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

CloudWatch

Think Cloud Services for Government, Business & Research

This is the initial version of an incremental deliverable documenting the overall process adopted by CloudWatch2 to develop risk profiles for (prospective) cloud service customers from Public Administrations. Besides the actual process, this deliverable also presents the results of desktop research, which will be used to develop specific risk profiles in the second and final iteration of this document (D3.5). 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), and validated through real-world use cases.

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 he lp 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 se rvices 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.

The information, views and suggestions set out in this publication are those of the CloudWATCH2 Consortium and of its pool of international experts and cannot be considered to reflect the views of the European Commission.

Document Information Summary

Document title:	D3.2 Risk-Based Decision Making Mechanisms For Cloud Service In The Public Sector
Main Author(s):	Jesus Luna (CSA)
Contributing author(s):	Marina Bregou, Damir Savanovic, CSA
Reviewer(s):	Nicholas Ferguson, Trust-IT; Theodora Dragan & Lucio Scudiero, ICT Legal Consulting

Executive Summary

Despite the undisputed advantages of cloud computing, customers (in particular 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 if this new computing paradigm is "good enough" for their security requirements. Traditional ICT risk management approaches usually adopt one-size-fits-all methodologies relying on (security) experts, which are usually not adequate for small organisations and Public Administrations (PA) that use relatively simple IT-components. One of the main drivers of CloudWatch2 is to develop a simplified cloud risk assessment/management approach, called "risk profile" in this document, with the requisite that SMEs/PAs need simple, flexible, efficient and cost-effective cloud security solutions.

This deliverable proposes a risk profiling methodology to assist PAs with the risk assessment process from the perspective of a cloud service customer (CSC) procuring a suitable cloud-based service. The proposed approach also provides information to cloud partners (e.g. cloud brokers) and CSPs, on the risk management methodology for cloud adoption used by a (prospective) customer organization. Despite the fact that the main focus of this deliverable being on PAs, we also discuss the appropriateness of the suggested risk profile methodology for SMEs (to be further expanded in Deliverable 3.5 or D3.5).

This incremental report also presents a fresh approach to the problem of leveraging risk profiles by analysing, from the risk management perspective, the specification of security in mechanisms like Service Level Agreements (SLA) as a promising approach to empower PAs (and also SMEs) in assessing and understanding their cloud requirements.

The next version of this deliverable (i.e. D3.5) will present the validation results of the presented risk profiles, both for SMEs and PAs, based on real-world use cases and end-user feedback. In addition D3.5 will further elaborate on end-user mechanisms/tools for instantiating the proposed risk profiling methodology.

Table of Contents

Table of figures

Table of Tables

1 Introduction

Although the varied functional and economic benefits of the cloud are substantial, security assurance and transparency still remain as open issues to enable the customer's trust in Cloud Service Providers (CSPs). This is particularly critical in the case of Small and Medium-sized Enterprises (SMEs) and Public Administrations (PAs), which typically are not cloud (security) experts.

Furthermore, the growing number of CSPs offering diverse cloud-enabled services (from virtual machines and storage, to containers and big data analytics services) opens up the possibility of deploying complex services and workflows leveraging the services of more than one CSP (i.e. a cloud supply chain or even a multi-cloud system). Given this complex setup, and despite the advocated advantages of the cloud, two issues arise:

a) How can a (non-security expert) SME/PA meaningfully assess if a cloud supply chain fulfills 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?

The following section discusses how these decision-making questions relate to the notion of risk profiling, which is the main objective of this CloudWatch2 report.

1.1 Risk profiles for PAs: scoping the problem

A commonly implemented approach by public CSPs has relied on the adoption of cloud-specific "security control frameworks" (e.g. CSA Cloud Control Matrix[1]) as a mechanism to provide customers a reasonable degree of security assurance and transparency. Further assurance is then provided through the adoption of security certifications based on those controls frameworks, like in the case of CSA Open Certification Framework[2]. However, over the implementation of their security controls, the CSP can only assume the type of data a customer will generate and use; the CSP is not aware of the additional security requirements or the tailored security controls deemed necessary to protect the PA's[3] data. Thus the cloud service customers crucially require mechanisms/tools that enable them to understand and assess what "good-enough security" [1] means and especially the changes in risk assessment/management that the cloud entails.

Adopting cloud-based solutions for PAs' operations does not inherently provide for the same level of security and for compliance with mandatory regulations or elicited requirements that were achieved in the traditional (non-cloud) ICT model. A cloud service customer's ability to

[1] Please refer to https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[2] Please refer to https://cloudsecurityalliance.org/group/open-certification/

[3] Despite the focus of this deliverable is on Public Administrations, the developed risk profiles can be also extrapolated to SMEs. This will be further explored in D3.5

comply with any business, regulatory, operational, or security requirements in a cloud computing environment is a direct result of the service and deployment model being adopted, the cloud architecture, and the deployment and management of the resources in the cloud environment. Therefore, it is imperative that PA stakeholders at all levels of the organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks[4] when adopting a cloud computing solution for their information systems.

For each use case of an information system for which a cloud-based solution is adopted, it is necessary for the consumer to evaluate the particular security requirements in the specific cloud architectural context, and to map them to proper security controls and practices in technical, operational, and management classes. Such a *risk management* approach usually requires a rich body of knowledge around general information security management practices and cloud computing characteristics, which is usually out of reach for many PAs.

In the above-mentioned cases the philosophy behind the generation of the simplified risk-management approach, referred as *risk profiling* in the rest of this document, is to guide non-expert users in the complexity of risk assessment activities. In doing so, some complex security matters can be simplified to the minimum necessary in order to achieve an acceptable i.e. good enough) security level. This leads to a step-wise approach that reveals threat exposure/security posture from PAs by offering customized controls for a certain set of assets that are common to the cloud service to use. Elicited controls can then relate to bilateral agreements as Service Level Agreements to increase and monitor the levels of trust and transparency provided to PAs.

1.2 Objectives and Target Audience

This initial version of our incremental deliverable on risk profiles for SMEs/PAs, analyzes the challenges related to the specification and usage of state of the art risk management frameworks. Based on the identified challenges, this report proposes an initial version of a risk-profiling methodology specifically suited for PAs willing to adopt cloud services. The proposed approach also provides 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 validation and refinement of the proposed approach, although with a particular focus on SMEs, will be presented in D3.5

We also present a fresh view on the problem of developing risk profiles suitable for addressing the whole cloud lifecycle (i.e. procurement, operation, and termination), through the specification of security in attributes like Service Level Agreements (SLA). This is advocated as a promising approach to empower PAs in assessing and understanding their cloud requirements through the whole cloud service lifecycle.

This document also targets policy makers and standardisation bodies working on the creation of roadmaps motivating the (secure) usage of cloud computing in the private and public

[4] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

sectors. Our intention is that the methodology and risk profiles to be documented in both D3.2 and D3.5, can be used as a basis for developing standards and best practices aimed to increase their level of adoption both for SMEs and PAs.

1.3 Structure of this document

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

- Section 2 focuses on the elicitation of requirements for developing the risk profiles for PAs, based on a desktop research.
- Section 3 provides a high-level overview of the proposed methodology for developing risk profiles.
- Sections 4 – 6 describe in further detail the incremental steps of the risk profiling methodology.
- Section 7 concludes this report.

2 Desktop Research – Elicitation of Requirements

Relevant state-of-the-art frameworks for risk management include ENISA's "Security Framework for Governmental Clouds" document [5], the U.K's approach as pathfinder for other countries [6], EU projects (e.g. A4CLOUD [8], Cloud for Europe [10], RISCOSS [11], etc.), the MAS case study [13], ISACA's 10 Principles for Assessment [15], US National Institute of Standards and Technology (NIST 500-2915, 800 37 / 800 306), ISO 27001 (also ISO/IEC 27005), the COBIT framework from ISACA, etc.

More details on each of the above frameworks are included below. They are categorised according to sector: Academia, Projects, Standards, Case Studies, and Best Practices.

Table 1 gives a quick preview of the State-of-the-Art included here categorised in the mentioned sectors.

[5] NIST Cloud Computing standards

[6] NIST Cloud Computing Related Publications

Table 1. State of the Art

Academic Papers	Projects	Standards	Case Studies	Best Practices
-Comparative Study of Information Security Risk -Assessment Models for Cloud Computing systems -Addressing cloud computing security issues -A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems -QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security	EU FP7 A4Cloud EU FP7 Cloud for Europe EU FP7 RISCOSS EU FP7 ASSERT4SOA EU FP7 ANIKETOS EU FP7 NESSOS EU FP7 CIRRUS EU FP7 CUMULUS EU FP7 SPECS EU H2020 MUSAUS NSF "Risk Assessment Techniques for Off-line and On-line Security Evaluation of Cloud Computing"	NIST 800-37 ISO/IEC 27005 ISO/IEC 27017 NIST SP-800-144	Monetary Authority of Singapore FedRAMP International Development Authority of Singapore	ISACA's 10 Principles for Assessment ENISA, "Security Framework for Governmental Clouds" UK's Approach COBIT 5

2.1 Academic Papers

The paper on "Comparative Study of Information Security Risk - Assessment Models for Cloud Computing systems" examines in detail the quantitative security risk assessment models developed for or applied especially in the context of a Cloud Computing system. It analyses existing models in terms of aim; the stages of risk management addressed; key risk management concepts covered; and sources of probabilistic data. Based on the analysis, it also proposes a comparison between these models to pick out limits and advantages of every presented model. [40]

The "Addressing cloud computing security issues" paper, presents a solution that attempts to eliminate unique threats and introduces a Trusted Third Party, which is tasked with assuring security characteristics within a cloud environment. The solution employs Public Key Infrastructure in concert with SSO and LDAP. **Error! Reference source not found.**

The "A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems" paper presents various methodologies being designed and developed for performing risk assessment on both Cloud Service Provider (SP) and Infrastructure Provider (IP) levels. The main contributions of the work are the design and implementation of an effective and efficient risk assessment framework (methodologies of risk identification, evaluation, mitigation and monitoring) for Cloud service provision. Together with the corresponding mitigation strategies, the framework provides technological assurance that will lead to a higher confidence of Cloud service consumers on the one side, and a cost-effective and reliable productivity of SP and resources organized by individual Infrastructure Provider (IP) on the other side. [42]

"QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security." A quantitative risk and impact assessment framework (QUIRC) is presented, to assess the security risks associated with cloud computing platforms. This framework, called QUIRC, defines risk as a combination of the Probability of a security threat event and it's Severity, measured as its Impact. Six key Security Objectives (SO) are identified for cloud platforms, and it is proposed that most of the typical attack vectors and events map to one of these six categories. [43]

2.2 Standards

NIST's Guide for "Applying the Risk Management Framework to Federal Information Systems" (Special Publication 800-37 [17]), provides guidance on authorizing information system to operate, on monitoring the security controls in the environment of operation, the ongoing risk determination and acceptance, and the approved information system authorization to operated status. The purpose of this document is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. Among other reasons, the guidelines have been developed:

- To support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity; and
- To achieve more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.

ISO/IEC 27005:2011 [18] provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 [20] and ISO/IEC 27002 [21] is important for a complete understanding of ISO/IEC 27005:2011.

ISO/IEC 27005:2011 [18] is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations), which intend to manage risks that could compromise the organization's information security. It is important to mention that this International Standard does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS (information security management), context of risk management, or industry sector.

ISO/IEC 27017:2015 provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards. It gives guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation - International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers. [30]

NIST SP-800-144 is a set of recommendations on security and privacy in the cloud. It provides an overview of the security and privacy challenges facing public cloud computing and presents recommendations that organizations should consider when outsourcing data, applications and infrastructure to a public cloud environment. The document provides insights on threats, technology risks and safeguards related to public cloud environments to help organizations make informed decisions about this use of this technology.

The key guidelines include:

- Carefully plan the security and privacy aspects of cloud computing solutions before implementing them.
- Understand the public cloud-computing environment offered by the cloud provider.
- Ensure that a cloud computing solution—both cloud resources and cloud-based applications—satisfy organizational security and privacy requirements.

- Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments. [31]

2.3 EC-funded projects

A4Cloud[7] – Cloud Accountability Project

October 2012 – March 2016

The recently completed A4Cloud project [8] focused on the Accountability for Cloud and Other Future Internet Services as the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services. The goal of the project was to increase trust in cloud computing by devising methods and tools, by means of which cloud stakeholders can be made accountable for the privacy and confidentiality of the information stored in the cloud. These methods and tools were designed to combine risk analysis, policy enforcement, monitoring and compliance auditing. They contribute to the governance of cloud activities, providing transparency and assisting legal, regulatory and socio-economic policy enforcement. The sustainable output of the project is the A4Cloud toolkit[8], which supports accountable organisations in running accountability practices by implementing the accountability functions that should be executed by the cloud and data protection roles. At a high level, accountability functions can be classified as implementing relevant preventive, detective and corrective accountability mechanisms. Preventive mechanisms focus on mitigating the occurrence of an unauthorized action. The respective functions include assessing a risk, identifying and expressing appropriate policies to mitigate it, and enforcing these policies via mechanisms and procedures put in place. Detective mechanisms are used to identify the occurrence of an incident or risk that goes against the policies and procedures in place. The project also proposes a cloud adoption risk assessment model (CARAM), to help in assessing the various risks to business, security and privacy that cloud customers face when moving to the cloud by leveraging information from cloud customers, CSPs and several public sources. It is presented in the project's paper "A Cloud Adoption Risk Assessment Model" [16].

Cloud for Europe[9]

June 2013 – November 2016

Cloud for Europe, in the project's "Risk Analysis, Certification and Other Measures" document [10] determines a Risk Impact Analysis method and describes a method for mapping required measures derived from certification schemes on Perceived Risk Impact Levels. The project develops a scheme for Risk Impact Assessment suitable for Cloud for Europe and then applies it to the project's pilots. The project's goal is to address the objectives of the European Cloud Partnership and help partners to adopt a well-defined European Cloud Computing Strategy for the public sector.

[7] http://www.a4cloud.eu/

[8] http://www.a4cloud.eu/content/a4cloud-toolkit

[9] http://www.cloudforeurope.eu/

RISCOSS - Managing Risk and Costs in Open Source Software Adoption

November 2012 – October 2015

The RISCOSS project [11] offered novel risk identification, management and mitigation tools and methods for community-based and industry-supported OSS development, composition and life cycle management to individually, collectively and/or collaboratively manage OSS adoption risks. Using advanced software engineering techniques, RISCOSS has delivered a risk-aware technical decision-making management platform integrated in a business-oriented decision-making framework, which together support placing technical OSS adoption decisions into organizational, business strategy as well as the broader OSS community context. While leveraging recent advances in statistics, the RISCOSS platform is designed to cover the real-requirements provided by five use-cases. Telecommunications provider Ericsson Italia will use RISCOSS in the risk management program it is implementing to support its migration to a full open source paradigm.

