EUSEC
EU SECURITY CERTIFICATION

EUROPEAN SECURITY CERTIFICATION FRAMEWORK

D 1.2 SECURITY AND PRIVACY REQUIREMENTS AND CONTROLS

VERSION: 1.4

PROJECT NUMBER: 731845

PROJECT TITLE: EU-SEC

DUE DATE:	DELIVERY DATE:
31.08.2017	28.05.2019
AUTHOR: Anton Ujčič, SI-MPA Darja Lihteneger, SI-MPA	PARTNERS CONTRIBUTED: SI-MPA, NIXU, Fraunhofer, PwC, CaixaBank, CSA
DISSEMINATION LEVEL: *	NATURE OF THE DELIVERABLE: **
PU	R
INTERNAL REVIEWERS:	
Fraunhofer, NIXU	

*PU = Public, CO = Confidential

**R = Report, P = Prototype, D = Demonstrator, O = Other

This project has received funding from the European Union's HORIZON Framework Programme for research, technological development and demonstration under grant agreement no 731845.

VERSIONING

Version	Date	Comment	Name, Organisation
1.0	31/08/2017	Initial Version	Anton Ujčič, SI-MPA Darja Lihteneger, SI-MPA
1.1	13/10/2017	Updated combined table of requirements	Anton Ujčič, SI-MPA Darja Lihteneger, SI-MPA
1.2	19/12/2017	Editorial changes, update of content	Anton Ujčič, SI-MPA Darja Lihteneger, SI-MPA
1.3	15/12/2018	Revision of deliverable	Anton Ujčič, SI-MPA
1.4	28/05/2019	Deliverable updated with privacy require-ments	Anton Ujčič, SI-MPA Tuisku Sarrala, NIXU

EXECUTIVE SUMMARY

The European Security Certification Framework (EU-SEC) project strives to address the security, privacy and transparency challenges associated with the greater externalisation of IT to Cloud services. This deliverable is part of work package 1 (WP1) with its main task to collect requirements for the design of efficient and effective security certification methods. It is focused on security and privacy requirements.

A common methodology was defined for the collection and evaluation of the requirements which was composed of two phases: the requirements gathering in Phase 1, and the requirements consolidation in Phase 2. The thematic scope of input sources was set to the international and national standards related to cloud computing, legislation (mostly related to public sector), technical specifications and guidelines and documents important for the banking sector.

The requirements were collected from several input documents and for every identified requirement we evaluated how they correspond with the security and privacy controls. The comparing and mapping was done using the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) and following the CSA Standard Mapping Methodology. CCM is a cloud relevant information assurance control framework that gives a detailed understanding of security concepts and principles and is widely adopted by both cloud service providers (CSP) and cloud service consumers.

The findings showed 804 relevant requirements that were categorised into three different levels of gaps in the mapping to the CCM controls. Most of the requirements (71%) were satisfactory covered with the CCM controls and they presented no gap in the mapping. The requirements where we found partial or full gap served as a basis for updating the existing CCM controls or to define new controls. Both components, the existing CCM and the proposed changes or new controls are the basis for the EU-SEC Requirements and Controls Repository.

The collected requirements will be further addressed in the EU-SEC project pilots. The experiences from this deliverable also indicated the need to ensure that the new requirements could be continuously captured and covered by the up-to-date security and privacy controls. This might influence the EU-SEC framework governance mechanism.

We appreciate the contributions of project partners in the collection and evaluation of the requirements. Especially, we would like to thank to the EU-SEC Advisory Board for their consultation in the preparation of this deliverable.

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Communities. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

ABBREVIATIONS

AB	(EU-SEC) Advisory Board
AICPA	American Institute of Certified Public Accountants
ANSSI	Agence nationale de la sécurité des systèmes d'information (en. National Cybersecurity Agency of France)
ASEC	AICPA Assurance Services Executive Committee
BDSG	Bundesdatenschutzgesetz (en. German Federal Data Protection Act)
BYOD	Bring Your Own Device
CCM	Cloud Control Matrix
CCRA	Cloud Computing Risk Assessment
CCSM	Cloud Certification Schemes Meta framework
COBIT	Control Objectives for Information and related Technology (Formerly known as Control Objectives for Information and related Technology (COBIT); now used only as the acronym in its fifth iteration – COBIT 5)
CoC	Code of Conduct
CPA	Certified Public Accountant
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
D1.2	Deliverable 1.2 (D1.2 Security and Privacy Requirements and Controls)
D2.3	Deliverable 2.3 (D2.3 Privacy Code of Conduct)
DBaaS	Database as a Service
DevOPSaaS	Development Operations as a Service
DoW	Description of Work
DPA	Data Protection Authorities

DPO	Data Protection Officer
DSP	Digital Service Provider
EBA	European Banking Authority
eIDAS	electronic IDentification, Authentication and trust Services
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
EU	European Union
EU-SEC	European Security Certification Framework
GDPR	General Data Protection Regulation
IaaS	Infrastructure as a Service
ICT	Information and communication technology
IDW	Institut der Wirtschaftsprüfer (en. Financial Auditor Institute)
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information technology
ITU	International Telecommunication Union
MCC	Model Contract Clause
NATO	North Atlantic Treaty Organization
NIS Directive	Directive on security of network and information systems
NIST	National Institute of Standards and Technology
PA	Public administration
PaaS	Platform as a Service

PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
PLA	Privacy Level Agreement
PwC	PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft
SaaS	Software as a Service
SECaaS	Security as a Service
SGC	Slovenian Government Cloud (sl: DRO - Državni računalniški oblak)
SI-MPA	Republic of Slovenia Ministry of Public Administration
SLA	Service Level Agreement
SO	Security Objective
STAR	Security, Trust & Assurance Registry
TFEU	Treaty on the Functioning of the European Union
TSC	Trust Services Criteria
TSP	Trust Services Principles
WP	Work Package

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

TERMINOLOGY AND DEFINITIONS

A single control can be required or not. A required control is a requirement.

Availability: Property of being accessible and usable upon demand by an authorised entity (ISO/IEC 27000:2016).

CCM control domain: Or domain; equivalent to the term "Family" used in NIST-800 series of standards, where each family contains security controls related to the security functionality of the family (CCM mapping methodology).

CCM control: Or security control; safeguard or countermeasure requirement prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (CCM mapping methodology).

Cloud service provider (CSP): A cloud provider is a company that offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals.[1]

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes (ISO/IEC 27000:2016).

Control: Measure that is modifying risk; controls include any process, policy, device, practice, or other actions which modify risk (from (ISO/IEC 27000:2016)).

Controller [C] means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. (Article 4 (7) GDPR).

Information privacy: The relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

[1] http://searchcloudprovider.techtarget.com/definition/cloud-provider

Information security control is a control, that in general lowers the risk information (and other correlated assets) is exposed to. Security requirements in this context is a set of information security controls, needed to achieve an envisioned level of information security in cloud computing environment.

Information security: Preservation of confidentiality, integrity and availability of information (from (ISO/IEC 27000:2016)).

Integrity: Property of accuracy and completeness (ISO/IEC 27000:2016).

Internal control: A process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies (in accounting and auditing).

Interoperability: The ability of software and hardware on different machines from different vendors to share data.[2]

Portability (cloud): In cloud (cloud computing) terminology, the phrase "cloud portability" means the ability to move applications and its associated data between one cloud provider and another with minimal disruption and downtime. Often, cloud portability involves moving between private and public cloud environments.[3]

Privacy requirements is a need or expectation to achieve a level of personal data protection stated in national and international laws and regulations and codes of ethics in cloud computing environment.

Privacy, in general, is the ability (and in modern democracies the right) of an individual or group to seclude themselves, or information about themselves, and thereby express themselves selectively (Wikipedia[4]). Privacy may be divided into four categories (1) Physical: restriction on others to experience a person or situation through one or more of the human senses; (2) Informational: restriction on searching for or revealing facts that are unknown or unknowable to others; (3) Decisional: restriction on interfering in decisions that are exclusive to an entity; (4) Dispositional: restriction on attempts to know an individual's state of mind (BusinessDictionary.com[5]).

Processor [P] means a natural or legal person, public authority, agency or other body which

[2] http://www.webopedia.com/TERM/I/interoperability.html
[3] http://www.webopedia.com/TERM/C/cloud_portability.html
[4] https://en.wikipedia.org/wiki/Privacy
[5] http://www.businessdictionary.com/definition/privacy.html

processes personal data on behalf of the controller (Article 4 (8) GDPR).

Requirement is a need or expectation that is stated in a standard, law, regulation or other documented information, generally implied (i.e. it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied), or obligatory (usually stated in laws and regulations) (ISO/IEC 27000:2016).

Risk: Effect of uncertainty on objectives, where uncertainty is the state of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Security measure: Providers have security measures in place, to reach the security objectives. Security measures are sometimes called "controls" or "security controls" (ENISA MSM-DSP).

Security objective: Providers have security objectives. Objectives are high-level goals and usually do not include many technical details. For example, "we offer an uptime of 99.9%", or "customer data cannot be accessed by unauthorized personnel". Security objectives are sometimes grouped in "security domains" (e.g. "software security"). Security objectives are sometimes called "control objectives" (ENISA MSM-DSP).

Security requirement: Customers have security requirements. In the procurement phase customers usually check which security requirements are met by the security objectives of the provider. This process is often referred to as due-diligence (ENISA MSM-DSP).

Security: The state of being free from danger or threat; the extent to which a computer system is protected from data corruption, destruction, interception, loss, or unauthorized access (computing).

1 INTRODUCTION

The European Security Certification Framework (EU-SEC) project strives to address the security, privacy and transparency challenges associated with the greater externalisation of IT to Cloud services.

EU-SEC will create a certification framework under which existing certification and assurance schemes can co-exist. Furthermore, it will feature a tailored architecture and provide a set of tools to improve the efficiency and effectiveness of current assurance schemes targeting security, governance, risks management and compliance in the Cloud. It will be tested and validated in pilots involving industry partners.

This deliverable is part of work package 1 (WP1) with its main task to collect requirements for the design of efficient and effective security certification methods. Four different categories of requirements will be elicited:

1. Information security and privacy requirements
2. Auditing requirements
3. Mutual / Multi party recognition requirements
4. Continuous monitoring-based certification requirements.

This collection will result in a set of harmonized requirements for the EU-SEC framework.

1.1 OBJECTIVES AND SCOPE

This deliverable D1.2 Security and privacy requirements and controls addresses objective 1 of the work package 1 (WP1) that has been defined as:

> *Objective 1: Information security and privacy requirements:*
>
> *These are the technical security specification and control objectives that are normally coupled with the security requirements of an organization. These requirements will be collected from existing security standards such CSA CCM, ISO27001, ISO27017, ISO27018, AICPA Trust and Security Principles, ENISA Information Assurance Framework, German Federal Security Agency (BSI) C5, ANSSI cloud certification standard, Slovenian Ministry of Public Administration, CaixaBank, etc. Moreover, in the context of this WP a project advisory board will be consulted.*

Source: DoW in EU SEC project documentation, updated with amendment.

