ETSI TS 103 992 V1.1.1 (2024-05)

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

Reference
DTS/CYBER-00113

Keywords
cyber security; cyber-defence; cybersecurity

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

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 Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 [i.1] aims to minimize security risks and enhance resilience of identified public and private entities in Member States through implementation of sets of horizontal best-practice requirements. These requirements are to be applied to "essential and important entities" in scope of the NIS2 Directive [i.1] and supply chains, under the surveillance of responsible authorities in Member States. 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 (CSIRTs). The NIS2 Directive [i.1] also provides specific responsibilities to Member States, notably in the preparation of national cybersecurity strategies and related policies.

The present document demonstrates that most of the technical objectives and provisions of the NIS2 Directive [i.1] can benefit from application of, amongst other described specifications, Critical Security Control Safeguards and Facilitation Mechanisms, including Privacy Enhancements, specified in:

- ETSI TR 103 305-1 [i.9]

- ETSI TR 103 305-3 [i.10]
- ETSI TR 103 305-4 [i.11]
- ETSI TR 103 305-5 [i.12]

Further benefits can be obtained by application of the MISP-Project tools and methods [i.18], [i.19]. The use of OSCAL [i.21], combined with the Control mapping mechanisms, provides additional accommodations for the different identified entities to meet definitive tailored implementations within their sectors or mandated by national authorities within the European 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 requirements of the NIS2 Directive [i.1]. The NIS2 Directive [i.1] includes potential European cybersecurity certification schemes which are not addressed in the present document.

The use of OSCAL [i.21] as an essential means for interoperability and openness among all the operational and regulatory standards faced by network service providers under NIS2 Directive [i.1] requirements, as well as automated continuous compliance, was explored by the European Union's Horizon 2020 MEDINA Project [i.20]. Embracing the use of a Zero Trust Security Model by EU Members and affected entities is described in [i.34], [i.35] and annex B.

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 B).

In 2020, the European Commission proposed a revision to the NIS Directive, named the "NIS2 Directive" [i.1]. The co-legislators reached a provisional agreement on the text on 13 May 2022 and the EU Parliament and the Council adopted the final text in November 2022 [i.6], which was then applied the following day.

The present document responds to the NIS2 Directive [i.1], based on the previous ETSI TR 103 456 [i.8] developed in support of the initial NIS Directive. The revised Directive [i.1] is similar to NIS1, but Risk Management measures were made explicit and many changes were 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 also added. For ICT, entities under the regime were significantly expanded to include cloud virtualization, encryption, 5G mobile network operators, among others. It is expected that the wider applicability of the NIS2 Directive [i.1] 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 NIS2 Directive [i.1] is significantly expanded under Art. 26 to an array of entities providing services in Europe and subject to the provisions of the Directive.

Recent ETSI standardization work and publications are highly relevant and applicable to the NIS2 Directive [i1], which include:

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 NIS2 Directive [i.1] requirements and identify specific Control Safeguards. The Critical Security Controls also implement:

1) the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework (see [i.45]), 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) [i.21], which facilitates interoperability among Control frameworks and Safeguards [i.11].

Notably, the ETSI Critical Security Controls are also acknowledged by the ITU-T in Recommendation X.1500 [i.14] (its basic global intergovernmental standard for cybersecurity information exchange) as 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*". It is envisioned that the ETSI Critical Security Controls can be considered under Arts. 21 and 25 of the NIS2 Directive [i.1] concerning international standards.

Given the regulatory nature of the NIS2 Directive [i.1] 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 [i.1] in clause 4 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 standards are also provided.

The NIS2 Directive [i.1] 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 that apply to trust services under eIDAS need to take into account any requirements for the NIS2 Directive [i.1] 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 [i.1], and the annexes identifying essential and important entities are aligned.

The NIS2 Directive [i.1] omits treatment of the recent emergence of a Zero Trust (ZT) Security Model (see [i.34], [i.35] and Annex B). The present document describes the introduction of a ZT Model in the context of the NIS2 Directive [i.1] 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.

The present document also considers, and makes reference to, the work being done by ETSI ESI on Trust Services.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

Not applicable.

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 1: 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.

[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".

[i.7] 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 Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 3: Internet of Things Sector".

[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; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.18] MISP Threat Sharing.

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

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

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

[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.

[i.24] FIRST: "CSIRT Services Framework".

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

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

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

[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.

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

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

[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.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.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.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).

[i.45] MITRE ATT&CK®.

[i.46] EU Council Resolution on Encryption Security through encryption and security despite encryption, adopted 14 December 2020.

[i.47] ETSI TR 103 954: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Mobile Communications Sector".

[i.48] ETSI TR 103 959: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud Sector".

[i.49] NIST Special Publication 800-160, Volume 2, Revision 1: "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach", November 2022.

[i.50] IEC 62443 series: "Industrial communication networks - Network and system security".

[i.51] ISO/IEC 27000 family: "Information security management".

[i.52] ETSI GR ETI 002: "Encrypted Traffic Integration (ETI); Requirements definition and analysis".

[i.53] ANSSI: "Le modèle Zero Trust".