ASSERT4SOA - Advanced Security Service cERTificate for SOA

September 2010 – October 2013

The project's goal was to develop enhanced methods for the certification of complex and continuously evolving SOA–based software systems and services and make use of existing certification processes within the SOA context (where possible), (ii) develop mechanisms and tools for the assessment of SOA–based systems' and services' trustworthiness, both at design time and runtime, based on systems and service certification, (iii) integrate the methods, mechanisms and tools of (i)–(ii) into the SOA lifecycle. [25] ASSERT4SOA produced novel techniques, tools, and an architecture for expressing, assessing, and certifying security properties for complex service-oriented applications, composed of distributed software services that may dynamically be selected, assembled and replaced, and running within complex and continuously evolving software ecosystems. [29] The project reached all its key objectives, defined all advanced concepts of ASSERT4SOA (language, ontology, composition) and worked on the integration of the solutions, developed within the different activities, in a common framework. In more detail, ASSERT4SOA developed:

- Conceptual instruments including a consolidated version of the ASSERTs language, a common scheme for the three kinds of certificates, a refined version of the ASSERT4SOA query language, schemes for composition of certificates and ASSERT4SOA ontology
- Software components and prototypes. All components of ASSERT4SOA and a common integration framework were developed, as well as demonstrators for the more advanced concepts.

ASSERT4SOA also defined a common, business motivated scenario based on a service marketplace), which was the basis for the validation of the framework. [46]

ANIKETOS[10] - Ensuring Trustworthiness and Security in Service Composition

[10] http://www.aniketos.eu/project

August 2010 – May 2014

ANIKETOS considered the problem of ensuring security and trustworthiness of services, which are composed dynamically at runtime. It provided methods to analyze new threats and vulnerabilities and methods on how to solve them by providing a platform for security and trust management of composite services. [26] The platform offers a set of design time and runtime capabilities to support service developers and service providers to establish security and trust in service composition, and monitor such attributes in composite service enactment. It, also, supports the online community with services for exposing reference implementations, demonstrations and training material. The final Aniketos platform integration delivers the appropriate testbed for evaluating the effectiveness of the Aniketos concepts to support real life scenarios in critical domains. The project fulfilled all its primary goals and the four components of the platform (the basic edition of the package) can be found in the project's open source community space at https://github.com/ AniketosEU.

The full set of functionalities is provided under a professional edition at a competitive price, which in addition offers the ability to extend the current list of threats and their associated countermeasures of the threat management system.

NESSOS - Network of Excellence on Engineering Secure Future Internet Software Services and Systems

October 2010 – March 2014

NESSOS has analysed the problem of engineering secure software-based services and systems. The project vision is based on the idea that this kind of goal can only be achieved by addressing security concerns from the beginning of system analysis and design. This approach can in fact reduce the probability of service vulnerabilities and integrate security treatment within the engineering process. NESSoS Cloud Execution Environment (CEE) consists of a cloud system that allows NESSoS users to execute virtual machines. Its main purpose is to provide a machine to run test suites of standalone and integrated NESSoS-related tools. A list of integrated tools and a brief description of them can be found in the following and at the NESSoS SDE site [11] (e.g. CORAS Tool: a model-driven approach to risk analysis that consists of three tightly integrated building blocks, namely the CORAS method, the CORAS language and the CORAS tool). [27] Already 25 tools have been integrated in this environment. The research excellence of NESSoS helps to increase the trustworthiness of the Future Internet by improving the overall security of software services and systems. This supports European competitiveness in this vital area. [45]

CIRRUS - Certification, InteRnationalisation and standaRdization in cloUd Security

October 2012 – December 2014

CIRRUS focused on solutions for security and privacy in cloud computing. It aimed to address those security and privacy concerns introduced by the need of moving sensitive services and data to the cloud, migrating data between different cloud providers, and facilitating businesses

[11] SDE. Service Development Environment. http://www.nessos-project.eu/sde, 2013

in joining the cloud infrastructure. CIRRUS also launched the CEN/CENELEC workshop [12] on Requirements and Recommendations for Assurance in the Cloud in order to provide recommendations for future cloud assurance standards [28]. In its green paper[13] for the finalization of the project, it provides guidance on Security, Privacy / Data Protection and Service Level Agreements (SLA) covering technological, policy and legal aspects related to cloud security. This CIRRUS Green Paper contains a set of 21 recommendations and overall identifies trust, assurance and transparency as major enablers for cloud adoption, while highlights specific actions needed in the areas of security, privacy and SLAs.

Published in 2015, this paper provided recommendations for the next 5 years in Cloud computing, which focus on the areas of policy definition and enforcement, standard and research. Some highlights of those recommendations are:

- Recommendation 1 - Increase transparency and assurance though awareness, education and certification of service and skills.
- Recommendation 3 - Follow up to the European Cloud Strategy
- Recommendation 5 - Reuse existing resources to develop EU attribute exchange infrastructure (AXI)
- Recommendation 8 – Create standardized metrics and protocols for the monitoring of Cloud security attributes.
- Recommendation 10 - Designate Cloud forensics as an explicit subject in CSP/user agreements
- Recommendation 15 - Standardize data deletion vocabulary and define good practices for deletion in Cloud services.
- Recommendation 20 - Support cloud customers though standardization, certification and tools for the management of Cloud security SLAs.
- Recommendation 21 – Support CSPs in the definition of automated tools for managing Cloud security SLAs.

CUMULUS - Certification infrastrUcture for MUlti-layer cloUd Services

October 2012 – September 2015

CUMULUS extended the work carried out in ASSERT4SOA. It focused on developing an integrated framework of models, processes, and tools supporting the certification of security properties at infrastructure (IaaS), platform (PaaS), and software application (SaaS) layers. Its final goal was to put service users, service providers, and cloud suppliers together with certification authorities to ensure security certificate validity in the cloud. For this reason it developed an infrastructure for realizing certification processes, and certification models that specify different types of security properties of cloud services, along with engineering support to address requirements. [32]

[12] CEN/CENELEC CIRRUS Workshop. http://www.cirrus-project.eu/sites/default/files/content-files/events/Programme_final_v10_0.pdf

[13] D2.3 Green Paper – Final version. CIRRUS

The CUMULUS infrastructure can be used to define certification models, which reflect certification profiles and processes used by traditional certification schemes (e.g. common criteria) or new certification profiles. The defined certification models are then automatically executed by the CUMULUS infrastructure to realise the relevant certification processes and generate the documentation, evidence and digital certificates expected by them. [44]

SPECS - Secure Provisioning of Cloud Services based on SLA management

November 2013 - May 2016

SPECS produced a framework supporting techniques and tools for user-centric negotiation of security parameters in SLA, monitoring-based verification of SLAs, and enforcement of SLAs in the cloud. The SPECS framework provides techniques and tools for:

- Enabling a user-centric negotiation of security parameters in Cloud SLA, along with a trade-off evaluation process among users and CSPs, in order to compose and use Cloud services fulfilling a minimum required security level (termed QoSec or Quality of Security in SPECS).
- Monitoring in real-time the fulfillment of SLAs agreed with one or more CSP. SPECS' monitoring services also enable notifying both users and CSPs, when an SLA is not being fulfilled (e.g. due to a cyber-attack).
- Enforcing agreed Cloud SLA in order to keep a sustained QoSec that fulfills the specified security parameters. SPECS' enforcement framework also "reacts and adapts" in real-time to fluctuations in the QoSec by advising/applying the correct countermeasures (e.g. triggering a two-factor authentication mechanism). [33]

MUSA - MUlti-cloud Secure Applications

January 2014 – December 2017

The main objective of MUSA is to support the security-intelligent lifecycle management of distributed applications over heterogeneous cloud resources, through a security framework that includes:

- security-by-design mechanisms to allow application self-protection at runtime, and
- methods and tools for the integrated security assurance in both the engineering and operation of multi-cloud applications.

The MUSA framework leverages security-by-design, agile and DevOps approaches in multi-cloud applications, and enables the security-aware development and operation of multi-cloud applications. [34]

Projects funded by US National Science Foundation

Finally, research projects funded by the US National Science Foundation (NSF) also focused on different aspects of cloud security and assurance. The "Risk Assessment Techniques for Off-line and On-line Security Evaluation of Cloud Computing" (2013) project considers the need of a security risk evaluation framework for cloud computing. It focuses on offline risk management and online trust evaluation, and aims to support users in the evaluation of cloud service/resource trustworthiness. It aims to develop an on-line assessment methodology for cloud service providers assessment based on different applications, services and vendor compositions. [29]

2.4 Case Studies

The Monetary Authority of Singapore (MAS) [13] issued the Technology Risk Management Guidelines (TRMG) in 2013, which address the existing and emerging technology risks within the financial institutions.

The objective of the TRMG is for financial firms to establish a sound and robust technology risk management framework, strengthen system security, reliability, resiliency, recoverability, and deploy strong authentication to protect customer data and systems.

Finally, the Federal Risk and Authorization Management Program (FedRAMP) provided a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. In particular, it released a document describing best practices for acquiring IT as a service (CIO 2012)[14]. The FedRAMP baseline security requirements and unified framework for authorizing cloud environments allow Federal agencies to safely and securely use the cloud, and enables re-use of these authorizations under Federal Information Security Management Act (FISMA). The FedRAMP baseline security requirements and unified framework for authorizing cloud environments allow Federal agencies to safely and securely use the cloud, and enables re-use of these authorizations under FISMA. [35]

The Info-Communications Development Authority (IDA) of Singapore [36] updated its Cloud Service Provider (CSP) Registry in 2014 to provide potential cloud consumers real-time information on performance and availability of a CSP on top of existing static listings via the Registry.

The reason behind this was to provide greater transparency for the benefit of cloud adopters by making available online information about CSPs.

The near real-time enhancement is enabled through a Memorandum of Intent between the IDA and Dynatrace[15] (formerly Compuware) to access information on CSPs' availability and performance in near real-time. Dynatrace was aimed at providing free use of software tools and expertise for the project. Also, the latest 2015 edition of the Cloud Computing in Singapore booklet[16] provides an overview of Singapore's cloud computing ecosystem and consists of variety of cloud adoption case studies; featuring Cloud Service Providers' journey achieving Multi-Tier Cloud Security certification. The booklet also contains directory listings of IaaS/PaaS, SaaS, Cloud Technology Companies and Cloud Training Providers. [38]

[14] CIO 2012: https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

[15] Dynatrace: http://www.dynatrace.com/en/

[16] Cloud Computing in Singapore: https://dl.dropboxusercontent.com/u/66814130/Cloud Computing in Singapore Booklet/2015 edition/Cloud Computing in Singapore (2015 Edition).pdf

2.5 Best Practices

ENISA's "Security Framework for Governmental Clouds" document [5] provides formalization of a generic security framework for governmental clouds. The proposed security framework is based on a collection and analysis of existing Cloud computing security literature, other relevant security best practices, and on the few existing real life case studies of Governmental Clouds in Europe. The final result is a security framework modelled into four (4) phases, nine (9) security activities and fourteen (14) steps that details the set of actions that we believe each Member States should follow for the definition and implementation of a secure Gov Cloud. The generic security framework has been empirically validated through the analysis of four (4) Gov Cloud case studies namely Estonia, Greece, Spain and UK. The real life validation of the security framework also serves the purpose of defining examples on how some EU Member States are implementing security into their Gov Cloud approaches. ENISA has also produced a "Cloud Security Guide for SMEs" document in 2015 to help SMEs understand the network and information security risks and opportunities they should take into account when using the cloud. [39]

The UK's approach [6] to other countries is detailed in the second of a two-part paper that assesses current trends in the adoption of public sector cloud computing by governments around the world. Part I briefly overviews the potential for and inhibitors to government cloud growth, focusing on security and risk management concerns and suggesting a role for ISO standards, especially ISO 27001 and ISE 27018, in effectively addressing these inhibitors. Part II focuses on the structured approaches to cloud adoption taken by a number of countries including the UK, and suggests that countries looking to develop their public sector clouds but without wishing to reinvent this particular wheel could validly start from the UK's approach as a pathfinder.

"10 Principles and a Framework for Assessment" by ISACA [15]: these 10 principles of cloud computing risk provide a framework for cloud computing migration, and is presented in a case study. The principles are based on the ISACA Business Model for Information Security (BMIS) and cloud assessment road map consisting of four guiding principles: vision, visibility, accountability and sustainability.

The framework suggested is not a panacea, as variations occur in each of the different service models (SaaS, PaaS or IaaS) and deployment models. Variations also occur depending on whether the private/community clouds are onsite, outsourced or virtual (virtual private clouds) The proposed framework could be tailored to map various cloud models (public, community, private, or hybrid), and it could be expanded by mapping to detailed controls within ISO 27001, COBIT, NIST and other guidance and regulatory requirements in various industries.

COBIT 5 [19] is ISACA's new framework for IT governance, risk security and auditing. COBIT 5 is a business framework for the governance and management of enterprise IT. It provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems. COBIT 5 builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources, including ISACA's Val IT, Risk IT and BMIS. It is also aligned with significant guidance and standards, such as ITIL17 and ISO. The COBIT 5 framework is built on five basic principles, which are covered in detail and includes extensive guidance on enablers for governance and management of enterprise IT.

2.6 Elicited Requirements

Based on the desktop research presented here, we proceeded to analyze and elicit an initial set of requirements for the development of the proposed risk profiles for Public Administrations. These requirements are shown in Table 2.

Table 2. 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 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 moving 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.

[17] ITIL - http://www.itlibrary.org

ID	Requirement	Comment
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.

The set of requirements presented in the previous table has been used as a starting point to develop the risk profile process shown in the next section.

3 Overview of the Risk Profile Development Process

This section presents an overview of the methodological approach proposed by CloudWatch2 to allow PAs developing and using (i.e. deploy and monitor) cloud risk profiles. The proposed approach has been designed taking into consideration the requirements elicited in the previous section, and will be further validated and refined in D3.5

As mentioned in the previous section, most of the surveyed approaches to the assessment and management of security risks generally focus on the needs of large organizations and non-cloud systems. A simple approach designed for PAs with the role of (prospective) cloud customers does not exist at the state of the art, or at least not in the form of best practices and tools.

One of the goals in CloudWatch2 is to provide SMEs/PAs with a simple, efficient and inexpensive approach to identifying and managing their (cloud) security risks both from the technological and organization perspectives. The resulting simplified approach, i.e. the developed risk profile, provides small organizations and public administrations with a means to perform cloud security self-assessments. The approach has taken into account the requirements elicited from relevant state of the art works (cf. Section 2), and it is instantiated on top of well-known CSA's best practices namely Cloud Control Matrix (CCM18), and the Enterprise Architecture (EA19). It is important to note that both CSA CCM and CSA EA are widely-use industrial practices, and have been mapped to relevant standards like NIST 800-53v4 and ISO/IEC 27002.

From the PA perspective the proposed approach brings the following benefits:

- ***Simplicity***, thanks to a guided self-assessment for PAs willing to develop a risk profile without the need of (cloud) security expert knowledge.

[18] Please refer to https://cloudsecurityalliance.org/group/cloud-controls-matrix/

[19] Please refer to https://cloudsecurityalliance.org/group/enterprise-architecture/#_overview

- ***Technical and organisational focus***: the proposed approach aims guiding PAs in the elicitation of security controls, which are "good enough" for their requirements. These controls are based on the well-known CSA CCM, and cover both technical and organisational aspects of the (prospective) cloud customer.
- ***A repeatable process*** for developing and using the risk profiles, which allows PAs to periodically re-assess their risks in order to identify opportunities for improvement.
- The whole process has a ***high automation potential***, therefore facilitating the development of software applications to empower PAs in the creation and usage of risk profiles.
- ***Standards-based***: in order to facilitate the industrial uptake of the proposed approach, we have leveraged well-known standards and best-practices into its development. As mentioned above, the underlying CSA CCM and CSA EA are based on international standards from ISO/IEC and NIST.
- ***Cloud-specificity***: to the best of our knowledge there are not other approaches aimed to develop cloud-specific risk profiles for PAs.