The scope of this document is composed of security and privacy requirements from existing standards, laws and regulations, collected from project community and from the project advisory board.

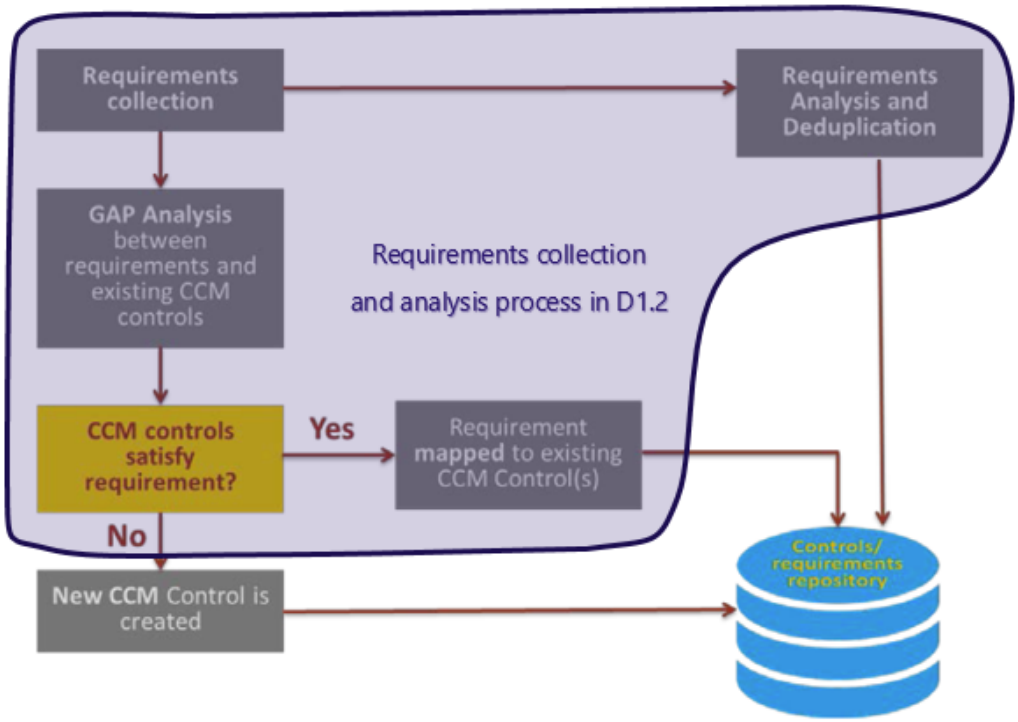

Figure 1: Requirements collection and analysis process in D1.2

The scope of the task is presented in Figure 1. This is a high-level view of the workflow implementing the requirements and controls standardisation process. The sequence starts with a definition of requirements (e.g. those initially elicited by the EU Member State or standardisation body), followed by an analysis to decide if the requirement is satisfied by an existing security control objective or if a new control must be created.

The approach followed by EU-SEC starts from the existing technologies, products and certification schemes (DoW). The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is one of the foundational pieces of the EU-SEC Framework. CSA CCM is a cloud relevant information assurance control framework that gives a detailed understanding of security concepts and principles. The foundations of the CCM rest on its customised 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 CIP. CCM is widely adopted by both cloud service providers (CSP) and cloud service consumers and is integrated in the only cloud aware

security certification scheme - STAR. The CCM continuously evolves to integrate the latest technological development, business information security control requirements and emerging risks. Those characteristics together with the established methodology for integration of new control frameworks in the CCM, defined by CSA, provides a suitable basis to use the CCM as foundation for the repository of requirements and controls in the EU-SEC project.

The repository of requirements and controls will be additionally updated with the requirements and controls defined through the EU-SEC project. This will ensure a broad applicability of the repository from different industry and government sectors i.e. public administration, CSP companies, banking specific sector etc.

1.2 WORKPACKAGE DEPENDENCIES

The EU-SEC project consists of seven work packages. The work package 1 (WP 1) provides the essential information on requirements that are important for further work. The internal dependencies are illustrated in Figure 2. While WP 1 shows dependencies to many other WPs, the actual dependencies of the work in this deliverable are limited.

The requirements coming from standards, national legal basis (relevant for public sector), European Union and international legal basis, technical and good practice documents and banking sector legislation and documents, are captured, analysed and will be used in the EU-SEC framework and the pilots.

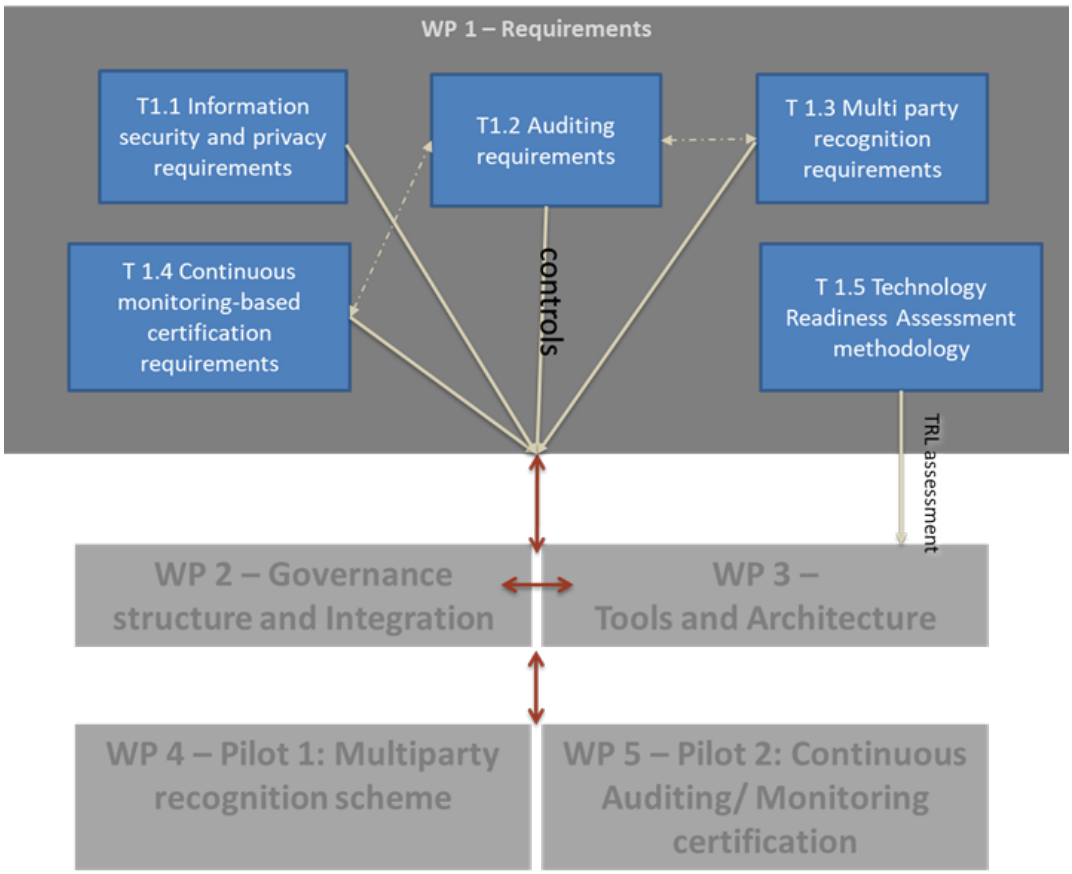

Figure 2: Work package dependencies

1.3 STRUCTURE OF THE DOCUMENT

The structure of the document is combined of five main chapters and three appendixes:

Chapter 1 provides a brief introduction of task, the objective we are trying to achieve and the scope of the task.

Chapter 2 provides explanation of the methodology used. The methodology is composed of these phases. The first phase defined the thematic domains from which we collected the requirements, and the common process of gathering and evaluation of the requirements, which in the core used the CCM mapping methodology for the evaluation of requirements. The second phase presents the consolidation of requirements and format for the requirements documentation that will be used for the EU-SEC requirements and controls repository.

Chapter 3 provides the lists of input documents from different thematic domains.

Chapter 4 provides a statistical analysis of security and privacy requirements and gap levels.

Chapter 5 provides final conclusions.

Appendix A contains a list of all input documents, with abbreviation, short name, title, year of publication, short description and accessibility of the document.

Appendix B contains an introduction to the General Data Protection Regulation (GDPR).

Appendix C contains references.

Appendix D includes the combined table of requirements and mapping to the CCM framework.

2 METHODOLOGY

2.1 METHODOLOGY OVERVIEW

As one of the first steps in the requirements collection, a common methodology for the requirements identification and evaluation was defined. The purpose was to create one EU-SEC wide set of requirements, covering as much of the relevant sources of requirements as possible and feasible. It ensured more uniform, comparable and transparent work in the selection of input documents, and in the identification, evaluation and analysis of the requirements.

The methodology included two phases (Figure 3).

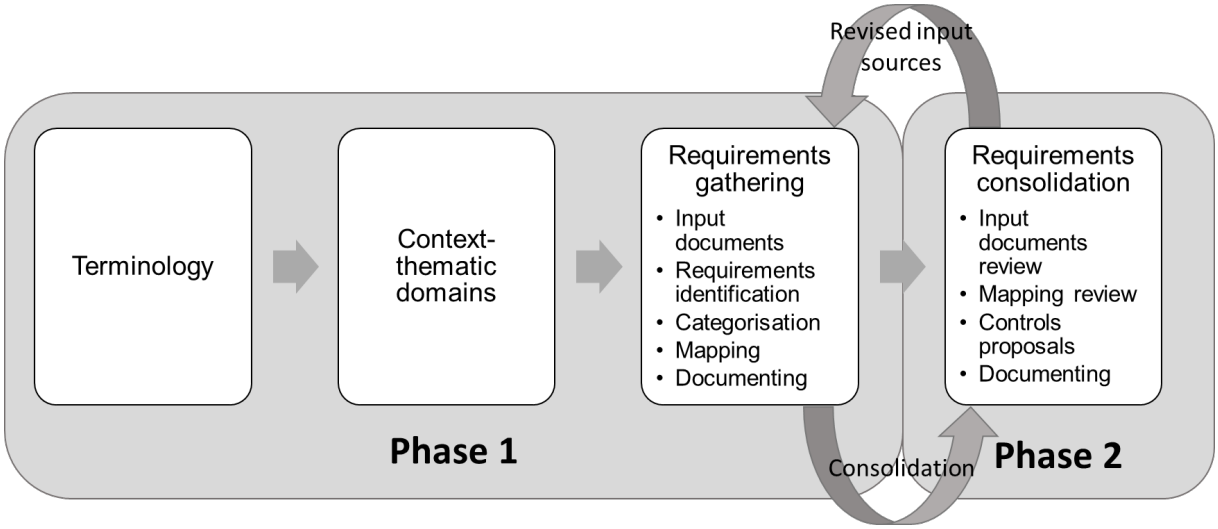

Figure 3: Methodology

The first phase included the setting of terminology (among others the meaning of requirement, control, and the relationship between them), specifying the thematic domains for the selection of input sources for requirements, and defining the requirements gathering process which included the activities of requirements identification and mapping to the controls framework.

