



## TECHNICAL REPORT

### **Cyber Security (CYBER); Risk Management Ecosystem** *(<https://standards.iteh.ai>)* **Document Preview**

[ETSI TR 104 117 V1.1.1 \(2025-12\)](#)

<https://standards.iteh.ai/catalog/standards/etsi/39566e06-a3be-4f30-ab1b-7f81ab6cd037/etsi-tr-104-117-v1-1-1-2025-12>

---

 Reference
 

---

DTR/CYBER-00141

---

 Keywords
 

---

cybersecurity, 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.

<https://standards.iteh.ai/catalog/standards/39566-06-c3be-4f30-ab1b-7f81-b6cd037/etsi-tr-104-117-v1-1-1-2025-12>

***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
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.....	10
3.1    Terms.....	10
3.2    Symbols.....	10
3.3    Abbreviations .....	10
4    History.....	11
4.1    Timeline of risk management.....	11
4.2    Early period 1940 - 1995.....	11
4.3    Contemporary period after 1995 .....	13
4.4    Emerging trends: software assurance and expansion of venues .....	15
5    Risk management ecosystem.....	16
5.0    The ecosystem ontology .....	16
5.1    Core Risk management process standards.....	16
5.2    Risk management derivative standards clusters .....	18
5.2.1    International standards .....	18
5.2.2    National standards .....	20
5.2.3    Industry sector guidelines .....	22
5.2.4    Implementation tools market .....	22
5.2.5    Legal obligations .....	22
Annex A: / / Bibliography .....	24
History .....	25

# 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

## (<https://standards.iteh.ai>) Document Preview

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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.

## Introduction

ICT Risk Management systems have existed since their inception in various forms of telecommunication and computational systems over the centuries as a means of achieving sufficient levels of security or resilience against threats and vulnerabilities.

The risk management ecosystem basically consists of sets of tools or processes that allow an assessment of security or resilience sufficiency for a particular device or system in a particular context followed by the application of corrective measures.

After the digital network technology evolved significantly in 1964 to bring about merger of telecommunication and computer systems, risk management initiatives almost immediately emerged within the U.S. Federal government as sets of processes. As increasingly complex, open, and autonomous ICT infrastructures and products emerged over the decades, a continuing series of risk management initiatives and tools were developed. After 2010, the threats and complexities increased significantly and resulted in major risk management efforts worldwide. Recently, risk management has been manifested as DevSecOps to encompass the complex risk management iterative cycles of software/product development, operational use, threat discovery, and remediation. After 2020, the European Union integrated risk management into multiple legislative instruments and the activities of EU bodies.