D3.5 Risk-based decision making mechanisms for cloud service (Final report)

This is the final report of an incremental deliverable documenting the overall process adopted by CloudWATCH2 to develop risk profiles for (prospective) cloud service customers from Public Administrations and Small and Medium-sized Enterprises. This deliverable presents the methodology used to develop specific risk profiles for Public Administrations/SMEs usage of cloud services. The expected outcome from the associated task (T3.3) is to produce a set of risk profiles and corresponding security controls, applicable to both Public Administrations and Small and Medium-sized Enterprises (SMEs).

CloudWATCH Mission

CloudWATCH2 takes a pragmatic approach to market uptake and sustainable competitiveness for wider uptake and commercial exploitation. It provides a set of services to help European R&I initiatives capture the value proposition and business case as key to boosting the European economy.

CloudWATCH2 services include:

- A cloud market structure roadmap with transparent pricing to enable R&I projects to chart exploitation paths in ways they had not previously considered, or help them avoid approaches that would not have been successful
- Mapping the EU cloud ecosystem of products, services and solutions emerging from EU R&I projects. Identifying software champions and best practices in mitigating risks associated with open source projects, and ultimately, enable faster time-to-value and commercialisation
- Impact meetings for clustering and convergence on common themes and challenges. Re-use of technologies will also be of paramount importance
- Promoting trusted & secure services through roadshows and deep dive training sessions. Giving R&I initiatives a route to users at major conferences or in local ICT clusters
- A portfolio of standards for interoperability and security that can facilitate the realisation of an ecosystem of interoperable services for Europe
- Cloud interoperability testing in an international developer-oriented and hands-on environment. Findings will be transferred into guidance documents and standards
- Risk management and legal guides to the cloud for private and public organisations to lower barriers and ensure a trusted European cloud market

Disclaimer

CloudWATCH2 (A European Cloud Observatory supporting cloud policies, standard profiles and services) is funded by the European Commission's Unit on Software and Services, Cloud Computing within DG Connect under Horizon 2020.

Document Information Summary

Document title:	D3.5 Risk-based decision making mechanisms for cloud service (Final report)
Main Author(s):	Cloud Security Alliance
Contributing author(s):	Cloud Security Alliance
Reviewer(s):	ICT-Legal, Strategic Blue, Trust-It
Target audiences:	Public Administration, SMEs, Policy Makers, Standardisation Bodies
Keywords:	Cloud security, Risk management, Risk profile
Deliverable nature:	Report
Dissemination level: (Confidentiality)	Public
Contractual delivery date:	June-30th, 2017
Actual delivery date:	July-31st, 2017
Version:	V1.0
Reference to related publications	N/A

Executive Summary

As presented in the previous deliverable D3.2, Public Administrations or PAs, and Small and Medium-sized Enterprises or SMEs are still in need of "meaningful" understanding of the security and risk management changes the cloud entails, in order to assess how "good enough" is the new computing paradigm for their security requirements.

Here we present the CloudWATCH2 approach to the development of a simplified risk assessment and management approach to uptake of cloud services, called "risk profiling", based on the presumption that SMEs/PAs need simple, flexible, efficient and cost-effective cloud solutions that can be effectively secured.

This deliverable proposes a risk profiling methodology to assist PAs and SMEs in the next step of their risk assessment process from the perspective of a cloud service customer (CSC) procuring a suitably secure cloud-based service. The proposed approach also provides information to cloud partners (e.g. cloud brokers) and cloud service providers (CSPs), on the risk management methodology for cloud adoption used by a (prospective) customer organization. For the context of the deliverable, feedback was collected by European PAs and SMEs on the applicability of the proposed risk profile approach by non-expert users.

This final report continues with the leveraging of cloud risk assessment (presented in D3.2) by helping and empowering PAs and SMEs in validating and understanding their cloud security requirements.

This deliverable (i.e. D3.5) presents a risk profile table, equally appropriate for both SMEs and PAs, based on the risk profile table of the ENISA deliverable "Information Package for SMEs" as well as on end-user feedback. **The proposed methodology leverages best practices such as that offered by the Cloud Security Alliance's "Cloud Controls Matrix" (CCM)**.

Table of Contents

Table of Tables

Table of Figures

1 Introduction

We propose a risk-based decision-making framework to contribute to the selection of cloud services from a security perspective. Comparison of competing cloud services needs to be fair, and for a Public Administration (PA) in particular, auditably so. Following a standardized approach to assigning cloud solutions to standardized security risk profiles, enables such a fair comparison.

This is the validation of the proposed risk profiling approach in D3.2, with a particular focus on its applicability by non-security expert users from European SMEs and PAs. To achieve this, we drafted a framework that can be a business risk assessment enabler and explores, at a managerial level, the threats, vulnerabilities, security, interoperability, legal requirements, and the potential impact a PA/SME faces in relation to its IT systems and the information they store, disseminate and protect.

