Business Plan for the CEN Workshop on

Requirements and Recommendations for Assurance in Cloud Security
WS Acronym: RACS
Workshop

1. Status of the Business Plan

This Business Plan was approved during the Kick-off meeting held in Brussels on 11 February 2014.

2. Background to the Workshop

Cloud computing is such a broad and diverse phenomenon that it is easy to become confused about its many forms and the ways organisations can benefit from it. Put simply, cloud computing is an approach in which infrastructure and software resources are provided by an external vendor or by your internal IT department over the Internet. These resources are highly scalable and at competitive costs, which make cloud services highly attractive in a business environment in which organisations are required to reduce their IT capital expenditure and costs and improve the flexibility and agility of their IT services delivery.

However, whilst the market is not yet fully matured on all offerings, cloud computing security risks, barriers, and set-up costs can be significant. One of the main challenges for organisations consists in building trust and confidence in cloud computing services, including, e.g. concern over maintaining data privacy and security, unproven service level agreements, the difficulty to monitor and enforce security policy in the cloud etc. Concerns are being voiced about the compliance issues as well as the effectiveness and efficiency of traditional governance and protection mechanisms. The key to address the above challenges is the definition of globally accepted requirements and recommendations for assurance as a basis for certification.

Cloud industry, as well as the research community, is already moving fast in order to address these challenges and different certification schemes and frameworks appeared to allow global, accredited, trusted certification of cloud providers. These schemes address a number of requirements, from incremental and multi-layered certification processes, according to the existing security guidance and control objectives, to the issues such as revocation or representation of certificates.

Given the fact that a number of third-party assessments, certification and attestation statements already exist, the main principle should be to avoid duplication of effort and costs and to build upon the existing efforts. As of today these are mainly building on top of the existing standards, such as ISO/IEC 27001, and have to meet minimum cloud security specific standards promoted by industry such as the CSA Cloud Control Matrix. In parallel, European research projects have already delivered some results in regard to the requirements and standards for the cloud security assurance based on continuous monitoring and audit data collection, machine readable

certificates and other advances that will eventually enable certification on demand, at any point in time.

In 2012 the FP7-project „Certification, InteRnationalisation and standaRdization in cloUd Security“(CIRRUS) was initiated to give support to these ongoing efforts, as well as to coordinate several related projects and initiatives. The project has strong links with heterogeneous efforts in cloud computing security, with special emphasis on issues such as standardization, global collaboration, best practices, certification and compliance. Co-funded by the European Commission´s FP7 programme, CIRRUS project aims to address the above mentioned issues with a holistic, but pragmatic and practical approach, that includes promotion of its results through the CEN Workshop Agreement. The CEN Workshop ‘Requirements and Recommendations for Assurance in Cloud Security’ (RACS) intends to use the findings of several projects co-funded by the European Commission, and provide possible a set of requirements and recommendations to tackle the challenges related to the assurance in the cloud.

Further information on the FP 7-project CIRRUS are available at http://www.cirrus-project.eu.

3. Workshop proposers and Workshop participants

Workshop proposers are the following participants of the EU research project CIRRUS:

- ATOS SPAIN SA, ATOS SPAIN SA,
- CLOUD SECURITY ALLIANCE (EUROPE) LBG,
- AUSTRIAN STANDARDS INSTITUTE,
- PORTAKAL TEKNOLOJI EGITIM DANISMANLIK YAZILIM TURIZM TAAHHUT VE TICARET LTD STI,
- INCORPORATED ADMINISTRATIVE AGENCY INFORMATION – TECHNOLOGY PROMOTION AGENCY,
- GRANT THORNTON FORENSIC & INVESTIGATION SERVICES BV.

The Workshop will be open to any interested party.

4. Workshop scope and objectives

The Workshop will consist of two Working Groups delivering one Workshop Agreement each.

a) WG1: ISO/IEC has recently published standards ISO/IEC 27001:2013 and ISO/IEC 27002:2013. There is also a working draft of ISO/IEC 27009 – Sector-specific Application of ISO/IEC 27001 – Requirements, which defines the requirements for the use of ISO/IEC 27001 for sector-specific applications. The cloud computing specific requirements and controls are not listed in the ISO 27001:2013. CIRRUS CWA will

capture the requirements from cloud computing stakeholders that have an interest in using ISO/IEC 27009 in order to interpret and add controls to ISO/IEC 27001. CIRRUS CWA will list these requirements and controls for the security. At a later stage, data protection and privacy in the context of EU regulatory framework may also be taken into account. This deliverable will also include a comprehensive overview on regulatory and standardization activities related to Security in Cloud Computing, including representative samples of ICT technical specifications developed by consortia and fora.

b) WG2: Certification based on the current audit frameworks (such as CWA 15499 from 2006) gives assurance limited in time and scope. The WG will explore emerging requirements for audit frameworks such as 'Continuous Monitoring' to ensure optimal and future proof solutions. The outcome will be presented in the form of a list of recommendations for the emerging and future standards.