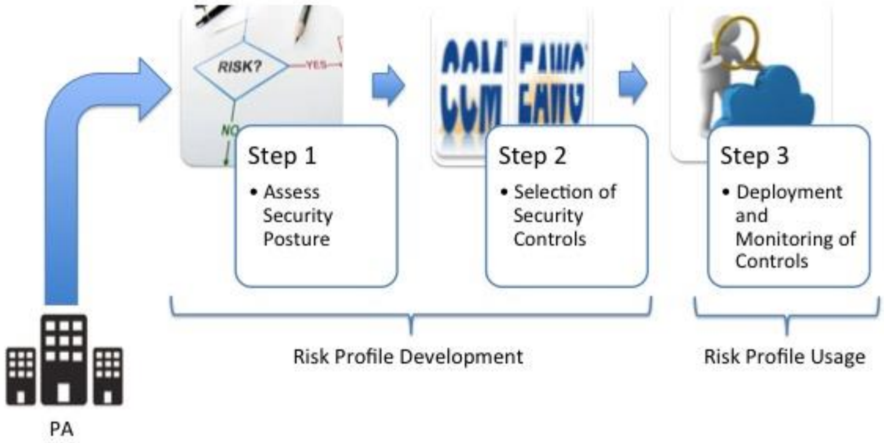
RISK?
YES
NO
CCM
EA
Step 1
• Assess Security Posture
Step 2
• Selection of Security Controls
Step 3
• Deployment and Monitoring of Controls
Risk Profile Development
Risk Profile Usage
PA

Figure 1. Development and Usage of Risk Profiles.

In D3.5 we will 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.

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). During the first step (Security Posture Assessment) the user will qualitatively assess its security posture (i.e. obtain the resulting Impact Level) through a set of questions designed to self-direct the PA in the assessment of inherent cloud-specific risks. Afterwards, during Step 2, the obtained Impact Level (any of Low, Moderate or High) will be used to select (i) a set of components from the cloud security enterprise architecture (CSA EA), and (ii) the corresponding CSA CCM security controls. Finally, during Step 3 the SME/PA will deploy the controls and continuously monitor them through mechanisms like e.g. cloud Service Level Agreements (SLAs).

The rest of this document will further present the three proposed steps, which will be validated and refined in D3.5 (with a particular focus on SMEs).

4 Step 1: Assessing the Security Posture

To create risk profiles for PAs we need to determine what information security risk management is appropriate for them i.e. to assess their security posture. To achieve this, we propose in Table 3 a questionnaire to explore, at a managerial level, the threats, vulnerabilities and the potential impact a PA face in relation to its IT systems and the information they contain. The designed questions collect the information about the level of exposure to threats and vulnerabilities that come from organization's business context, level of exposure to information security incidents, problems and instabilities, level of exposure to information security threats and vulnerabilities as a result of IT systems and the way of using them, potential impacts as a result of its business, value of the information processed and/or stored on IT systems and value of IT systems to organization's business.

Table 3. PA questionnaire for assessing its security posture

1. Please choose the statement below which best expresses how large and complex your organization is:
   a. *Local public administration or small agency, no contractors, or very few, a small number of offices*
   b. *Local public administration, medium-sized agency or regional publich administration, sometimes using contractors, a number of offices in the country*
   c. *Regional public administration, large agency or central public administration, a number of contractors, a number of offices in the country*
   d. *Central public administration or European public administration, many contractors, offices in one or more countries*
2. Please choose the statement below which best expresses your organization's attitude to change and innovation:
   a. *Our organization changes slowly and innovation is not a high priority*
   b. *Our organization changes to meet market and other requirements and we innovate as necessary*
   c. *Our organization embraces change and seeks to innovate wherever possible*
   d. *Change and innovation are critical to our organization's business model*
3. To what extent do you feel that you may have information security incidents, problems and instabilities caused by non-human factors?
   a. *Very little*
   b. *Some*
   c. *Potentially significant*
   d. *Potentially critical*
4. To what extent do you feel that you have information security incidents, problems and instabilities as a result of human-related incidents from people either within your

organization (such as disgruntled employees or employees making mistakes) or outside your organization (such as competitors, criminals, social activists or terrorists)?

a. *Very little*
b. *Some*
c. *Potentially significant*
d. *Potentially critical*

5. Do you think that the people either within or outside your organization, who may cause incidents, problems and instabilities, are likely to be knowledgeable and have the resources to attack you?

a. *Unlikely to be knowledeable and have effective resources*
b. *May have knowledge and effective resources*
c. *Likely to have knowledge and effective resources*
d. *Certain to have knowledge and effective resources*

6. Which of the statements below best describes the complexity of your IT resources (e.g. number of different applications, systems and legacy software)?

a. *Little complexity*
b. *Some complexity, but no legacy systems*
c. *Some complexity*
d. *Much complexity*

7. Which of the statements below best describes your use of the Internet?

a. *Internet access insignificant*
b. *Internet access useful to our business*
c. *Internet access important to our business*
d. *Internet access is business critical*

8. Which of the statements below best describes the access that pther PAs have to your organization's IT networks and resources (and vice versa)?

a. *No access*
b. *Some access, but restricted and not important to the business*
c. *Access is not widely used, but is important*
d. *Access is widely used and/or business critical*

9. Which of the statements below best describes home working and remote working in your organization?

a. *No home or remote working*
b. *We have a small number of home and remote workers*
c. *Most of our employees and contractors sometimes work remotely or from home*
d. *Home and remote working is an integral and important part of our business model*

10. How strongly is your business affected by legal and regulatory requirements?

a. *Not very*
b. *Somewhat*
c. *Significantly*
d. *Critically*

11. What would the likely impact on your organization be of your inability to access business critical information from your IT systems?

a. *Little impact*

   b. *Significant impact*
   c. *Severe impact*
   d. *Critical impact, including breakdown of the organization*

12. What would the likely impact on your organization be if changes were made to business critical information on your IT systems without your knowledge or authorisation?
    a. *Little impact*
    b. *Significant impact*
    c. *Severe impact*
    d. *Critical impact, including breakdown of the organization*
13. What would the likely impact on your organization be if the confidentiality of the business critical information on your IT systems was compromised?
    a. *Little impact*
    b. *Significant impact*
    c. *Severe impact*
    d. *Critical impact, including breakdown of the organization*
14. How significant are your organization's IT systems in enabling you to achieve your business objectives?
    a. *Incidental to our objectives*
    b. *Useful in achieving our objectives*
    c. *Very valuable in helping us to achieve our objectives*
    d. *Critical to enabling us achieve our objectives*
15. What would the impact be on your business partners, customers and external stakeholders of a disaster to your IT systems?
    a. *Negligible or small*
    b. *Significant*
    c. *Very significant*
    d. *Would cause severe damage*

The PA's answers to the questionnaire shown in Table 3 can be processed in order to compute its actual security posture i.e. resulting impact level. Details related to the computation of the impact level will be presented in D3.5.

The following section will assume that an impact level has been computed, so it can then be possible to proceed with the selection of security controls suitable for that specific PA.

5 Step 2: Selection of Security Controls

The next step in the proposed methodology takes as input the PA's impact level (resulting from the application of the questionnaire in Step 1), in order to recommend a set of security controls suitable for mitigating the identified risks. At the state of practice, there is not rule of thumb for mapping security controls to impact levels. To the best of our knowledge only NIST has performed a similar approach in the past for its control framework SP 800-54 rev4 [22], but with a particular focus on US-based Pas, which may not necessarily be cloud customers.

The approach proposed in this deliverable leverages well-known security practices developed by CSA due to (i) its market adoption, and (ii) opportunity to enhance them with the conclusions from both D3.2 and D3.5. In particular we refer to CSA CCM and CSA EA as introduced next.

5.1 Introduction to Cloud Controls Matrix and Enterprise Architecture

The CSA CCM [23] provides a controls framework that gives detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. The foundations of the CCM rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry.

The CSA CCM is suitable for the purposes of developing risk profiles, because it is aimed at enhancing existing information security control environments by emphasizing business information security control requirements, reducing and identifying consistent security threats and vulnerabilities in the cloud, providing standardized security and operational risk management, and seeking to normalize security expectations, cloud taxonomy and terminology, and security measures implemented in the cloud.

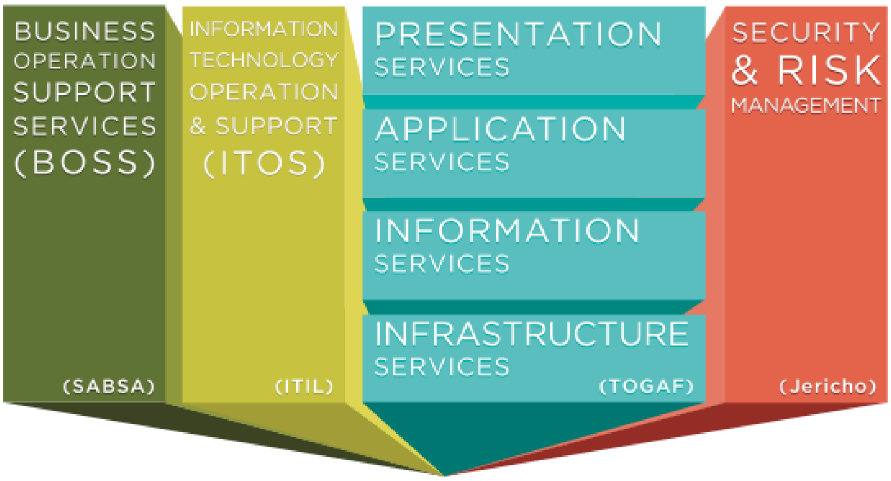
BUSINESS OPERATION SUPPORT SERVICES (BOSS)
(SABSA)
INFORMATION TECHNOLOGY OPERATION & SUPPORT (ITOS)
(ITIL)
PRESENTATION SERVICES
APPLICATION SERVICES
INFORMATION SERVICES
INFRASTRUCTURE SERVICES
(TOGAF)
SECURITY & RISK MANAGEMENT
(Jericho)

Figure 2. CSA Enterprise Architecture.

Cloud Security Alliance's Enterprise Architecture (EA [24]) is both a methodology and a set of tools that enable security architects, enterprise architects and risk management professionals to leverage a common set of solutions that fulfill their common needs to be able to assess where their internal IT and their cloud providers are in terms of security capabilities and to plan a roadmap to meet the security needs of their business. The CSA EA (shown in Figure 18) is structured in a hierarchical manner. Seven domains exist at the top level (e.g. BOSS and ITOS), which are composed of containers, and in turn these are comprised of one or more capabilities. The EA fulfills a set of common requirements that PA risk managers must assess regarding the operational status of internal IT security and cloud provider controls. These controls are expressed in terms of security capabilities and designed to create a common roadmap to meet the security needs of their organisations.

To fully define a risk profile, both CCM and EA can be mapped to the impact levels resulting from the PA's assessment of its security posture. The initial version of such mapping, presented in the next section, will be based on NIST 800-53 rev4 framework [22]. The final version of the risk profiles (to appear in D3.5) will be also mapped to CSA CCM.

5.2 Mapping Impact Levels to Security Controls

In order for PAs to select a set of security controls and EA components (i.e. domains, containers and capabilities) corresponding to the computed impact level, we have developed a mapping linking all of these elements. The proposed mapping has been developed for the purposes of this deliverable by leveraging the joint expertise of CSA and NIST, taking into account that the latter has performed a similar exercise with its own NIST 800-53 rev4 framework [22]. It is worth noting that the mapping presented in this deliverable (cf. Appendix A) should be considered as a draft version of the final CCM mapping to be documented in D3.5.

The NIST 800-53 v4 controls reported under each one of columns Low Impact Level, Moderate Impact Level and High Impact Level refer to the recommended controls that should be implemented by the CSC/CSP (please also refer to Section 6). Controls shown in the form "Control_ID(priority number)" refer to Tables D-3 to D-19 from NIST 800-53 v4. Please note that Appendix A is also organized according to the elements referenced by CSA EA (i.e., Domain, Container and Capability), in order to allow interested parties to focus deployment efforts on specific building blocks of the cloud architecture.

Let us take for example Table 4 which shows an excerpt of the full set of mapped controls presented in Appendix A. In this case a Public Administration would be able to choose for each one of the capabilities "OS Virtualization" and "TPM Virtualization" a set of baseline and complementary controls as required by the corresponding impact level. If the Public Administration's resulting impact level equals to "Moderate", then only control SA-17 (Developer Security Architecture and Design) should be required to the CSP. However, in the case of capability "TPM Virtualization" it is required the implementation of CM-5 (Access Restrictions for Configuration Change), SI-7 (Software, Firmware, and Information Integrity – baseline implementation), and also a so-called control enhancement SI-7 (1) "software, firmware, and information integrity | integrity checks". It should be noticed that recommended controls are not incremental, therefore the "Low" impact level controls are not required to be implemented by the CSP in this particular example.

Table 4. Mapping Impact Levels to NIST 800-53 v4 Security Controls

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Infrastructure Services	Virtual Infrastructure: Server Virtualization	OS Virtualization	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure:	TPM Virtualization	AC-3, PL-8, SC-12, SC-13	CM-5, SI-7, SI-7(1)	CM-5(3), SI-7(6), SI-7(9),

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
	Server Virtualization				SI-7(10), SI-7(15)

6 Step 3: Deployment and Monitoring of the Risk Profile

Sandhu [1] introduced the concept of good-enough security driven by the principle of "everything should be made as secure as necessary, but not securer." As discussed earlier on this deliverable, the classical PDCA approaches (Plan-Do-Check-Act [2]) are increasingly being considered by SMEs/PAs for assessing and managing their IT risk and security exposure following adoption of cloud services. In this section we further elaborate on the usage of cloud SLAs[20] to instantiate, deploy and monitor risk profiles with the target to achieve "good-enough security" in the cloud.

6.1 Cloud security SLAs (secSLAs)

Stakeholders in the cloud community (e.g. the European Network and Information Security Agency -ENISA[21]-) have identified that specifying measurable cloud attributes in Service-Level Agreements is useful in order to establish common semantics to provide and manage assurance both for CSP's, and Cloud customers alike. This is especially important from the security perspective, where the specification of security attributes is directly related to the development and usage of the risk profiles advocated in this report. In this rest of this section, those "security SLAs" will be simply termed secSLAs.

Organizations targeting cloud secSLA as a means to implement good-enough security typically start with an introspective view that identifies both the assets to protect, and the (probabilistic) risks to consider when migrating to the cloud, that is, the development of a suitable risk profile as introduced in Section 3. The selected cloud delivery model and the service type, in association with risk profile and corresponding security controls selected for the ecosystem, need to be chosen such that the system preserves its security requirements.

