

ETSI TS 103 305-1 V5.1.1 (2025-09)



Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls

Document Preview

[ETSI TS 103 305-1 V5.1.1 \(2025-09\)](https://standards.iteh.ai/catalog/standards/etsi/08705e47-e98d-48d1-8412-f24e8b94f790/etsi-ts-103-305-1-v5-1-1-2025-09)

<https://standards.iteh.ai/catalog/standards/etsi/08705e47-e98d-48d1-8412-f24e8b94f790/etsi-ts-103-305-1-v5-1-1-2025-09>

Reference

RTS/CYBER-00159

Keywords

cyber security, cyber-defence,
information assurance

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	7
Foreword.....	7
Modal verbs terminology.....	7
Executive summary	7
Introduction	8
1 Scope	10
2 References	10
2.1 Normative references	10
2.2 Informative references.....	10
3 Definition of terms, symbols and abbreviations.....	12
3.1 Terms.....	12
3.2 Symbols.....	17
3.3 Abbreviations	17
4 Critical Security Controls.....	19
4.0 Structure of the Critical Security Controls	19
4.0.1 Introduction.....	19
4.0.1a Asset Types.....	20
4.0.2 Security Functions	23
4.0.3 Implementation Groups	23
4.0.4 Specific action	24
4.1 Control 1: Inventory and Control of Enterprise Assets	24
4.1.0 Overview	24
4.1.1 Establish and maintain detailed enterprise asset inventory	25
4.1.2 Address unauthorized assets	25
4.1.3 Utilize an active discovery tool.....	26
4.1.4 Use Dynamic Host Configuration Protocol (DHCP) logging to update enterprise asset inventory.....	26
4.1.5 Use a passive asset discovery tool	26
4.2 Control 2: Inventory and Control of Software Assets	26
4.2.0 Overview	26
4.2.1 Establish and maintain a software inventory	27
4.2.2 Ensure authorized software is currently supported	27
4.2.3 Address unauthorized software	27
4.2.4 Utilize automated software inventory tools	28
4.2.5 Allowlist authorized software	28
4.2.6 Allowlist authorized libraries.....	28
4.2.7 Allowlist authorized scripts	28
4.3 Control 3: Data Protection.....	29
4.3.0 Overview	29
4.3.1 Establish and maintain a data management process	29
4.3.2 Establish and maintain a data inventory	30
4.3.3 Configure data access control lists.....	30
4.3.4 Enforce data retention	30
4.3.5 Securely dispose of data	30
4.3.6 Encrypt data on end-user devices	30
4.3.7 Establish and maintain a data classification scheme.....	30
4.3.8 Document data flows	31
4.3.9 Encrypt data on removable media.....	31
4.3.10 Safeguard Encrypt sensitive data in transit	31
4.3.11 Encrypt sensitive data at rest.....	31
4.3.12 Segment data processing and storage based on sensitivity	31
4.3.13 Deploy a data loss prevention solution	31
4.3.14 Log sensitive data access	32
4.4 Control 4: Secure Configuration of Enterprise Assets and Software	32