This framework answers the 2 issues that arise for the risk assessment process in the previous deliverable D3.2:

a) How can a (non-security expert) SME/PA meaningfully assess if a cloud supply chain fulfils their security requirements?
b) How can the sustained provision of security assurance to the SME/PA during the full cloud service life cycle be guaranteed?

Based on early research and feedback, we substituted step 1 from D3.2 (Assessing the security posture) by questionnaire, with a 4x4 table that presents 4 main risk areas for cloud services to be purchased by PAs or SMEs.

Step 2 (Selection of security controls) presents a set of security controls (Cloud Security Alliance's Cloud Controls Matrix[1]) suitable for mitigating the identified risks.

Step 3 (Deployment and Monitoring of the Risk Profile) can be carried out by the PA/SME by validating the amount of security controls they implement according to the risk level that is more relevant to their organization and services.

To sum up, this deliverable presents the creation of risk profiles for SMEs and PAs and the definition of the minimum-security measures mapped against the 3 risk levels (high, medium and low).

1.1 Scope of the document

Cloud Service Providers (CSPs) are delivering scalable, on-demand services that are cost effective because a common service is being provided to a wide range of customers. The obligation then typically falls on the cloud service customer (CSC) to ensure that the cloud service meets their requirements, rather than the other way around. The CSP will have chosen a particular set of methodologies for securing their cloud services, and these are generally documented, and made available to the CSC. It is then the CSC's task to confirm that the documentation describes security that meets their data security requirements.

Thus, the cloud service customers desperately need mechanisms and tools that enable them to assess the perceived risks in management, security, regulatory, etc. that use of the cloud entails that may be different and less familiar than those currently in use.

When adopting a cloud computing solution for their information systems, a PA/SME needs to understand its responsibilities for achieving adequate information security and for managing information system-related security risks at all service levels of the organization.

Any time the consumers adopt a cloud-based solution, they need to evaluate the specifics and place them under the umbrella of security requirements such as technical, operational and management classes. Most SMEs/PAs, however, lack the rich body of knowledge and hands-on cloud computing experience necessary for such a risk management approach.

[1] https://cloudsecurityalliance.org/download/cloud-controls-matrix-v3-0-1/

The risk profiling approach in the rest of this document simplifies the procedures enabling its guidelines to become user-friendly for non-experts. Thus, CSPs can be assigned to the appropriate security level, such that one or more with a 'good enough'[2] security level can be rapidly selected.

This provides the cloud service customer with a step-by-step procedure that allows them to customize controls for a certain set of digital assets, common to the cloud service, by exposing threats or security posture. Mapped controls can then relate to bilateral agreements as Service Level Agreements to increase and monitor the levels of trust and transparency provided to PAs/SMEs.

1.2 Objectives and Target Audience

This final version of our incremental deliverable on risk profiles for SMEs/PAs, proposes a risk profile evaluation table based on ENISA's 'Information Package for SMEs'[1] document.

The goal is for PAs and SMEs to identify their businesses' different applications risk profile. The risk context is derived from the business and the external environment of an organization and can be divided into **four risk areas**: Legal and Regulatory, Reputation and Customer Confidence, Operations, and Financial Stability.

Here we aspire to offer the validation and refinement of the risk assessment approach, that was presented in D3.2[3], focusing on SMEs and PAs.

After analyzing the challenges related to the specification and use of state-of-the-art risk management frameworks and based on the identified challenges, this report proposes a final version of a risk-profiling methodology specifically suited for PAs and SMEs keen to adopt cloud services. The proposed approach can also provide information to cloud partners (e.g. cloud brokers) and cloud service providers, on the risk management methodology for cloud adoption by a customer organization.

The approach to solving the problem of how best to develop security risk profiles for cloud solution that we present here, addresses the whole cloud lifecycle from procurement, through operation up to and including termination and off boarding. This is done by specifying the security attributes that should be outlined in the Service Level Agreements (SLA). This is advocated as a promising approach to empower PAs and SMEs in assessing and understanding their cloud requirements through the whole cloud service lifecycle.

Whilst intended for non-expert users belonging to European SMEs and PAs, this document will also benefit policy makers and standardisation bodies working on the creation of roadmaps motivating the (secure) usage of cloud computing in the private and public sectors. Our intention is that the methodology and risk profiles documented in both D3.2

[2] The concept analysed in D3.2 that was introduced by Sandhu, "everything should be made as secure as necessary, but not securer".

[3] D3.2 Risk-Based Decision Making Mechanisms For Cloud Service In The Public Sector.

and D3.5, can be used as a basis for developing standards and best practices aimed to increase their level of adoption both from the SMEs and PAs part.