The key element for the successful adoption of a cloud solution based on secSLA's is the cloud service customer's understanding of the cloud-specific characteristics, the architectural components for each cloud service type and deployment model, along with each cloud actor's precise role in orchestrating a secure ecosystem. The SME/PA's confidence in accepting the risk from using cloud services depends on how much trust they place in those involved in the cloud ecosystem's orchestration. The risk profile and its overlaying risk management process

[20] Cloud SLAs are one of the most promising approaches to deploy and continuously monitor risk profiles, but the authors acknowledge that some other mechanisms will continue to appear in the short term (e.g. cloud security certifications).

[21] Please refer to ENISA's report "Survey and analysis of security parameters in Cloud SLA's across the European public sector."

ensure that issues are identified and mitigated early in the investment cycle and followed by periodic reviews. 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.

6.2 From Risk Profiles to cloud secSLAs

Cloud customers need to leverage their contractual agreements to hold the CSPs (and Cloud brokers, when applicable) accountable for the implementation of the security controls stated in the resulting risk profile. They also need to assess the correct implementation and continuously monitor all the identified security controls. But what are the elements of a successful cloud risk profiling strategy in order to enable the usage of secSLAs?

A well-orchestrated process for SMEs/PAs willing to manage cloud risks by leveraging risk profiles into cloud secSLAs was initially proposed by one of the authors of this deliverable in [4]. The proposed approach, partially based on the more general Cloud Adapted Risk Management Framework (CRMF) [3], is a cyclically executed process composed of a set of coordinated activities for overseeing and controlling risks. This set of activities consists of the following tasks:

- Risk Profiling/Assessment,
- Risk Treatment, and
- Risk Control.

These tasks collectively target the enhancement of strategic and tactical security through secSLAs. A cloud customer-centric approach for implementing the activities mentioned above is shown in Figure 2 and presented next:

Risk Profiling/Assessment Activities: these activities aim to (i) create the risk profile for the SME/PA, and (ii) select the baseline and tailored supplemental cloud security controls/cloud enterprise architecture components. Both stages have been presented in Sections 4 and 5 respectively.

Risk Treatment Activities: once the security controls have been elicited, the following steps take place:

- Step 3 – Select the Cloud ecosystem architecture (based on CSA EA) that best suits the assessment results for the system.
- Step 4 – Assess the CSP options. Identify the security controls needed for the system the CSP has implemented. Negotiate the implementation of any additional security controls that are identified. Identify any remaining security controls that fall under the SME/PA's responsibility for their implementation.

Risk Control Activities: this final stage aims to deploy and continuously monitor/refine the secSLA. The following steps take place:

- Step 5 – Select and authorize a CSP to host the SME/PA's information system. Draft a SLA/secSLA that lists the negotiated contractual terms and conditions.

- Step 6 – Monitor the agreed CSP secSLA to ensure that all service levels objectives (SLOs) are being met, and the risk profile is kept under acceptable thresholds (i.e. the cloud-based system maintains the necessary security posture). Monitor the security controls that fall under the SME/PA's responsibility.

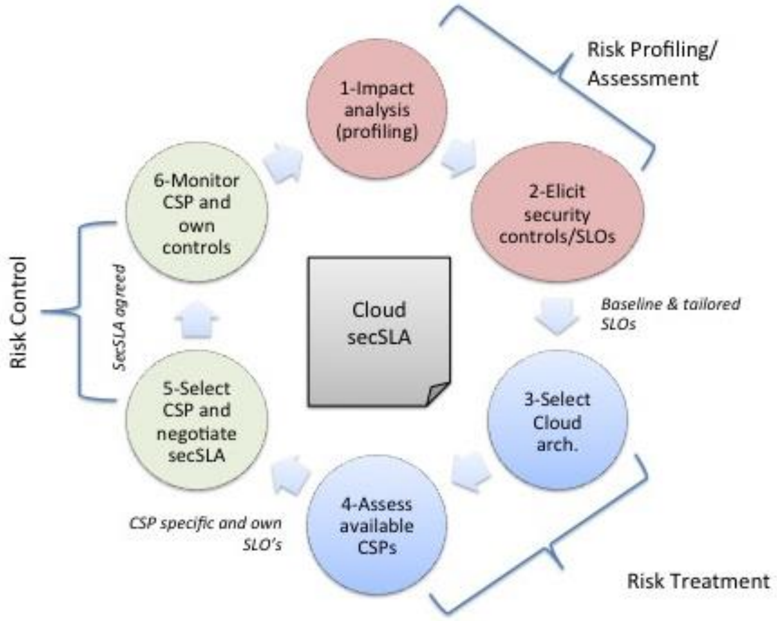
Risk Profiling/
Assessment
1-Impact analysis (profiling)
2-Elicit security controls/SLOs
Baseline & tailored SLOs
3-Select Cloud arch.
4-Assess available CSPs
Risk Treatment
CSP specific and own SLO's
5-Select CSP and negotiate secSLA
6-Monitor CSP and own controls
SecSLA agreed
Risk Control
Cloud secSLA

Figure 3. Cloud secSLA development within a risk management framework.

A risk-based approach to managing information systems is an holistic activity that should be fully integrated into every aspect of the SME/PA, from planning and system development life cycle processes (Steps 1 – 2) to security controls allocation (Steps 3 – 5). The selection and specification of risk profiles and security controls support effectiveness, efficiency, and constraints via appropriate laws, directives, policies, standards, and regulations. The resulting risk profile and set of security controls (baseline, tailored controls, controls inherited from providers and under SME/PA's direct implementation and management) derived from applying the proposed approach (Steps 1 - 4) leads gradually to the creation of the secSLA in Step 5. Readers interested on the details associated to the creation of a secSLA based on the elicited security controls can refer to [4]. The following subsection briefly discusses an approach for SMEs/PAs to continuously guarantee compliance with a developed risk profile based on the agreed CSP secSLA.

6.3 Risk control through Cloud secSLA.

Once a Cloud secSLA is built and agreed with the CSP, the SME/PA now has a mechanism to monitor the fulfilment of the requested security SLOs. This is the essence of the risk control stage in the proposed approach. Despite its apparent feasibility, to the best of our knowledge, there is a paucity of efforts exploring this area. One reason limiting the development of such secSLA monitoring solutions arises from the lack of cloud-specific standards associated with SLA's, SLO's, and metrics/measurements.

Once the mechanisms for monitoring cloud secSLA's are in place, it is possible to assess both the fulfilment of agreed security SLO's and by consequence also of elicited security controls associated with the risk profile. When the monitoring stage detects potential deviations from expected values (i.e. SLA violations), these can be managed by the CSP through actions ranging from changes to the current secSLA, to termination of the agreed cloud service. Once again, the academic/industry efforts addressing this issue seem to be lacking. Some prominent works in this specific area will be discussed in D3.5

7 Conclusions

Despite the evident usefulness of ICT security risk assessments for (prospective) cloud customers, in particular from public sector, this deliverable has acknowledged the complexity associated to state of practice approaches. The inherent requirements of traditional risk management methodologies (e.g., the need for security experts), has motivated the ICT security community to look for simplified approaches which are more appropriate for PAs and SMEs. In this report we have advocated for the use of risk profiles as an approach to simp lify assessing the security posture of a PA that is (i) considering moving to the cloud, or (ii) is already a user of this technology.

Based on a desktop research this report has elicited a set of requirements aimed to develop a methodological approach for creating and using risk profiles, which are particularly suited for Public Administrations. The proposed methodology consists of three well-identified steps covering the whole security lifecycle from a risk-management perspective. Our proposed approach does not require the use of expert knowledge and has the added benefit of allowing the continuous optimization of the PA's security level. Furthermore, we have shown the flexibility of the contributed approach by leveraging risk profiles into cloud Service Level Agreements as just one potential mechanism for deploying/monitoring/improving the PA's "risk appetite".

The next version of this document (i.e., D3.5) will present a validated version of the proposed methodology. The validation process will take place by developing relevant real-world use cases, and getting feedback from stakeholders (e.g., by consulting the EU FP7 "Cloud for Europe" project). Also D3.5 will document a set o risk profiles (covering both PAs and SMEs), and provide a further focus on best practices for deploying automated tools instantiating the different stages of the contributed risk profiling methodology. Also, we are planning to show how to leverage the proposed methodology using best practices like CSA Cloud Controls Matrix.

8 Appendix A. Security Controls Mapped to Impact Levels

This appendix contains the full list of NIST 800-43 v3 security controls mapped to (i) impact levels, and (ii) CSA Enterprise Architecture building blocks. Section 5 presents in further details the data shown in this table.

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Compliance	Intellectual Property Protection	AC-1, AC-2, AC-3, AC-8, AC-17, AC-18, AC-19, AC-20, AU-1, AU-2, AU-3, AU-12, AU-6, AU-9, AT-1, AT-2, AT-3, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-10, CM-11, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-6, IA-7, IA-8, MA-1, MA-2, MA-3, MA-4, MA-5, MP-1, MP-2, MP-4, MP-5, MP-6, PE-1, PE-2, PE-3, PE-6, PL-1, PL-4, PS-1, PS-2,PS-3, PS-4, PS-5, PS-6, PS-7, RA-1, RA-2, RA-3, RA-5, SC-1, SC-7, SC-8, SC-12, SC-13, SC-15, SC-28, SC-39	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(7), AC-2(9), AC-2(10), AC-2(12), AC-4, AC-4(21), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10), AC-10, AC-11, AC-11(1), AC-12, AC-17(9), AC-18(1), AC-19, AC-19(5), AC-20(1), AC-20(2), AC-21, AU-2(3), AU-3(1), CM-2(1), CM-2(3), CM-2(7), CM-3(2), CM-5, CM-6, CM-7(2), CM-7(5), CM-8(1), CM-8(3), CM-8(5), IA-5(4), IA-5(6), IA-5(7), MA-3(3), MA-5(1), MP-5(4), PE-4, PE-5, PE-6(1), PL-4(1), RA-5(1), RA-5(2), RA-5(5), SC-2, SC-4, SC-7(5), SC-7(7), SC-8(1), SC-10, SC-18, SC-23, SC-28(1), SI-3(1), SI-3(2), SI-4(4), SI-7, SI-10, SI-16	AC-2(11), AC-2(13), AC-6(3), AC-6(7), AC-6(8), AC-18(4), AC-21(2), AU-13, CM-3(1), CM-5(1), CM-5(3), CM-5(4), CM-6(2), CM-8(4), MA-4(3), PE-2(3), PE-3(1), PE-6(4), PS-4(2), PS-6(3), RA-5(4), RA-5(6), RA-5(10), SC-3, SC-7(8), SC-7(10), SC-7(11), SC-7(14), SC-7(15), SC-7(18), SC-7(21), SC-24, SI-7(10), SI-10(5)
BOSS	Data Governance	Handling/ Labeling/ Security Policy	AC-1, AC-3, AC-4, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, MP-2, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1, SI-12	MP-3, MP-5, MP-5(4)	AC-16

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Data Governance	Clear Desk Policy	MP-1, MP-2, MP-7	MP-4, MP-5, MP-5(4), MP-7(1), PE-5	
BOSS	Data Governance	Rules for Information Leakage Prevention	AC-1, CP-1, IA-1, IR-1, SC-1, SI-1, Appendix J		
BOSS	Human Resource Security	Employee Awareness	AT-1, AT-2, AR-5	AT-2(2)	
BOSS	Security Monitoring Services	Market Threat Intelligence	AU-6, CA-2, IR-4, IR-5	AU-6(1), AU-6(3), CA-2(2)	AU-6(5), AU-6(6), IR-4(4), IR-4(6), IR-4(7), IR-4(8), IR-5(1), SI-4(19), AU-6(9)
BOSS	Security Monitoring Services	Knowledge Base	PL-2, SA-5	PL-7, PL-8	-
BOSS	Compliance	Audit Planning	CA-2, CA-2(1), CA-7, PL-2	CA-2(2), CA-7(1), PL-2(3)	PL-8(1), PL-8(2)
BOSS	Compliance	Internal Audits	CA-2, CA-2(1), CA-7, PL-2	CA-2(2), CA-7(1), CA-8, CA-8(1), PL-2(3)	CA-7(3)
BOSS	Security Monitoring Services	Event Mining	AU-6, CA-7, RA-5, SI-4	AU-6(3), RA-5(6), RA-5(8, SI-4(2)	AU-6(4), CA-7(3), SI-4(11), SI-4(13), SI-4(18)
BOSS	Security Monitoring Services	Event Correlation	AU-6, CA-7, IR-4, RA-5, SI-4	AU-6(3), SI-4(16)	AU-6(6), AU-6(9), IR-4(4), IR-4(8), RA-5(10)
BOSS	Security Monitoring Services	Email Journaling	SI-3, SI-4	SI-3(7), SI-4(5)	SI-4(10), SI-4(12)
BOSS	Security Monitoring Services	User Behaviors and Profile Patterns	AC-2, AU-1, AU-2, AU-3, AU-6, AU-12,	AC-2(12), AU-2(3), AU-3(1), AU-6(7)	AU-6(8)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Legal Services	E-Discovery	AU-1, AU-2, AU-3, AU-4, AU-8, AU-9, AU-11, AU-12, IR-4, IR-5, IR-6, IR-7	AU-3(1), AU-7, AU-7(1), AU-9(2), AU-9(4), IR-4(1), IR-6(1), IR-7(1), IR-7(2)	AU-3(2), AU-9(3), AU-12(1), IR-5(1), AU-9(5), AU-9(6), AU-10, AU-10(1), AU-10(3), IR-4(7), IR-4(8)
BOSS	Legal Services	Incident Response Legal Preparation	AU-1, IR-1	-	AU-10, AU-10(1), AU-10(3)
BOSS	Internal Investigations	Forensic Analysis	AU-6, IR-5, IR-7	AU-6(1), AU-6(3), AU-7, AU-7(1)	AU-6(5), AU-6(6), AU-6(7), AU-6(8), IR-5(1)
BOSS	Internal Investigations	e-Mail Journaling	AU-1, AU-2, AU-3, AU-8, AU-8(1), AU-9, AU-11, AU-12, IR-1, IR-6, SC-1, SI-4	AU-3(1), AU-7, AU-7(1), AU-9(4), IR-6(1)	AU-9(2), AU-9(3), AU-12(1), AU-12(3), AU-14, AU-14(2)
BOSS	Compliance	Independent Audits	CA-1, CA-2, CA-2(1), CA-7, RA-3, RA-5	CA-2(2), CA-7(1), CA-8, CA-8(1), RA-5(1), RA-5(2), RA-5(3), RA-5(6), RA-5(9), SA-11	CA-7(3), SA-11(3)
BOSS	Compliance	Third Party's Compliance	AC-20, CA-3, PS-7, SA-9, SA-12	AC-20(1), SA-9(1), SA-9(2), SA-9(3), SA-9(4), SA-9(5)	-
BOSS	Operational Risk Management	Business Impact Analysis	CM-4, CP-2, RA-1, RA-2, RA-3, PS-2, SA-3, SA-9	CM-3, CM-9, CP-2(3), CP-2(8), CP-8, CP-8(1)	CP-2(4), CP-2(5), SA-14
BOSS	Operational Risk Management	Business Continuity	CP-1, CP-2, CP-3, CP-4, CP-10, IR-4	CP-2(1), CP-2(3), CP-2(8), CP-4(1), CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2), CP-7(3), CP-8, CP-8(1), CP8-(2), CP-9, CP-9(1), CP-10(2)	CP-2(2), CP-2(4), CP-2(5), CP-2(7), CP-3(1), CP-4(2), CP-6(2), CP-7(4), CP-8(3), CP-8(4), CP-9(2), CP-9(3), CP-9(5), CP-10(4), IR-4(3)
BOSS	Operational Risk Management	Crisis Management	CP-1, CP-2, CP-3, CP-4, CP-10, IR-1, IR-2, IR-4, IR-5, IR-6, IR-7, IR-8	CP-2(1), CP-2(3), CP2(8), CP-4(1), CP-10(2), IR-3, IR-3(2), IR-4(1), IR-6(1), IR-7(1)	CP-3(1), CP-10(4), IR-2(1), IR-2(2), IR-4(4), IR-5(1), IR-3(1), IR-4(3), IR-4(7), IR-4(8), IR-4(10), IR-9, IR-10