4.4.0	Overview	32
4.4.1	Establish and maintain a secure configuration process.....	33
4.4.2	Establish and maintain a secure configuration process for network infrastructure	33
4.4.3	Configure automatic session locking on enterprise assets	34
4.4.4	Implement and manage a firewall on servers.....	34
4.4.5	Implement and manage a firewall on end-user devices	34
4.4.6	Securely manage enterprise assets and software.....	34
4.4.7	Manage default accounts on enterprise assets and software	34
4.4.8	Uninstall or disable unnecessary services on enterprise assets and software.....	35
4.4.9	Configure trusted DNS servers on enterprise assets	35
4.4.10	Enforce automatic device lockout on portable end-user devices	35
4.4.11	Enforce remote wipe capability on portable end-user devices.....	35
4.4.12	Separate enterprise workspaces on mobile end-user devices	35
4.5	Control 5: Account Management	36
4.5.0	Overview	36
4.5.1	Establish and maintain an inventory of accounts.....	36
4.5.2	Use unique passwords.....	37
4.5.3	Disable dormant accounts.....	37
4.5.4	Restrict administrator privileges to dedicated administrator accounts.....	37
4.5.5	Establish and maintain an inventory of service accounts.....	37
4.5.6	Centralize account management	37
4.6	Control 6: Access Control Management	38
4.6.0	Overview	38
4.6.1	Establish an access granting process.....	38
4.6.2	Establish an access revoking process.....	39
4.6.3	Implement MFA for externally-exposed applications	39
4.6.4	Implement MFA for remote network access.....	39
4.6.5	Implement MFA for administrative access.....	39
4.6.6	Establish and maintain an inventory of authentication and authorization systems	39
4.6.7	Centralize access control	40
4.6.8	Define and maintain role-based access control.....	40
4.7	Control 7: Continuous Vulnerability Management	40
4.7.0	Overview	40
4.7.1	Establish and maintain a vulnerability management process.....	41
4.7.2	Establish and maintain a remediation process	41
4.7.3	Perform automated operating system patch management.....	42
4.7.4	Perform automated application patch management.....	42
4.7.5	Perform automated vulnerability scans of internal enterprise assets	42
4.7.6	Perform automated vulnerability scans of externally-exposed enterprise assets	42
4.7.7	Remediate detected vulnerabilities	42
4.8	Control 8: Audit Log Management	43
4.8.0	Overview	43
4.8.1	Establish and maintain an audit log management process	43
4.8.2	Collect audit logs	43
4.8.3	Ensure adequate audit log storage.....	44
4.8.4	Standardize time synchronization.....	44
4.8.5	Collect detailed audit logs.....	44
4.8.6	Collect DNS query audit logs	44
4.8.7	Collect URL request audit logs.....	44
4.8.8	Collect command-line audit logs	44
4.8.9	Centralize audit logs	45
4.8.10	Retain audit logs	45
4.8.11	Conduct audit log reviews	45
4.8.12	Collect service provider logs	45
4.9	Control 9: Email and Web Browser Protections.....	45
4.9.0	Overview	45
4.9.1	Ensure use of only fully supported browsers and email clients	46
4.9.2	Use DNS filtering services	46
4.9.3	Maintain and enforce network-based URL filters.....	46
4.9.4	Restrict unnecessary or unauthorized browser and email client extensions.....	47
4.9.5	Implement DMARC	47
4.9.6	Block unnecessary file types.....	47

4.9.7	Deploy and maintain email server anti-malware protections	47
4.10	Control 10: Malware Defences	47
4.10.0	Overview	47
4.10.1	Deploy and maintain anti-malware software	48
4.10.2	Configure automatic anti-malware signature updates	48
4.10.3	Disable autorun and autoplay for removable media	48
4.10.4	Configure automatic anti-malware scanning of removable media	48
4.10.5	Enable anti-exploitation features	48
4.10.6	Centrally manage anti-malware software	49
4.10.7	Use behaviour-based anti-malware software	49
4.11	Control 11: Data Recovery	49
4.11.0	Overview	49
4.11.1	Establish and maintain a data recovery process	50
4.11.2	Perform automated backups	50
4.11.3	Protect recovery data	50
4.11.4	Establish and maintain an isolated instance of recovery data	50
4.11.5	Test data recovery	50
4.12	Control 12: Network Infrastructure Management	51
4.12.0	Overview	51
4.12.1	Ensure network infrastructure is up-to-date	51
4.12.2	Establish and maintain a secure network architecture	52
4.12.3	Securely manage network infrastructure	52
4.12.4	Establish and maintain architecture diagram(s)	52
4.12.5	Centralize network Authentication, Authorization, and Auditing (AAA)	52
4.12.6	Use of secure network management and communication protocols	52
4.12.7	Ensure remote devices utilize a VPN and are connecting to an enterprise's AAA infrastructure	52
4.12.8	Establish and maintain dedicated computing resources for all administrative work	53
4.13	Control 13: Network Monitoring and Defence	53
4.13.0	Overview	53
4.13.1	Centralize security event alerting	54
4.13.2	Deploy a host-based intrusion detection solution	54
4.13.3	Deploy a network intrusion detection solution	54
4.13.4	Perform traffic filtering between network segments	54
4.13.5	Manage access control for remote assets	55
4.13.6	Collect network traffic flow logs	55
4.13.7	Deploy a host-based intrusion prevention solution	55
4.13.8	Deploy a network intrusion prevention solution	55
4.13.9	Deploy port-level access control	55
4.13.10	Perform application layer filtering	55
4.13.11	Tune security event alerting thresholds	56
4.14	Control 14: Security Awareness and Skills Training	56
4.14.0	Overview	56
4.14.1	Establish and maintain a security awareness program	56
4.14.2	Train workforce members to recognize social engineering attacks	57
4.14.3	Train workforce members on authentication best practices	57
4.14.4	Train workforce on data handling best practices	57
4.14.5	Train workforce members on causes of unintentional data exposure	57
4.14.6	Train workforce members on recognizing and reporting security incidents	57
4.14.7	Train workforce on how to identify and report if their enterprise assets are missing security updates	58
4.14.8	Train workforce on the dangers of connecting to and transmitting enterprise data over insecure networks	58
4.14.9	Conduct role-specific security awareness and skills training	58
4.15	Control 15: Service Provider Management	58
4.15.0	Overview	58
4.15.1	Establish and maintain an inventory of service providers	59
4.15.2	Establish and maintain a service provider management policy	59
4.15.3	Classify service providers	60
4.15.4	Ensure service provider contracts include security requirements	60
4.15.5	Assess service providers	60
4.15.6	Monitor service providers	60
4.15.7	Securely decommission service providers	61
4.16	Control 16: Application Software Security	61