1.3 Structure of this document

The rest of this document is structured in the following manner:

- Section 2 presents the requirements elicited in D3.2 and that were used as a baseline for the risk profile approach that is applicable to both PAs and SMEs.
- Section 3 introduces the methodology previously leveraged for risk profiling.
- Section 4 provides a high-level overview of the proposed methodology for developing risk profiles and how it leveraged the risk assessment methodology from D3.2 (D3.2 Risk-Based Decision Making Mechanisms For Cloud Service In The Public Sector).
- Section 5 presents the Risk Profile Table for Public Administrations
- Section 6 presents the Risk Profile Table for SMEs
- Section 7 describes the mapping of CCM controls to the risk areas
- Section 8 discusses the recommendation of this methodology for PAs/SMEs
- Section 9 concludes this report.

2 Elicited Requirements

After the extensive desktop research documented in D3.2, an initial set of requirements for the development of risk profiles for Public Administrations was elicited and analyzed. It is presented here in the following table. These requirements were used to steer the Risk Profile approach shown in the next section.

As the following requirements are a general and initial step for the development of the approach, we believe that this simplified self-assessment risk profile approach (cf. section 4.1) can apply the same to PAs and SMEs with some slight differences regarding the audience of these two sectors and the data they handle.

Table 1: Risk Profile Requirements

ID	Requirement	Comment
R1	High assurance	Despite aiming for a simplified approach for assessing risks, the developed risk profiling methodology should guarantee the high assurance of the obtained results (i.e., resulting impact level for the PA).
R2	Practicability	The risk profiling methodology should be easy to use and understand, even by non-security experts.
R3	Standards/best practices-based	In order to facilitate its adoption, the risk profiling methodology should be based on well-known standards and

ID	Requirement	Comment
		best practices.
R4	Non-cloud specific	The risk profiling methodology should not be cloud specific so also prospective cloud customers can also apply it before deciding to move to the cloud.
R5	Adaptable	The methodology should enable capturing the different in the threat scenarios found in the PAs.
R6	Self-directed	The proposed approach should methodologically guide PAs towards the elicitation of their risk profile.
R7	Context-based	The methodology should capture the current state of security practice within the PA (even if it is not a cloud customer yet). Please also refer to R4.
R8	Focused on critical assets	Like any other risk assessment process, the risk profiles should be able to identify the risk related to the PA's more critical assets (even if these are not cloud-based).
R9	Improve security posture	Outcomes of the risk profiling process should aim towards prioritizing areas of improvement and setting the security strategy for the PA.
R10	Focused on highest risks	Apart from identifying the most critical assets (cf. R8) of the PA, the proposed methodology should also clearly relate the most relevant risks associated to those assets.
R11	Automation	The risk profiles should be feasible to instantiate through mechanisms like Service Level Agreements, but also using software tools to empower customer PAs.

3 Assessing the risk context – Leveraging the Risk Profile Development Process

D3.2 identified and presented all relevant state-of-the-art frameworks for risk management which were categorised in Academia, Projects, Standards, Case Studies, and Best Practices. A few notable examples would be: ENISA's "Security Framework for Governmental Clouds" document [2], the U.K's approach as pathfinder for other countries [3], relevant EU projects (e.g. A4CLOUD [4], Cloud for Europe [5], RISCOSS [6], etc.), the MAS case study [7], ISACA's 10 Principles for Assessment [8], US National Institute of Standards and Technology (NIST

500-291 , 800 37 / 800 30), ISO 27001 (also ISO/IEC 27005), the COBIT framework from ISACA, etc.

However, and based on the elicited requirements that were captured from these State-of-The-Art frameworks, the most relevant framework for risk profiling include ENISA's Information Package for SMEs, with examples of Risk Assessment / Risk Management for two SMEs [1]. By taking inspiration from one of the 2 use cases it presents, we leveraged the security posture in D3.2 by providing organisations with the opportunity to evaluate their business risk profile using a predefined set of qualitative criteria, instead of a questionnaire like it was conducted in D3.2.

This approach is further analyzed in the following sections.

4 Approach

In D3.2 the proposed approach consists of three incremental steps (cf. Figure 1), which were designed to fully cover the more traditional security management lifecycle (Plan-Do-Check-Act). Collection and analysis of security, interoperability and legal requirements was carried through which resulted in the elicited requirements presented above in Table 1.

Figure 1: Development and Usage of risk Profiles

In D3.5 we present the results of the empirical validation of the proposed risk profiling approach, with a particular focus on its applicability by non-security expert users from European SMEs and PAs.

This same philosophy stood behind the ENISA document 'Information Package for SMEs' [1] which aimed to shield (non-expert) users from the complexity of risk management and risk assessment activities.

For this purpose and based on the elicited requirements (security, interoperability, legal) from D3.2 we provide a simplified risk profile approach which can be used as an example of good practice for assessing information risks by a PA/SME in order to have a 'good enough' security level for their services and applications hosted in a cloud environment.

4.1 Step 1: Evaluate business risk profile

STEP 1: Assessing the security posture presented in D3.2 has been now updated and substituted by the 4x4 table.

The main idea behind this table is to help organizations with self-assessment. Now in STEP 1, a PA's/SME's assessment team, can evaluate their business risk profile by using a predefined set of qualitative criteria by using the risk evaluation table (cf. Table 2) which helps them identify their risk context.