[i.54] BSI: "Bundesinnenministerium: Zero-Trust-Architektur wird angestrebt".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in the NIS2 Directive [i.1] 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: 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
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information (National Agency for the Security of Information Systems) (France)
Art.	Article
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) (Germany)
CAP	Common Alerting Protocol
CERT	Computer Emergency Response Team
CISA	Cybersecurity and Infrastructure Security Agency (USA)
CSC	Critical Security Controls
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CVD	Coordinated Vulnerability Disclosure
CVSS	Common Vulnerability Scoring System
CyCLONe	Cyber Crisis Liaison Organization Network
DMARC	Domain-based Message Authentication, Reporting & Conformance
EEA	European Economic Area

EEC	European Economic Community
eIDAS	electronic Identification, Authentication and Trust Services
ENISA	European union agency for Network and Information Security
ESI	Electronic Signatures and Infrastructures
ETI	Encrypted Traffic Integration
EU	European Union
EUCS	European Cybersecurity Certification Scheme for Cloud Service
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation [i.42]
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Centre
ISG	Industry Specification Group
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union Telecommunications Standardization Sector
MANRS	Mutually Agreed Norms for Routing Security
MISP	Malware Information Sharing Platform
NCSC	National Cyber Security Centre (UK)
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OSCAL	Open Security Controls Assessment Language
para.	paragraph
PSIRT	Product Security Incident Response Team
SME	Small and Medium Enterprise
TF-CSIRT	Task Force on Computer Security Incident Response Teams
ZT	Zero Trust

4 Measures common to Directive requirements

4.1 Description

The NIS2 Directive [i.1] requires the implementation of cybersecurity measures by different types of stakeholders that are articulated in different contexts in the individual articles and annexes that are identified in clause 5, below. It should be noted that the entities included in the annexes are subject to change under existing and subsequent EU legislative instruments (see [i.15], [i.37] and [i.44]). These measures can be distilled into ten categories that are described below, together with the means for effectively implementing them - largely through the Control Safeguards of the Critical Security Controls and facilitating mechanisms (see [i.9], [i.10] and [i.11]). Several sector-specific implementations are also available (see [i.10], [i.47] and [i.48]). A mapping of the NIS2 Directive [i.1] requirements identified in clause 4 and the Critical Security Control Safeguards [i.9] is provided in Annex A. For information sharing and reporting requirements, as well as reporting vulnerabilities, additional capabilities are needed, for which guidance is provided.

4.2 Exchanging best practices, information sharing, and reporting

The treatment of exchanging best practices, information sharing, and reporting is threaded though most of the Directive provisions and expressly found in the Cooperation Group (Art. 14), and information sharing (Arts. 29 and 30) [i.1].

Exchanging best practices, information sharing, and reporting can be addressed through the use of Critical Security Control Safeguards which establish a prioritized set of actions to protect the assets through the use of technical and procedural Safeguards that are measurable and can establish risk levels. Specific Safeguards for exchanging best practices, information sharing and reporting include:

- Control 4 - Secure Configuration of Enterprise Assets and Software;
- Control 9 - Email and Web Browser Protections;
- Control 14 - Security Awareness and Skills Training;

- Control 16 - Application Software Security;
- Control 17 - Incident Response Management; and
- Control 18 - Penetration Testing.

The implementation group levels include IG1 (SME), IG2 (medium enterprise) and IG3 (large and critical enterprises) [i.9].

The proposed Control safeguards do not address how essential and important entities can find and get in touch with relevant communities to perform information sharing. Forum such as FIRST and TF-CSIRT, national platforms (depending on national policies), and sector specific ISACs can all provide information exchange, be it in the form of physical and online meetings, discussion spaces, and online tools, e.g. for Cyber Threat Intelligence (CTI).

Control 4 consists of twelve Safeguard subsets that describe the procedures and tools at three implementation group security levels to establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications). The different subsets include best practices, information sharing and reporting specifics that will vary by implementation group level, assumed risk, and industry/regulatory requirements.

Control 9 consists of seven Safeguard subsets that improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement. The different Safeguard subsets include best practices, information sharing and reporting specifics that will vary by implementation group level, assumed risk, and industry/regulatory requirements. Also recommended in conjunction with this control is initiating Domain-based Message Authentication, Reporting and Conformance (DMARC) which helps reduce spam and phishing activities. Installing an encryption tool to secure email and communications adds another layer of user and network-based security.

Control 14 consists of nine Safeguard subsets that establish and maintain a security awareness program to influence behaviour among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise. The different Safeguard subsets include best practices that are largely the same except for advanced skill sets appropriate for higher implementation group levels, assumed risk, and industry/regulatory requirements. Control Safeguard Subsets 14.6 and 14.7 that involve training workforce members to recognize potential incidents and verify software patch installations are especially relevant.

Control 16 consists of 14 Safeguard subsets that manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise. The different Safeguard subsets include best practices, information sharing and reporting specifics that will vary by implementation group level, assumed risk, and industry/regulatory requirements.

Control 17 consists of nine Safeguard subsets that establish a program to develop and maintain an incident response capability (e.g. policies, plans, procedures, defined roles, training and communications) to prepare, detect, and quickly respond to an attack. The different Safeguard subsets include best practices, information sharing and reporting specifics that will vary by implementation group level, assumed risk, and industry/regulatory requirements.

Control 18 consists of five Safeguard subsets that test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker. The different Safeguard subsets include best practices, information sharing and reporting specifics that will vary by implementation group level, assumed risk, and industry/regulatory requirements. In addition to the above Control Safeguards, an array of important, continuously-evolving relevant tools are found in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs [i.10] and [i.11]. The Privacy enhancements for each Control Safeguard are also valuable [i.12]. Notably, the Community Defense Model includes the use of playbooks which have emerged as a set of structured steps to be performed based on a logical process and may be triggered by an automated or manual event or observation that provides guidance on how to address a certain security event, incident, problem, attack, or compromise [i.23].

