ETSI TR 103 305-4 V2.1.1 (2018-09)

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 4: Facilitation Mechanisms

Reference
RTR/CYBER-0034-4

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, 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.

Foreword

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

The present document is part 4 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence. Full details of the entire series can be found in part 1 [i.1].

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 Critical Security Controls represent perhaps the most valuable cyber defence mechanism worldwide and across multiple ICT sectors because of the many facilitation mechanisms which have been developed to assist with their implementation and use. The present document is an evolving repository for some of the most important facilitation mechanism for Critical Security Control.

Introduction

The Critical Security Controls ("the Controls") exist within a larger cyber security ecosystem that relies on the Controls as critically important defensive measures. There are a variety of facilitation mechanisms for their use. The present document provides a placeholder for reference information for several especially useful mechanisms: Hardened Images, Mappings and Compliance, Guide for Small- and Medium-Sized Enterprises, and Risk Assessment Method.

1 Scope

The present document is an evolving repository for diverse facilitation mechanism guidelines for Critical Security Control implementations.

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

[i.2] Critical Security Controls: "Hardened Images".

NOTE: Available at https://www.cisecurity.org/services/hardened-virtual-images/.

[i.3] Critical Security Controls: "Mappings and Compliance".

NOTE: Available at https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/.

[i.4] Critical Security Controls: "Guide for Small- and Medium-Sized Enterprises (SMEs)".

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf.

[i.5] Critical Security Controls: "Risk Assessment Method (RAM)".

NOTE: Available at https://learn.cisecurity.org/cis-ram.

[i.6] Mappings to the CIS Critical Security Controls.

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf.

[i.7] ETSI TR 103 305-5: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts [i.1]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CSC	Critical Security Control
FISMA	Federal Information Security Modernization Act
GDPR	General Data Protection Regulation
PCI DSS	Payment Card Industry Data Security Standard
SME	Small- and Medium-sized Enterprises

4 Hardened Images

4.1 Description

One of the potentially most effective new means for implementing the Critical Security Controls - especially in a cloud data center environment is to use Hardened Images via major cloud computing vendors which have been facilitated by the Center for Internet Security [i.2]. Hardened Images are securely configured according to applicable CIS benchmarks. The Hardened Images include most major cloud data center platforms.

4.2 Virtual Image vs. Hardened Virtual Image

A virtual image is a snapshot of a virtual machine (VM) used to create a running instance in a virtual environment, thus providing the same functionality as a physical computer. Virtual images reside on the cloud and let you cost-effectively perform routine computing operations without investing in local hardware and software.

Hardening is a process of limiting potential weaknesses that make systems vulnerable to cyber attacks. Examples include:

- Disabling unnecessary ports/services
- Eliminating unneeded programs and internal root accounts
- Limiting/denying visitor access

More secure than a standard image, hardened virtual images reduce system vulnerabilities to help protect against denial of service, unauthorized data access, and other cyber threats.

4.3 Benefits of Hardened Images

The available images are hardened to meet the Critical Security Control benchmarks, secure configuration standards that are collaboratively developed and used by thousands worldwide. The benchmarks are vendor-agnostic and securely configured, regardless of the cloud platform chosen. Benefits include:

- Conformance to recommended cybersecurity best practices
- Flexible deployability across networks by administrators
- Elimination of initial investments in hardware
- Ability to scale virtual resources and security quickly
- Inclusion of reports showing conformance to applicable benchmarks

5 Mappings and Compliance

5.1 Description

A broad array of national government agencies, regional authorities, and industry sector organizations have published cyber security compliance "frameworks". The Critical Security Controls can support most of these framework requirements, and continuing efforts exist to maintain and publish mappings from the Controls to all the diverse frameworks. See Critical Security Controls: Mapping and Compliance [i.3].

The CIS Mapping and Compliance ensemble of materials [i.3] is continually collected and updated with existing and newly available compilation. One of the most useful generic compilations is a very large matrix of the the Critical Security Controls Version 6 against more than 20 different frameworks from diverse countries, government agencies, and industry sectors, including health and electrical power systems [i.6].

Additional sector compliance requirements of significance are the Payment Card Industry Data Security Standard (PCI DSS) within the banking industry, and the Federal Information Security Modernization Act (FISMA) requirements among government agencies. Compliance mappings for these sectors can be found on the CIS Mapping and Compliance site [i.3].

Mappings of the Controls relating to privacy requirements, including the GDPR are contained in part 5 of the present document [i.7].

6 Guide for Small and Medium-sized Enterprises (SMEs)

6.1 Description

Credit card breaches, identity theft, ransomware, theft of intellectual property, loss of privacy, denial of service have emerged as daily cyber security incidents. Victims with large budgets can take steps to mitigate these attacks. However, organizations with small budgets and limited staff are less able to respond. Common concerns of SMEs include:

- Theft of company information - External hackers and dissatisfied employees steal company information and customer lists.
- Website defacement - Hackers corrupt your website to benefit competitors.
- Phishing attacks - Email is designed to look like legitimate correspondence that tricks recipients into clicking on a link that installs malware on the system.
- Ransomware - Types of malicious software block access to a computer so that criminals can hold your data for ransom.
- Data loss due to natural events and accidents.

A guide for Small and Medium-sized Enterprises (SMEs) with a small number of high priority actions based on the Critical Security Controls can be especially useful and is available online [i.4]. The guide contains a small sub-set of the Controls specifically selected to help protect SMEs.

To help prioritize SME efforts, the Guide recommends using a phased approach. Phase 1 involves knowing what is on the SME network and understanding the cybersecurity baseline. Phase 2 focuses on protecting the SME security baseline through education and prevention. Phase 3 helps SMEs to prepare in advance for disruptive events. Each phase has specific questions to be answered, along with action items and tools that will help you achieve SME cyber security goals.

7 Risk Assessment Method (RAM)

7.1 Description

Risk assessment is a term used to describe the overall process or method where an organization identifies hazards and risk factors that have the potential to cause harm (hazard identification), and then analyses and evaluates the risk associated with that hazard in some systematic and quantifiable manner. The constantly evolving, enormous array of cyber security vulnerabilities and incidents today in the face of finite resources is perhaps the biggest challenge of most organizations. The Critical Security Controls are enormously useful, but their effective implementation is necessitating some kind of risk assessment method.

The Critical Security Controls user community has contributed to a Risk Assessment Method (RAM) [i.5] to help organizations plan and justify their implementation of Controls - whether those controls are fully or partially operating. Few organizations can apply all controls to all information assets, because - while reducing some risks - security controls also introduce new risks to efficiency, collaboration, utility, productivity, or available funds and resources.

Laws, regulations, and information security standards all consider the need to balance security against an organization's purpose and its objectives, and require risk assessments to find and document that balance. The risk assessment method described provides a basis for communicating cybersecurity risk among security professionals, business management, legal authorities, and regulators using a common language that is meaningful to all parties.

The RAM uses established information security risk assessment standards. Organizations can evaluate risks and safeguards using the concept of "due care" and "reasonable safeguards" that the legal community and regulators use to determine whether organizations act as a "reasonable person".