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Operational Risk Management	Risk Management Framework	RA-3	-	SA-14
BOSS	Operational Risk Management	Independent Risk Management	CA-2, CA-7, RA-3	CA-2(1), CA-7(1)	CA-8, CA-8(1)
BOSS	Security Monitoring Services	Database Monitoring	AU-1, AU-2, AU-3, AU-8, AU-12, CA-7, SI-4	AU-2(3), AU-3(1), AU-8(1), CA-7(1), SI-4(1), SI-4(4)	AU-12(1), AU-3(2), AU-12(3), SI-4(14), SI-4(19), CA-7(3), SI-4(20), SI-4(22), SI-4(23)
BOSS	Security Monitoring Services	Application Monitoring	AU-1, AU-2, AU-3, AU-8, AU-12, CA-7, SI-4	AU-2(3), AU-3(1), AU-8(1), CA-7(1), SI-4(1), SI-4(4)	AU-12(1), AU-3(2), AU-12(3), SI-4(14), SI-4(19), CA-7(3), SI-4(20), SI-4(22), SI-4(23)
BOSS	Security Monitoring Services	End-Point Monitoring	AU-1, AU-2, AU-3, AU-8, AU-12, CA-7, SI-4	AU-2(3), AU-3(1), AU-8(1), CA-7(1), SI-4(1), SI-4(4)	AU-12(1), AU-3(2), AU-12(3), SI-4(14), SI-4(19), CA-7(3), SI-4(20), SI-4(22), SI-4(23)
BOSS	Security Monitoring Services	Cloud Monitoring	AU-1, AU-2, AU-3, AU-8, AU-12, CA-7, SI-4	AU-2(3), AU-3(1), AU-8(1), CA-7(1), SI-4(1), SI-4(4)	AU-12(1), AU-3(2), AU-12(3), SI-4(14), SI-4(19), CA-7(3), SI-4(20), SI-4(22), SI-4(23)
BOSS	Data Governance	Secure Disposal of Data	SA-3, MP-6	MP-6(2)	MP-6(1), AC-4(13), MP-6(8)
BOSS	Human Resource Security	Employee Termination	AC-2, PE-2, PS-4, PS-5		PS-4(2), PS-4(1)
BOSS	Human Resource Security	Employment Agreements	AC-20, AT-2, CA-3, PL-4, PS-6, PS-7, SA-9	AC-6, AC-20(1), AC-20(2), CP-6, CP-7, CP-8, PL-4(1)	SA-12, SA-12(12)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Human Resource Security	Background Screening	PS-2, PS-3, PS-7, SA-9	PS-3(3)	PS-3(1), SA-21
BOSS	Human Resource Security	Job Descriptions	AC-1, AT-1, AU-1, CA-1, CA-2, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-4, PS-1, PS-2, PS-3, PS-7, RA-1, SA-1, SA-3, SC-1, SI-1	CM-9	-
BOSS	Human Resource Security	Roles and Responsibilities	-	AC-5, AC-6	
BOSS	Human Resource Security	Employee Code of Conduct	PL-4, PS-6, PS-8	PL-4(1)	
BOSS	Compliance	Information Systems Regulatory Mapping	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-4, PS-1, RA-1, SA-1, SC-1, SI-1	-	-
BOSS	Data Governance	Data Ownership / Stewardship	AC-1, AC-2, AC-3, AC-17, AC-18, AC-19, AC-20, AT-3, CM-8, IA-2, IA-8, MA-5, PL-4, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, RA-2	AC-4, AC-4(5), AC-4(6), AC-6, AC-6(6), AC-10, AC-12, CM-9, CP-2	AC-9, SI-7(2), AC-3(7), AC-3(8), AC-3(9), AC-4(8), AC-4(18), AC-6(7), AC-16, AC-24, PS-6(1), PS-6(3)
BOSS	Data Governance	Data Classification	RA-2, RA-3		
BOSS	Security Monitoring Services	Managed (Outsourced) Security Services	AC-20, PS-7, SA-4, SA-9	AC-20(1), SA-4(1), SA-9(2)	SA-4(5), SA-9(3), SA-9(5)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Legal Services	Contracts	SA-1, SA-4, SA-9	SA-4(1), SA-4(2), SA-4(9), SA-9(2)	SA-12, SA-4(3), SA-4(5), SA-9(1), SA-9(3), SA-9(4), SA-9(5), SA-12(1), SA-12(2), SA-12(7)
BOSS	Security Monitoring Services	Honey Pot	-	-	SC-26, SC-35
BOSS	Security Monitoring Services	Real Time Internetwork Defense (SCAP)	CA-7, SI-4	CA-7(1), SI-4(2), SI-4(4)	SI-4(11), SI-4(12), SI-4(18), SI-4(22)
BOSS	Data Governance	Rules for Data Retention	AU-11, MP-6, SA-3, SI-12	-	-
BOSS	Security Monitoring Services	Security Information and Event Management (SIEM) Platform	AU-6, AU-12, SI-4	AU-6(1), AU-6(3), SI-4(5),	AU-6(5), AU-6(6), AU-6(9), AU-12(1),AU-12(3), SI-4(3), SI-4(16), SI-4(17), SI-4(23)
BOSS	Security Monitoring Services	Anti Phishing	SC-7, SI-4, SI-8	SI-8(1), SI-8(2)	SC-7(11), SI-4(10), SI-4(23)
BOSS	Compliance	Contract/ Authority Maintenance	AC-2, AU-1, AU-2, AU-3, AU-6, AU-12, CA-2, CA-5, IR-5, PE-3, PE-6, PE-8, RA-1, RA-3, RA-5, SC-7, SI-2, SI-4, SI-7	AC-2(4), AC-6, AC-6(9), AU-2(3), AU-3(1), AU-6(1), AU-6(3), CM-3, CM-5	AC-2(12), AU-3(2), AU-6(5), AU-6(6), AU-12(1), AU-12(3), CM-5(1), IR-5(1), AU-6(4), AU-6(7), AU-6(9), AU-12(2), AU-14, AU-14(2), AU-16, RA-5(8), RA-6, SC-7(9), SC-7(15), SI-7(8)
BOSS	Operational Risk Management	Operational Risk Committee	CA-2, RA-1, RA-2, RA-3, RA-5	CA-2(2)	

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
BOSS	Operational Risk Management	Key Risk Indicators	RA-1, RA-3		RA-6, SA-14
BOSS	Security Monitoring Services	Counter Threat Management	CA-7, RA-3	CA-7(1), CA-8, CA-8(1)	CA-7(3)
BOSS	Security Monitoring Services	Security Operation Center (SOC) Portal	AU-12, CA-7, SI-4	CA-7(1), SI-4(5)	AU-12(1),AU-12(3), SI-4(3), SI-4(16), SI-4(17), SI-4(23)
BOSS	Security Monitoring Services	Branding Protection	-	-	AU-13, AU-13(1), AU-13(2)
ITOS	IT Operations	Resource Management	-	AC-5	-
ITOS	IT Operations	Resource Management	AC-2, AC-3, AC-20, AT-2, IA-4, IA-5, IA-8, MA-5, PL-4, PS-6, PS-7, SA-9	AC-6, AC-20(1), CM-5, IA-5(3)	AC-2(11), AC-2(12), CM-5(5), SA-21, SC-43
ITOS	Service Delivery	Information Technology Resiliency	CP-1, CP-2, CP-3, CP-4, CP-9, CP-10	CP-2(2), CP-2(3), CP-2(8), CP-6, CP-7, CP-8, PE-11	PE-11(1), CP-2(4), CP-2(5), AU-15, CP-2(6), CP-11, CP-12, CP-13, PE-11(2), SI-13
ITOS	Service Delivery	Information Technology Resiliency	AU-4, CP-2, SA-2, SC-5	CP-2(2), PE-11	PE-11(1), SC-5(2), AU-4(1), PE-11(2)
ITOS	Service Support	Configuration Management	CA-7, CM-2, CM-3, CM-8	CA-7(1), CM-2(1), CM-2(3), CM-2(7), CM-3(2), CM-8(1), CM-8(3), CM-8(5)	CM-2(2), CM-3(1), CM-8(2), CM-8(4), CM-8(7)
ITOS	Service Support	Problem Management	AU-1, AU-2, AU-3, AU-6, AU-12, CA-7	AU-2(3), AU-3(1), AU-6(1), AU-6(3), CA-7(1)	AU-3(2), AU-6(5), AU-12(2), CA-(3)
ITOS	Service Support	Problem Management	IR-4	-	-

