ETSI TR 104 168 V1.1.1 (2025-09)

TECHNICAL REPORT

Cyber Security (CYBER);
Critical Security Controls for
Network and Information Security Directive 2 (NIS2)

Reference
DTR/CYBER-00164

Keywords
cyber security

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 the ETSI Search & Browse Standards application.

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 on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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 present document provides a mapping of the Critical Security Controls [i.10] to support NIS2 Directive provisions.

Introduction

The present document is one of several ETSI publications [i.8], [i.11], [i.12], [i.13] and [i.14] directed at supporting the EU NIS2 Directive and related legislative instruments [i.1], [i.2], [i.3], [i.4], [i.5], [i.6] and [i.7].

1 Scope

The present document item provides a mapping between the Critical Security Controls and NIS2 provisions.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[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).

[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".

[i.5] Recommendation 2003/361/EC: "Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises".

[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".

[i.7] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

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

[i.9] Center for Internet Security: "CIS Controls v8.1, Mapping to NIS2 Directive 2022/2555".

[i.10] ETSI TS 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[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 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.14] ETSI TS 103 992: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

COTS	Commercial Off The Shelf
CSC	Critical Security Controls
CSF	Computer Security Framework
DHCP	Dynamic Host Configuration Protocol
ERM	Enterprise Risk Management
IG1	Implementation Group 1
IG2	Implementation Group 2
IG3	Implementation Group 3
NIS2	Network and Information Security Directive 2
SSO	Single Sign-On

4 Applying the Critical Security Controls for effective implementation of the NIS2 Directive

4.1 Methodology and Use

Methodology

The methodology used to create the mapping can be useful to anyone attempting to understand the relationships between the Critical Security Controls and NIS2. The overall goal for Control mappings is to be as specific as possible, leaning towards under-mapping versus over-mapping. The general strategy used is to identify all of the aspects within a control and attempt to discern if both items state the same thing. For instance:

Control 6.1 - Establish an Access Granting Process

Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user. For a defensive mitigation to map to this CSC Safeguard it is required by NIS2 to have at least one of the following:

- A clearly documented process, covering both new employees and changes in access.
- All relevant enterprise access control is required by NIS2 to be covered under this process, there can be no separation where different teams control access to different assets.

- Automated tools are ideally used, such as a SSO provider or routing access control through a directory service.
- The same process is followed every time a user's rights change, so a user never amasses greater rights access without documentation.

If the two concepts are effectively equal, they are mapped with the relationship "equivalent". If they are not equal but still related, the exact type of relationship between two defensive mitigations can be further explored. The relationships can be further analysed to understand how similar or different the two defensive mitigations are. The relationship column will contain one of four possible values:

- Equivalent: The defensive mitigation contains the exact same security concept as the Control.
- Superset: The Control is partially or mostly related to the defensive mitigation in question, but the Control is broader in concept.
- Subset: The Safeguard is partially or mostly related yet is still subsumed within the defensive mitigation. The defensive mitigation in question is broader in concept than the Control.
- No relationship: This will be represented by a blank cell.

The relationships should be read from left to right, like a sentence. Control Safeguard X is Equivalent to this < >.

EXAMPLES: Safeguard 16.8 "Separate Production and Non-Production Systems" is EQUIVALENT to NIST CSF PR.DS-7 "The development and testing environment(s) are separate from the production environment".

Safeguard 3.5 "Securely Dispose of Data" is a SUBSET of NIST CSF PR.DS-3 "Assets are formally managed throughout removal, transfers, and disposition".

The Critical Security Controls are written with certain principles in mind, such as only having one ask per Safeguard. This means many of the mapping targets are written in a way that contain multiple Safeguards within the same defensive mitigation, so the relationship can often be "Subset".

Mappings are available from a variety of sources online, and different individuals may make their own decisions on the type of relationship. Critical Security Controls mappings are intended to be as objective as possible, and improvements are encouraged.

Use

The clauses in the Critical Security Controls concerning delineation of Asset Types, Security Functions, and Implementation Groups apply to the mappings below. For reference, these delineations are repeated in part here.

Asset Types are shown in Figure 4.1-1.