4.16.0	Overview	61
4.16.1	Establish and maintain a secure application development process	63
4.16.2	Establish and maintain a process to accept and address software vulnerabilities	63
4.16.3	Perform root cause analysis on security vulnerabilities	63
4.16.4	Establish and manage an inventory of third-party software components	64
4.16.5	Use up-to-date and trusted third-party software components	64
4.16.6	Establish and maintain a severity rating system and process for application vulnerabilities	64
4.16.7	Use standard hardening configuration templates for application infrastructure	64
4.16.8	Separate production and non-production systems	65
4.16.9	Train developers in application security concepts and secure coding	65
4.16.10	Apply secure design principles in application architectures	65
4.16.11	Leverage vetted modules or services for application security components	65
4.16.12	Implement code-level security checks	66
4.16.13	Conduct application penetration testing	66
4.16.14	Conduct threat modelling	66
4.17	Control 17: Incidence Response Management	66
4.17.0	Overview	66
4.17.1	Designate personnel to manage incident handling	67
4.17.2	Establish and maintain contact information for reporting security incidents	67
4.17.3	Establish and maintain an enterprise process for reporting incidents	68
4.17.4	Establish and maintain an incident response process	68
4.17.5	Assign key roles and responsibilities	68
4.17.6	Define mechanisms for communicating during incident response	68
4.17.7	Conduct routine incident response exercises	69
4.17.8	Conduct post-incident reviews	69
4.17.9	Establish and maintain security incident thresholds	69
4.18	Control 18: Penetration Testing	69
4.18.0	Overview	69
4.18.1	Establish and maintain a penetration testing program	70
4.18.2	Perform periodic external penetration tests	71
4.18.3	Remediate penetration test findings	71
4.18.4	Validate security measures	71
4.18.5	Perform periodic internal penetration tests	71
Annex A:	Version changes to the Controls	72
Annex B:	Bibliography	73
History		74

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 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 present document captures and describes the prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. These actions are specified by ETSI in the present document, the Critical Security Controls (CSCs), which are developed and maintained by the Center for Internet Security (CIS) as an independent, expert, global non-profit organization [i.46].

The latest version of the Controls is found in the present document. It is the normative version of the ETSI Critical Security Controls. Parts of ETSI TR/TS 103 305, as well as related ETSI Technical Reports and Specifications, assist in the implementation. ETSI publishes derivative international versions. A global array of expert individuals and organizations contribute to provide ongoing development, support, adoption, and use of these Critical Security Controls.