The second phase included the requirements consolidation process that aimed to converge the identified requirements and strengthen their relevance for the EU-SEC project.

2.2 TERMINOLOGY

In the scope of this work, the requirement is a need or expectation that is stated, generally implied or obligatory (ISO 27000:2016), while the control includes an appropriate measure that modifies the risk and it can be any process, policy, device, practice, or other actions which modify risk (ISO 27000:2016).
"Generally implied" means that it is custom or common practice for the organisation and interested parties that the need or expectation under consideration is implied (ISO 27000:2016). One requirement could be covered with one control (one-to-one relationship), or several requirements could be covered with one control (many-to-one relationships).

2.3 CONTEXT - THEMATIC DOMAINS

The purpose of the requirements collection is provided in the project DoW. It focused on gathering a set of functional and non-functional requirements from diverse sources, such as:

- Applicable security control frameworks
- Security auditing approaches
- Schemes for mutual recognition of certifications
- International standards
- Practices, projects, recent technologies, as well as laws and regulations.

Based on this description, we identified a few high-level thematic domains that provided the relevant knowledge base or influenced cloud computing providers and users. The context of the high-level thematic domains was used to select the potential input documents that needed to be taken into consideration during the requirements identification and analysis.

The following thematic domains were identified for capturing requirements:

- **Standards**: The international or national standards that are adopted by the official standardisation bodies. Examples of documents that were expected in this thematic domain were: ISO standards, CEN standards, BSI standards (Germany), ANSSI standards (France).
- **National legal basis**: covers national laws, and other levels of national or sub-national legislation and legal acts (rules, recommendations) applicable to public sector. The selection of national legislation was limited to the countries of the participating partners in the EU-SEC project

- **European Union and international legal basis:** include regulations, directives, decisions or other legal acts that are relevant for defining the security and privacy requirements for cloud computing. Examples of documents that were expected in this thematic domain were: General Data Protection Regulation – GDPR (2016/679), NIS Directive (2016/1148), Electronic identification and trust services Regulation - eIDAS (910/2014).
- **Technical and good practice documents:** covers technical specifications, agreements, frameworks, good practice documents, guidelines, or tools that are developed within the wider national or international communities (e.g. international or national associations) or within individual organisations. Examples of documents that were expected in this thematic domain were: CSA specifications, ENISA guidelines and reports, AICPA Trust and Security Principles.
- **Banking sector legislation and documents:** covers the documents providing sector and business specific requirements. The banking sector was selected because it has a long history and practice of control (incidents, risk management, crisis, but also assuring trust, reliability, and privacy, etc.) where the control has already reached an elevated level of maturity because of supervisory institutions. The banking sector services rely on information technology (IT) and are spread beyond the national borders. The cloud computing is one of the areas that could help developing new customer experiences, enable effective collaboration and information technology efficiency. Examples of documents that were expected in this thematic domain were: sector or business specific legislation, sector specific specifications.

The context of the high-level thematic domains is presented in Figure 4.

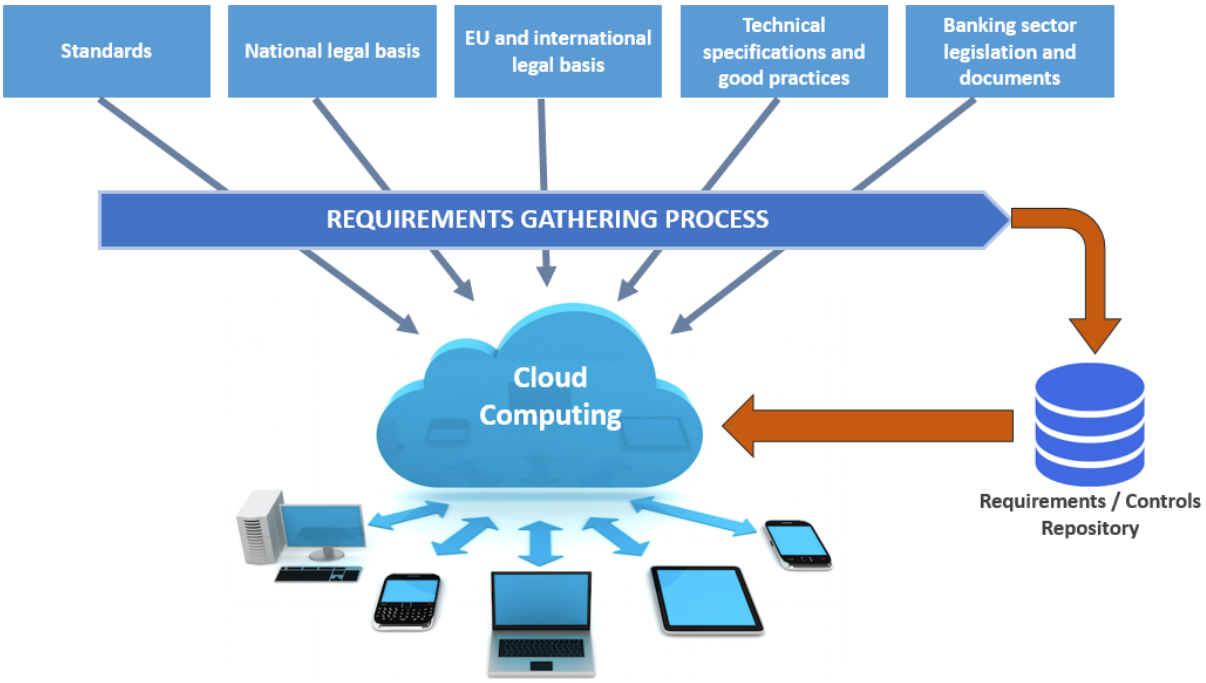

Figure 4: The context of the high-level thematic domains

2.4 REQUIREMENTS GATHERING PROCESS

The process of gathering requirements was comprised of the following main steps (Figure 5):

- Collection of potential documents
- Selection and documentation of sources
- Identifying requirements, controls and impacts in relevant documents
- Categorisation of requirements
- Comparing, mapping and documenting requirements.

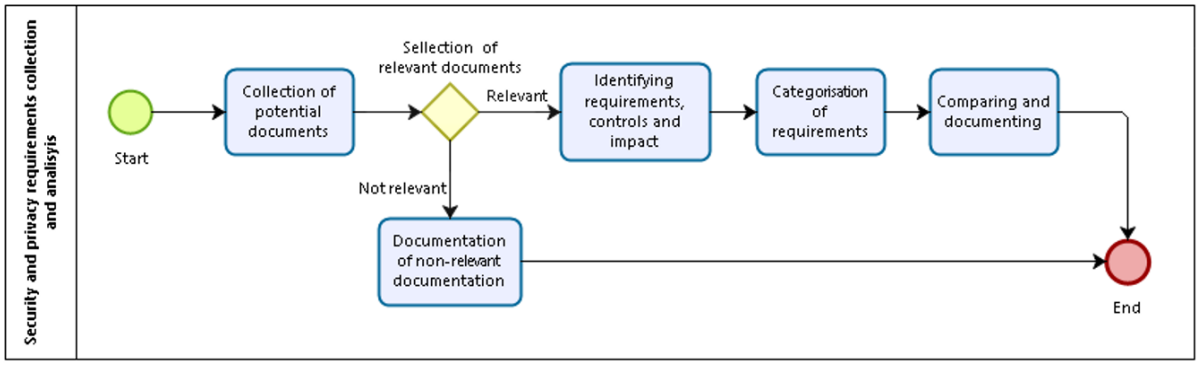

Figure 5: Collection and analysis process

2.4.1 COLLECTION OF POTENTIAL DOCUMENTS

The starting activity in the process collected all potential documents that included requirements related to information security, data privacy, cloud computing or information and communication technology. These potential documents were selected from the identified thematic domains (2.3).

2.4.2 SELECTION AND DOCUMENTATION OF SOURCES

The selection of relevant documents for the requirements identification was based on the following criteria:

- International or national standards for information security management systems, information security, cyber security or cloud computing
- Documents that included specifications or obligations related to the use and development of cloud computing or information systems, data processing, information security, privacy and personal data protection, including legislation, guidelines, technical specifications and good practice documents
- Stable documents without foreseen changes in the near future
- Latest editions of the documents
- Documents that are mostly used in practice and day-to-day activities
- Excluding documents in preparation (e.g. draft legislation).

The details of the selected input documents are described in Appendix A.

2.4.3 IDENTIFYING REQUIREMENTS, CONTROLS AND IMPACT

The selected input documents from the thematic domains were used for the identification of the requirements. The guiding criteria for the identification of the requirements was the relation or impact on the information security and privacy within the scope of cloud computing, information systems or information and communication technology in a broader meaning. Identification of requirements was done based on expert judgement and experiences.

This activity identified all relevant requirements in a range from high-level descriptions to more specific or technically oriented requirements.

2.4.4 EVALUATION: CATEGORISATION, COMPARING, MAPPING AND DOCUMENTING

These activities used two existing components:

- The CSA CCM (Version 3.0.1 from 10.06.2016) was used as a set of security and privacy controls and objectives, and
- The CSA Standards Mapping Methodology (CCM mapping methodology) was used for the mapping of the requirements to the CCM control domains and controls.

The CCM includes 16 control domains (described below) that further include 133 controls. The CCM includes the following control domains (Table 1).

Table 1: CCM control domains

CCM Control Domain	Acronym
Application & Interface Security	AIS
Audit Assurance & Compliance	AAC
Business Continuity Management & Operational Resilience	BCR
Change Control & Configuration Management	CCC
Data Security & Information Lifecycle Management	DSI
Datacentre Security	DCS
Encryption & Key Management	EKM
Governance and Risk Management	GRM
Human Resources	HRS
Identity & Access Management	IAM
Infrastructure & Virtualization Security	IVS
Interoperability & Portability	IPY
Mobile Security	MOS
Security Incident Management, E-Discovery, & Cloud Forensics	SEF
Supply Chain Management, Transparency, and Accountability	STA
Threat and Vulnerability Management.	TVM

The CCM mapping methodology is composed of four steps (Figure 6, source: CCM mapping methodology). The first three steps were used in the requirements gathering and verification process, whereas the fourth step, “New requirements integration”, will be addressed in other EU-SEC project tasks.