To create risk profiles for Public Administrations/SMEs we need to determine what information security risk management is appropriate for them. As mentioned earlier the approach and the risk areas are the same for both SMEs and PAs with only differences the description of the risk areas according to the audience of the organization and the data they handle.

While in ENISA's 'Information Package for SMEs' the risk context derived from the business and the external environment of the organization is divided into four risk areas: Legal and Regulatory, Reputation and Customer Confidence, Productivity, and Financial Stability, here we divide also in four risk areas which are namely: **Legal and Regulatory**, **Operations**, **Financial Stability**, and **Reputation and Loss of Citizen's service**.

Table 2: Risk Profile Evaluation Table

Risk Areas	High	Medium	Low
Legal and Regulatory			
Operations			
Financial Stability			
Reputation and Loss of Service			

The **Legal and Regulatory** framework used by an organization must be consistent with all laws, regulations, and standards of due care with which the organization must comply regarding all possible form of data it handles (personal data, special categories of personal

data, judicial data, non-personal data[4]). It is up to the organization to define which data it considers sensitive and are of high importance to avoid any possible leak.

Operational practices focus on technology-related issues dealing with how people use, interact with, and protect technology. They are subject to changes as technology advances and new or updated practices arise to deal with those changes. An example of typical operational practice areas usually includes: Physical security, Information Technology Security, Staff Security.

Financial Stability profile is also considered to have sensitive financial information. An organization handling customers' money and responsible for transactions is required to protect the privacy of its customers. The organization's security policy should explicitly require role-based access to information. Apart from access control mechanisms, this profile covers also the issues of Application and Interface Security, Business Continuity, Encryption, Human Actors, etc.

Reputation and Loss of Service profile considers a broad range of potential threat sources and allows an organization to identify the threats to its critical assets based on known potential sources of threat like Human Actors, System Problems, Physical Access problems, etc.

Each of the above risk areas is classified in three classes/levels: **High, Medium** and **Low**. These risk levels help categorize services within SMEs/PAs between those who are of high risk profile and would need additional security controls, medium risk profile (don't have highly valuable assets but cannot be considered of low risk either) or low risk profile with less security controls.

These classes express quantitative criteria for the organization in question with regard to the risk area and help identify a risk level. The organization's assessment team evaluates risks identified for every area in order to produce the organization risk profile.

They define the risk profile of the services that the organization is offering/creating and can also locate various services in various risk profiles.

A high risk carried in the Operations risk area marks a high-risk profile for the application moving/developed in the cloud. Equally, a medium-risk leads to a medium risk profile and low risks to low-risk profiles. For example, a low risk carried in the Financial risk area, in Legal and Regulatory and Reputation but a high risk in Operations risk area concludes to a high organization risk profile.

4.2 Step 2: Mapping of CCM Security Controls

STEP 2 in D3.2, Selection of Security Controls, we recommended a set of security controls suitable for mitigating the identified risks.

[4] Following the terminology set forth in the GDPR (Art. 4 and 9, 10)

In order for PAs to select a set of security controls and Enterprise Architecture components (i.e. domains, containers and capabilities) corresponding to the computed impact level, we had developed a mapping linking all of these elements that was the joint expertise of CSA and NIST 800-53 rev4 [9].

However, the approach followed by NIST for its control framework SP 800-54 rev4 [9], focused particularly on US-based PAs, which may not necessarily be cloud customers. While here, for the purposes of CloudWATCH2 we address European PAs and SMEs from the cloud customer perspective.

Therefore, we now leverage Step 2 by mapping each risk area and risk level to the 133 security controls that are described in the CSA's Cloud Controls Matrix. This way, the PA/SME can see what is the minimum of the security controls they need to implement when they link their service to a cloud service model.

4.3 Step 3: Proof of Concept

With the Proof of Concept step we are reinforcing STEP 3 from D3.2, Deployment and Monitoring of the Risk Profile.

As SMEs/PAs and CSPs have differing degrees of control over cloud-based IT resources, they need to equitably share the responsibility of implementing and continuously assessing the security requirements.

By asking organizations to assess their cloud hosted services and then propose to them which CCM security controls should be implemented for them to have the good-enough security principle (everything should be made as secure as necessary, but not securer) [10] we help guide them and the CSPs in the Deployment and Monitoring phase of the risk profile.

By going through the security controls one by one for each risk area-level their service applies to, an organization can double check and assess which controls they are implementing, which they have not included and think would be of additional value, as well as monitor the SLA agreement with their cloud service provider.

Appendix B.provides an anonymous example of Proof of Concept done by a European PA in the context of this deliverable. The PA agrees that such organizations should do a self-assessment and believed the approach presented is good enough for all kind and size of Public Administration in the European area.

