ETSI TR 103 958 V1.1.1 (2025-03)

Cyber Security (CYBER);
Study Implementation of the
Resilience of Critical Entities Directive

Reference
DTR/CYBER-00105

Keywords
cyber security, resilience, 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

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 EU Resilience of Critical Entities Directive (CER) is a kind of companion legislative instrument to multiple other cybersecurity enactments [i.1] to [i.10]. The CER identifies "critical entities of particular European significance", excludes some categories, and lays down the obligations on Member States to enhance the resilience and ability to provide services of those entities. In addition to providing an overview of the CER, the present technical report identifies useful guidance and specifications to meet those CER objectives.

Introduction

The EU maintains a CER website to provide basic information and the latest developments [i.16]. The Directive on the Resilience of Critical Entities entered into force on 16 January 2023. Member States have until 17 October 2024 to adopt national legislation to transpose the Directive.

The Directive aims to strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies. Under the new rules:

- Member States will need to adopt a national strategy and carry out regular risk assessments to identify entities that are considered critical or vital for society and the economy. The Commission adopted a list of essential services in all the sectors covered by the Directive. Risk assessments will be carried out as regards these essential services, so that critical entities in each Member State can be identified.
- In turn, the critical entities will need to carry out risk assessments of their own and take technical, security and organizational measures to enhance their resilience and notify incidents.
- Critical entities in the EU providing essential services in six or more Member States will benefit from extra advice on how best to meet their obligations to assess risks and take resilience-enhancing measures.
- Member States will need to provide support to critical entities in enhancing their resilience. The Commission will provide complementary support to Member States and critical entities, by developing a Union-level overview of cross-border and cross-sectoral risks, best practices, guidance material, methodologies, cross-border training activities and exercises to test the resilience of critical entities, among others.

The Directive covers eleven sectors:

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health
- Drinking water
- Wastewater
- Digital infrastructure
- Public administration
- Space
- Production, processing and distribution of food

The European Commission has published an implementation timeline going forward that includes references to the Critical Entities Resilience Group work program [i.35].

1 Scope

The present document studies and identifies gaps aimed at implementation guidance for relevant provisions of the EU Resilience of Critical Entities (CER) Directive, especially related to transportation, eHealth, space systems and encryption.

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) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance).

[i.2] 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.3] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance).

[i.4] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance).

[i.5] 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.6] 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.7] 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.8] Resolution (EC) 13084/1/20: "Council Resolution on Encryption - Security through encryption and security despite encryption".

[i.9] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (Text with EEA relevance) (notified under document number C(2003) 1422).

[i.10] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167 /2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance.

[i.11] Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive).

[i.12] Opinion of the European Economic and Social Committee on 'Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)'.

[i.13] Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines.

[i.14] Commission Delegated Regulation supplementing Directive (2022)2557 establishing a list of essential services.

[i.15] EU-Lex: "Making critical entities more resilient".

[i.16] European Commission: "Critical infrastructure resilience".

[i.17] NATO: "Resilience, civil preparedness and Article 3".

[i.18] European Commission: NIS Cooperation Group, Publications.

[i.19] European Commission: "Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors".

[i.20] U.S. Department of Homeland Security: "Mitigating Artificial Intelligence (AI) Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators".

[i.21] CISA: "Transportation Systems Sector Cybersecurity Framework Implementation Guide".

[i.22] ETSI TR 103 305-1: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.23] ETSI TR 103 305-4: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

[i.24] ETSI TR 103 305-5: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 5: Privacy and personal data protection enhancement".

[i.25] ETSI TR 103 866: "Cyber Security (CYBER); Implementation of the Revised Network and Information Security (NIS2) Directive applying Critical Security Controls".

[i.26] 3GPP TR 33.700-28: "Technical Specification Group Services and System Aspects; Study on security aspects of satellite access (Rel.18)".

[i.27] ETSI TR 103 401: "Smart Grid Systems and Other Radio Systems suitable for Utility Operations, and their long-term spectrum requirements".

[i.28] ETSI TR 102 641: "Satellite Earth Stations and Systems (SES); Overview of present satellite emergency communications resources".

[i.29] ETSI EN 303 979: "Satellite Earth Stations and Systems (SES); Harmonised EN for Earth Stations on Mobile Platforms (ESOMP) transmitting towards satellites in non-geostationary orbit in the 27,5 GHz to 29,1 GHz and 29,5 GHz to 30,0 GHz frequency bands covering the essential requirements of article 3.2 of the R&TTE Directive".

[i.30] Cybersecurity & Infrastructure Security Agency (CISA): "Recommendations to Space System Operators for Improving Cybersecurity".

[i.31] ETSI TS 104 100: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Industrial Control Systems (ICS) Sector".

[i.32] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (Text with EEA relevance).

[i.33] Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

[i.34] European Commission: COM(2024) 198 final: "Communication from the Commission to the European Parliament and the Council on the Seventh Progress Report on the implementation of the EU Security Union Strategy".

[i.35] European Commission: "Critical infrastructure resilience at EU-level".

[i.36] 3GPP TR 33.700-29: "Study on Security and Privacy Aspects of 5G Satellite Access Phase 3".