The implementation of NIS2 through cybersecurity controls includes an enormous amount of continuously exchanged structured information, The specific interfaces and protocols used worldwide for the actual structuring and exchanges of the information vary. The principle recommended platforms that are widely used by industry and government for exchanging can be found in ETSI TR 103 331 [i.13]. Of special note for structured threat information sharing is the emergence of MISP as the leading Open Source Threat Intelligence Platform, including an open standard for powering intelligence and information exchange, sharing and modelling among a number of different fields [i.18].

Those fields include cybersecurity intelligence, threat intelligence, financial fraud, vulnerability information, digital forensic and incident response, among others. ENISA promotes the use of MISP and its tools for CSIRT orchestration [i.19]. Therefore, the use of MISP [i.18] is recommended.

The evolution and implementation of CSIRT structured Information sharing practices and standards as well as the exchange of information has been significantly advanced by the Forum of Incident Response and Security Teams (FIRST) and its CSIRT Services Framework, which includes Product Security Incident Response Teams (PSIRTs) in the form of an All Services Frameworks [i.24]. FIRST also maintains the Traffic Light Protocol, which is used as an indicator of confidentiality level in many information sharing scenarios [i.25].

4.3 Addressing cyber threats

The treatment of cyber threats in the NIS2 Directive [i.1] can be found in the following articles:

- Scope (Art. 2);
- national strategies (Art. 7);
- CSIRT tasking (Arts. 10, 11);
- national cooperation (Art. 13);
- Cooperation Group (Art. 14);
- CSIRTs network (Art. 15);
- CyCLONE (Art. 16);
- Risk Management (Art. 21);
- critical supply chains (Art. 22);
- reporting obligations (Art. 23);
- information sharing (Art. 29); and
- voluntary notification (Art. 30).

According to [i.1], a cybersecurity threat refers to 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. Threats can be external or internal, and of human, environmental or technological origin. Human threats can be malicious or non malicious, as well as accidental or intentional. Threat effects can include:

1) destruction, corruption, disclosure, or illegal usage of information;
2) denial of use; and/or
3) elevation of information system privileges.

Cyber threats can be addressed through the use of Critical Security Control Safeguards [i.9], which establish a prioritized set of actions to protect the assets through the use of technical and procedural Safeguards that are measurable and can establish risk levels. Specific threat-related Safeguards are found in ten Critical Security Controls in [i.9] and include:

- Control 5 - Account Management;
- Control 7 - Continuous Vulnerability Management;
- Control 8 - Audit Log Management;
- Control 9 - Email and Web Browser Protections;
- Control 10 - Malware Defences;
- Control 11 - Data Recovery;

- Control 13 - Network Monitoring and Defence;
- Control 14 - Security Awareness and Skills Training;
- Control 16 - Application Software Security; and
- Control 17 - Incident Response Management.

In addition to the above Critical Security Control Safeguards, an array of important, continuously-evolving, relevant tools are specified in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs [i.5], [i.10] and [i.11]. For cloud data centre implementations, hardened images identified in the Facilitation Mechanisms [i.11] are especially important. The Privacy enhancements for each Control Safeguard [i.12] are also valuable.

The defence of increasingly dispersed and complex networks from sophisticated cyber threats to secure sensitive data, systems, and services can be significantly enhanced by embracing a Zero Trust Security Model necessary to deploy and operate a system engineered according to Zero Trust principles. A breach is assumed to be inevitable or likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (resources - including data - and services) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors. Determining anomalous, out-of-ordinary or malicious activity versus expected, modelled behaviour can further be used to lower the risk of (unintentional) data exfiltration or leaking of sensitive data. To be fully effective to minimize risk and enable robust and timely responses, Zero Trust principles and concepts need to permeate most aspects of the network and its operations ecosystem. To enable real-time risk determination and deliver ongoing protection in evolving organizations, contextual data is analysed and frequently re-evaluated with machine learning algorithms. Guidance from national and industry security authorities is essential, per [i.3], [i.4] and [i.35] (see annex B). Therefore, the implementation of a Zero Trust Security Model is highly recommended.

NOTE: Clause 4.9 of the present document stresses the importance of encryption. Encrypted traffic can still be categorized as valid or possibly malicious and subject to remediation (per [i.3] and [i.4]).

4.4 Addressing incidents and near misses

The treatment of incidents and near misses in the NIS2 Directive [i.1] can be found in the following articles:

- Scope (Art. 2);
- national strategies (Art. 7);
- national cooperation (Art. 3);
- Cooperation Group (Art. 14);
- CSIRTs network (Art. 15);
- reporting obligations (Art. 23); and
- voluntary notification (Art. 30).

According to [i.1], a cybersecurity incident refers to any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems. Because near misses are part of voluntary notification arrangements under Art. 30 of [i.1], entities that are uncertain about the criteria for the characterization of near misses could ask the national CSIRT for guidance.

Cyber incidents can be addressed through the use of Critical Security Control Safeguards [i.9], which establish a prioritized set of actions. Specific incident related Safeguards are found in ten Critical Security Controls in [i.9] and include:

- Control 1 - Inventory and Control of Enterprise Assets;

- Control 3 - Data Protection;
- Control 4 - Secure Configuration of Enterprise Assets and Software;
- Control 8 - Audit Log Management;
- Control 10 - Malware Defences;
- Control 11 - Data Recovery;
- Control 13 - Network Monitoring and Defence;
- Control 14 - Security Awareness and Skills Training;
- Control 15 - Service Provider Management; and
- Control 17 - Incident Response Management.

In addition to the above Critical Security Control Safeguards, an array of important, continuously evolving relevant tools are found in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs (per [i.10] and [i.11]). The Privacy enhancements for each Control Safeguard [i.12] are also valuable.