Figure 6: Steps toward a successful mapping methodology

The activities categorisation, comparing and mapping were used to gradually evaluate how the identified requirements are covered with the controls from the CCM following the CSA CCM mapping methodology.

2.4.4.1 CATEGORISATION

In the evaluation of the requirements, each requirement was categorised according to these criteria:

- The requirement type: if the requirement covered security, privacy, both or other elements
- The mapping of the requirement to the CCM control domains.

2.4.4.2 COMPARING AND MAPPING

Mapping to CCM controls

The comparison and mapping includes a more detailed mapping of the requirement to one or more CCM controls that are available within each CCM control domain. The mapping was done in one direction only that is from the requirement to the CCM control. This way of mapping is described in the CCM mapping methodology as a "reverse mapping". The detailed mapping guidelines are described in the CCM mapping methodology.

Gap analysis

After the mapping between the requirement and the CCM control(s), the gap analysis provided precise information about the level of gap between the requirement and the CCM control. The level of gap is identified as full or partial gap.
The situation, where the mapping between the requirement and the CCM control shows no material divergence, meaning that the CCM control covers the requirement in an adequate way, is known as "No gap". The CCM mapping methodology allows more fine tuning of this mapping using special notation symbols "-", "+" and "0".

The CCM mapping methodology defines the gap levels as following:

- **Full gap:** A full gap exists where a control of standard A has no mappings to any control of standard B (CCM mapping methodology).
  Note: In the scope of this deliverable, the standard A refers to the collected requirements and standard B refers to CCM.
- **Partial gap:** A control of standard B exists that can be mapped to that of standard A, but does NOT fully cover the requirements of the corresponding control provided within standard A (same holds in reverse mapping). To address these gaps, a set of new controls will need to be created or existing modified and added in the form of an annex or referenced via a link to a similar control already in place within standard B (CCM mapping methodology).
  Note: In the scope of this deliverable, the standard A refers to the collected requirements and standard B refers to the CCM.
- **No gap:** An equivalent control or set of controls from standard B (within the same or different security domains) are validated of fully covering the requirements of the corresponding control of standard A (CCM mapping methodology).
  Note: In the scope of this deliverable, the standard A refers to the collected requirements and standard B refers to the CCM.

2.4.4.3 DOCUMENTATION

The process was completed with a concise description of matching patterns or explanation of differences in the case of gaps.

Thus, a comprehensive table of requirements and their mapping to the CCM controls was created. This table includes all identified requirements and detailed information about the mapping to CCM. It ensures the transparency and repeatability of the process, the traceability of mapping and easier use in other project activities.

2.4.4.4 SPECIFIC CASES IN MAPPING TO CCM

The detailed mapping of the requirement to the CCM control(s) was done in two steps. The CCM control domains, that combine the CCM controls into semantic areas, were used as a starting point in mapping before considering more detailed CCM controls.

During the mapping between the requirements and the CCM control domains and controls, using the common CCM mapping methodology, we encountered diverse mapping relationships, from one-to-one to one-to-many shown in Figure 7 and Table 2.

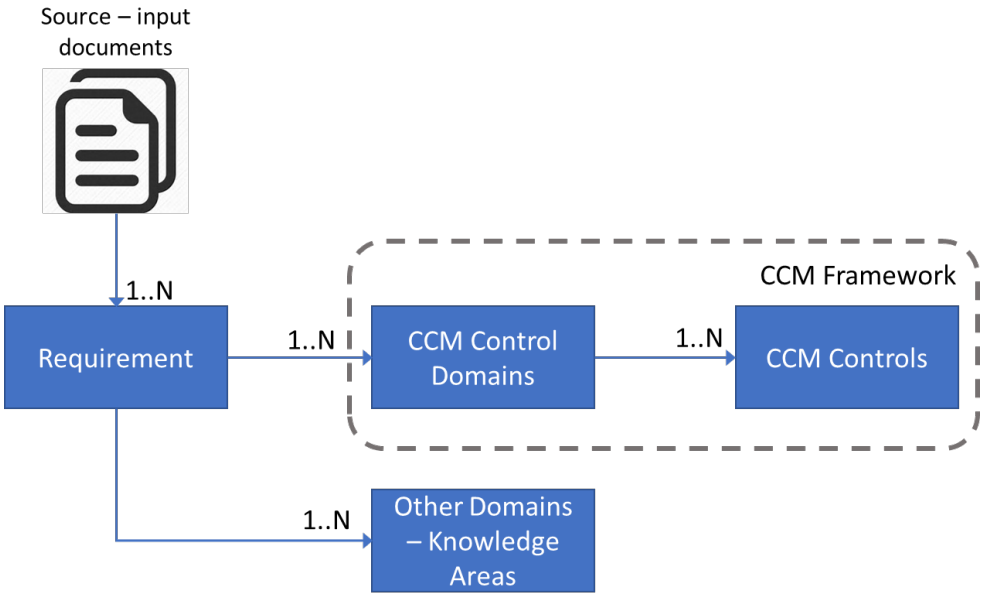

Figure 7: Requirement – domain – control relationship

Table 2: Mapping patterns

Requirement	CCM Control Domain	CCM Control	Other Domains	Description
1	1	1		One-to-one mapping
1	1	N		Requirement is mapped to one CCM control domain and within that to several controls
1	M	N		Requirement is mapped to several CCM control domains, and in every domain to several controls
1			1...N	Requirement is mapped to one or more new domains or knowledge areas outside of the CCM framework

The complete mapping to CCM covered the following situations:

One-to-one mapping (one CCM control domain)

This mapping pattern applied when only one CCM control, was selected or when several CCM controls from the same CCM control domain were selected. In such cases, the correlated CCM control domain was assigned.

Table 3: Example: one-to-one mapping to CCM

Source Document	Requirement Description	CCM Control Domain	CCM Controls
CBK-02	Requirement 10: Track and monitor all access to network resources and card-holder data / Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.	Infrastructure & Virtualization Security	IVS-01
SI-07	Production: There shall be the documented procedures for any change in the information system in a production environment allowing return to the state before the change.	Change Control & Configuration Management	CCC-03, CCC-05

Multiple mapping to several CCM control domains and controls

The multiple mapping presented the cases where the requirements were mapped to several CCM controls which were related to diverse CCM control domains (one-to-many mapping). This situation was solved in two ways:

- **Multiple mapping where one major CCM control domain was selected:** When several CCM control domains could be selected and one of them could be identified as a major, first or a representative domain, then that specific control domain was selected from the list of the CCM control domains. The list of all identified CCM controls was also provided.
- **Multiple mapping without a selection of the CCM control domain**: a temporarily solution was to use additional newly defined category "To be decided (Mapping exists)"

that indicated that diverse CCM controls were assigned. The list of all identified CCM controls was also provided.

Table 4: Example: multiple mapping to several CCM control domains and controls

Source Document	Requirement Description	CCM Control Domain	CCM Controls
ES-01	Security controls should be periodically analysed for its effectiveness.	Governance and Risk Management	GRM-01, GRM-09, GRM-08, STA-08
TSC_2016	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	To be decided (Mapping exists)	DSI-06, GRM-06, HRS-03, HRS-09, SEF-03, STA-03, STA-05, STA-09

No mapping to CCM

When the requirement couldn't be mapped to the CCM control domains and controls, a temporarily solution was to define a new category "To be decided (No mapping)". In some cases, the additional information about the new thematic areas or domains to which the requirement was related was provided.

Table 5: Example: no mapping to CCM

Source Document	Requirement Description	CCM Control Domain	CCM Controls
ISO27017	6 Organisation of information security / 6.1 Internal organization / 6.1.5 Information security in project management	To be decided (No mapping)	

Gap level in one-to-many mapping

The same approach was used in the identification of the gap level in the case of one-to-many mapping. The new temporarily category "To be decided" was used in addition to the CCM mapping methodology which defines three gap levels: no gap, partial gap and full gap.

2.5 REQUIREMENTS CONSOLIDATION PROCESS

The requirements gathering process in the first phase included the initial evaluation and mapping of the requirements to the CCM. The result of this phase demonstrated 509 requirements. By using the statistical analysis, we evaluated which CCM controls were most frequently used

in the mapping. The outcome of this process led to some uncertainties like similar requirements, or not confirmed mappings. The vast amount of information collected in Phase 1 presented also practical implementation difficulties in the EU-SEC project which aims to test and use the requirements in pilot projects using adapted tools. Therefore, the next phase (Phase 2) provided a requirements consolidation process that aimed to converge the requirements and to review their mapping to the CCM controls (Figure 8).

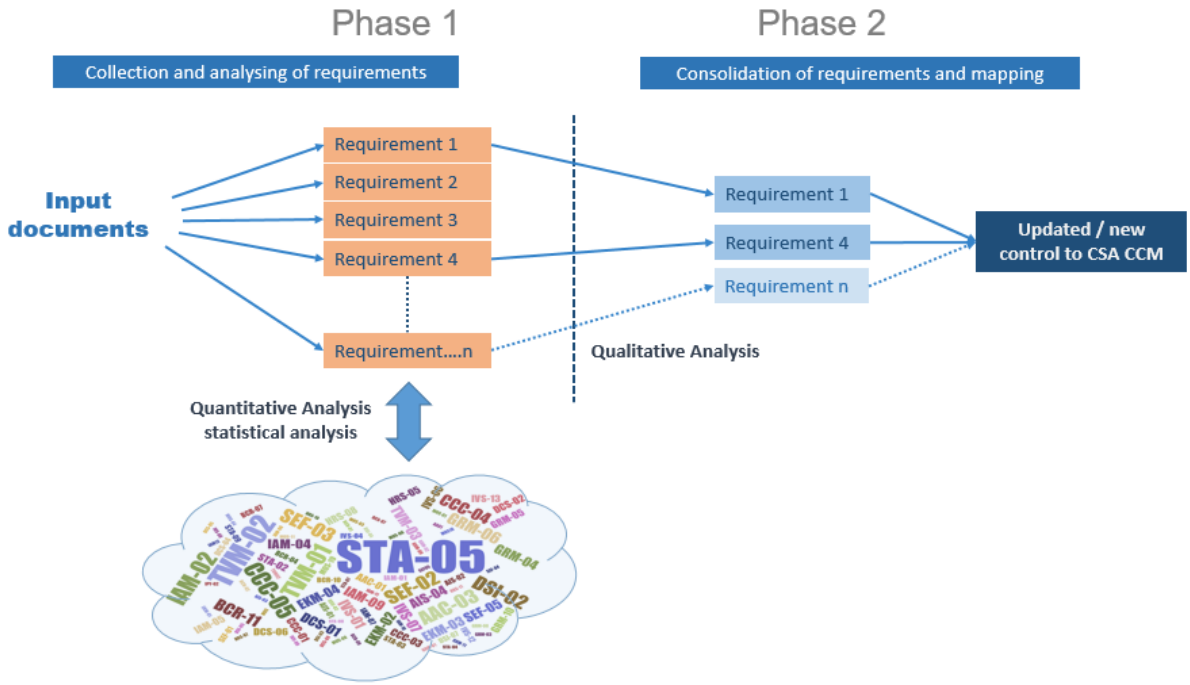

Figure 8: Phases of requirements collection and mapping to controls

The consolidation process involved the experts who participated in the initial mapping, the CCM experts, and other information security and cloud computing experts who met at the dedicated workshop to analyse the requirements collected in Phase 1.