5 Risk assessment for Public Administrations

The qualitative criteria included in the table below (cf. Table 3) aims at providing a general spectrum of important focus areas that can become an umbrella for all possible assets according to how a cloud customer categorizes them regarding the importance they bear to their business. For the purposes of this document, we do not care to narrow rather than

broad the meaning of the risk area to the importance the cloud customer (PA in this case) gives to the data it has in possession and handles when using a cloud service. It is the organizations risk assessment team that proceeds with identification and definition of the organization's critical assets.

From feedback received from contacted European PAs, the content of the risk areas has been formulated as appears below. The majority of the PAs contacted, agreed with the risk profile approach and the structure of the 4 risk areas, or pointed out it was similar to the regulation system their country had for cloud security measures. Suggested changes were formulated from the point of view of a small country, but also taking into consideration that big countries have small municipalities which would perceive the limit of 5 M € as relatively high for their Financial Stability, for example. Equally, Operations High impact is defined as a relatively good level of 1000 citizens served (in comparison to 500 citizens daily in the original description, which was considered to be a low number) and Reputation and Loss of Service High impact is set on level of more than 30% of citizens served (from originally having set it at 70%), who would face inconvenience and storm the PA.

Table 3: Risk Profile Table for PAs

Risk Areas	High	Medium	Low
Legal and Regulatory	The Public Administration handles citizen's special categories of personal data and/or data relating to criminal convictions and offences as defined in the EU Data Protection Law. (Here belongs also data that is classified as Top Secret, Secret and Confidential).	The PA handles only citizen's personal data as defined by the EU Data Protection Law. (Here belongs also data that is classified as of restricted level)	The PA does not handle/require personal data of the citizen that use its service through a cloud provider.

Operations	The PA serves more than 1000 citizens who have a daily need to access its applications and services.	The PA serves more than 500 citizens and less than 1000 who have a daily need to access its applications and services.	The PA serves less than 500 citizens who have a daily need to access its applications and services.
Financial Stability	Annual profitability of the PA exceeds 25M Euros or/and financial transactions with third parties or citizens are taking place as part of the PA as usual process.	Annual profitability of the PA does not exceed 25 M. Euros.	Annual profitability of the PA does not exceed 0.5M euros.
Reputation and Loss of Citizen's service	Unavailability or Service Quality directly impact the offered services of the PA or/and more than 30% of citizens have online access to PA's applications and services.	Unavailability or Service Quality can indirectly impact the services of the organization and/or less than 30% of citizens have online access to PA's applications and services.	Unavailability or Service Quality cannot directly or indirectly impact the services of the PA or result in loss of revenues.

6 Risk Assessment for SMEs

The same qualitative criteria as in the PA risk profile table (cf. Section 5) is used here, after being adapted to the SMEs profile so that a non-expert user can make use of it when she/he use Cloud services for running part of their business.

Table 4: Risk Profile Table for SME's

Risk Areas	High	Medium	Low

Legal and Regulatory	The organization handles citizen's special categories of personal data and/or data relating to criminal convictions and offences as defined in the EU Data Protection Law. (Here belongs also data that is classified as Top Secret, Secret and Confidential).	The organization handles only citizen's personal data as defined by the EU Data Protection Law. (Here belongs also data that is classified as of restricted level)	The organization does not handle personal data other than those of the people employed by the organization.
Operations	The organization employs more than 100 employees who have a daily need to access business applications and services.	The organization employs more than 10 employees and less than 100 employees who have a daily need to access business applications and services.	The organization employs less than 10 employees who have a daily need to access business applications and services.
Financial Stability	Annual profitability of the organization exceeds 25M Euros or/and financial transactions with third parties or customers are taking place as part of the business as usual process.	Annual profitability of the organization does not exceed 25 M. Euros.	Annual profitability of the organization does not exceed 5M euros.
Reputation and Loss of Citizen's service	Unavailability or Service Quality directly impact the businesses of the organization or/and more than 70% of customer base have online access to business products and services.	Unavailability or Service Quality can indirectly impact the businesses of the organization and/or less than 5% of customer base have online access to business products and services.	Unavailability or Service Quality cannot directly or indirectly impact the businesses of the organization or result in loss of revenues.

7 Mapping of security controls to risk levels

In each Risk Area like Legal and Regulatory and in each Risk Level such as high, medium and low, we mapped 133 security controls that are included in the Cloud Controls Matrix (CCM) [11]. These represent the minimum of security controls that an organization needs to implement in order to have a 'good enough' security level. The CCM security controls include mapping to different security standards, such as NIST 800-53 which was presented in D3.2.

CCM covers 16 different security domains that are cross-walked to other industry-accepted security standards, regulations, and controls frameworks that vary from Information Technology Security, Human Resources Security, Encryption and Key Management, Governance and Risk Management, Interoperability & Portability, Supply Chain Management, Transparency and Accountability, Threat and Vulnerability Management to Mobile Security, etc.

Appendix A. presents the table with all security controls mapped to each level and which a PA/SME can use to achieve the principle of "everything should be made as secure as necessary, but not securer".