4.5 Addressing vulnerabilities

The treatment of vulnerabilities in the NIS2 Directive [i.1] can be found in the following articles:

- national strategies (Art. 7);
- coordinated vulnerability disclosure (Art. 6);
- CSIRT tasking (Arts. 9, 10);
- Cooperation Group (Art. 14);
- CSIRT's network (Art. 15);
- risk management (Art. 21);
- critical supply chains (Art. 22); and
- information sharing (Art. 29).

Vulnerabilities can be addressed through the use of Critical Security Control Safeguards [i.9], which establish a prioritized set of actions and include:

- Control 1 - Inventory and Control of Enterprise Assets;
- Control 3 - Data Protection;
- Control 7 - Continuous Vulnerability Management;
- Control 8 - Audit Log Management;
- Control 10 - Malware Defences;
- Control 14 - Security Awareness and Skills Training;
- Control 16 - Application Software Security;
- Control 17 - Incident Response Management; and
- Control 18 - Penetration Testing.

In addition to the above Critical Security Control Safeguards, an array of important, continuously evolving relevant tools are found in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs (per [i.10] and [i.11]). For cloud data centre implementations, hardened images identified in the Facilitation Mechanisms [i.11] are especially important. The Privacy enhancements for each Control Safeguard [i.12] are also valuable.

4.6 Instituting risk management measures

Risk management in the NIS2 directive [i.1] encompasses a broad array of subjects that include:

- risk analysis;
- incident handling;
- business continuity;
- supply chain security;
- systems acquisition, development, and maintenance security;
- certification, testing and auditing;
- cyber hygiene and training;
- use of cryptography and encryption; and
- authentication and secured communications.

The instituting of risk management measures in the NIS2 Directive [i.1] can be found in:

- Subject Matter (Art. 1);
- Scope (Art. 2);
- peer review (Art. 16);
- governance (Art. 17);
- risk management measures (Art. 21);
- critical supply chains (Art. 22); and
- supervision and enforcement for essential and important entities (Arts. 29 and 30).

Risk management measures can be addressed through the use of Critical Security Control Safeguards [i.9], which establish a prioritized set of actions and include:

- Control 1 - Inventory and Control of Enterprise Assets;
- Control 2 - Inventory and Control of Software Assets;
- Control 4 - Secure Configuration of Enterprise Assets and Software;
- Control 5 - Account Management;
- Control 6 - Access Control Management;
- Control 7 - Continuous Vulnerability Management;
- Control 9 - Email and Web Browser Protections;
- Control 10 - Malware Defences;
- Control 11 - Data Recovery;
- Control 12 - Network Infrastructure Management;

- Control 13 - Network Monitoring and Defence;
- Control 14 - Security Awareness and Skills Training;
- Control 15 - Service Provider Management;
- Control 16 - Application Software Security; and
- Control 18 - Penetration Testing, Advanced or Multifactor Authentication, and Secured Communications.

In addition to the above Control Safeguards, an array of important, continuously evolving relevant tools are found in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs (per [i.10] and [i.11]). For cloud data centre implementations, hardened images identified in the Facilitation Mechanisms [i.11] are especially important. For managing "basic computer hygiene practice" (as stated in Article 18 of the NIS2 Directive [i.1]), the Critical Security Control Malware Defences Safeguard [i.9] provides a good foundation and support. However, considering the need for effective protection against ever evolving zero-day exploits by sophisticated threat actors, additional Control Safeguards supported by AI based or non-signature-based malware protection is required. Such predictive malware protection has advantages over signature-based protection in that its protection is typically more current and requires fewer updates. The Privacy enhancements for each Control Safeguard [i.12] are also valuable.

4.7 Capacity, awareness-raising initiatives, trainings, exercises and skills

The treatment of capacity, awareness-raising initiatives, trainings, exercises and skills in the NIS2 Directive [i.1] can be found in the following articles:

- national strategy (Art. 7);
- crisis management (Art. 7);
- CSIRT tasking (Arts. 10, 11);
- Cooperation Group (Art. 14);
- CSIRT's network (Art. 15);
- CyCLONe (Art. 16);
- governance (Art. 17);
- standardization (Art. 22); and
- information sharing (Art. 29).

Capacity, awareness-raising initiatives, trainings, exercises and skills can be addressed through the use of Critical Security Control Safeguards which establish a prioritized set of actions and include:

- Control 14 - Security Awareness and Skills Training;
- Control 17 - Incident Response Management; and
- Control 18 - Penetration Testing [i.9].

In addition to the above Control Safeguards, an array of important, continuously evolving relevant tools are found in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs (per [i.10] and [i.11]). The Privacy enhancements for each Control Safeguard [i.12] are also valuable.

4.8 Standards and technical specifications

The treatment of standards and technical specifications in the NIS2 Directive [i.1] can be found in the following articles:

- Cooperation Group (Art. 14);
- CSIRT's network (Art. 15);
- risk management (Art. 21);
- critical supply chains (Art. 22); and
- standardization (Art. 25).

Standards and technical specifications can be addressed through the use of Critical Security Control Safeguards in their entirety. The ETSI Critical Security Controls are also acknowledged by Recommendation ITU-T X.1500 [i.14], ITU-T's basic global intergovernmental standard for cybersecurity information exchange, where it states Critical Security Controls are 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*".

In addition to the Critical Security Control Safeguards, an array of important, continuously-evolving, relevant tools are found in the Control Facilitation Mechanisms, and include: the Community Defense Model, Risk Assessment Methods, playbooks, and applications to specific provider communities and SMEs (per [i.10] and [i.11]). The Privacy enhancements for each Critical Security Control Safeguard [i.12] should be provided. Especially significant among the Facilitation Mechanisms are the Mappings to every other commonly used frameworks, controls, and standards use by different industry sectors and nations. The Critical Security Controls also implement:

1) the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework [i.45] 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) [i.21] which facilitates interoperability among Control frameworks and Safeguards.