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
ITOS	Service Delivery	Asset Management			
ITOS	Service Support	Configuration Management	RA-5, SA-3, SA-4	SA-8, SA-10, SA-11, SI-7, SI-7(1), SI-7(7)	SA-15, SA-17, SI-6, SI-7(2), SI-7(5),
ITOS	Service Support	Configuration Management	CM-1, CM-2, CM-6	CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(2), CM-5	CM-2(2), CM-3(1), CM-5(1), CM-5(2), CM-5(3), CM-6(1), CM-6(2)
ITOS	Service Support	Configuration Management	CM-8	CM-8(1), CM-8(3), CM-8(5)	CM-8(2), CM-8(4), CM-8(8)
ITOS	Service Support	Knowledge Management	SI-5	-	-
ITOS	Service Support	Knowledge Management	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1		
ITOS	Service Support	Knowledge Management	AT-1, AT-2, AT-3		-
ITOS	Service Support	Change Management	CM-1, CM-2	CM-3, CM-3(2), CM-5, CM-5(3), CM-9, SA-10	CM-3(1), CM-5(2), CM-3(4), CM-5(4)
ITOS	Service Support	Change Management	CM-1, CM-4, CM-6	CM-3, CM-3(2), CM-5, CM-5(3), CM-9	CM-3(1), CM-4(1), CM-6(1), CM-3(4)
ITOS	Service Support	Change Management	CM-1, CM-4	CM-3, CM-9, SA-10	CM-3(4)
ITOS	Service Support	Change Management	CM-1, CM-2, CM-4, CM-6	CM-3, CM-3(2), CM-9	CM-3(1), CM-4(1), CM-3(4), CM-4(2)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
ITOS	Service Support	Release Management	CM-1, CM-2, CM-8, SI-2	CM-2(1), CM-2(2), CM-2(3), CM-3, CM-3(2), CM-9, SA-10	CM-3(1), CM-8(4), CM-3(5), CM-8(9), SA-10(4), SA-10(5), SI-2(6)
ITOS	Service Support	Release Management	CM-1, CM-2, CM-5, CM-8, SI-2	CM-2(2), CM-2(3), CM-3, CM-3(2), CM-8(1), SA-10	CM-3(1), CM-8(2), CM-8(4), CM-3(5), CM-8(9), SA-10(4), SA-10(5), SI-2(6)
ITOS	IT Operations	DRP	CP-1, CP-2		
ITOS	Service Support	Configuration Management	AU-4, CP-2, SA-2, SC-5	CP-2(2), PE-11	PE-11(1), SC-5(2), AU-4(1), PE-11(2)
ITOS	Service Support	Incident Management	CP-2, IR-1, IR-4, IR-5, IR-6, IR-7, IR-8,	IR-4(1), IR-6(1)	IR-4(2), IR-4(3), IR-4(4), IR-4(6), IR-4(7), IR-4(8), IR-4(5), IR-4(9), IR-4(10), IR-9, IR-10
ITOS	Service Support	Incident Management	AU-6, SI-4	AU-6(1), SI-4(2), SI-4(5)	SI-4(7), SI-4(12)
ITOS	Service Support	Incident Management	IR-4, IR-5, IR-8	IR-4(1)	IR-5(1)
ITOS	Service Support	Incident Management	IR-1, IR-4, IR-5, IR-6, IR-8	IR-4(1)	IR-4(4), IR-4(7), IR-4(8), IR-5(1), IR-4(10), IR-10
ITOS	Service Support	Problem Management	AU-6, CA-7, IR-5, RA-3, RA-5	AU-6(1), AU-6(3), CA-7(1)	AU-6(5), IR-5(1), CA-7(3), RA-5(6)
ITOS	Service Support	Problem Management	IR-1, IR-2, IR-4, IR-8		IR-4(4)
ITOS	Service Support	Knowledge Management	AU-6, CA-7, IR-1, IR-4, IR-5, MA-6, RA-5	AU-6(1), AU-6(3)	AU-6(5), AU-6(6), IR-4(4), IR-5(1), AU-6(4), AU-6(9), CA-7(3), MA-6(2), RA-5(6)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
ITOS	Service Support	Change Management	SI-2	CM-3, CM-5, CM-9, SA-10	CM-3(1)
ITOS	Service Support	Release Management	SI-2	CM-3, CM-3(2), CM-9, SA-10, SI-2(2)	SI-2(1)
ITOS	Service Delivery	Asset Management			
ITOS	Service Support	Incident Management	IR-1, IR-4, IR-5, IR-6, IR-7, IR-8	IR-4(1), IR-6(1), IR-7(1), PL-8	IR-4(4), IR-5(1), SA-17, IR-4(3), IR-4(7), IR-4(8), IR-4(9)
ITOS	Service Delivery	Application Performance Monitoring			
ITOS	Service Support	Release Management	CM-2, CM-4, SI-2	CM-3, CM-3(2), SA-10	CM-3(1), CM-3(4), CM-4(1), CM-2(6), CM-4(2)
ITOS	Service Support	Release Management	CM-2, CM-6	-	CM-2(2), CM-6(1)
ITOS	IT Operations	DRP (Digital rights protection)	CM-10	CM-10(1)	-
ITOS	IT Operations	IT Governance	-	PL-8, SA-8	SA-15, SA-17, SA-17(1), SA-17(3)
ITOS	IT Operations	IT Governance	-	-	-
ITOS	IT Operations	PMO	AU-6, CA-7, IR-5, RA-3, RA-5	AU-6(1), AU-6(3)	AU-6(5), IR-5(1), RA-5(6), IR-10
ITOS	IT Operations	PMO		SA-8	SA-15, SA-15(1), SA-15(2)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
ITOS	IT Operations	PMO	CA-2, CA-5, CA-7, RA-3, RA-5, SI-2	CM-3, SA-11, SI-2(2), SI-2(3)	SI-2(1), CA-7(3), SI-2(5)}
ITOS	IT Operations	Portfolio Management	CP-2, PL-1, PL-2, RA-2, RA-3	CP-2(8), PL-8	SA-8, SA-14
ITOS	IT Operations	Portfolio Management	CP-2, PL-1, PL-2, RA-2, RA-3	CP-2(8), PL-8	SA-8, SA-14
ITOS	Service Delivery	Service Level Management	SA-9	CP-8	
ITOS	Service Delivery	Service Level Management	SA-9	CP-8	
ITOS	Service Delivery	Service Level Management	AC-20, CA-2, CA-7, PS-7, RA-2, RA-3, SA-1, SA-4, SA-9, SI-4	AC-20(1), AC-20(2), CA-2(1), CA-7(1), SA-4(1), SA-4(2), SA-4(9), SA-4(10), SA-9(2), SA-11, SI-4(2), SI-4(4), SI-4(5)	CA-2(2), SA-9(1), SA-9(3), SA-9(5), SA-12, SA-15, SA-16, SA-17
ITOS	Service Delivery	Service Level Management	AU-12, CA-7, SA-4, SA-9, SI-4	CA-7(1), SA-4(1), SA-4(2), SA-4(9), SA-4(10), SA-9(1), SA-9(3), SI-4(2), SI-4(4), SI-4(5)	AU-12(1), AU-12(3), SI-4(3), SI-4(16), SI-4(17), SI-4(23)
ITOS	Service Delivery	Asset Management	CA-5, RA-3, SA-2	-	-
ITOS	Service Delivery	Asset Management	RA-3, SA-2	-	-
ITOS	Service Support	Problem Management	CM-1, CM-2, CM-3, CM-4, CM-6, CM-7, CM-8, CM-9	CM-2(1), CM-2(3), CM-3(2), CM-8(3), CM-8(5)	CM-2(2), CM-3(1), CM-6(1)
ITOS	Service Support	Knowledge Management			
Application Services	Security Knowledge Lifecycle	Attack Patterns	RA-5, SA-11, SC-5, SI-4	RA-5(1), RA-5(2), SI-4(2)	RA-5(6), RA-5(10), SA-11(6), SA-15, SA-15(5), SC-5(3), SI-4(13)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Application Services	Connectivity & Delivery				
Application Services	Security Knowledge Lifecycle	Security Design Patterns	SA-3, SA-4	PL-8, SA-4(2), SA-4(8), SA-4(9), SA-8, SA-10, SA-11	SA-15, SA-17, PL-8(1), SA-4(5), SA-10(5), SA-11(6), SA-15(3), SA-15(5)
Application Services	Security Knowledge Lifecycle	Security Application Framework - ACEGI	SA-3, SA-4	SA-8	SA-15, SA-17, SA-4(3)
Application Services	Development Processes	Self Service	RA-5	SA-10, SA-11, SA-11(1)	SA-10(4), SA-10(5), SA-11(4), SA-11(8)
Application Services	Development Processes	Self Service	RA-5	RA-5(1), RA-5(2), RA-5(5)	
Application Services	Development Processes	Self Service	AU-4, AU-5, CP-2, SA-2, SC-5	CP-2(2)	SC-5(2), SC-5(3), AU-5(3)
Application Services	Development Processes	Software Quality Assurance	CA-2, RA-5, SA-4, SA-8, SI-2	CA-2(2), CA-8, CM-3, CM-3(2), SA-10, SA-11, SA-11(2)	SA-11(5), RA-5(3), SA-11(1), SA-11(4), SA-11(8)
Application Services	Integration Middleware		AC-3	SI-7, SI-7(1)	AU-10, SI-7(2), SI-7(5), AC-16, AU-10(1), AU-10(2), SA-18
Application Services	Abstraction		AC-1, AC-2, AC-3, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-5(11), IA-8	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4, AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10), AC-12, IA-2(2), IA-2(3), IA-2(8), IA-2(11)	AC-2(13), AC-6(3), { AC-16, AC-25 }
Application Services	Programming Interfaces	Input Validation	-	SI-10	SI-10(2), SI-10(3), SI-10(4), SI-10(5)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Application Services	Security Knowledge Lifecycle	Code Samples	AT-3, RA-5, SA-8	SA-11	SA-11(1), SA-11(4), SA-11(8)
Information Services	BOSS	Audit Findings	CA-1, CA-2, CA-2(1), CA-5, CA-7, RA-3, RA-5	CA-2(2), CA-7(1), CA-8, CA-8(1), RA-5(1), RA-5(2), RA-5(3), RA-5(6), SA-11	SA-11(3)
Information Services	Security Monitoring	eDiscovery Events	AU-2, AU-3, AU-4, AU-9, AU-11, IR-4, PE-6, SI-4, SI-12	AU-3(1), AU-7, AU-7(1)	AU-7(2), AU-11(1), PE-6(3)
Information Services	Reporting Services	Dashboard			
Information Services	Reporting Services	Data Mining			AC-23, AU-13
Information Services	Reporting Services	Reporting Tools	AU-6, AU-7, AU-12	AU-6(1), AU-6(3), AU-7(1)	AU-6(5), AU-6(4), AU-7(2)
Information Services	Reporting Services	Business Intelligence			
Information Services	ITOS	Problem Management	AT-2, AT-3, AU-1, AU-2, AU-3, AU-6, AU-7, AU-11, AU-12, CA-7, IR-1, IR-2, IR-4, IR-5, IR-6, IR-7, IR-8, PE-6, PL-2, RA-5, SI-4, SI-7	AU-2(3), AU-6(1), AU-6(3), CM-3, IR-3, IR-4(1), IR-7(1), IR-7(2), SI-4(2), SI-7(7)	AU-6(5), AU-6(6), IR-4(4), IR-4(8), IR-5(1), AU-6(4), AU-6(9), CA-7(3), IR-4(10), IR-10, RA-5(6), RA-5(8), RA-5(10), SI-4(4), SI-4(11), SI-4(13), SI-4(16), SI-4(17), SI-4(18), SI-4(23), SI-4(24)
Information Services	Service Delivery	SLA´s			-
Information Services	ITOS	CMDB (Configuration Management DB)	CM-1, CM-2, CM-6, CM-8	CM-6(1), CM-8, CM-8(1), CM-8(3), SA-10	CM-6(2), CM-8(2), CM-8(4), CM-8(7), CM-8(9)
Information Services	ITOS	Change Management	CM-1, CM-2, CM-4, CM-6	CM-3, CM-3(2), CM-5, CM-5(3), CM-9, SA-10	CM-3(1), CM-3(4), CM-5(1), CM-5(2), CM-5(4)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Information Services	Service Support	Configuration Rules (Metadata)	CM-1, CM-2, CM-6	CM-3	-
Information Services	Service Support	Configuration Management Database (CMDB)	CM-1, CM-2, CM-6	CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(2), CM-5, CM-9	CM-2(2), CM-3(1), CM-5(1), CM-5(2), CM-5(3), CM-6(1), CM-6(2)
Information Services	Service Support	Change Logs	AU-1, AU-2, AU-3, AU-8, AU-12, CM-2, CM-6, SI-4	AU-2(3), AU-3(1), AU-8(1), CM-2(1, CM-2(3), CM-2(7), CM-3, CM-3(2), CM-6, SI-4(1), SI-4(4)	AU-12(1), AU-3(2), AU-12(3), CM-3(1), CM-6(1), CM-6(2), SI-4(14), SI-4(19), SI-4(20), SI-4(22), SI-4(23)
Information Services	Security Monitoring	Compliance Monitoring	CM-1, CM-2, CM-4, CM-6, CM-8	CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(2), CM-5, CM-8(1), CM-8(5)	CM-2(2), CM-3(1), CM-5(1), CM-5(2), CM-5(3), CM-6(1), CM-6(2)
Information Services	Security Monitoring	Privilege Usage Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12 SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-6(8), AU-12(1), AU-12(3), SI-4(20)
Information Services	Service Delivery	Recovery Plans	CP-1, CP-2, CP-10, IR-4, IR-8	CP-2(1)	
Information Services	BOSS	HR Data (Employee & Contractors)	PS-2, PS-3, PS-7	-	
Information Services	Security Monitoring	Authorization Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-6(8), AU-12(1), AU-12(3), SI-4(20)
Information Services	Security Monitoring	Authentication Events	AU-2, AU-3, AU-6, AU-8, AU-12	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-12(1)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Information Services	Security Monitoring	ACL´s	AC-3	AC-6, AC-6(1)	AC-3(5), AC-3(7)
Information Services	Security Monitoring	CRL´s	AC-3, IA-5, SC-12	IA-5(2), SC-17	AC-3(8)
Information Services	User Directory Services	Active Directory Services	AC-1, AC-2, AC-3, AC-20, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-5(11), IA-7, IA-8	AC-2(2), AC-2(3), AC-2(7), AC-3(7), IA-2(2), IA-2(3), IA-2(5), IA-2(8), IA-2(11), IA-3, PL-8	AC-2(11), AC-2(12), AC-2(13), IA-2(9), AC-2(9), AC-2(10), AC-3(7)
Information Services	User Directory Services	LDAP Repositories	AC-1, AC-2, AC-3, AC-20, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-5(11), IA-7, IA-8	AC-2(2), AC-2(3), AC-2(7), AC-3(7), IA-2(2), IA-2(3), IA-2(5), IA-2(8), IA-2(11), IA-3, PL-8	AC-2(11), AC-2(12), AC-2(13), IA-2(9), AC-2(9), AC-2(10), AC-3(7)
Information Services	User Directory Services	X.500 Repositories	AC-1, AC-2, AC-3, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-5(11), IA-7, IA-8	AC-2(2), AC-2(3), AC-2(7), AC-3(7), IA-2(2), IA-2(3), IA-2(5), IA-2(8), IA-2(11), IA-3, PL-8	AC-2(11), AC-2(12), AC-2(13), IA-2(9), AC-2(9), AC-2(10), AC-3(7)
Information Services	User Directory Services	DBMS Repositories	AC-1, AC-2, AC-3, AC-20, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-5(11), IA-7, IA-8	AC-2(2), AC-2(3), AC-2(7), AC-3(7), IA-2(2), IA-2(3), IA-2(5), IA-2(8), IA-2(11), IA-3, PL-8	AC-2(11), AC-2(12), AC-2(13), IA-2(9), AC-2(9), AC-2(10), AC-3(7)
Information Services	User Directory Services	Registry Services	AC-1, AC-2, AC-3, AC-20, IA-1, IA-2, IA-2(1), IA-4, IA-5, IA-5(1), IA-5(11), IA-7, IA-8	AC-2(2), AC-2(3), AC-2(7), AC-3(7), IA-2(2), IA-2(3), IA-2(5), IA-2(8), IA-2(11), IA-3, PL-8	AC-2(11), AC-2(12), AC-2(13), AC-2(9), AC-2(10), AC-3(7)
Information Services	User Directory Services	Location Services	CM-8		CM-8(8), PE-20
Information Services	User Directory Services	Federated Services	CA-1, CA-2, CA-3, CA-7, SA-1, SA-9	CA-3(5)	SA-9(1), SA-9(3), SC-13

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Information Services	User Directory Services	Virtual Directory Services	-		
Information Services	ITOS	Incident Management	IR-1, IR-4, IR-5, IR-6, IR-8	IR-6(1)	IR-4(4), IR-5(1)
Information Services	Service Support	Service Events	AU-2, AU-3, AU-6, CM-2, CM-4, CM-6, PL-2, SI-5	AU-2(3), AU-7, CM-3, PL-2(3), SA-10, SI-7, SI-7(7)	CM-4(2), RA-5(4), SI-5(1), SI-7(5), AU-7(2), PL-7, SI-7(8), SI-7(9)
Information Services	BOSS	Data Classification	RA-2	-	-
Information Services	Data Governance	Risk Assessments	CA-1, CA-2, CA-7, RA-1, RA-2, RA-3, RA-5, SI-1, SI-4	-	RA-6, SC-38
Information Services	Risk Management	RA - Risk Assessments	RA-3	-	-
Information Services	Risk Management	Business Impact Assessment (BIA)	CP-2, CM-4	CP-2(3), CP-2(8)	
Information Services	Risk Management	VRA - Vendor (Third Party) Risk Assessment	RA-3, SA-9	-	SA-12, SA-12(2), SA-9(1), SA-9(3), SA-12(5), SA-12(8), SA-12(14), SA-12(15)
Information Services	Risk Management	TVM - Threat and Vulnerability Management	CA-2, CA-7, PE-3, RA-3, RA-5	CA-2(2), CA-8, CA-8(2), RA-5(2), RA-5(3), RA-5(8), SA-11, SA-11(2)	SA-11(5), PE-3(6), SC-38
Information Services	Service Delivery	OLAs - Operation Level Agreements	-	-	-
Information Services	Data Governance	Non-Production Data	SA-1	-	SA-15, SA-15(9)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Information Services	Security Monitoring	NIPS Events	SI-4	SI-4(1), SI-4(2), SI-4(4), SI-4(14)	SI-4(11), SI-4(13), SI-4(18), SI-4(15)
Information Services	Security Monitoring	DLP Events - Data Leakage Prevention Events	-	AC-4	AC-4(1), AC-4(6), AC-4(19), AC-16, SC-16
Information Services	Data Governance	Information Leakage Metadata	AC-1, SC-1	AC-4	AC-4(1), AC-4(6), AC-4(19), AC-16, SC-16
Information Services	Data Governance	Data Segregation	AC-1, AC-2, AC-3, AC-20, IA-1, IA-2, IA-4, IA-5, IA-8, SC-1, SC-7	AC-4, AC-4(21), AC-6, AC-20(1), AC-20(2), IA-3, SC-2	SC-3, SC-7(21), AC-6(4), IA-9, SC-3(1), SC-3(2), SC-7(22)
Information Services	Security Monitoring	Transformation Services	AU-6, AU-12, SI-4	AU-6(1), AU-6(3), SI-4(5)	AU-6(5), AU-6(6), AU-6(9), AU-12(1), SI-4(3), SI-4(16), SI-4(17)
Information Services	Security Monitoring	Session Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-12(1)
Information Services	Security Monitoring	Application Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5),	AU-3(2), AU-6(5), AU-6(6), AU-12(1)
Information Services	Security Monitoring	Network Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-12(1)
Information Services	Security Monitoring	Computer Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-12(1)
Information Services	Security Monitoring	Host Intrusion Protection Systems (HIPS)	SI-4	SI-4(2), SI-4(4), SI-4(5)	SI-4(23)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Information Services	Security Monitoring	Database Events	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), SI-4(2), SI-4(5)	AU-3(2), AU-6(5), AU-6(6), AU-12(1)
Information Services	Service Delivery	Contracts	-	-	-
Information Services	ITOS	Strategy	CA-2, CA-7, CM-4, RA-3, RA-5, SA-2		
Information Services	ITOS	Roadmap			
Information Services	ITOS	Service Management			
Information Services	BOSS	Risk Assessments	RA-1, RA-2, RA-3, RA-5		SC-38
Information Services	BOSS	Process Ownership			
Information Services	BOSS	Business Strategy	PL-2, RA-3		
Information Services	Service Support	Knowledge Repository	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1		
Information Services	Risk Management	GRC - Governance, Risk & Compliance	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1	-	-
Information Services	Risk Management	DR & BC Plans - Disaster Recovery &Business Continuity	CP-1, CP-2, CP-4, CP-9, CP-10	CP-2(1), CP-2(3), CP-2(8), CP-4(1), CP-6, CP-7, CP-8, CP-10(2)	CP-2(4), CP-2(5), CP-2(7), CP-10(4)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	Block-Based Virtualization	PL-8	SA-17	
Infrastructure Services	Internal Infrastructure: Network Services	Authoritative Time Source	AU-8	AU-8(1)	-
Infrastructure Services	Internal Infrastructure: Servers	Secure Build & Image Management	CM-1, CM-2, CM-4, CM-6	CM-2(1), CM-2(2), CM-2(3), CM-3, CM-3(2), CM-5, CM-5(3)	CM-3(1), CM-5(1), CM-5(2), CM-6(1), CM-6(2), CM-3(3), CM-3(4), CM-3(5), CM-3(6)
Infrastructure	Internal Infrastructure: Availability Services		CP-1, CP-2, CP-3, CP-4, CP-9	CP-2(3), CP-6, CP-6(1), CP-6(3), CP-7, CP-7(1), CP-7(2), AP-7(3), CP-9(1), CP-9(3)	CP-7(4), CP-9(5), CP-9(6), SI-13
Infrastructure Services	Internal Infrastructure: Patch Management	Service Discovery	CM-1, CM-2, CM-8, RA-1, RA-5	CM-2(1), CM-8(1), CM-8(3), RA-5(1), RA-5(2)	CM-2(2), CM-8(2)
Infrastructure Services	Internal Infrastructure: Equipment Maintenance		MA-1, MA-2	MA-6	MA-6(1), MA-6(2), SI-13
Infrastructure Services	Internal Infrastructure: Storage Services		AC-1, AC-2, AC-20, AU-4, AU-5, CP-1, CP-2, CP-9, MP-6, RA-2, RA-3, SA-9	CP-6, CP-6(1), CP-6(3), CP-9(1), MP-4	CP-2(2), CP-2(4), CP-2(5), CP-9(3), CP-9(5), AC-20(4), CP-2(6), SC-36
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	Block-Based Virtualization	**PL-8**, SC-7	SA-17	-
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	PE-3	-	PE-18
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	PE-3	-	PE-3(2), PE-3(3)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	PE-6	PE-6(1)	PE-6(4), PE-6(2), PE-6(3)
Infrastructure Services	Internal Infrastructure: Facility Security	Controlled Physical Access	PE-2, PE-3	-	PE-2(2)
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	PL-8	SA-17	
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	PL-8	SA-17	
Infrastructure Services	Internal Infrastructure: Facility Security	Asset Handling	CM-8, PE-1, PE-3, PE-16	CM-8(1), PE-5	PE-18, CM-8(4), CM-8(8), PE-3(4), PE-3(5)
Infrastructure Services	Internal Infrastructure: Facility Security	Environmental Risk Management	RA-3, PE-3, PE-12, PE-13, PE-14	PE-9, PE-10, PE-11	PE-18
Infrastructure Services	Internal Infrastructure: Facility Security	Environmental Risk Management	PE-1, PE-12, PE-13, PE-14, PE-15, SA-9	PE-5, PE-9, PE-10, PE-11, SA-9(5)	PE-18, PE-18(1)
Infrastructure Services	Internal Infrastructure: Facility Security	Environmental Risk Management	-	PE-11	PE-11(1), PE-11(2)
Infrastructure Services	Internal Infrastructure: Network Services	Network Segmentation	PL-8, RA-2, RA-3, SC-1, SC-7	SA-17, SC-7(5), SC-7(8)	SC-7(14), SC-7(21), SC-7(13), SC-7(20), SC-7(22)
Infrastructure Services	**Virtual Infrastructure**: Desktop "Client" Virtualization	Local	PL-8, SC-7	SA-17	SC-7(21), IA-3(3), SC-25, SC-37