To each risk area and risk level we mapped controls coming from all 16 domains. The High risk level for each of the four risk areas contains all 133 controls, while for the Medium level, we have mapped an important smaller number of minimum controls and the Low level contains substantially even less controls that need to be implemented in order to have the minimum security for a cloud-hosted service/application.

8 Recommendations

The Risk Profile approach presented in the above sections was recognised and accepted by different PAs (mainly government organisations, e.g. ministry of Public Administration, etc.) and SMEs as helpful and adequate for ranking PAs/SMEs and the data they handle. This approach and the criteria it presents were considered good enough for all kind and size of Public Administrations/SMEs in the EU area or even wider.

What we provide here is a framework for SMEs/PAs to perform a self assessment of the data and services they handle, categorize their services in relevant risk areas and, they can follow the implementation of the security controls in collaboration with their cloud service provider which would contribute to the governance of cloud activities, providing transparency and assisting in the monitoring of services and the enforcement of SLAs.

Even in the case where an organisation has its own security standard, as did one of the PAs we contacted, they can still benefit from this approach as both the organisation (PA/SME) and the Cloud Security Alliance can work on mapping the new Security Standard to the CCM controls. This way the organisation would be able to identify the minimum security controls for their services, while CSA would enrich the CCM with one more Standard.

9 Conclusions

Prospective cloud service customers in particular from the public sector find the ICT security assessment particularly useful. The inherent requirements of traditional risk management methodologies (e.g. the need for security experts), has led the ICT security community to search for more straightforward approaches ideally suited to PAs and SMEs.

Risk profiling allows the assessment of the security posture of a PA/SME in a more simple and direct way leading the CSCs who either consider using the Cloud or are already users of this technology.

Based on a previous work done by ENISA, this document aimed to develop a methodological approach for using risk profiles, which are particularly suited and simple to use for Public Administrations and Small and Medium-sized Enterprises. The proposed methodology consists of a 4x4 table that brings organizations in the position to identify the risk context of their cloud based applications. The risk context is derived from the business and the external environment of an organization and is divided into four risk areas: Legal and Regulatory, Reputation and Customer Confidence, Operations, and Financial Stability. This proposed approach does not require the use of expert knowledge and has the added benefit of allowing the continuous optimization of the SME's/PA's security level.

It offers space for flexible solutions as Cloud Service Level agreement acts as one potential mechanism for deploying/ monitoring/ improving the PA's/SME's "risk appetite".

This deliverable presents a validated version of the proposed methodology which resulted from the feedback from different stakeholders (e.g. European SME/PA representatives)

Also, we leveraged the proposed methodology using best practices like CSA Cloud Controls Matrix, which is a mechanism that helps to further deploy automated tools instantiating the different stages of the contributed risk profiling methodology.

Appendix A.

Table 5: Mapping the CCM security controls to each risk area and level

Risk Areas	High	Medium	Low
Legal and Regulatory CCM controls	AIS-01, AIS-02, AIS0-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12, IVS-13, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05, MOS-01, MOS-02, MOS-03, MOS-04, MOS-05, MOS-06, MOS-07, MOS-08, MOS-09, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-	AIS-01, AIS-02, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, , DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-02, DCS-03, DCS-04, DCS-05, DCS-07, DCS-08, DCS-09, , EKM-02, EKM-03, GRM-01, GRM-02, GRM-03, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, , IAM-05, IAM-06, IAM-07, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-03, IVS-04, IVS-06, IVS-08, IVS-09, IVS-12, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-03, STA-05, STA-09, TVM-01, TVM-02	AIS-01, GRM-03, IAM-03, IAM-05, IAM-10, STA-03

	19, MOS-20, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09, TVM-01, TVM-02, TVM-03		
Operations **CCM Controls**	AIS-01, AIS-02, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12, IVS-13, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05, MOS-01, MOS-02, MOS-03, MOS-04, MOS-05, MOS-06, MOS-07, MOS-08, MOS-09, MOS-	AIS-01, AIS-02, AIS-03, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-02, EKM-03, GRM-01, GRM-02, GRM-03, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-05, IAM-06, IAM-07, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-03, IVS-04, IVS-06, IVS-08, IVS-09, IVS-12, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-03, STA-05, STA-09, TVM-01, TVM-02	AIS-01, AIS-02, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-04, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-03, DSI-05, DSI-06, DSI-07, DCS-03, DCS-04, DCS-05, EKM-03, GRM-01, GRM-02, GRM-03, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-04, HRS-05, HRS-06, HRS-09, HRS-10, IAM-03, IAM-05, IAM-07, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-04, IVS-06, IVS-09, IVS-12 SEF-03, SEF-04, STA-03, STA-05, STA-09, TVM-01, TVM-02