[i.37] ETI TS 133 401: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401).

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:

CER	Critical Entities Resilience
CERG	Critical Entities Resilience Group
ICS	Industrial Control Systems
SES	Satellite Earth Stations and Systems

4 CER Implementation

4.1 Requirements

In July 2023, the Commission adopted a delegated regulation supplementing the CER and establishing a list of essential services [i.14]. The services list is used for multiple EU legislative instruments, and central to the CER. See Annex A.

The European Commission maintains a common website related to the CER [i.15]. The Critical Entities Resilience Group (CERG), was established by the Directive and facilitates cooperation among Member States and with the Commission. It will allow for the exchange of information and good practices on issues relating to the resilience of critical infrastructure and critical entities. The Commission has also established a common website for collaboration on Critical infrastructure resilience, including creation of the CERG and maintenance of its records and work of the CERG-NIS2 Cooperation Group [i.16].

The materials of the CERG are not publicly available. Based on its 2023 meeting agendas and minutes, the activity has been focussed on critical infrastructure stress tests, related activities in Member States and NATO, climate proofing, and drone use. Some members stressed the importance of NATO's 7 Resilience Baseline Requirements [i.17]. The topic of standards arose at only one meeting - by the Confederation of European Security Services (CoESS) Critical Infrastructure Protection Committee. After five meetings of the CERG in 2023, no further meetings occurred. Joint meetings of the CERG-NIS2 Cooperation Group also occurred.

The NIS2 Cooperation Group has published a significant number of guidelines and related documents intended to address CER and NIS2 needs [i.18]. Facilitative private-sector reference sites have also emerged [i.30]. Notably, the Commission has published implementing regulations applicable to CER segments [i.32], [i.1], [i.33] that can be met using ETSI published specifications described in clause 4.3, below, pursuant to the EC Seventh Progress Report on the EU Security Union Strategy [i.34] and the implementation timeline going forward [i.35].

4.2 Available standards and tools

4.2.0 Introduction

ETSI Technical Committees CYBER (Cybersecurity), EE (Environmental Engineering), ITS (Intelligent Transport Systems), RT (Railway telecommunications), eHealth (health ICT domain), ESI (Electronic Signatures and Infrastructures) and SES (Satellite Earth Stations and Systems), and ISGs NFV are dedicated to producing technical standards designed to meet the resilience provision of the CER.

4.2.1 Energy Sector

- Sectorial implementation of the NIS Directive in the Energy sector [i.18].
- Assessment report on cyber resilience [i.19].

4.2.2 Transport Sector

- Transportation Systems Sector Cybersecurity Framework Implementation Guidance and its companion workbook [i.21].

4.2.3 Health Sector

- Threats and risk management in the health sector under the NIS Directive [i.18].

4.2.4 Digital Infrastructure Sector

- Technical Guideline: Security Measures for Top-Level-Domain Name Registries [i.18].

4.2.5 Public Administration Sector

- Compendium on Elections Cybersecurity and Resilience [i.18].

4.2.6 Space Sector

- ETSI TC SES has published several documents relevant to Space Sector resilience [i.27], [i.28] and [i.29].
- CISA published recommendations for improving space system cybersecurity [i.30].

4.2.7 Multiple Sectors

- Reference document on security measures for Operators of Essential Services [i.18].
- Reference document on incident notification for Operators of Essential Services (circumstances of notification) [i.18].
- Cybersecurity incident taxonomy [i.18].
- Guidelines on notification of Operators of Essential Services incidents (formats and procedures) [i.18].
- Guidelines on notification of Digital Service Providers incidents (formats and procedures) [i.18].
- Reference document on the identification of Operators of Essential Services (modalities of the consultation process in cases with cross-border impact) [i.18].
- Guidelines for the Member States on voluntary information exchange on cross-border dependencies [i.18].
- Sectorial implementation of the NIS Directive in the Energy sector [i.18].
- Assessment report on the telecommunications sector [i.19].

4.3 Gaps

Many of the CER critical infrastructure sector operators and service providers use the Critical Security Controls [i.22] thru [i.25]. ETSI's new ICS Guidance for the Controls will assist in those implementations [i.31]. A knowledge base mapping Control tools and implementations to the individual CER sectors does not presently exist.

The rapidly expanding use of Artificial Intelligence systems and tools into critical infrastructure has the potential to make those systems more vulnerable to critical failures, physical attacks, and cyberattacks [i.10]. At the same time, AI-powered technologies also present new ways for adversaries to expand and enhance attacks on critical infrastructure systems. Generic guidelines specifically addressing those risks have been published [i.20]. However, a gap remains going forward - especially in the EC - to harmonise the CER and AI Acts and devise implementable responsive capabilities. This harmonisation includes the ancillary effects of the draft EU AI Liability Directive as it relates to critical infrastructure [i.11] to [i.13].

Individual ETSI Technical Committees treating critical infrastructure resilience should enhance awareness of their work through the Commission to Member States.