The creation of the Controls Workbench as a means to deal with the complexity is notable as it enables each implementation to select all the relevant jurisdiction, sector/national, context and risk variables to facilitate the NIS2 Directive [i.1] requirements and identify specific Critical Security Control Safeguards.

4.9 Trust Services measures

The treatment of Trust Services and their provision in the NIS2 Directive [i.1] can be found in the following articles:

- Scope (Art. 2);
- Definitions (Art. 4);
- risk management (Art. 21);
- reporting (Art. 23);
- certification schemes (Art. 21); and
- Digital Infrastructure sectors of high criticality (Annex I, Sector 8).

Trust services providers should take appropriate and proportionate measures to manage the risks posed to their services, including in relation to customers and reliant third parties, and to report security incidents under the NIS2 Directive [i.1] pursuant to ETSI EN 319 401 [i.16] and ETSI EN 319 403 [i.17] that implement eIDAS Regulation [i.2] and [i.37]. The NIS2 Directive [i.1] provisions provide for additional actions by Member States, the Commission, and CSIRTs:

- The requirements found in the NIS2 Directive [i.1] for trust services risk management, including privacy and security, are already extensively treated by eIDAS and supporting ETSI EN 319 401 [i.16] and [i.42].

- NIS2 Directive [i.1] provisions relating to incident reporting, management, and training requirements are also found in eIDAS and extensively treated in the related ETSI EN 319 401 [i.16]. The NIS2 certification requirements are similarly found in ETSI EN 319 403 [i.17].

Any new NIS2 Directive [i.1] requirements should be addressed in conformance with the existing ETSI EN 319 401 [i.16]. This approach includes any certification framework established for the NIS2 Directive [i.1].

4.10 Encryption measures

The NIS2 Directive [i.1] includes an array of new actions and requirements related to encryption that is consonant with [i.46]. ETSI's ISG on Encrypted Traffic Integration (ETI) has published ETSI GR ETI 006 [i.22] specifically relating to matters relating to the [i.46] and the NIS2 Directive [i.1]. ETSI ISG ETI has also published ETSI GR ETI 002 [i.52], which identifies requirements for allowing encrypted traffic integration across an abstracted network architecture, informed in part by a Zero Trust Security Model.

In addition, the NIS2 Directive [i.1] sets the risk management measures for regulated entities (see Article 18 of [i.1]) and promotes or mandates where necessary the deployment and use of end-to-end encryption as a possible risk mitigation, mindful of the potential adverse effects.

5 Implementation of NIS2 Directive

5.1 Description

The present clause suggests how requirements of the NIS2 Directive [i.1] can be effectively met using ETSI Critical Control Safeguards [i.9], [i.10], [i.11] and [i.12] together with associated facilitation mechanism, privacy enhancements, and sector guides.

NOTE: Articles of the NIS2 Directive that treat legislative process, jurisdiction, enforcement, and other purely legal matters are not addressed in the present document.

EXAMPLE: The classification of very large online platforms can be treated as essential entities under the Digital Services Act [i.37]. Additionally, the treatment of personal data under the GDPR [i.42], which applies to multiple NIS2 capability requirements, can alter their implementation.

The Critical Security Control Safeguard groups identified in [i.9], [i.10], [i.11] and [i.12] are as follows:

1) Inventory and Control of Enterprise Assets
2) Inventory and Control of Software Assets
3) Data Protection
4) Secure Configuration of Enterprise Assets and Software
5) Account Management
6) Access Control Management
7) Continuous Vulnerability Management
8) Audit Log Management
9) Email and Web Browser Protections
10) Malware Defences
11) Data Recovery
12) Network Infrastructure Management
13) Network Monitoring and Defence

14) Security Awareness and Skills Training

15) Service Provider Management

16) Application Software Security

17) Incident Response Management

18) Penetration Testing

NOTE: The selection of specific controls from each group is contextual and are further described below.

The use of MISP Project [i.18] tools, community collaboration, instances, and standards are important to effective implementation of these capabilities. The MISP Project [i.18] is substantially EU based, supported by ENISA, and deployed in EU Member States, making it relevant for NIS2 Directive [i.1] purposes.

Similarly, OSCAL use for meeting NIS2 Directive [i.1] requirements:

1) has been significantly advanced through EU funded research and development;

2) provides for open availability and interoperability among relevant regulatory requirements and standards; and

3) enables use automated tools for implementing tailored requirements for both initial certification and continuous monitoring that are especially important for SME and Micro Enterprises.

The application of OSCAL [i.21] for implementing multiple NIS2 Directive [i.1] provisions can be used where affected providers need to meet an array of different, constantly changing requirements in diverse contexts.

Implementation of a Zero Trust Security Model (see [i.34], [i.35] and relevant entries in Annex B) necessitates multiple NIS2 Directive [i.1] related actions.

5.2 National cybersecurity strategy (Art. 7)

Article 7 of the NIS2 Directive [i.1] requires each EU Member State to adopt a national cybersecurity strategy defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity.

5.3 Coordinated vulnerability disclosure (Art. 12)

Article 6 of the NIS2 Directive [i.1] requires each EU Member State to designate one of its CSIRTs as a coordinator for the purpose of Coordinated Vulnerability Disclosure (CVD). It additionally requires ENISA to develop and maintain a European vulnerability database, in consultation with the Cooperation Group.