	10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09, TVM-01, TVM-02, TVM-03.		
Financial Stability **CCM Controls**	AIS-01, AIS-02, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12, IVS-13, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05, MOS-01, MOS-02, MOS-03, MOS-04, MOS-05, MOS-06, MOS-07, MOS-08, MOS-09, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04,	AIS-01, AIS-02, AIS-03, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-02, EKM-03, GRM-01, GRM-02, GRM-03, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-05, IAM-06, IAM-07, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-03, IVS-04, IVS-06, IVS-08, IVS-09, IVS-12, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-03, STA-05, STA-09, TVM-01, TVM-02	AIS-01, AIS-02, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-04, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-03, DSI-05, DSI-06, DSI-07, DCS-03, DCS-04, DCS-05, EKM-03, GRM-01, GRM-02, GRM-03, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-04, HRS-05, HRS-06, HRS-09, HRS-10, IAM-03, IAM-05, IAM-07, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-04, IVS-06, IVS-09, IVS-12, SEF-03, SEF-04, STA-03, STA-05, STA-09, TVM-01, TVM-02

	STA-05, STA-06, STA-07, STA-08, STA-09, TVM-01, TVM-02, TVM-03		
Reputation and Loss of Citizen's service **CCM Controls**	AIS-01, AIS-02, AIS0-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05, IVS-06, IVS-07, IVS-08, IVS-09, IVS-10, IVS-11, IVS-12, IVS-13, IPY-01, IPY-02, IPY-03, IPY-04, IPY-05, MOS-01, MOS-02, MOS-03, MOS-04, MOS-05, MOS-06, MOS-07, MOS-08, MOS-09, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14,	AIS-01, AIS-02, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-04, DSI-05, DSI-06, DSI-07, DCS-02, DCS-04, DCS-05, DCS-07, DCS-08, DCS-09, EKM-02, EKM-03, GRM-01, GRM-03, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, IAM-03, IAM-05, IAM-06, IAM-07, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-03, IVS-04, IVS-06, IVS-09, SEF-01, SEF-02, SEF-03, SEF-04, STA-03, STA-05, STA-09, TVM-01, TVM-02	AIS-01, DSI-06, DCS-05, GRM-03, IAM-03, STA-03

	MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08, STA-09, TVM-01, TVM-02, TVM-03		

Appendix B.

This appendix contains the anonymous example of the Proof of Concept that was carried out by a European Public Administration within the context of this deliverable. The PA sent a self-assessment that its IT-Directorate made regarding the services and applications the organization implements on the cloud. According to the Cloud Controls Matrix security controls we had mapped to each risk area for the purposes of this deliverable, the PA recognized which of those controls it has implemented or are in the implementation phase regarding the cloud services they offer to the citizens of their country.

The PA identified as having a high-risk profile for all its services in the mentioned risk areas of Legal and Regulatory, Operations, Financial Stability and Reputation and Loss of Citizen's Services. In bold are the CCM controls that the PA verifies as being implemented or as being in the implementation phase for its security framework in comparison to the proposed number of minimum mapped security controls.

As can be observed in the table below, most of the suggested CCM controls have been or are being mapped (controls that cover security domains such as Identity and Access Management, Infrastructure and Virtualization Security, Application and Interface Security, Audit Assurance, Business Continuity, Data Center Security, Human Resources, etc.). The controls that cover the security domains of Mobile Security, and Interoperability and Portability are the ones with the least controls implemented which indicates that PAs are not yet considering mobile security for their applications/services and migration of applications is not an issue taken into consideration in the agreement process with the cloud providers.

Risk Areas	High
Legal and Regulatory CCM controls	**AIS-01, AIS-02**, AIS0-03**, AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02**, BCR-03, **BCR-04, BCR-05, BCR-06, BCR-07, BCR-08**, BCR-09, **BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05**, **DSI-01, DSI-02**, DSI-03, DSI-04, **DSI-05**, DSI-06, **DSI-07**, **DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05**, IVS-06, **IVS-07, IVS-08, IVS-09**, IVS-10, **IVS-11, IVS-12, IVS-13**, IPY-01, **IPY-02**, IPY-03, IPY-04, IPY-05, **MOS-01**, MOS-02, MOS-03, MOS-04, **MOS-05,** MOS-06, MOS-07, MOS-08, **MOS-09**, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, **SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08**, STA-09, **TVM-01**, **TVM-02**, TVM-03
Operations CCM Controls	**AIS-01, AIS-02**, AIS-03, **AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02**, BCR-03, **BCR-04, BCR-05, BCR-06, BCR-07, BCR-08**, BCR-09, **BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05**, **DSI-01, DSI-02**, DSI-03, DSI-04, **DSI-05**, DSI-06, **DSI-07**, **DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05**, IVS-06, **IVS-07, IVS-08, IVS-09**, IVS-10, **IVS-11, IVS-12, IVS-13**, IPY-01, **IPY-02**, IPY-03, IPY-04, IPY-05, **MOS-01**, MOS-02, MOS-03, MOS-04, **MOS-05**, MOS-06, MOS-07, MOS-08, **MOS-09**, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, **SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08**, STA-09, **TVM-01**, **TVM-02**, TVM-03.