The consolidation process was composed of the following activities:

- Reviewing the input documents
- Reviewing the requirements from the point of view of their relevance for the cloud service providers
- Reviewing the requirements mapping to the CCM (gap level, selection of CCM controls) by using the CCM mapping methodology
- Documenting the proposed modifications to the existing CCM controls or new controls.

Confirmation of input documents

The consolidation process was used to confirm the input documents, exclude non-relevant documents and propose additional documents. The excluded input documents were the obsolete documents, those documents that were in the updating process, and those that were addressing the classified information topics, that are primarily a responsibility of Cloud Service Consumers. The information security and cloud computing that would include classified information were out of scope of the EU-SEC project.

The selection of national legislation was focused on public sector where the partners in the EU-SEC project provided the necessary information. We identified and used the relevant legislation from Germany, Slovenia and Spain, while the legislation from the Republic of Slovakia hasn't been included due to currently under-going work.

The GDPR was recognised as one of the most important pieces of legislation for privacy and data protection. This legal act has been considered in another task in the EU-SEC project (D2.3 Privacy Code of Conduct), led by CSA. In this current version of deliverable D1.2 (Ver. 1.4) we included outcome from D2.3 Privacy code of conduct and integrate privacy controls in EU SEC repository.

Relevance to cloud service providers

This perspective was another criterion for the selection of requirements for the scope of the EU-SEC project. The requirements that were related to the internal organisation, development of the information systems or obligations of the cloud service customers (users) were excluded.

Requirements review and documentation

Requirements that were mapped to the CCM without gaps were recognised as a stable basis. Still, those requirements might include different hierarchical levels or granularity (general vs. specific) and could imply specific restrictions to the implementation of the controls.

The focus of the consolidation process was on the requirements where a partial or full gap was identified in the mapping to the CCM in Phase 1. Those requirements could be a potential source for the modification of the existing CCM controls or new controls for the EU-SEC requirements and controls repository.

Outcome

The outcome of the consolidation process provided:

- The revised list of input documents for the requirements collection
- The revised set of requirements and their mapping to the CCM, indicating full coverage of controls (no gap), or gaps where the existing CCM controls could be updated (partial gap) or the new controls will have to be designed to cover the requirements (full gap).

3 INPUT DOCUMENTS ANALYSIS

3.1 LIST OF INPUT DOCUMENTS

Initially in Phase 1, we identified 34 input documents (out of 75 potential documents) that were used for the selection of the requirements and the initial mapping to the CCM. That list of input documents was revised in Phase 2 to confirm 23 input documents.

The list of input documents used for the requirements selection and analysis is provided in the next table, and additional information in Appendix A.

Table 6: List of input documents

Id	Abbreviation	Title	Year	Status	Thematic area
BDSG	BDSG	BDSG German Federal Data Protection Act	2014	Sub-national law	National legal basis
ES-01	BOE-A-2010-1330	Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of Electronic Administration.	2010	National law	National legal basis
ES-02	BOE-A-2011-7630	Law 8/2011, of 28 April, which establishes measures for the protection of critical infrastructures.	2011	National law	National legal basis
ES-03	Law 56/2007	Law 56/2007, of 28 December, Measures to boost the information society	2007	National law	National legal basis
ES-04	Law 59/2003	Law 59/2003, of 19 December, of Electronic Signature	2003	National law	National legal basis
FAIT5	IDW RS FAIT 5	IDW Statement on Accounting: Principles of accounting in case of outsourcing of the accounting-relevant processes and functions, including cloud computing	2015	Regulation	National legal basis
SI-07	IVPJU	Recommendations of the information security policy of public administration	2010	Recommendation	National legal basis
SI-09	GTZ	Generic Technological Requirements for Information Systems Development, V2.2.3, 2017	2017	Rules	National legal basis
SI-10	JNIT	Guidelines for the procurement of IT solutions, 2017	2017	Guidelines	National legal basis

Id	Abbreviation	Title	Year	Status	Thematic area
CBK-01	ENISA CCFS	Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations (ENISA)	2015	EU / Guidelines	Sector - banking
CBK-02	PCI DSS	Payment Card Industry Data Security Standard - Requirements and Security Assessment Procedures (version 3.2)	2016	Standard	Sector - banking
CBK-03	EBA/GL/2017/05	Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)	2017	EU / Guidelines	Sector - banking
CBK-04	EBA/GL/2014/12-Rev1	Final Guidelines on the security of internet payments	2014	EU / Guidelines	Sector - banking
CBK-05	EBA/CP/2017/06	Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010	2017	EU / Guidelines	Sector - banking
CBK-06	PCI PIN	Payment Card Industry PIN Security Requirements (version 2.0)	2014	Rules	Sector - banking
CBK-07	PCI HSM	Payment Card Industry Hardware Security Module - Security Requirements (version 1.0)	2009	Rules	Sector - banking
ENISA_MSM_DSP	ENISA_MSM_DSP	Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, December 2016	2016	Guidelines	Technical and good practice documents
TSC_2016	TSC	AICPA Trust Services Principles and Criteria	2016	Guidelines	Technical and good practice documents
C5-2016	C5-2016	BSI Cloud Computing Compliance Control Catalogue and Referencing Cloud Computing Compliance Controls Catalogue (C5) to International Standards (Refers to version 1.0 of C5), Version 1.0, 2016	2015	Standard	Standards
ISO27001	ISO27001	Information technology - Security techniques - Information security management systems - Requirements	2013	Standard	Standards

Id	Abbreviation	Title	Year	Status	Thematic area
ISO27017	ISO27017	Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services	2015	Standard	Standards
ISO27018	ISO27018	Information technology - Security techniques - Code of practice for PII protection in public clouds acting as PII processors	2014	Standard	Standards
SecNumCloud	SecNumCloud	Cloud Service Providers (SecNumCloud) Requirements - Essential Level, Version 3.0, 08.12.2016	2016	Standard	Standards
PLA CoC	PLA CoC	Privacy Level Agreement, Code of Practice Template Annex 1 - CSA Code of Conduct	2018	Guidelines	Technical and good practice documents

3.2 STANDARDS

The CSA CCM has already been aligned with several industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI DSS, NIST, AICPA TSC and others.

The identification of the relevant standards as input documents was therefore on those standards that have not been mapped to the CCM framework yet. The selected standards provide information security controls, information security management systems, certification, applicability to cloud computing and are relevant for the cloud service providers and customers.

Cloud Computing Compliance Control Catalogue (C5)

C5 is a standard published by German Federal Office for Information Security (BSI) and standardised the requirements on information security from existing and well-known international and national standards and regulations. C5 aims to provide customer a better cloud overview for a higher level of security and avoiding redundant audits and unnecessary efforts. The C5 catalogue is divided into 17 thematic sections (e.g. organisation of information security, physical security). Here, the BSI makes use of recognised security standards such as 27001, the Cloud Controls Matrix of the Cloud Security Alliance as well as BSI publications and uses these requirements wherever appropriate.

ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organisation. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organisations, regardless of type, size or nature.

ISO/IEC 27017: Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services.

ISO/IEC 27018: Information technology - Security techniques - Code of practice for PII protection in public clouds acting as PII processors

ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

SecNumCloud

National Cybersecurity Agency of France (ANSSI) published a set of requirements for secure cloud computing and cloud service providers in the first version of the repository, then called Secure Cloud, in September 2014. The repository defined a set of security rules that are imposed on administrative authorities in the security of their information systems. It also proposed good practices in the security of information systems that the administrative authorities were free to apply. After 2014, ANSSI carried out an experimental phase and tested in real conditions the relevance of the requirements of the Secure Cloud defined in 2014. The reference system has been updated to take into account the feedback from the experimental phase and involved market players. The requirements framework evolved towards two documents: SecNumCloud - Requirements Repository - Essential level - v.3 that was published in 2016, and the Advanced Requirements (formerly Secure Cloud Plus) that will be published later.

3.3 NATIONAL LEGAL BASIS

3.3.1 SLOVENIA

3.3.1.1 SLOVENIAN GOVERNMENTAL CLOUD – SGC (DRO)

Slovenian Government Cloud (SGC) or National Computer Cloud (sl. Državni računalniški oblak - DRO) is a dedicated computing infrastructure owned and operated by the country allowing state institutions (direct budget users) to use the concept of cloud computing quickly and cheaply. It offers computing, storage, development, business and other capabilities in the form of services. This infrastructure is owned and run by the state. Services have access to sensitive information, personal data and other information that the state would like to keep inside a secure computing environment and/or within the national borders. Currently, traditional IT solutions are being migrated to the cloud infrastructure. The goal is not only to migrate the existing e-applications, but to transform them into proper cloud-ready applications i.e. cloud services (SaaS) as well. New application development methodology is aligned with cloud computing concepts and supported by tools, standards, software patterns and trainings. Services are delivered in all flavours as: IaaS, PaaS, SaaS and also specific derivatives such as DBaaS, DevOPSaaS, SECaaS and similar.

With the introduction of cloud infrastructure, we will establish a standardized platform, ensuring innovative environment, increase the efficiency of public administration by saving time and reducing costs, provide elasticity service, integrated information security and lower IT maintenance costs due to the use of technologies of cloud computing. Also, we intend to achieve the introduction of open standards, providing connectivity services, ensuring the availability of services from anywhere and anytime, simpler services for citizens and businesses and the creation of new digital jobs.

3.3.1.2 IDENTIFICATION OF INPUT DOCUMENTS

Information security and protection of personal data are included in many legal and strategic documents.

Constitution of the Republic of Slovenia

The Constitution of the Republic of Slovenia (Constitution RS) as the highest national legal act

already includes the protection of the right to privacy and personality (Article 35) and protection of personal data (Article 38). The Constitution also provides in Article 38:

- The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.
- Collection, processing, designated use, supervision and protection of the confidentiality of personal data shall be provided by law.
- Everyone has the right of access to the collected personal data that relates to him and the right to judicial protection in the event of any abuse of such data.

Laws, implementing regulations and guidelines

Protection of personal data, creation of databases of personal data, other registers and the elements of information security are set out in detail in individual laws, implementing regulations and guidelines governing the sectoral areas, business interaction or interaction between individuals and the public administration.