5. Workshop programme

The purpose of the CEN Workshop will be to embed the findings of the FP 7 project CIRRUS and additional inputs from other WS participants into two CEN Workshop Agreements(CWAs) This will allow all parties interested in the activity to discuss and contribute to the development of the CWAs.

The working language will be English. The CWA will be published in English. The duration of the WS RACS will be 7 months, which might be extended.

The CEN Workshop will have two plenary meetings to consider the drafts of the CWAs. A 60-day public comment period is proposed. The Workshop will give full consideration to the comments expressed. The CWA will be approved in line with the CEN rules.

Tentative workshop schedule:

Date	**Place**	**Meeting**	**Activity of item**	**Responsibility**
2014-02-11	Brussels	WS Kick off	Approval of the CIRRUS CWA business plan Discussion of CWA deliverables	Workshop chairman and secretariat CCMC
2014-05-XX	Brussels	CWA Interim meeting	Review of the feedback received and the presentation of the initial draft of two CWA deliverables. Approval of the Draft CWA for 60-day public comment period	Workshop participants
2014-09-xx	TBC.	CWA final meeting	Comments resolution meeting Approval of the final text of the CWA Update of Business Plan if there is a request from WG2	Workshop participants

Note: Depending on the progress of the work program, an additional meeting of WG2 could take place. In between the meetings, the Workshop will work electronically.

6. Workshop structure

The responsibilities of the Workshop Chair include the following tasks:

- To chair Workshop plenary meetings;
- To ensure that the Workshop delivers in line with its Business Plan;
- To manage the consensus building process.

Austrian Standards Institute will provide the Workshop Secretariat, subject to formal acceptance of the business plan and the co-ordination of administrative duties:

- To ensure that the CWA is available in time on the appropriate CEN format.
- To interface with the CCMC regarding strategic issues, problems arising, external relationships, etc.

7. Resource requirements

All costs related to the participation of interested parties in the Workshop's activities have to be borne by themselves.

Participation in the CEN Workshop is open to all interested parties and free of charge. CWA participants shall be able to use e-mail and an Internet browser in order to participate in the work of the CWA, as all documentation will be drafted and supplied electronically.

8. Related activities and liaisons

Since there are international standardization activities on cloud computing services in ISO/IEC JTC 1/SC 27 "IT Security techniques" and ISO/IEC/JTC 1/SC 38 WG 3 "Distributes applications platforms and services (DAPS)" as well as ETSI has an interest in cloud computing services, liaison is welcome with

- ISO/IEC JTC 1/SC 27;
- ISO/IEC/JTC 1/SC 38;
- ETSI Could Standards Coordination (CSC).

The Secretariats of ISO/IEC JTC 1/SC 27 and ISO/IEC JTC 1/SC 38 were informed.

9. Contact points

Chairpersons:

WG 1 and overall:
Aljosa Pasic
ATOS Spain
Albarracin 25, E-28037 Madrid
Tel.: +34 91 214 8800
e-mail: aljosa.pasic@atos.net

WG 2:
Prof. Ernesto Damiani
Universita' degli Studi di Milano
via Bramante, 65, I-26013 Crema (CR), Italia
Tel.: +39 02 50330010
e-mail: ernesto.damiani@unimi.it

Vice-chair WG 1:
Bora Gungoren
Portakal Teknoloji Egitim Danismanlik Yazilim Tur. Taah. Ve Tic. Ltd. Sti.
ODTU Teknokent Gumus Blok No: 9 Cankaya
Ankara Turkey
Tel.: +90 312 210 1874
e-mail: bora@portakalteknoloji.com

Vice-chair WG 2:
Erkuden Rios
Leire Orue-Echevarria (TECNALIA)
Parque Tecnológico de Bizkaia. Ibaizabal Bidea, Edificio 202. E-48170 Zamudio Spain.
Tel.: +34 902 760 009
e-mail: Erkuden.Rios@tecnalia.com

CEN-CENELEC Management Centre
Alina Iatan
Programme Manager
Avenue Marnix, 17
B-1000 Brussels
Tel: +32 2 550 08 16
Fax: +32 2 550 08 19
e-mail : aiatan@cencenelec.eu

CWA Secretariat:
Karl Stumwoehrer
Austrian Standards Institute
Heinestraße 38
1020 Vienna, Austria
Tel.: +43 1 213 00 723
e-mail: k.stumwoehrer@austrian-standards.at
web: www.austrian-standards.at