

**CEN**

**CWA 16871-1**

**WORKSHOP**

March 2015

**AGREEMENT**

---

ICS 33.020

English version

## Requirements and Recommendations for Assurance in Cloud Security - Part 1: Contributed recommendations from European projects

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels**

# Contents

Page

Foreword.....	3
Introduction .....	4
1 Scope .....	5
2 Normative references .....	5
3 Background and Definitions .....	5
3.1 General.....	5
3.2 Cloud .....	5
3.3 Models.....	5
3.4 Frameworks .....	6
3.5 Recommendations and Requirements .....	6
3.6 Security Controls and Control Areas.....	7
3.7 Additional terms and definitions related to CWA RACS.....	7
3.8 Auditing process.....	8
3.8.1 What? .....	8
3.8.2 How? .....	9
3.9 Automation and Continuous Monitoring.....	9
3.10 Technical Specifications and Languages .....	10
4 Format of Inputs.....	11
5 Recommendations from EU research projects .....	11
5.1 ANIKETOS .....	11
5.2 Assert4SOA .....	12
5.3 CUMULUS .....	13
5.4 PCAS .....	15
6 Recommendations from the CIRRUS Green paper .....	16
6.1 General.....	16
6.2 Identity .....	16
6.2.1 Recommendations for Cloud Customers/Service Providers .....	16
6.2.2 Recommendations for Standardization Bodies.....	17
6.2.3 Recommendations for all Stakeholders .....	17
6.2.4 Incident management.....	17
6.3 Privacy .....	18
6.3.1 Recommendations for all stakeholders .....	18
6.3.2 Recommendations for Policy Makers.....	18
6.3.3 Recommendations for (industrial) Research Leaders .....	19
6.4 Monitoring .....	19
6.4.1 Recommendations for Standardization Bodies.....	19
6.4.2 Recommendations for Cloud Customers/Service Providers CxOs.....	19
6.4.3 Recommendations for all Stakeholders .....	20
6.5 Certifications .....	20
6.5.1 Recommendations for Policy Makers and Certification “industry” .....	20
6.5.2 Recommendations for Cloud Customers/Service Providers CxOs.....	21
6.5.3 Recommendations for all Stakeholders .....	21
7 Miscellaneous contributions .....	21
8 Other recommendations .....	23
9 Conclusion .....	24
Annex A (normative) Recommendations summary .....	25

## Foreword

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties on 2014-11-18, the constitution of which was supported by CEN following the public call for participation made on 2014-02-11.

A list of the individuals and organizations which supported the technical consensus represented by the CEN Workshop Agreement is available to purchasers from the CEN-CENELEC Management Centre. These organizations were drawn from the following economic sectors: chemical industry, environmental technology and research institutes, construction, public authorities and academia.

The formal process followed by the Workshop in the development of the CEN Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of the CEN Workshop Agreement or possible conflict with standards or legislation. This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its members.

The final review/endorsement round for this CWA was started on 2014-02-11 and was successfully closed on 2014-11-18. The final text of this CWA was submitted to CEN for publication on 2015-02-16.

This CEN Workshop has mainly been proposed by the CIRRUS consortium. The European FP7 funded project Certification, Internationalisation and standardization in cloud Security (CIRRUS) is supported under the 7<sup>th</sup> Framework Programme of the EU, Theme FP7 ICT-2011-8, and grant agreement no. 317738.

The CEN Workshop members who have supported the document are:

- Atos Spain Sa, Atos Spain Sa,
- Austrian Standards Institute,
- Centre d'Excellence en Technologies de l'Information et de la Communication (Cetic),
- Eurocloud,
- Leire Orue-Echevarria (Tecnalia),
- Portakal Teknoloji Egitim Danismanlik Yazilim Turizm Taahhut Ve Ticaret Ltd Sti,
- Universita' Degli Studi di Milano.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

This CEN Workshop Agreement is publicly available as a reference document from the National Members of The following countries: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Comments or suggestions from the users of the CEN Workshop Agreement are welcome and should be addressed to the CEN-CENELEC Management Centre.

## Introduction

This CEN Workshop Agreement (CWA) provides a set of recommendations for assurance in cloud security.

This CWA is related to the effort lead by ETSI to “cut through the jungle of standards” requested by the European Commission that led to the report “Cloud Standards Coordination” published November 2013.

The aim of this CWA was to provide recommendations for further work. This document has been developed through the collaboration of a number of contributing partners, representing a wide mix of interests. These include academia, industry and standardization bodies. The present CWA has received the support of representatives of these sectors.

## 1 Scope

CWA Recommendations for Assurance in Cloud Security (RACS) promotes recommendations on security assurance management in the context of auditing and certification of cloud-based services and systems. The recommendations in the present document have been collected from a number of EU research pioneer projects in cloud assurance and from RACS target different stakeholders (policy makers, industry and final users) interested in upcoming challenges concerning cloud security assurance. The focus of CWA RACS is mainly on the type of assurance and assessment activities that can be done without the physical presence of an auditor and at any point in time.

## 2 Normative references

The following references, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the cited edition applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

## 3 Background and Definitions

### 3.1 General

CWA RACS provides recommendations toward the definition of a cloud-focused assurance scheme suitable for the specific features of cloud computing, including: multi-layer definition, service dynamics, cross boundary computing, incremental definition of services, composition, and heterogeneity. All assurance techniques should rely on standard syntax and semantics in order to allow certain forms of composition of such assurance or certification claims. This section summarizes some **basic definitions** at the basis of requirements and recommendations in the remainder of the document.

### 3.2 Cloud

One of the first and simplest definitions of *Cloud* can be found in NIST's NIST Definition of Cloud Computing, Special Publication 800-145. It defines the notion of Cloud through a 3-4-5 pattern model: three cloud service models (SaaS, PaaS, IaaS), four deployment models (public, private, hybrid, community) and five essential characteristics (internet access, rapid elasticity, measured service, on-demand self-service and resource pooling).

**CWA RACS is looking at emerging and future cloud trends** that go beyond the current NIST definition of cloud. Service models have changed and are continuously shifting the definition of *cloud space*, while the trend of brokerage or multi-cloud settings is extending the notion of *cloud* to include the concepts *cloud ecosystem* and *cloud supply chain*.

### 3.3 Models

**Cloud reference models provide abstract synopses of the cloud infrastructure.** Models can be classified according to different criteria (e.g. distinguishing between business-oriented and architecture models).

A cloud reference model can be used for different purposes. For instance, i) architects can use it as a template for composing architectures, ii) consultants can use it to make logical divisions and groupings within architectures. A Cloud Architecture Reference Model is an abstraction of cloud computing concepts and relationships that can be used for educational purposes, as a basis for standards and for adoption decisions.

For the specific purpose of assurance and certification, analogously to the well-known OSI conceptual model (ISO/IEC 7498-1), the most widely used model relies on division into layers that go from physical facilities and hardware to the application layer and presentation modality (e.g. mobile). While this model is useful for the assignment of roles and responsibilities in a single cloud service provisioning model (between CSP and user), emerging and future models will have to include external stakeholders and components.