Strategic documents

The most recent strategic development documents of the Government RS in various fields provide guidance for the development of information technology and information security, for example:

- Cyber security in the Digital Slovenia 2020 – Development strategy for the information society until 2020, http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/DSI_2020_3-2016_pic1.pdf
- Efficient IT, increased use of e-services and interoperability of IT solutions in the Development Strategy for Public Administration 2015 – 2020), http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/JAVNA_UPRAVA/Kakovost/Strategija_razvoja_SLO_final_web.pdf
- The strategic objectives of ensuring cyber security and measures to achieve them in the Cyber Security Strategy, 2016, http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/Cyber_Security_Strategy_Slovenia.pdf .

Reorganisation of information technology and solutions in public administration

Among the active strategic development projects of the Slovene public administration, is the project Reorganization of IT in Public administration (http://www.vlada.si/teme_in_projekti/projektna_pisarna/p4_reorganizacija_informatike_v_drzavni_upravi/). The main role of the project is to set up and ensure the functioning of a variety of new organisational, financial,

personnel and information technology solutions (cost optimisation, establishment of a unified system of the IT security, human resources consolidation, migration of information systems, etc.) and processes at all levels of information and communication technologies, among which was a very important project for the establishment of the Slovenian Government Cloud in 2015. The Slovenian Government Cloud sets up a computing infrastructure for direct budget users, which provides them with storage, development, business and other capabilities in the form of (cloud computing) services. Two more cloud computing platforms will be in place in the coming years: the hybrid cloud, offering solutions to the public sector, and Development and Innovation Cloud as a cloud development platform for educational institutions and start-up companies.

A selection of documents for analysis of the requirements of information security and privacy

Due to the great heterogeneity of the areas and the types of documents that partly govern information security and privacy, the selection of potential documents for the analysis of requirements in the context of the EU-SEC project was focused on the most relevant national laws and their implementing regulations and guidelines affecting the establishment and functioning of the Slovenian Government Cloud, information systems in public administration or use of information and communication technologies, particularly in terms of information security and privacy. It should be noted that cloud computing is not directly mentioned in the legislation. On the other hand, especially older legislation includes elements that lag the applicability of modern information and communication technology. Among the 16 potential documents, we analysed eight documents. The final selection did not include the draft legislation under development and those legal acts that will soon be changed to align with the acquis of the European Union, for example, the Law on Personal Data Protection will be harmonised with the European regulation GDPR. The regulation GDPR has been also included in the scope of the EU-SEC project.

The following input documents were selected:

- SI-07: Recommendations of the information security policy of public administration (IVPJU)
- SI-09: Generic Technological Requirements for Information Systems Development (GTZ), V2.2.3, 2017
- SI-10: Guidelines for the procurement of IT solutions, 2017 (JNIT).

3.3.2 SPAIN

Identification of input documents was focused on the national laws, implementing rules and guidelines that have an influence on SGC or information and communication technology (ICT) from the security and privacy point of view.

Royal Decree 3/2010 (ES-01) regulates the use of electronic means, through measures which ensure the security of systems, data, communications, and electronic services used by public Administrations to execute its duties.

Law 8/2011 regulates the protection of critical infrastructures in Spain against deliberate attacks of all kinds.

National law protecting information of personal character (Organic Law 15/1999) and its implementing rules (Royal Decree 1720/2007) were not considered, because the current legislation will be substituted by GDPR during the execution of EU-SEC project.

Other national laws focused on security and privacy in Spain were not considered, due to its partial application or because they were too generic (Spanish Constitution, Law 5/2014 Private Security).

The list of selected input documents included:

- ES-01: Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of Electronic Administration (BOE-A-2010-1330)
- ES-02: Law 8/2011, of 28 April, which establishes measures for the protection of critical infrastructures (BOE-A-2011-7630)
- ES-03: Law 56/2007, of 28 December, Measures to boost the information society
- ES-04: Law 59/2003, of 19 December, of Electronic Signature.

3.3.3 GERMANY

The list of input documents contained the sub national law and the regulation. The BDSG German Federal Data Protection Act serves the purpose to protect the individual against his/her right to privacy being impaired through the handling of his/her personal data. This Act has to be applied to collecting, processing and the usage of private data.

IDW RS FAIT 5 was published by the "Institut der Wirtschaftsprüfer" (Financial Auditor Institute) to determine the outsourcing processes of IT services with regard to the German Commercial Code.

3.4 TECHNICAL SPECIFICATIONS AND GOOD PRACTICES

AICPA Trust Services Principles and Criteria

The AICPA Assurance Services Executive Committee (ASEC) has developed a set of principles and criteria (trust services principles (TSP) and criteria). The TSP built the categories for the more detailed Trust Services Criteria (TSC), which are the specific requirements against which the auditee's controls are mapped.

TSP/TSC presents the trust services principles and criteria for assessing the effectiveness of an entity's controls over a system relevant to the security, availability, processing integrity, confidentiality, or privacy. Management of an entity may use the trust services principles and criteria to evaluate its controls over a system or may engage a certified public accountant (CPA) to report on or provide consulting services related to those controls.

The analysis of the trust services principles and criteria (TSP/TSC) is based on the reversed mapping from TSC to CCM. The mapping, already existing in CCM, used the old version of TSC from 2014. Since AICPA has updated its requirements in 2016, the analysis of TSC requirements in this deliverable is based on the old mapping in the CCM, but extended and re-performed to map TSC 2016 requirements to CCM. Compared to the old mapping in the CCM, 36 TSC requirements have new mapping results.

ENISA – Minimum Security Measures for DSPs

The European Union agency for Network and Information Security (ENISA) has written many papers on cloud computing security, among them:

- The 2009 cloud security risk assessment[6] is widely referred to, across EU member states, and outside the EU.
- Following up on this risk assessment, ENISA published an assurance framework for governing the information security risks when going cloud[7]. This assurance framework is being used as the basis for some industry initiatives on cloud assurance.
- In 2011 ENISA published a report on security and resilience in government clouds[8].

[6] https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
[7] https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework/
[8] https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds/

- In 2017 ENISA published Technical guidelines for the implementation of minimum-security measures for DSPs (ENISA MSM-DSP)[9].

Initially in this work, the project partners started to analyse the ENISA report Cloud Computing Risk Assessment (1st bullet point in the list above) which provides an in-depth and independent analysis that outlines some of the information security benefits, key security risks of cloud computing and practical recommendations.

Based on the recommendation from the ENISA member of the EU-SEC project Advisory Board we changed that approach and selected the latest report on the implementation of minimum-security measures for DSPs (last bullet point in the list above) as the input document for requirements collection and analysis.

ENISA has issued this report to assist Member States and DSPs in providing a common approach regarding the security measures for DSPs. It has brought light to some important findings that can add to existing security objectives and measures in information technology infrastructures in Europe.

The report is based on the Cloud Certification Schemes Meta framework (CCSM) released in November 2014 by ENISA, regarding cloud service providers. In addition, ENISA enriched the study with the additional security objectives concerning cloud services that may have come into play since 2014, and the latest information about the security controls and measures implemented, along with good practices and standards deployed by DSP and in particular online market places and online search engines. This report also provides a mapping between security objectives and the following industry standards, certification schemes and national frameworks:

- ISO/IEC 27001:2013
- CSA CCM : Cloud Controls Matrix v3.0.1
- BSI C5: Cloud Computing Compliance Controls Catalogue (C5), criteria to assess the information security of cloud services, version 1.0 – as of February 2016
- COBIT5: Framework for the governance and management of enterprise IT
- CCS CSC: The CIS Critical Security Controls for Effective Cyber Defence, Version 6.1, August 31, 2016
- OCF: CSA STAR PROGRAM & OPEN CERTIFICATION FRAMEWORK IN 2016 AND BEYOND

[9] https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

- NIST: Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, February 12, 2014
- PCI DSS: Payment Card Industry (PCI) Security Standards Council, Data Security Standard Requirements and Security Assessment Procedures, Version 3.2, April 2016
- CES: Cyber Essentials Scheme, Requirements for basic technical protection from cyber-attacks, June 2014.

The selected report Technical Guidelines for the implementation of minimum-security measures for Digital Service Providers (ENISA MSM-DSP) defines 27 security objectives (SO). For each security objective is provided:

- Brief description of the security objective
- Levels of sophistication on the implementation of security measures with examples
- A mapping with industry standards, certification schemes and national frameworks.

The report defines three levels of sophistication of the security measure:

- Level 1 - Basic: Basic security measures that could be implemented to reach the security objective.
- Level 2 – Industry standard: Industry standard security measures to reach the objective and an ad-hoc review of the implementation, following changes or incidents.
- Level 3 - State of the art: State of the art (advanced) security measures, and continuous monitoring of implementation, structural review of implementation, taking into account changes, incidents, tests and exercises, to proactively improve the implementation of security measures.

The sophistication levels are applied independently to each objective. As a result, a DSP may receive different sophistication ratings for different objectives. It is important to realise that the sophistication levels that are applicable to a given organisation depend on its specific characteristics such as its size or the services provided.

The report also includes the mapping of the security objectives and the correlated measures to the CCM framework. The result of that mapping is included in this document.

The Cloud Security Alliance (CSA) Code of Conduct (CoC) for GDPR Compliance

The GDPR was recognised as one of the most important pieces of legislation for privacy and data protection. This legal act has been considered in another task in the EU-SEC project (D2.3

Privacy Code of Conduct). The CSA Code of Conduct (CoC) for GDPR Compliance aims to provide Cloud Service Providers (CSPs) and cloud consumers a solution for GDPR compliance and to provide transparency guidelines regarding the level of data protection offered by the CSP.

The CSA CoC for GDPR Compliance is essentially intended to provide:

- Cloud customers of any size with a tool to evaluate the level of personal data protection offered by different CSPs (and thus to support informed decisions)
- CSPs of any size and geographic location with a guidance to comply with European Union (EU) personal data protection legislation and to disclose, in a structured way, the level of personal data protection they offer to customers.

The CSA CoC for GDPR compliance is based on two major components, the Privacy Level Agreement Code of Practise (PLA CoP), which is a technical standard that specifies the requirements included in the GDPR, as well as the certification scheme and adherence mechanisms associated with it. The CSA CoC for GDPR Compliance (also referred to as the "CSA Code of Conduct", the "CoC" or "the Code" in this document) is structured in three parts:

- Part 1 describes scope, objectives, scope, methodology and assumptions; and provides explanatory notes.
- Part 2 describes the PLA Code of Practise [V3] and its substantial provisions, developed by the CSA PLA Working Group.
- Part 3 outlines the governance structure and the mechanisms of adherence to the CSA Code of Conduct.

In this deliverable we collected all the privacy requirements from PLA Code of Practise [V3] and include them in EU SEC Repository. With this work we contributed to a more comprehensive overview on privacy requirements for CSP's.

3.5 BANKING SECTOR LEGISLATION AND DOCUMENTS

The identification of input documents was focused on the main rules published by the EBA (European Banking Authority), as well as some guidelines and market standards, which are mandatory when treating with some information related to means of payments. Specific guidelines for secure use of Cloud in financial institutions issued by ENISA (European Union Agency for Network and Information Security) was also included.