Implementation of the relevant Critical Security Control Safeguards together with the relevant Control Facilitation Mechanisms and Privacy can be used for effective implementation of coordinated vulnerability disclosure requirements. In practice, Critical Security Control Safeguards 16.2, 16.3, and 16.6 cover the discovery and management of vulnerabilities, but this is from an application security perspective. CVD practices and specifications exist in publications of multiple organizations that provide standards and guidance documents with greater details into to CVD processes. Exchanged information should be labelled using the Traffic Light Protocol, and for triage and expression of criticality, the CVSS [i.27] should be employed.

General, single organization CVD requirements pursuant to NIS2 Directive [i.1], Art. 12, para. 1 can be met using the following:

- FIRST All Service Frameworks CSIRTs and PSIRTs [i.24]
- ETSI TR 103 838 (guide to CVD) [i.28]
- ISO/IEC 29147 [i.29]
- ISO/IEC 30111 [i.30]

General, multi-party CVD requirements can be met using the following:

- FIRST Guide to Multi Party CVD [i.26]
- ISO/IEC TR 5895 [i.31]

5.4 Crisis management, CSIRT, cooperation, peer review (Arts. 9 to 16, 19)

Art. 9 of the NIS2 Directive [i.1] requires each Member State designate one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises to identify capabilities, assets and procedures that can be deployed in case of a crisis and adopt a national cybersecurity incident and crisis response plan. Arts. 10 - 16 describe the implementation of CSIRTs, their requirements and tasks, their cooperation at the national level, creation of an EU Cooperation Group (EU CSIRT), an EU CSIRTs network, and the European cyber crises liaison organization network (EU - CyCLONe). Art. 19 requires the Cooperation Group establish a peer learning system.

Implementation of the relevant Critical Security Control Safeguards together with the relevant Control Facilitation Mechanisms and Privacy can be used for effective implementation of crisis management, CSIRT, cooperation, and peer review requirements. Use of the MISP Project [i.18] tools, community collaboration, instances, and standards are important for effective implementation of some of these requirements. The MISP Project [i.18] is already in wide use today in ENISA and various other national cybersecurity agencies around the world for automated cyber-threat intelligence information sharing and visualization. MISP can be used for NIS2 Directive requirements [i.1] pertaining to crisis management, CSIRT, cooperation, and peer review capabilities. Therefore, the use of MISP [i.18] is recommended.

Article 9, paragraph 4 of the NIS2 Directive [i.1] requires each Member State to adopt a national cybersecurity incident and crisis response plan that encompasses 'cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels', 'the relevant public and private stakeholders and infrastructure involved,' and 'national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at Union level'. These requirements infer that fast and secure alerting is needed to a plethora of entities and endpoints, of whom can be located in different regions and countries, in order to collect information and connect people for situational awareness. Furthermore, the dissemination of critical security information might need to be followed by immediate action and/or coordinating activities. To facilitate this, personnel might need to acknowledge receipt of the critical security information. The OASIS Common Alerting Protocol (CAP) [i.33] is specifically designed for enabling large-scale crisis management. OASIS CAP [i.33] provides a general format for exchanging emergency alerts and public warnings over any kind of network, enabling consistent warning messages to be disseminated simultaneously over a multitude of warning systems. In particular, OASIS CAP [i.33] offers the following features and functionalities that may be useful for some NIS2 Directive requirements [i.1] and possibly other EU resilience and risk management requirements (e.g. [i.6] and [i.36]):

- flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- multilingual and multi-audience messaging;
- phased and delayed effective times and expirations;
- enhanced message update, acknowledgement, and cancellation features;
- template support for framing complete and effective warning messages;
- compatible with digital signature capability; and
- facility for digital images and audio.

5.5 Cybersecurity risk management and critical supply chain (Arts. 20 to 22)

Art. 20, para. 1 of the NIS2 Directive [i.1] requires Member State management bodies of essential and important entities approve the cybersecurity risk management measures taken by those entities, oversee its implementation and holding them accountable for the non-compliance. Art. 20, para. 2 requires Member States to ensure that the management bodies of essential and important entities are required to be trained on risk-management measures and offer it to their employees. Art. 21 requires Member States to ensure that essential and important entities take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services.

Art. 22 states that the Cooperation Group, in cooperation with the Commission and ENISA, can carry out coordinated security risk assessments of specific critical ICT services, systems, or product supply chains, taking into account technical and where relevant, non-technical risk factors. In addition, Art. 22 requires the Commission, after consulting with the Cooperation Group and ENISA, identify the specific critical ICT services, systems or products that may be subject to the coordinated risk assessment.

Implementation of the relevant Critical Security Control Safeguards together with the relevant Control Facilitation Mechanisms and Privacy are all essential for effective implementation of risk management and critical supply chain requirements. Use of the MISP Project [i.18] tools, community collaboration, instances, and standards are important to effective implementation of these capabilities. The application of OSCAL for implementing multiple NIS2 provisions can be appropriate where affected providers need to meet an array of different, constantly changing requirements in diverse contexts. Art. 24, paras. 1 and 2 deal with the use of certified products by essential and important entities. Art. 14, para. 3 deals with the definition of a candidate scheme. Providers and vendors are likely to be faced with innumerable different regulatory and industry certification requirements in different jurisdictions. OSCAL was created to facilitate compliance with such complex environments.

NOTE: The adoption of the proposed European Commission draft Cyber Resilience Act (CRA) [i.32]- which significantly expands on the NIS2 Directive risk management and critical supply chain requirements – could potentially affect the implementation of NIS2 Directive Articles 20-22.

ETSI GR ETI 006 [i.22] provides useful guidance for implementing Art. 21, para. 2(h) requirements.

ETSI EN 319 401 [i.16] should be implemented as it is essential to the implementation of the NIS2 Directive's [i.1] risk management requirements for trust services and providers.