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Infrastructure Services	**Virtual Infrastructure**: Desktop "Client" Virtualization	Remote	PL-8	SA-17	
Infrastructure Services	**Virtual Infrastructure**: Desktop "Client" Virtualization	Remote	AC-2, AC-3, AC-17, IA-2, IA-4, IA-5, PL-8, SC-7	AC-2(1), AC-2(2), AC-2(3), AC-10, AC-17(1), AC-17(2), AC-17(4), IA-2(11), SA-17	AC-2(11, AC-2(12), AC-2(13), SC-7(21), AC-2(6), AC-2(8), AC-3(8)
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	Block-Based Virtualization	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	**Virtual Infrastructure:** Storage Virtualization	File-Based Virtualization	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	**Virtual Infrastructure:** Application Virtualization	Client Application Streaming	PL-8	SA-17	
Infrastructure Services	**Virtual Infrastructure:** Application Virtualization	Server Application Streaming	PL-8	SA-17	-
Infrastructure Services	Virtual Infrastructure: Virtual Workspaces	Vertical Isolation	PL-8, SC-7	SA-17, SC-7(13)	SC-3, SC-7(21), SC-3(5), SC-7(20), SC-7(21), SC-39
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Machines (host based)	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Machines (host based)	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Machines (host based)	PL-8, SC-7	SA-17	SC-7(21)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Infrastructure Services	Virtual Infrastructure: Server Virtualization	OS Virtualization	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure: Server Virtualization	TPM Virtualization	AC-3, PL-8, SC-12, SC-13	CM-5, SI-7, SI-7(1)	CM-5(3), SI-7(6), SI-7(9), SI-7(10), SI-7(15)
Infrastructure Services	Virtual Infrastructure: Server Virtualization	Virtual Memory	PL-8	SA-17, SI-16	
Infrastructure Services	Virtual Infrastructure: Network	Network Address Space	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure: Network	Network Address Space	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure: Network	VLAN (external)	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	Virtual Infrastructure: Network	VNIC (internal)	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	**Virtual Infrastructure:** Database Virtualization	-	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	**Virtual Infrastructure:** Mobile Device Virtualization	-	PL-8, SC-7	SA-17	SC-7(21)
Infrastructure Services	**Virtual Infrastructure:** Smartcard Virtualization	-	IA-2, IA-2(12), IA-5, IA-8, IA-8(1), PL-8	SA-17	IA-5(10)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
Infrastructure Services	Internal Infrastructure: Patch Management	Compliance Monitoring	AU-1, AU-2, AU-3, AU-6, AU-8, AU-12, CA-1, CA-2, CA-2(1), CA-7, SI-1, SI-4	AU-2(3), AU-3(1), AU-6(1), AU-6(3), AU-8(1), CA-7(1), SI-4(1), SI-4(2), SI-4(4), SI-4(5)	AU-3(2), AU-12(1), AU-12(3), CA-2(3), SI-4(11)*, SI-4(13)*, SI-4(14)*, SI-4(16)*, SI-4(18)*, SI-4(21)*, SI-4(23*) *see notes
S & RM	Privilege Management Infrastructure	Privilege Usage Management	IA-2, IA-2(1), SC-7, SC-10	AC-6, IA-2(2), IA-2(8), IA-2(11), SC-2, SC-23	AC-6(3), IA-2(9), SC-3, IA-2(6), IA-2(7), SC-2(1), SC-7(15)
S & RM	Infrastructure Protection Services	Server	CM-7	CM-7(5)	-
S & RM	Infrastructure Protection Services	Server	SC-7	SC-7(12)	-
S & RM	Infrastructure Protection Services	End-Point	SC-7	SC-7(12)	-
S & RM	Infrastructure Protection Services	End-Point	SC-7	AC-4, SC-7(5)	AC-4(1), AC-4(4), AC-4(6), AC-4(8), AC-4(10), AC-4(11), AC-4(14), SI-15
S & RM	Infrastructure Protection Services	End-Point	CA-3, CM-7, SC-7	CA-3(5), SC-7(5)	CA-7(5)
S & RM	Infrastructure Protection Services	Network	SC-7	AC-4, SC-7(5)	AC-4(4), AC-4(21), SC-7(10), SC-7(11)
S & RM	Infrastructure Protection Services	Network	SC-7	AC-4	AC-4(4), AC-4(21), SC-7(10), SC-7(11)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Infrastructure Protection Services	Network	CA-3, CM-7, SC-7	CA-3(5), CM-7(4), SC-7(5)	
S & RM	Infrastructure Protection Services	Application	SC-7	AC-4	-
S & RM	Infrastructure Protection Services	Application	SC-15	AC-21	-
S & RM	Infrastructure Protection Services	Application	SC-7, SI-4	AC-4, SI-4(2), SI-4(4)	SC-7(8), AC-4(8), AC-4(11), SC-7(19), SI-4(7), SI-4(13)
S & RM	Data Protection	Data Lifecycle Management	-	AC-4, SI-7	AC-4(6), AC-4(19), AC-16
S & RM	Data Protection	Data Lifecycle Management	-	-	-
S & RM	Data Protection	Intellectual Property Prevention	CM-10	-	-
S & RM	Policies and Standards	Role Based Awareness	AC-1, AC-2, AC-3, AT-3	AC-2(4)	AC-2(7), AC-3(7)
S & RM	Governance Risk & Compliance	Technical Awareness and Training	AT-3	-	-
S & RM	Governance Risk & Compliance	Compliance Management	CA-1, CA-2, CA-2(1), CA-9, CM-6, SI-1	CA-9(1), CM-6(1)	-

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Governance Risk & Compliance	Audit Management	AU-1, AU-2, AU-3, AU-9, AU-12, CA-1, CA-2, CA-2(1), CA-7, RA-3, RA-5	AU-2(2), AU-3(1), AU-9(4), CA-2(2), CA-7(1), CA-8, CA-8(1), RA-5(1), RA-5(2), RA-5(3), RA-5(6), RA-5(9), SA-11	AU-3(2), AU-9(1)*, AU-9(2), AU-9(3), AU-9(5)*, AU-9(6)*, AU-12(1), AU-12(3) *see note
S & RM	Threat and Vulnerability Management	Compliance Testing	-	-	-
S & RM	Policies and Standards	Best Practices & Regulatory correlation	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1	-	-
S & RM	InfoSec Management	Capability Mapping	PL-1, PL-2	PL-8	-
S & RM	Infrastructure Protection Services	End-Point	CM-8	-	CM-8(2), CM-8(4), CM-8(7)
S & RM	Data Protection	Intellectual Property Prevention	CM-10	-	-
S & RM	Policies and Standards	Operational Security Baselines	CM-1, CM-2, CM-6	CM-2(1), CM-2(3), CM-2(7)	CM-2(2), CM-6(1), CM-6(2)
S & RM	Policies and Standards	Job Aid Guidelines	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SA-5, SC-1, SI-1		
S & RM	Privilege Management Infrastructure	Identity Management	IA-2, IA-4, IA-8	IA-3	-

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Privilege Management Infrastructure	Identity Management	AC-3	AC-4	AC-3(3), AC-3(4), AC-4(1), AC-4(2), AC-4(12), AC-4(13), AC-4(14), AC-4(15), AC-4(19), AC-4(22), AC-4(22)
S & RM	Privilege Management Infrastructure	Identity Management	AC-1, AC-2, AC-3	AC-2(1)	AC-3(3), AC-3(4), AC-3(8), AC-16)
S & RM	Privilege Management Infrastructure	Identity Management	AC-1, AC-2, AC-3	AC-2(1)	AC-3(3), AC-3(4), AC-3(8), AC-16
S & RM	Privilege Management Infrastructure	Authorization Services	AC-1, AC-2, AC-3	-	AC-3(2), AC-3(8)
S & RM	Privilege Management Infrastructure	Authorization Services	AC-1, AC-2, AC-3	-	AC-24
S & RM	Privilege Management Infrastructure	Authorization Services	AC-1, AC-2, AC-3	-	AC-2(6), AC-2(8), AC-3(3), AC-3(4), AC-3(8), AC-16, AC-16(1), AC-16(3), AC-16(4), AC-16(6), AC-16(8), AC-16(9), AC-16(10), AC-24
S & RM	Privilege Management Infrastructure	Authorization Services	-	-	-
S & RM	Privilege Management Infrastructure	Authorization Services	AC-1, AC-2, AC-3, IA-1, IA-4, IA-5	AC-2(1), AC-2(2), AC-2(3), AC-3(4), AC-5, AC-6, AC-6(2), AC-6(5), AC-6(9), AC-6(10)	AC-2(11), AC-2(12), AC-2(13), AC-2(7), AC-3(7), AC-6(7)
S & RM	Privilege Management Infrastructure	Authorization Services	-	-	-

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Privilege Management Infrastructure	Authorization Services	-	-	-
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-4, IA-5, IA-8, IA-8(4)	-	-
S & RM	Privilege Management Infrastructure	Authentication Services	AC-1, AC-2, AC-3, IA-1, IA-4, IA-5	AC-2(1), AC-2(2), AC-2(3), AC-3(4), AC-5, AC-6, AC-6(2), AC-6(5), AC-6(9), AC-6(10)	AC-2(11), AC-2(12), AC-2(13), AC-2(7), AC-3(7), AC-6(7)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-2(1), IA-4, IA-5(1), IA-5(11), IA-8, IA-8(1), IA-8(2), IA-8(3), IA-8(4)	IA-2(2), IA-2(3), IA-2(8), IA-2(11)	IA-2(4); IA-2(9), IA-2(6), IA-2(7), IA-5(12), IA-5(15),IA-8(5)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-2(1), IA-4, IA-5, IA-8	IA-2(2), IA-2(3), IA-2(8), IA-2(11)	IA-2(4), IA-2(9), IA-5(8)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-2(12), IA-4, IA-5, IA-7, IA-8, IA-8(1), IA-8(2), IA-8(3), IA-8(4)	IA-5(2), IA-5(3), IA-5(11)	IA-4(3), IA-4(7), IA-5(14), IA-5(15), IA-8(5)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-5, IA-5(1)	-	IA-5(4)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-4, IA-5, IA-8	-	IA-5(12)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-4, IA-5, IA-8	IA-3, IA-2(1), IA-2(2), IA-2(8), IA-2(11), IA-5(1), IA-5(2), IA-5(11)	IA-2(9), IA-2(6), IA-2(7)
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-5, IA-8	-	IA-2(10), IA-5(8)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Privilege Management Infrastructure	Authentication Services	IA-4, IA-5	IA-3	
S & RM	Privilege Management Infrastructure	Authentication Services	-	IA-3	-
S & RM	Privilege Management Infrastructure	Authentication Services	IA-2, IA-2(12), IA-5, IA-5(11), IA-5(12), IA-8, IA-8(1)	-	IA-8(5)
S & RM	Privilege Management Infrastructure	Authentication Services	-	-	-
S & RM	Privilege Management Infrastructure	Privilege Usage Management	AU-2, AU-3, AU-12	AC-6, AC-6(9), AU-3(1)	AU-14
S & RM	Privilege Management Infrastructure	Privilege Usage Management	AC-3, IA-5	AC-6, IA-5(1), IA-5(6), SC-28	-
S & RM	Threat and Vulnerability Management	Compliance Testing	CA-2, CA-2(1), CA-3, CA-7, CA-9	CA-3(5), CA-8, CA-8(1)	CA-2(4)
S & RM	Infrastructure Protection Services	End-Point	AU-2, AU-6, AU-11	AU-6(1),AU-7(1), IR-4(1), SA-9(5)	IR-5(1), IR-10, SI-4(24)
S & RM	Infrastructure Protection Services	End-Point	MP-1, MP-2, MP-7	MP-4	-
S & RM	InfoSec Management	Residual Risk Management	CA-7, RA-3, RA-5	SC-4	-
S & RM	Governance Risk & Compliance	Policy Management	SC-15	CA-3(5), CM-7(4), CM-7(5), SC-7(4), SC-7(5)	SI-7(14), SC-42

