# ETSI TR 103 305-2 V2.1.1 (2018-09)


**CYBER;**
**Critical Security Controls for Effective Cyber Defence;**
**Part 2: Measurement and auditing**

Reference
RTR/CYBER-0034-2

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 2 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.3].

# 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 present document is intended as an evolving repository for guidelines on measurement and auditing of Critical Security Control implementations. Measurements and metrics are essential components of any successful security program. To support good decision-making, the current state of a protected IT system or network should be assessed - ideally by automated methods. Means should exist to measure and report on progress. The records kept constitute an audit.

# Introduction

The Critical Security Controls ("the Controls") have always included a set of Metrics for every Control in order to help adopters manage implementation projects. Adopters can use the sample Metrics as a starting point to identify key information to help track progress, and to encourage the use of automation.

However, there is considerable security "fog" around the use of the terms. For example, there are lots of things that can be measured, but it is very unclear which of them are in fact worth measuring (in terms of adding value to security decisions). And since there are very few "absolutes" in security, there is always the challenge of making a judgment about the measurement value that is "good enough" in terms of managing risk.

The problem of inconsistent terminology across the industry cannot be solved, but consistency within the Critical Security Controls can be enhanced. The definitions found in a NIST article, Cyber Security Metrics and Measures are a useful point of departure [i.2]. This approach separates the attribute being measured (the "Measure") from a value judgment of what is "good" or "good enough".

The introduction of the six sigma measurement analysis for each sub-control for Version 7 of the controls is a major evolution enabling automated tools. This was done by removing the measures and metrics information from the Controls tables in part 1 [i.3], expanding the related knowledge base, and providing the information in in both textual and spreadsheet formats online [i.1]. The on-line representations also allow the knowledge base to be more easily evolved.

# 1 Scope

The present document is an evolving repository for measurement and effectiveness tests of Critical Security Control implementations. The CSC are a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber attacks.

The present document is also technically equivalent and compatible with the 7.0 version of the "CIS Controls Measures and Metrics for Verion 7," March 2018 [i.1].

# 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] The Center for Internet Cybersecurity: "CIS Controls Measures and Metrics for Verion 7," March 2018.

NOTE: Available at https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics.

[i.2] Paul E. Black, Karen Scarfone and Murugiah Souppaya: "Cyber Security Metrics and Measures", in Handbook of Science and Technology for Homeland Security, Vol. 5, Edited by John G. Voeller.

NOTE: Available at https://hissa.nist.gov/~black/Papers/cyberSecurityMetrics2007proof.pdf.

[i.3] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

# 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.3]

**measure:** concrete, objective attribute, such as the percentage of systems within an organization that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide [i.2]

**metric:** abstract, somewhat subjective attribute, such as how well an organization's systems are secured against external threats or how effective the organization's incident response team is [i.2]

## 3.2 Abbreviations

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

| | |
|---|---|
| CIS | Center for Internet Security |
| CSC | Critical Security Control or Capability |
| ID | Identifier |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |

# 4 Critical Security Controls: Measures and Metrics

## 4.1 Automated measures and metrics

One of the major advances of V7 of the Critical Security Controls is an evolution toward automated measures and metrics. This was accomplished by moving the information to separate on-line representations that can facilitate automation and be more easily adjusted. For each Sub-Control, a list of Measures and metrics are available in either tablular text form or an excel spreadsheet [i.1]. Each Measure is given a unique ID number to allow tracking, together with a "sensor", measure and values for six sigmas.

# History

| Document history | | |
|---|---|---|
| V1.1.1 | August 2016 | Publication |
| V2.1.1 | September 2018 | Publication |
| | | |
| | | |
| | | |