Implementation of a Zero Trust Security Model (see [i.34], [i.35] and Annex B) should be considered in the context of risk management and critical supply chains. Potential compromise of devices and applications in the supply chain is assumed even if certified. Privileges and access to data are controlled, minimized, and monitored; segmentation is enforced by policy; and analytics are used to monitor for anomalous activity. Complementary to the Zero Trust Security Model, implementing a Moving Target Defence methodology (which includes deception, dynamic positioning, and non-persistence) can help provide a proactive defence, increasing a system's resilience and protection against zero-day attacks (see [i.49]). The goal is to prevent unauthorized access to resources and services coupled with making the access control enforcement as granular as possible.

5.6 European cybersecurity certification scheme (Art. 24)

Art. 24 of the NIS2 Directive [i.1] states that Member States may require essential and important entities to use particular ICT products, services and processes certified under specific European cybersecurity certification schemes. It further notes that the Commission may adopt implementing acts specifying which categories of essential or important entities will be required to use certain certified ICT products, services, and processes or obtain a certificate under a European cybersecurity certification scheme. The Commission can request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme in cases where no appropriate European cybersecurity certification scheme is available [i.39].

The application of OSCAL [i.21] for implementing multiple NIS2 Directive [i.1] provisions may be necessary where affected essential and important entities need to meet an array of different, constantly changing requirements in diverse contexts.

NOTE: The MEDINA Project [i.20] is an EU-funded research project developing a framework to achieve continuous audit-based certification in compliance with the EU Cybersecurity Certification Scheme for Cloud Services (EUCS). It is investigating the usage of OSCAL [i.21] for compliance automation in support of relevant regulations including the NIS2 Directive [i.1].

5.7 Standardization (Art. 25)

Art. 25 of the NIS2 Directive [i.1] requires, with respect to risk management measures, that Member States encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems. Furthermore, that ENISA, in collaboration with Member States, draw up advice and guidelines regarding the technical areas to be considered as well as regarding already existing standards, including Member States' national standards, which would allow for those areas to be covered [i.39] and [i.40].

Implementation of the relevant Critical Security Control Safeguards ([i.9]) together with the relevant Control Facilitation Mechanisms and Privacy can be used for implementation of standardization requirements. Use of MISP Project tools, community collaboration, instances, and standards are important to effective implementation of these capabilities.

Use of a Zero Trust Security Model (see [i.34], [i.35] and Annex B), government security, and industry standards and guidelines should be considered to enhance cybersecurity postures.

5.8 Reporting and information-sharing (Arts. 23, 29, 30)

Art. 23 of the NIS2 Directive [i.1] requires Member States establish an extensive array of reporting and sharing obligations concerning any incident having a significant impact on the provision of services and mitigation measures. Art. 29 requires Member States ensure that essential and important entities may exchange on a voluntary basis relevant cybersecurity information among themselves including information relating to cyber threats, near misses, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools. Art. 30 requires Member States that essential and important entities may notify, on a voluntary basis, to the competent authorities or the CSIRTs any relevant incidents, cyber threats or near misses. Special requirements apply to trust service providers [i.33] and the treatment of personal data under the GDPR [i.42].

Implementation of the relevant Critical Security Control Safeguards ([i.9]) together with the relevant Control Facilitation Mechanisms and Privacy can be used for implementation of reporting and information-sharing requirements. Use of MISP Project [i.18] tools, community collaboration, instances, and standards are important to effective implementation of these capabilities. The information sharing may include routing threat and mitigation information using MANRS (see Annex B).

Art. 23 implementations, however, requires an array of potentially difficult-to-implement information sharing and reporting capabilities and best practices described in clause 4.1 of the present document. For example, Art. 23, para. 1 of the NIS2 Directive [i.1] requires the reporting of incidents that have a significant impact on the provision of an entity's services ("significant incident"). Art. 23, para. 3 provides some guidance on classifying an incident as significant, however, additional guidance is needed to characterize certain stated terms e.g. severe operational disruption, (severe) financial losses, considerable material losses. An additional example involves the Art. 23, para. 4 and Art. 30 notification processes where stakeholders need to know what channels have been established by the national CSIRTs or national authorities. Important and essential entities that are newcomers to the NIS2 Directive [i.1] need to be informed of the technical and operational interfaces with the national CSIRTs.

Similarly, Art. 29 of the NIS2 Directive [i.1] also concerns information sharing. MISP [i.18] and other CTI protocols are relevant to implement this requirement at a technical level. Yet, the objective of the article is that EU Member States ensure that there are communities in place where information can be exchanged in digital or physical form, as per Art. 29, para. 2. These capabilities can consist of the national platforms and communities put in place by the CERT/CSIRTs. The implementation of Art. 29 requires the effective identification and participation of essential and important entities in the communities.

Implementation of ETSI EN 319 401 [i.16] is essential to the implementation of reporting requirements for trust services and providers according to the NIS2 Directive [i.1].

Enhancing continuous reporting and information-sharing capabilities to support implementations of a Zero Trust Security Model (see [i.34], [i.35] and Annex B) should be considered to enhance cybersecurity postures.

6 Recommendations

The Critical Security Control Safeguards profiled to be part of Implementation Group 1 as defined in ETSI TR 103 305-1 [i.9] shall be implemented by entities. All other Critical Security Control safeguards from ETSI TR 103 305-1 [i.9] and privacy enhancements specified in ETSI TR 103 305-5 [i.12], as detailed in the subclauses of 4 and 5 of the present document, should also be implemented.