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Governance Risk & Compliance	Policy Management	AU-1, AU-2, AU-3, AU-8, AU-12, CA-2, CA-7, RA-3, RA-5, SI-4	AU-2(3), AU-3(1), AU-8(1), RA-5(1), RA-5(2), RA-5(5), SI-4(1), SI-4(2), SI-4(4), SI-5(5)	AU-3(2), AU-12(1), AU-12(3), CA-2(2), RA-5(4), RA-5(3)*, RA-5(6)*, RA-5(8)*, SI-4(14), SI-4(19), SI-4(20), SI-4(22), SI-4(23) *See note
S & RM	InfoSec Management	Risk Dashboard	RA-1, AU-12, CA-2, CA-2(1), CA-5, CA-7, CM-1, CM-2, CM-6, RA-3 SA-9, SI-4	CA-7(1), CM-2(1), CM-2(3), CM-2(7), CM-3, CM-3(2), SA-9(2), SI-4(2), SI-4(5)	AU-12(1), AU-12(3), CM-2(2), CM-3(1), CM-6(1), CM-6(2), SA-9(1)*, SI-4(3), SI-4(16)*, SI-4(17), SI-4(23)*
S & RM	Threat and Vulnerability Management	Vulnerability Management	AU-6, CA-2, CA-5, CA-7, CA-8, RA-1, RA-5, SI-2	AU-6(1), AU-6(3), RA-5(1), RA-5(2), RA-5(5) SA-11(2), SI-2(2)	AU-6(5), AU-6(6), CA-2(2), RA-5(6), SA-11(2), SA-15, SA-15(2), SA-15(4), SA-15(7), SI-2(1)
S & RM	Threat and Vulnerability Management	Vulnerability Management	AU-6, CA-2, CA-5, CA-7, CA-8, RA-1, RA-5, SI-2	AU-6(1), AU-6(3), RA-5(1), RA-5(2), RA-5(5) SA-11, SI-2(2)	AU-6(5), AU-6(6), CA-2(2), RA-5(6), SA-11(2), SA-15, SA-15(2), SA-15(4), SA-15(7), SI-2(1)
S & RM	Threat and Vulnerability Management	Vulnerability Management	AU-6, CA-2, CA-5, CA-7, CA-8, RA-1, RA-5, SI-2	AU-6(1), AU-6(3), RA-5(1), RA-5(2), RA-5(5) SA-11(2), SI-2(2)	AU-6(5), AU-6(6), CA-2(2), RA-5(6), SA-11(2), SA-15, SA-15(2), SA-15(4), SA-15(7), SI-2(1)
S & RM	Threat and Vulnerability Management	Penetration Testing	CA-2	CA-2(2), CA-8	-
S & RM	Threat and Vulnerability Management	Penetration Testing	CA-2	CA-2(2), CA-8, SA-11, ~~SA-11(5)~~	SA-11(5), CA-8(1), CA-8(2)}

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Threat and Vulnerability Management	Threat Management	-	SA-11	SA-11(1), SA-11(8)
S & RM	Threat and Vulnerability Management	Threat Management	RA-3	SA-11	SA-15, SA-11(2), SA-15(4), SA-15(8)
S & RM	Policies and Standards	Data / Asset Classification	RA-2, RA-3		AC-16, AC-16(1), AC-16(2), AC-16(3), AC-16(4), AC-16(6), AC-16(6), AC-16(7), AC-16(8), AC-16(9), AC-16(10), SC-16, SC-16(1)
S & RM	Governance Risk & Compliance	Vendor Management	AC-20, SA-1, SA-4, SA-9,	SA-4(1), SA-4(2), SA-4(9), SA-9(2), SA-10, SA-11, SA-17, SC-7(12)	SA-12, SA-9(3), SA-9(5), SA-21, SA-19
S & RM	Data Protection	Data Lifecycle Management	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, MA-1, MP-1, MP-6, PE-1, PL-1, PS-1, RA-1, RA-2, RA-3, SA-1, SA-3, SC-1, SI-1, SI-12	MP-3	-
S & RM	Policies and Standards	Technical Security Standards	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1	-	-
S & RM	Privilege Management Infrastructure	Privilege Usage Management	AC-3, AC-8, AC-20, AT-2, AU-6, CM-5, CM-11, PL-4, PS-6, PS-8	AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10), AC-20(1), AC-20(2)	AC-6(3), AC-3(2), AC-3(3), AC-3(4), AC-3(7), SC-42, SC-42(2), SC-43

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Infrastructure Protection Services	Network	SC-5, SC-7	-	SC-7(10), SC-7(17)
S & RM	Infrastructure Protection Services	Network	AC-18, SC-12, SC-13	AC-18(1), IA-3, SC-8, SC-8(1),	AC-18(4), AC-18(5), SC-40, SC-40(2), SC-40(3), SC-40(4)
S & RM	Infrastructure Protection Services	Network	AC-3, CM-2, CM-6, CM-7, SC-5, SC-7	AC-6, AC-6(1)	AC-3(5)
S & RM	Infrastructure Protection Services	Application	-	-	-
S & RM	Infrastructure Protection Services	Application	SC-12, SC-13	SC-8, SC-8(1)	AU-10, SC-8(3)
S & RM	Data Protection	Data Lifecycle Management	AC-22, MP-6	-	-
S & RM	Data Protection	Data Lifecycle Management	SA-18, SC-7	-	SA-18(1), SC-7(16), SC-30
S & RM	Data Protection	Data Lifecycle Management	AC-4	-	AC-4(6), AC-16, SC-16
S & RM	Data Protection	Data Lifecycle Management	SA-18, SC-7	-	SA-18(1), SC-7(16), SC-30
S & RM	Data Protection	Data Leakage Prevention	RA-2, RA-3, RA-5	RA-5(1), RA-5(2), RA-5(5)	RA-5(4), AU-13, PE-19
S & RM	Data Protection	Data Leakage Prevention	AC-17, MA-4, SC-7, SC-12, SC-13, SI-4	AC-17(2), SC-8, SC-8(1)	MA-4(6), SC-8(3), SC-31, SC-31(1), SC-31(2), SC-31(3), SI-4(10)
S & RM	Data Protection	Data Leakage Prevention	AC-18, AC-19, SC-7, SC-13	AC-18(1), AC-19(5), SC-4	SC-7(21), AC-4(4), AC-16

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Data Protection	Data Leakage Prevention	AC-19, MP-5, SC-7, SC-13	AC-19(5), MP-5(4), SC-28, SC-28(1)	PE-19, SC-31, SC-31(1), SC-31(2), SC-31(3)
S & RM	Cryptographic Services	Key Management	SC-12	SC-12(2), SC-17	SC-12(1)
S & RM	Cryptographic Services	Key Management	SC-12	SC-12(3), SC-17	SC-12(1)
S & RM	Cryptographic Services	PKI	SC-12, IA-5	IA-5(2), SC-17, SC-12(2), SC-12(3)	SC12-1, IA-5(14)
S & RM	Cryptographic Services	Data in use (memory) Encryption	SC-12, SC-13	-	-
S & RM	Cryptographic Services	Data in Transit Encryption (Transitory, Fixed)	AC-17, MA-4, SC-12, SC-13	AC-17(2), SC-8, SC-8(1)	MA-4(6), SC-8(3)
S & RM	Cryptographic Services	Data as Rest Encryption (DB, File, SAN, Desktop, Mobile)	AC-19, MP-5, SC-13	AC-19(5), MP-5(4), SC-28, SC-28(1)	-
S & RM	Infrastructure Protection Services	Server	SI-2, SI-3, SI-4	SI-2(1), SI-3(1), SI-3(2), SI-4(2), SI-4(4), SI-4(5)	SI-2(2)
S & RM	Infrastructure Protection Services	Server	SI-4	SI-4(1), SI-4(2), SI-4(4), SI-4(5)	SI-4(7), SI-4(11), SI-4(13), SI-4(14), SI-4(18)
S & RM	Infrastructure Protection Services	End-Point	SI-2, SI-3, SI-4, SI-8	SI-2(1), SI-3(1), SI-3(2), SI-4(2), SI-4(4), SI-4(5), SI-8(1), SI-8(2)	-
S & RM	Infrastructure Protection Services	End-Point	SI-4	SI-4(2), SI-4(4), SI-4(5), SI-4(23)	SI-4(7), SI-4(11), SI-4(13), SI-4(18)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Infrastructure Protection Services	End-Point	-	SI-7	SC-3, AC-16, AC-16(8), SC-3(4)
S & RM	Infrastructure Protection Services	Network	SI-4	SI-4(2), SI-4(4), SI-4(5)	SI-4(7), SI-4(11), SI-4(13), SI-4(14), SI-4(15), SI-4(16), SI-4(18), SI-4(22)
S & RM	Data Protection	Data Lifecycle Management	SC-12, SC-13	SC-8, SC-8(1), SC-8(2), SI-7	AU-10, SI-7(6)
S & RM	Cryptographic Services	Signature Services	SC-12, SC-13	SC-8, SC-8(1), SC-8(2), SI-7	AU-10
S & RM	Governance Risk & Compliance	IT Risk Management	CA-1, CA-2, CA-2(1), CA-6, CA-7, CA-7(1), PS-2, RA-1, RA-2, RA-3	CA-8, CA-2(2)	-
S & RM	InfoSec Management	Risk Portfolio Management	AC-1, AT-1, AU-1, AU-2, AU-6, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1	-	-
S & RM	Privilege Management Infrastructure	Authorization Services	AC-1, AC-2, IA-1, IA-4	AC-2(1)	-
S & RM	Privilege Management Infrastructure	Authorization Services	AC-1, AC-2, AC-3, AC-17, AC-18, AC-19, AC-20, IA-4	AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-2(5), AC-2(7), AC-2(9), AC-2(10), AC-2(12), AC-4, AC-4(21), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(9), AC-6(10), AC-17(4), AC-17(9), AC-19, AC-20(1), AC-20(2)	AC-2(11), AC-2(13), AC-6(3), AC-6(7), AC-6(8), AC-18(4)

DOMAIN	CONTAINER	CAPABILITY (process or solution)	Low Impact Level	Moderate Impact Level	High Impact Level
S & RM	Policies and Standards	Information Security Polices	AC-1, AT-1, AU-1, AU-2, AU-6, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1	-	-

9 References

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

[2] "Information Technology, Security Techniques, Code of Practice for Information Security Management," ISO/IEC 27002, 2014.

[3] "Cloud-adapted Risk Management Framework", Draft NIST SP 800-173, 2014.

[4] J. Luna, N. Suri, M. Iorga, A. Karmel, "Leveraging the Potential of Cloud Security Service Level Agreements through Standards". In IEEE Cloud Computing Magazine, 2015

[5] "Security Framework for Governmental Clouds - All steps from design to deployment", ENISA, 2015.

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

[7] Available: http://www.kempitlaw.com/wp-content/uploads/2015/10/Part-II-Seeding-the-Global-Public-Sector-Cloud.pdf. Last accessed May 2016.

[8] EU A4CLOUD Project.

[9] Available: http://www.a4cloud.eu/content/a4cloud-toolkit. Last accessed May 2016.

[10] J. Colpaert, "D9.5 Risk Analysis, Certification and Other Measures", ver.1, Cloud for Europe project. 2015.

[11] EU RISCOSS Project. Available:

[12] http://www.riscoss.eu/bin/view/Discover/The_RISCOSS_Solution. Last accessed May 2016.

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

[14] Available: http://www.eci.com/blog/15695-monetary-authority-of-singapore-mas-technology-risk-management-guidelines-overview-.html. Last accessed May 2016.

[15] D. Vohradsky, "Cloud Risk—10 Principles and a Framework for Assessment". In ISACA. Vol. 5. 2012.

[16] A CLOUD ADOPTION RISK ASSESSMENT MODEL, 2014 IEEE/ACM 7th International Conference

[17] "Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach", NIST SP 800-37 rev. 1, 2010.

[18] "Information technology - Security techniques - Information security risk management", ISO/IEC 27005, 2011.

[19] "COBIT 5 Framework", ISACA. Available: https://www.isaca.org/Pages/default.aspx

[20] "Information technology - Security techniques - Information security management systems - Requirements", ISO/IEC 27001, 2013.

[21] "Information technology - Security techniques - Code of practice for information security controls", ISO/IEC 27002, 2013.

[22] "Security and Privacy Controls for Federal Information Systems and Organizations," NIST SP-800-53 rev. 4, 2013.

[23] "Cloud Controls Matrix", CSA. Available: https://cloudsecurityalliance.org/group/cloud-controls-matrix/ Last accessed May 2016

[24] "Enterprise Architecture", CSA. Available: https://cloudsecurityalliance.org/group/enterprise-architecture/#_downloads Last accessed May 2016
[25] ASSERT4SOA FP7 project. Available: http://www.assert4soa.eu
[26] ANIKETOS FP7 project. Available: http://www.aniketos.eu
[27] NESSOS FP7 project. Available: http://www.nessos-project.eu
[28] CIRRUS FP7 project. Available: http://www.cirrus-project.eu
[29] C. Ardagna, R. Asal, E. Damiani, Q. Vu, "From Security to Assurance in the Cloud: A Survey". In ACM Computing Surveys, Vol. 48, No. 1, Article 2. 2015.
[30] "Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services", ISO/IEC 27017, 2015
[31] "Guidelines on Security and Privacy in Public Cloud Computing", NIST SP-800-144, 2011.
[32] CUMULUS FP7 project: http://www.cumulus-project.eu
[33] SPECS FP7 project: http://www.specs-project.eu
[34] MUSA H2020 project: http://www.musa-project.eu
[35] "FedRAMP Forward", FedRAMP, 2014
[36] Info-Communication Development Authority of Singapore, IDA.
[37] Available: https://www.ida.gov.sg/Tech-Scene-News/Infrastructure/Cloud
[38] R. Joshi. "A close look at IDA's project on cloud providers & application performance", Enterprise Innovation. 2015
[39] "Cloud Security Guide for SMEs - Cloud computing security risks and opportunities for SMEs", ENISA, 2015.
[40] M. Jouini, L. Ben Arfa Rabai, "Comparative Study of Information Security Risk - Assessment Models for Cloud Computing systems". In Procedia Computer Science. Vol. 83, pp. 1084 – 1089. 2016.
[41] D. Zissis, D. Lekkas, "Addressing cloud computing security issues". In Future Generation Computer Systems, Vol. 28, Issue 3, pp. 583–592. 2012.
[42] K. Djemame, D. Armstrong, M. Kiran, M. Jiang, "A risk assessment framework and software toolkit for cloud service ecosystems". In CiteSeer, 2011.
[43] P. Saripalli, "QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security". In IEEE 3rd International Conference on Cloud Computing, pp. 280 – 288. 2010.
[44] CUMULUS Evaluation Report – Project Results summarized for external Evaluators, 2015.
[45] NESSOS FP7. Final project report "Network of Excellence on Engineering Secure Future Internet Software Services and Systems". Executive Summary.
[46] CORDIS. Projects & Results, ASSERT4SOA, Project reference: 257351, FP7-ICT, Publishable Summary. Record Number: 95250 / Last updated on: 2016-04-01.