The list of selected documents included:

- CBK-01: Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations (ENISA) (ENISA CCFS)
- CBK-02: Payment Card Industry Data Security Standard - Requirements and Security Assessment Procedures (version 3.2) (PCI DSS)
- CBK-03: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05)
- CBK-04: Final Guidelines on the security of internet payments (EBA/GL/2014/12-Rev1)
- CBK-05: Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010 (EBA/CP/2017/06)
- CBK-06: Payment Card Industry PIN Security Requirements (version 2.0) (PCI PIN)
- CBK-07: Payment Card Industry Hardware Security Module - Security Requirements (version 1.0) (PCI HSM).

4 ANALYSIS OF REQUIREMENTS

4.1 PRACTICAL IMPLEMENTATION

Collecting and analysing the security and privacy requirements from the thematic domains defined in Chapter (2.3) was carried out based on the prepared methodology and proposed assignment of work. The common process, templates and formats were prepared to collect and analyse the information and to align and streamline the activities of the participants. By using prepared methodology, we expected the obtained results could reflect greater consistency.

Activities performed in the scope of this deliverable are shown in Figure 9.

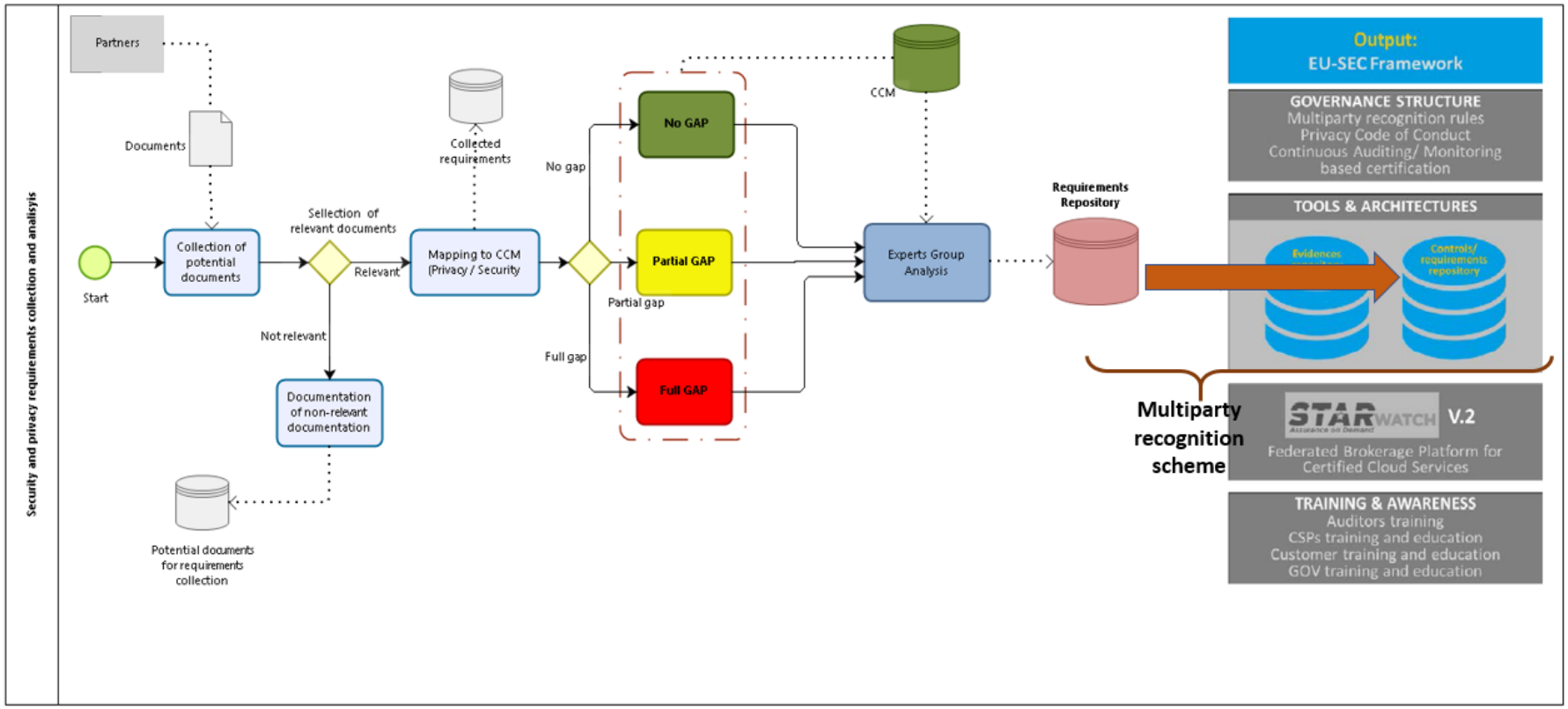

Figure 9: Requirements collection and analysis process in D1.2

The practical implementation uncovered many issues that we encountered when performing security and privacy collection and mapping. These issues mainly reflected in the delay in performing the task, problems with use of common terminology, different understanding of mapping process, substantial number of input documents etc. This increased the risk of delay in performing the task. While mapping the requirements to the CCM, we found out that a single requirement could be mapped to several controls which increased the number of relationships between the requirements and the CCM controls and the complexity of information for analysis.

The outcome provided 804 requirements which were evaluated how they could be covered with the CCM controls. Figure 10 shows the distribution of the requirements mapping to the CCM. The analysis of the mapping showed:

- Most of the requirements (649 or 80,7%) were collected from the identified standards. This situation is mostly related to the fact that those standards address information security and security in cloud computing and cloud services in a comprehensive way considering all aspects of information security, therefore defining many requirements or controls.
- Overall, 71% of the requirements were mapped to CCM controls without gaps (No gap). Still, some minor differences might occur in mapping where the security objectives of the requirements were slightly different and included more or less specific elements then the CCM controls.
- For 16% of requirements that were mapped to the CCM controls, some gaps were identified (Partial gap).
  For 13% of requirements, it wasn't possible to identify the mapping to the CCM controls (Full gap).
- The same CCM control could cover several requirements from diverse input sources. Such example was the CCM control IAM-02 which is related to the user access policies and procedures for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. The control IAM-02 was related as "No gap" to 50 different requirements coming from 9 diverse input sources.

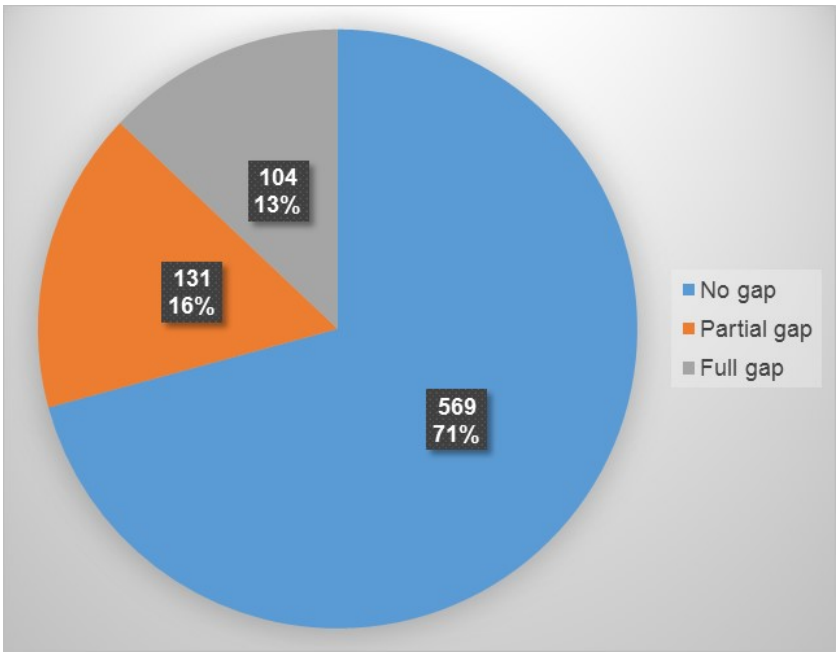

Figure 10: Requirements mapping to CCM gap level

4.2 REQUIREMENTS MAPPING AND GAP ANALYSIS

4.2.1 MAPPING TO THE CCM – NO GAP

Most of the requirements were mapped to the CCM without a gap. We were interested which domains and controls in the CCM were mostly addressed in the analysed documents. It turned out that those top five domains were (Figure 11):

- Governance and Risk Management (GRM)
- Identity & Access Management (IAM)
- Infrastructure & Virtualization Security (IVS)
- Business Continuity Management & Operational Resilience (BCR)
- Change Control & Configuration Management (CCC).

This suggested, the requirements that were mapped into these domains were well-known and had long been used in practice.

The less addressed domain was Interoperability & Portability (IPY). We estimated that the reason for a low number of requirements related to interoperability and portability is that the need to avoid lock-in situations has become more important only recently and hadn't been considered in the analysed documents yet. Those requirements are especially important for

cloud service customers to ensure the continuation and stability of their business operations and compliance (e.g. interoperable digital public services) in the changing world of technology and risks emerging from those cloud computing technologies. On the other hand, the cloud service providers are considering the ways to respond to those requirements to offer appropriate services also as a business advantage to attract new potential customers. This is relevant for the cloud service customers and providers.

