

[i.2] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.3] Directive (EU) 2016/1148 of The European Parliament and of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[i.4] Resolution (EC) 13084/1/20, Council Resolution on Encryption - Security through encryption and security despite encryption.

NOTE: Available at https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf.

[i.5] Recommendation 2003/361/EC, Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance).

[i.6] 2020/0365 (COD), COM(2020) 829 Final: "Proposal for a directive of the European Parliament and of the Council on the resilience of critical entities".

NOTE: Available at https://data.consilium.europa.eu/doc/document/ST-12414-2022-INIT/en/pdf.

[i.7] Consolidated text: Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) (Text with EEA relevance) Text with EEA relevance.

[i.8] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.9] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.10] ETSI TR 103 305-3: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations".

[i.11] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.12] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.13] ETSI TR 103 331: "Cyber Security (CYBER); Structured threat information sharing".

[i.14] Recommendation ITU-T X.1500, Amd. 12: "Overview of cybersecurity information exchange" (03/2018).

[i.15] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance).

[i.16] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.17] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.18] MISP Threat Sharing.

NOTE: Available at https://www.misp-project.org/.

[i.19] ENISA: "Orchestration of CSIRT Tools", December 2019.

NOTE: Available at: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/orchestration-of-csirt-tools-1/orchestration-of-csirt-tools-tools-analyst.pdf.

[i.20] ETSI Security Conference 2022, H2020 Project MEDINA.

NOTE: Available at https://docbox.etsi.org/Workshop/2022/10ETSISECURITYCONFERENCE/10_SECURITY_RESEARCH/FABASOFT_FANTA.pdf.

[i.21] NIST: "OSCAL: the Open Security Controls Assessment Language".

NOTE: Available at: https://pages.nist.gov/OSCAL/.

[i.22] ETSI GR ETI 006: "Encrypted Traffic Integration (ETI); Implementation of the EU Council Resolution on Encryption".

[i.23] OASIS CACAO Security Playbooks Version 1.0.

NOTE: Available at: https://docs.oasis-open.org/cacao/security-playbooks/v1.0/cs02/security-playbooks-v1.0-cs02.html.

[i.24] FIRST CSIRT Services Framework.

NOTE: Available at https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1.

[i.25] FIRST Traffic Light Protocol (TLP).

NOTE: Available at https://www.first.org/tlp/.

[i.26] FIRST: "Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure".

NOTE: Available at https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1.

[i.27] FIRST: "Common Vulnerability Scoring System (CVSS) v3.1".

NOTE: Available at https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[i.28] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.29] ISO/IEC 29147: "Information technology -- Security techniques -- Vulnerability disclosure".

[i.30] ISO/IEC 30111: "Information technology -- Security techniques -- Vulnerability handling processes".

[i.31] ISO/IEC TR 5895: "Cybersecurity -- Multi-party coordinated vulnerability disclosure and handling".

[i.32] 2022/0272 (COD), COM(2022) 454 final: "Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020".

[i.33] OASIS Common Alerting Protocol Version 1.2.

NOTE: Available at https://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html.

[i.34] NIST Special Publication 800-207: "Zero Trust Architecture", August 2020.

NOTE: Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[i.35] National Security Agency, PP-21-0191: "Embracing a Zero Trust Security Model", February 2021.

NOTE: Available at https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.

[i.36] 2020/0266 (COD), COM(2020) 595 final: "Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014".

[i.37] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance).

[i.38] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) (Text with EEA relevance).

[i.39] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (Text with EEA relevance).

[i.40] 2022/0021 (COD), COM(2022) 32 final: "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 1025/2012 as regards the decisions of European standardisation organisations concerning European standards and European standardisation deliverables".

[i.41] 2021/0136 (COD), COM(2021) 281 final: "Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity".

[i.42] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

[i.43] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance).

[i.44] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in the NIS Directive [i.1], including those referenced in EU legislations [i.7], [i.15], [i.37], [i.38], [i.39], [i.40], [i.41], [i.43], [i.44] and the following apply.

NOTE: It should be noted that the NIS2 created definitions of terms that are nuanced and may vary with those used elsewhere. Because the present document concerns the implementation of the NIS2 Directive, it builds on the definitions provided by NIS2 on key terms.

controls workbench: tool to inform users and enterprises exactly which Control Safeguards to implement to achieve desired or required levels of security and risk

NOTE: As defined in [i.11].

critical security Control: prioritized set of actions to protect information assets from threats, using technical or procedural Safeguards

NOTE: As defined in [i.9].

cybersecurity: activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats

NOTE: As defined in [i.1].

cyber threat: any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons

NOTE: As defined in [i.1].

impact: harm that may be suffered when a threat compromises an information asset

incident: any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

NOTE: As defined in [i.1].

incident handling: all actions and procedures aiming at prevention, detection, analysis, and containment of, response to, and recovery from an incident

NOTE: As defined in [i.1].

large-scale cybersecurity incident: incident whose disruption exceeds a Member State's capacity to respond to it or with a significant impact on at least two Member States

NOTE: As defined in [i.1].

near miss: event that could have compromised the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems, but was successfully prevented from transpiring or did not materialize

NOTE: As defined in [i.1].

risk: potential for loss or disruption caused by an incident and is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of that incident

NOTE: As defined in [i.1].

risk analysis: process of estimating the likelihood that an event will create an impact and includes as necessary components, the foreseeability of a threat, the expected effectiveness of Control Safeguards, and an evaluated result

risk assessment: comprehensive project that evaluates the potential for harm to occur within a scope of information assets, controls, and threats

risk management: process for analysing, mitigating, overseeing, and reducing risk

safeguard: technical or procedural protections that prevent or detect threats against information assets that are implementations of a Critical Security Control

NOTE: As defined in [i.9].

security of network and information systems: ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or of the services offered by, or accessible via, those network and information systems

NOTE: As defined in [i.1].

security playbook: playbook is a workflow for security orchestration containing a set of steps to be performed based on a logical process and may be triggered by an automated or manual event or observation, and provides guidance on how to address a certain security event, incident, problem, attack, or compromise

NOTE: As defined in [i.23].

significant cyber threat: cyber threat which, based on its technical characteristics, can be assumed to have the potential to severely impact the network and information systems of an entity or its users by causing considerable material or non-material losses

NOTE: As defined in [i.1].

vulnerability: weakness, susceptibility or flaw of ICT products or ICT services that can be exploited by a cyber threat

NOTE: As defined in [i.1].

zero trust security model: security model consisting of a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries and eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses

NOTE: As defined in [i.35].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
Art.	Article
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
CAP	Common Alerting Protocol
CERT	Computer Emergency Response Team
CRA	Cyber Resilience Act
CSC	Critical Security Controls
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVD	Coordinated Vulnerability Disclosure
CyCLONe	Cyber Crisis Liaison Organisation Network
DMARC	Domain-based Message Authentication, Reporting & Conformanc