



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

Document Preview

[ETSI TR 103 958 V1.1.1 \(2025-03\)](https://standards.iteh.ai/catalog/standards/etsi/18e348a5-c11d-4ad2-b174-8b0145023312/etsi-tr-103-958-v1-1-1-2025-03)

<https://standards.iteh.ai/catalog/standards/etsi/18e348a5-c11d-4ad2-b174-8b0145023312/etsi-tr-103-958-v1-1-1-2025-03>

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

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

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

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

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

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

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

Contents

Intellectual Property Rights	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary	4
Introduction	4
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	8
3.1 Terms.....	8
3.2 Symbols.....	8
3.3 Abbreviations	8
4 CER Implementation.....	9
4.1 Requirements.....	9
4.2 Available standards and tools.....	9
4.2.0 Introduction.....	9
4.2.1 Energy Sector.....	9
4.2.2 Transport Sector.....	9
4.2.3 Health Sector	9
4.2.4 Digital Infrastructure Sector	9
4.2.5 Public Administration Sector.....	10
4.2.6 Space Sector.....	10
4.2.7 Multiple Sectors.....	10
4.3 Gaps.....	10
Annex A: CER Provisions	11
A.1 Key Objectives	11
A.2 Parties subject to CER.....	11
A.2.1 CER Annex entities	11
A.2.2 CER excluded entities and requirements.....	12
A.3 CER treatment of frameworks.....	12
A.4 CER treatment of cooperation and reporting actions	12
A.5 CER treatment of implementation guidance	12
Annex B: 3GPP Space Systems Security.....	14
Annex C: Bibliography	15
History	16

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).