To help train a workforce to be cybersecurity aware, including such activities as verifying installations of software patches, entities should follow guidance in one or more of ETSI TR 103 305-1 [i.9], IEC 62443 series [i.50], and ISO 27000 family [i.51].

To help reduce the risk of spam and phishing activities, entities should implement Domain-based Message Authentication, Reporting and Conformance (DMARC). To further secure email and other communications, entities should also utilize encryption tools and protocols. ETSI GR ETI 006 [i.22] should be used for guidance.

To help address cyber threats within their networks and depending on national policy, entities shall implement the Zero Trust-related aspects of Art. 21, para. 2 of the NIS2 Directive [i.1], which include continuous authentication solutions; secured voice, video, and text communications; and secured emergency communication systems. Entities should implement other components of the Zero Trust Security Model, following guidelines provided by the entity's national authority (e.g. see [i.53] and [i.54]) or [i.34]. Entities should include a Moving Target Defence methodology (including deception, dynamic positioning, and non-persistence) in order to provide a proactive, resilient defence, protecting against zero-day attacks. AI-based or non-signature-based antimalware software to detect the most current malware should also be utilized by entities to support this.

To help address cyber threats in cloud data centre implementations, entities should utilize hardened images as identified in ETSI TR 103 305-4 [i.11].

For effective implementation and interoperability of crisis management, CSIRT, and cooperation requirements between Member States, entities shall use the MISP Project [i.18] tools, community collaboration, instances, and standards. To enable large crisis management, consideration should be given to utilizing OASIS CAP [i.33].

Annex A (informative): Mapping between the NIS2 Directive and the Critical Security Control Safeguards

This Annex provides a mapping between the articles of the EU NIS2 Directive [i.1] (excluding those that are informational i.e. Arts. 1 to 6) and the Critical Security Control Safeguards specified in ETSI TR 103 305-1 [i.9].

Table A.1: Mapping between the EU NIS2 Directive [i.1] and the Critical Security Control Safeguards [i.9]

Art. #	Art. Title	TS clause	NIS2 Directive Group							Critical Cybersecurity Control Safeguards																	
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
7	National cybersecurity strategy	5.1		X	X	X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
8	Competent authorities and single points of contact																										
9	National cybersecurity crisis management frameworks	5.3						X																		X	X
10	Computer security incident response teams (CSIRTs)	5.3		X		X		X		X				X		X	X	X	X	X		X	X		X	X	X
11	Requirements, technical capabilities and tasks of CSIRTs	5.3		X		X		X		X				X		X	X	X	X	X		X	X		X	X	X
12	Coordinated vulnerability disclosure and a European vulnerability database	5.2				X				X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
13	Cooperation at national level	5.3		X	X					X		X	X	X		X	X	X	X	X		X	X	X	X	X	
14	Cooperation Group	5.3	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
15	CSIRTs network	5.3		X	X	X		X		X		X	X	X		X	X	X	X	X		X	X	X	X	X	X
16	European cyber crises liaison organization network (EU-CyCLONe)	5.3		X				X						X		X	X	X	X	X		X	X		X	X	X
17	International cooperation																										
18	Report on the state of cybersecurity in the Union																										
19	Peer-reviews	5.3					X			X	X		X	X	X	X		X		X	X	X	X	X	X		X
20	Governance	5.3, 5.4					X	X		X	X		X	X	X	X		X		X	X	X	X	X	X	X	X
21	Cybersecurity risk management measures	5.4		X		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
22	Union level coordinated security risk assessments of critical supply chains	5.4		X		X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
23	Reporting obligations	5.7		X	X					X		X		X		X	X	X	X	X		X	X	X	X	X	
24	Use of European cybersecurity certification schemes	5.5																									
25	Standardization	5.6						X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
26	Jurisdiction and territoriality																										
27	Registry of entities																										
28	Database of domain name registration data																										
29	Cybersecurity information-sharing arrangements	5.7	X	X		X		X		X			X	X		X	X	X	X	X		X	X	X	X	X	X
30	Voluntary notification of relevant information	5.7		X	X					X		X		X		X	X	X	X	X		X	X	X	X	X	

Art. #	Art. Title	TS clause	NIS2 Directive Group							Critical Cybersecurity Control Safeguards																	
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
31	General aspects concerning supervision and enforcement																										
32	Supervision and enforcement for essential entities (Annex I)																										
33	Supervision and enforcement for important entities (Annex II)																										
34	General conditions for imposing administrative fines on essential and important entities																										
35	Infringements entailing a personal data breach																										

Annex B (informative): Bibliography

- ETSI Doc. CYBER(16)006023r1: "Deconstructing the EU NIS Directive: model, architecture, interfaces, expressions", 8th February 2016.
- ETSI Doc. CYBER(21)27b003: "Deconstruction and Implementation of the Revised Network and Information Security (NIS2) Directive Proposal", 7th December 2021.
- ETSI Security Week 2017, Session 1: "Standards and Legislation".

NOTE: The above is available only to those with an ETSI Online Account.

- NIST, Open Security Controls Assessment Language (OSCAL).
- NIST, OSCAL Concepts, Layers and Models.
- OSCAL community resources.
- MANRS Primer: "CSIRTs".
- ENISA Telecom Security Forum: "The MANRS Project".
- NCSC (UK): "Zero trust architecture design principles".
- CISA: "Zero Trust Maturity Model" April 2023, Version 2.0.
- 3GPP TR 33.894: "Technical Specification Group Services and System Aspects; Study on applicability of the Zero Trust Security principles in mobile networks (Release 18)".

Annex C (informative): Change history

Date	Version	Information about changes
May 2024	1.1.1	First publication

History

Document history		
V1.1.1	May 2024	Publication