

ETSI TR 103 960 V1.1.1 (2025-05)



Cyber Security (CYBER); Implementation of the Digital Operational Resilience Act (DORA)

Document Preview

[ETSI TR 103 960 V1.1.1 \(2025-05\)](https://standards.iteh.ai/catalog/standards/etsi/bc18a014-1f95-4ad6-835f-725d117241d9/etsi-tr-103-960-v1-1-1-2025-05)

<https://standards.iteh.ai/catalog/standards/etsi/bc18a014-1f95-4ad6-835f-725d117241d9/etsi-tr-103-960-v1-1-1-2025-05>

ReferenceDTR/CYBER-00110

Keywordscyber security, resilience, risk management

ETSI650 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	5
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definition of terms, symbols and abbreviations.....	10
3.1 Terms.....	10
3.2 Symbols.....	10
3.3 Abbreviations	10
4 DORA Implementation	11
4.0 Introduction	11
4.1 Standards Requirements	11
4.1.0 Organization and description of the requirements	11
4.1.1 Proportionality	11
4.1.2 ICT risk management.....	11
4.1.3 Handling, classification and reporting of ICT-related incidents	13
4.1.4 Digital operational resilience testing including threat-led penetration testing (TLPT).....	14
4.1.5 ICT third-party risk management.....	15
4.1.6 Oversight of critical third-party providers (CTTP).....	17
4.1.7 Agreements on the exchange of information and cyber crisis and emergency exercises.....	18
4.2 Available standards and tools.....	18
4.3 Avoiding duplication.....	18
4.3.1 Problem statement	18
4.3.2 EBA recommendations	18
4.4 Gaps.....	19
4.5 Post-quantum safeguards.....	19
4.6 European Commission implementing technical regulations	19
Annex A: DORA Provisions	20
A.1 Key Objectives	20
A.2 Parties subject to DORA	20
A.3 DORA treatment of standards	21
A.4 DORA regulatory standards deliverables.....	22
A.5 DORA treatment of encryption	23
Annex B: Non-EU Cybersecurity Regulations for Financial Services	24
B.1 FS-ISAC Financial Services Information Sharing and Analysis Center	24
B.2 United States Cybersecurity Regulations for the Sector	24
B.2.1 FDIC Banker Resource Center for Cybersecurity	24
B.2.2 FINRA Cybersecurity.....	24
B.3 Swiss Financial Sector Cyber Security Centre.....	25
Annex C: Bibliography	26
History	27

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 Digital Operational Resilience Act (DORA), came into effect on 16 January 2023, and focuses on the significant economic and systemic risk posed by the potential disruption of critical ICT systems, e.g. due to technical faults, operational error, or cybercrime, and becomes effective on 17 Jan 2025 [i.1]. It contains a broad range of measures aimed at improving the robustness of financial-sector ICT infrastructures, covering both in-house systems and services outsourced to third-party providers (TPPs). Twelve new mandates to issue eight technical standards, guidelines and reports were required in 2024. [Annex A] Concurrently with DORA, the Directive on Network and Information Security (NIS 2), the Directive on the Resilience of Critical Entities (CER) and several other instruments were adopted and also apply to certain financial-sector entities, specifically credit institutions and operators of financial market infrastructures, as well as to providers of digital infrastructure and ICT services who serve the financial sector [i.2] to [i.9].

Responsibility for implementing the DORA, NIS 2 and CER frameworks is assigned to a number of different authorities, both at member-state and Union level. [i.10] In addition, other countries with strong EU bindings have instituted requirements similar to DORA and related harmonisation efforts exist. [Annex B] The present document provides a comprehensive array of related information, including identification of related ETSI Technical Reports and Specifications related to the eight technical standards.