Annex A:
CER Provisions

A.1 Key Objectives

- lays down obligations on Member States to take specific measures aimed at ensuring that services which are essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market, in particular obligations to identify critical entities and to support critical entities in meeting the obligations imposed on them;
- lays down obligations for critical entities aimed at enhancing their resilience and ability to provide services in the internal market;
- establishes rules:
  - on the supervision of critical entities;
  - on enforcement;
  - for the identification of critical entities of particular European significance and on advisory missions to assess the measures that such entities have put in place to meet their CRE Resilience of Critical Entities obligations.
- establishes common procedures for cooperation and reporting on the application of the CRE;
- lays down measures with a view to achieving a high level of resilience of critical entities in order to ensure the provision of essential services within the Union and to improve the functioning of the internal market.

A.2 Parties subject to CER

A.2.1 CER Annex entities

Sector	Subsector/Categories
1. Energy	(a) Electricity, (b) District heating and cooling, (c) Oil,(d) Gas, (e) Hydrogen
2. Transport	(a) Air, (b) Rail, (c) Water, (d) Road, (e) public transport
3. Banking*	
4. Financial market infrastructure*	
5. Health	
6. Drinking water	
7. Waste water	
8. Digital infrastructure*	**– Providers of internet exchange points** **– DNS service providers** **– top-level-domain name registries** **– Providers of cloud computing services** **– Providers of data centre services** **– Providers of content delivery networks** **– Trust service providers** **– Providers of public electronic communications networks** **– Providers of electronic communications services**
9. Public administration	
10. Space	
11. Production, Processing, Food Distribution	

NOTE: ***** Sectors addressed by CER Art. 8 [i.1].

Figure A.1: CER Annex entities

A.2.2 CER excluded entities and requirements

- Does not apply to matters covered by the NIS2 Directive; and only partially to critical entities in the banking, financial market infrastructure and digital infrastructure sectors.
- Where provisions of sector-specific Union legal acts require critical entities to take measures to enhance their resilience and where those requirements are recognized by Member States as at least equivalent to the corresponding obligations laid down in this Directive, the relevant provisions of this Directive, including the CRE provisions on supervision and enforcement do not apply.
- Does not affect information that is confidential pursuant to Union or national rules, such as rules on business confidentiality, which is exchanged with the Commission and other relevant authorities in accordance with this Directive only where that exchange is necessary for the application of this Directive and subject to limitations.
- Does not affect Member States' responsibility for safeguarding national security and defence and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.
- Does not apply to public administration entities that carry out their activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences.
- Member States may decide that most CRE requirements, in whole or in part, do not apply to specific critical entities which carry out activities in the areas of national security, public security, defence or law enforcement, including the investigation, detection and prosecution of criminal offences, or which provide services exclusively to the public administration entities.
- Does not entail the supply of information the disclosure of which would be contrary to the essential interests of Member States' national security, public security or defence.
- Does not affect other provisions for the protection of personal data.

A.3 CER treatment of frameworks

- Art. 4 Strategy on the resilience of critical entities
- Art. 5 Risk assessment by Member States
- Arts. 6, 7 Identification of critical entities
- Art. 9 Competent authorities and single point of contact

A.4 CER treatment of cooperation and reporting actions

- Art. 19 Critical Entities Resilience Group
- Art. 20 Commission support to competent authorities and critical entities

A.5 CER treatment of implementation guidance

- Art. 4 Strategy on the resilience of critical entities:
  - facilitate the implementation of CRE obligations by small and medium-sized enterprises
- Art. 5 Risk assessment by Member States
- Arts. 6, 7 Identification of critical entities

- Art. 9 Competent authorities and single point of contact
- Art. 19 Critical Entities Resilience Group
- Art. 20 Commission support to competent authorities and critical entities

Annex B:
3GPP Space Systems Security

3GPP SA3 (security) investigated the security and privacy aspects of satellite access/Non-Terrestrial Networks and produced a study based on the architectural and functional requirements on integration of satellite components in the 5GS/EPS architecture, so as to ensure that the proposed solutions address the security and privacy implications on the architecture enhancements agreed in 3GPP TR 23.700-28 [i.26]. Specifically, it covered:

- the identified security and privacy issues, threats, and potential requirements for protecting the UE in the enhanced 5GS/EPS architecture supporting discontinuous coverage with satellite access; and
- the potential solutions addressing the identified security and privacy issues as above.

3GPP SA3 (security) relevant work items for Rel. 19 include:

- 3GPP TR 33.700-29 [i.36]: "Study on Security Aspects of 5G Satellite Access in the 5G architecture; Phase 3".
- 3GPP TS 33.401 [i.37]: "3GPP System Architecture Evolution (SAE); Security architecture".

Annex C: Bibliography

- Government of the Netherlands: "New European directive designed to improve security".
- Finnish Government: "Ministry sets up a project to improve resilience of critical infrastructure and to identify entities critical to the functioning of society".
- The MITRE Corp: "Cyber Best Practices for Small Satellites".
- NIST Special Publication SP 800-66r2: "Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide".
- CyberRisk GmbH: "The Transport Cybersecurity Toolkit".
- Cybersecurity & Infrastructure Security Agency (CISA), Space Systems Initiative.

History

Document history		
V1.1.1	March 2025	Publication