Financial Stability **CCM Controls**	**AIS-01, AIS-02**, AIS-03, **AIS-04, AAC-01, AAC-02, AAC-03, BCR-01, BCR-02**, BCR-03, **BCR-04, BCR-05, BCR-06, BCR-07, BCR-08**, BCR-09, **BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-02**, DSI-03, DSI-04, **DSI-05**, DSI-06, **DSI-07, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-01, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05**, IVS-06, **IVS-07, IVS-08, IVS-09**, IVS-10, **IVS-11, IVS-12, IVS-13**, IPY-01, **IPY-02**, IPY-03, IPY-04, IPY-05, **MOS-01**, MOS-02, MOS-03, MOS-04, **MOS-05**, MOS-06, MOS-07, MOS-08, **MOS-09**, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, **SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08**, STA-09, **TVM-01**, **TVM-02**, TVM-03
Reputation and Loss of Citizen's service **CCM Controls**	**AIS-01, AIS-02**, AIS-03, AIS-04, AAC-01, AAC-02, AAC-03, **BCR-01, BCR-02**, BCR-03, **BCR-04, BCR-05, BCR-06, BCR-07, BCR-08,** BCR-09, **BCR-10, BCR-11, CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, DSI-01, DSI-02**, DSI-03, DSI-04, **DSI-05**, DSI-06, **DSI-07, DCS-01, DCS-02, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, EKM-01, EKM-02, EKM-03, EKM-04, GRM-01, GRM-02, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, HRS-01, HRS-02, HRS-03, HRS-04, HRS-05, HRS-06, HRS-07, HRS-08, HRS-09, HRS-10, HRS-11, IAM-1, IAM-02, IAM-03, IAM-04, IAM-05, IAM-06, IAM-07, IAM-08, IAM-09, IAM-10, IAM-11, IAM-12, IAM-13, IVS-01, IVS-02, IVS-03, IVS-04, IVS-05**, IVS-06, **IVS-07, IVS-08, IVS-09**, IVS-10, **IVS-11, IVS-12, IVS-13**, IPY-01, **IPY-02**, IPY-03, IPY-04, IPY-05, **MOS-01,** MOS-02, MOS-03, MOS-04, **MOS-05**, MOS-06, MOS-07, MOS-08, **MOS-09**, MOS-10, MOS-11, MOS-12, MOS-13, MOS-14, MOS-15, MOS-16, MOS-17, MOS-18, MOS-19, MOS-20, **SEF-01, SEF-02, SEF-03, SEF-04, SEF-05, STA-01, STA-02, STA-03, STA-04, STA-05, STA-06, STA-07, STA-08**, STA-09, **TVM-01**, **TVM-02**, TVM-03

References

[1] ENISA. (2007). Information Package for SMEs, With examples of Risk Assessment / Risk Management for two SMEs.p20.

[2] ENISA. (2015). Security Framework for Governmental Clouds - All steps from design to deployment.

[3] R. Kemp. Seeding the Global Public Sector Cloud: Part II – The UK's Approach as Pathfinder for Other Countries.

[4] EU A4CLOUD Project. Available: http://www.a4cloud.eu/content/a4cloud-toolkit.

[5] J. Colpaert. (2015). D9.5 Risk Analysis, Certification and Other Measures. v.1. Cloud for Europe project.

[6] EU RISCOSS Project. Available: http://www.riscoss.eu/bin/view/Discover/The_RISCOSS_Solution

[7] G. Kulvinder. Monetary Authority of Singapore (MAS): Technology Risk Management Guidelines Overview.

[8] D. Vohradsky. (2012). Cloud Risk—10 Principles and a Framework for Assessment. ISACA. Vol. 5.

[9] NIST SP-800-53. rev. 4. (2013). Security and Privacy Controls for Federal Information Systems and Organizations.

[10] R. Sandhu. (2003). Good-enough security: toward a pragmatic business-driven discipline. IEEE Internet Computing. Vol. 7. No. 1. pp. 66-68.

[11] CSA. (2016). Cloud Controls Matrix. Available: https://cloudsecurityalliance.org/group/cloud-controls-matrix/. Last accessed June 2017.

Log Table

Version & Date	Action	Partner(s)
V0.1 – April 2017	Initial Table of Contents and Timeline	Marina Bregkou, John Yeoh, Damir Savanovic, CSA
V0.2 – May 2017	First full draft	Marina Bregkou, John Yeoh, Damir Savanovic, CSA
V0.3 – June 2017	Second full draft Internal consortium review	Nicola Franchetto, ICT-Legal; Nicholas Ferguson, Trust-IT; James Mitchell, Strategic Blue
V0.4 – July 2017	PMB Approval	Marina Bregkou, John Yeoh, CSA
V1.0- July 2017	Final version	Marina Bregkou, CSA