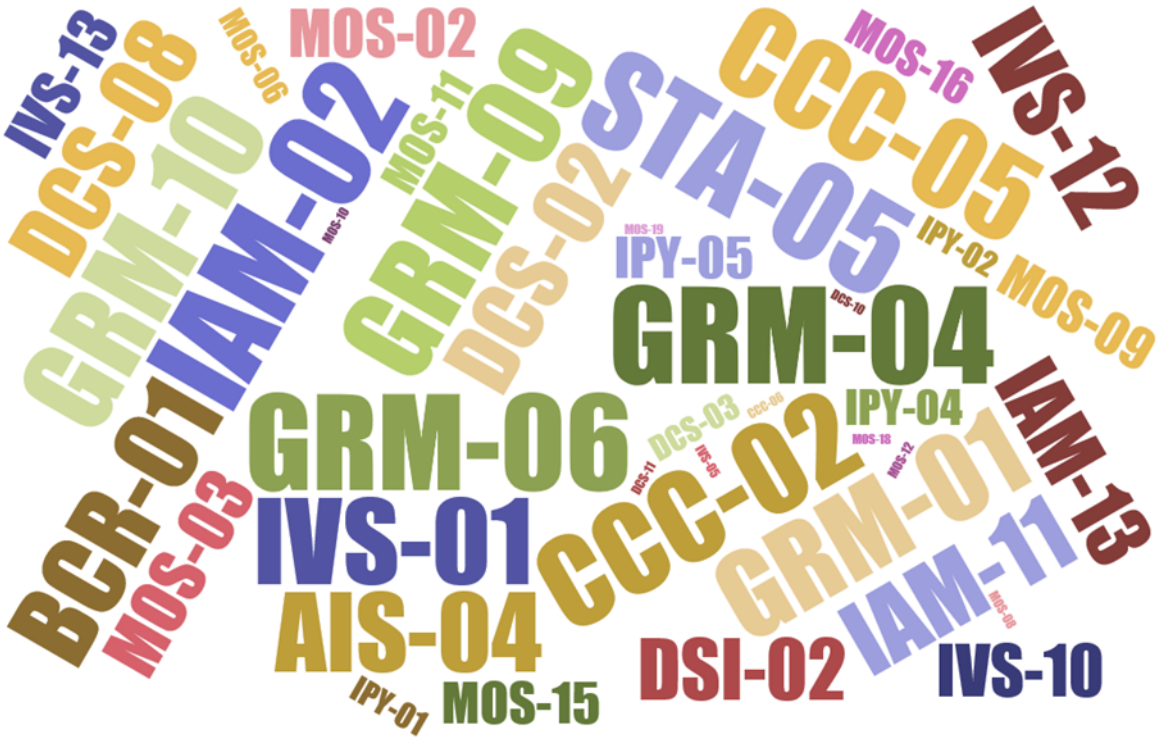

Figure 11: Requirements with no gap in mapping to CCM controls

4.2.2 MAPPING TO THE CCM - PARTIAL GAP

The outcome showed 131 requirements (16%) with established partial gap in the mapping to the CCM controls. The distribution of the CCM controls, to which the requirements were partially mapped is presented in Figure 12. The top five CCM control domains, to which the most requirements were mapped as "Partial gap" were:

- Governance and Risk Management (GRM)
- Business Continuity Management & Operational Resilience (BCR)
- Infrastructure & Virtualization Security (IVS)

- Identity & Access Management (IAM)
- Supply Chain Management, Transparency, and Accountability.

Figure 12: Requirements with partial gap in mapping to CCM controls

A few examples below describe some of the issue that weren't properly covered in the CCM framework and presented gaps (the complete information is available in the combined table of requirements in APPENDIX D Combined table of requirements and mapping):

- Responsibility to adopt the risk assessment methodology
- Controlled use of removable media
- Continuous improvement of the implemented security process
- Creating and retaining the record of detected or reported unauthorised disclosures of personal information
- Data distribution model, data location and data processing location
- Ensuring trusted networks for confidential and sensitive data
- Policies and procedures to detect vulnerabilities and manage software patch installations
- Security in physical media transfer

- To establish and maintain documented information
- Internal and external communications
- Intellectual property rights.

4.2.3 MAPPING TO THE CCM - FULL GAP

We found there were some of security and privacy requirements that could not be linked in any way to the CCM controls. Such requirements were 104, which is 13% of all. The requirements with full gap were related to, for example:

- Procurement in general term, including also public procurement, which is important procedure to obtain cloud services for public sector where the cloud service providers must demonstrate their capabilities (also certifications) and compliances
- Appropriate contacts with special interest groups or other specialist security professional associations and working groups
- Inclusion of information security in project management
- Authorisation for modification of data
- Defined roles in information security
- Requirements related to personally identifiable information (PII): more exact and defined requirements and rules for governance, communication, processes, and use, transfer, maintenance and disposal of material and media
- A full gap was also identified for the requirements that were addressing privacy elements. The CCM provides technical and security controls and the complementary work on privacy code of conduct and privacy level agreements in the EU-SEC project will cover the privacy elements, including the alignment with the GDPR. This work will be covered out in the deliverable D2.3 Privacy Code of Conduct.

4.3 DEVELOPING NEW CONTROLS - COVERING THE GAPS

The CCM was used as a baseline control framework and all the requirements were mapped to the controls in the CCM. Where the gap analysis revealed full or partial gaps, it was necessary to create new controls or to provide modifications to the existing controls to ensure that the gap level will be progressively and completely covered. Once the new controls would be established that will cover the identified gaps, the gap level of the requirements mapping to the controls in the EU-SEC repository will change respectively. The process is illustrated on Figure 13.

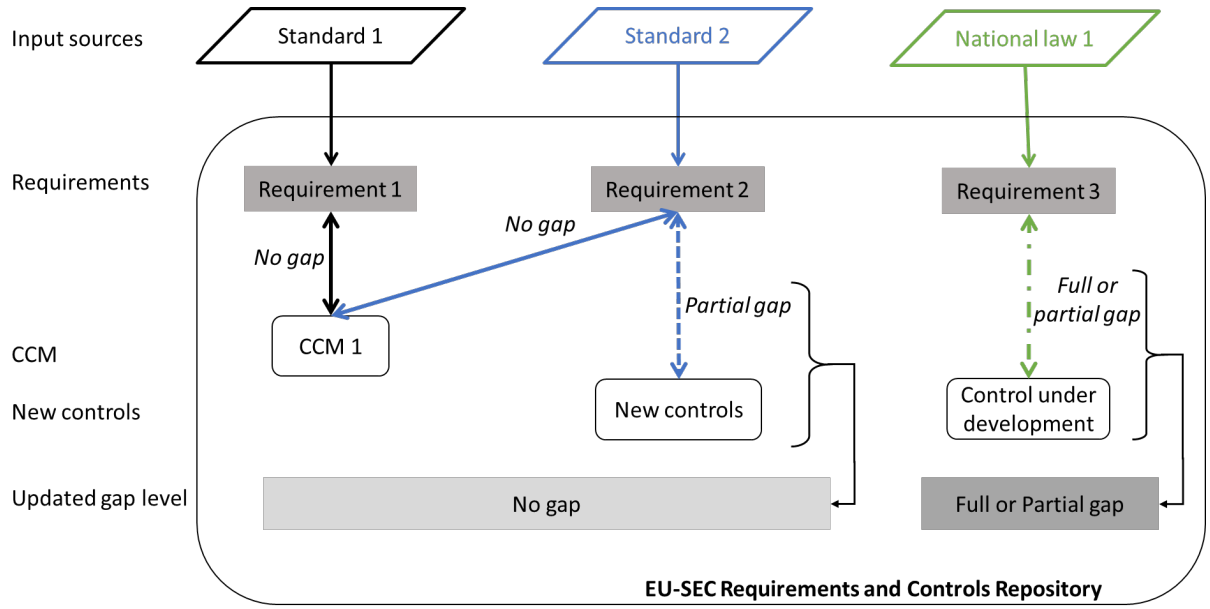

Figure 13: Creating new controls to cover the gaps

The second phase of the process (Figure 3) was used to propose and create the controls to cover the identified gaps ("Full gap", "Partial gap") which became part of the EU-SEC requirements and controls repository. For example:

- The requirement (SI-10-01) related to the preparation and documentation of public procurement were not explicitly covered in CCM, therefore "Full gap" was identified. As a solution, it was proposed to extend the CCM control domain Supply Chain Management, Transparency, and Accountability (STA), and create a new control which will more precisely cover the procurement, including public procurement (4.2.3).
- The requirement (SI-07-25) regarding the management of removable media was only partially covered by the controls in the CCM, therefore a "Partial gap" was identified (4.2.2). As a solution, it was proposed to extend the relevant control in the control domains Human Resources (HRS) or Datacenter Security (DCS) to address the issue of removable media lifecycle.

By creating new controls or extending the existing CCM controls that would cover the gaps, we could extend the EU-SEC requirements and controls repository and achieved a wider applicability of the EU-SEC framework to diverse thematic areas.

4.4 CREATING EU-SEC REQUIREMENTS AND CONTROLS REPOSITORY

As it is seen on Figure 9, the process of requirements collection and analysis provided detailed information that were used for the EU-SEC requirements and controls repository: the identified requirements, the mapping between the requirements and the CCM with gap levels, the CCM as the reference set of security controls, and a set of new controls or proposed modifications of the existing controls to cover the identified full or partial gaps.

The experiences of D1.2 had shown several characteristics of the process and the repository that indicated a high re-usability of the repository and its role as one of the fundamental pieces of the EU-SEC framework, as follows:

- The process ensured:
  - Transparency: clear methodology (2.1) and well-defined and described process (2.4)
  - Applicability: the same process was used for all input documents in several thematic domains and industry sectors, including new legislation, standards, certifications schemes or guidelines (2.3, 3)
- The detailed information for the EU-SEC requirements and controls repository provided:
  - Traceability: documented connections between the input sources, the requirements and the security controls, and the mapping between the requirements and the controls that indicated also the gap level (4.2).
  - Compatibility: the mapping to the common reference set of controls (CCM) allowed to track a semantic matching between the security objectives of requirements and controls, and how the same security controls were connected to diverse input sources (e.g. standards, certifications schemes, and others) (2.4.4, 2.5)
  - Extendibility: creating new controls or modifying existing controls satisfactory covered the new requirements and closed the identified full or partial gaps (4.3).

5 CONCLUSIONS

This deliverable, D1.2 Security and privacy requirements and controls, provides the information about the information security and privacy requirements.

The work was based on a common methodology which included two phases. In the first phase, we selected the requirements from the identified input documents and provided the initial mapping to the security controls. The second phase was used to consolidate the requirements and to indicate the potential contributions to the EU-SEC requirements and controls repository. The methodology also included two existing components: the CSA Cloud Controls Matrix (CCM) was used as the security controls scheme, and the comparison between the requirements and the CCM controls followed the CSA mapping methodology.

The outcome provided 804 relevant requirements and their relationships with the CCM security controls.

The CCM controls already satisfied 71% of requirements (no gap). This showed well-regulated areas where the CCM itself covered requirements from different thematic domains.

For 104 (13%) requirements, it wasn't possible to establish the mapping to the CCM controls (full gap), and for 131 (16%) requirements, we found partial gaps in the CCM controls. Both findings, full and partial gap presented the basis to form the potential updates or new controls in addition to the existing CCM controls. Both, the CCM and new findings in this work are valuable contributions to the EU-SEC requirements and controls repository.

The area of privacy and personal data protection is gaining the importance with the development of cloud computing and legal requirements, e.g. GDPR. In case of privacy requirements, we found other suitable measures outside of the CCM, e.g. privacy code of conduct (CoC) or privacy level agreements (PLA). The GDPR is considered in the deliverable D2.3 Privacy Code of Conduct. In current version of D1.2 (Ver 1.3) we integrate 126 privacy controls from D2.3 Code of conduct in EU SEC repository. With this we provide wider study and contribute more comprehensive view on security and privacy controls relevant to cloud computing.

The experiences from this deliverable also indicated the need to ensure that the new requirements could be continuously captured and covered by the up-to-date security and privacy controls. This might influence the EU-SEC framework governance mechanism.

The combined table of requirements with detailed information about the requirements mapping to the CCM control domains and controls is provided as MS Excel spreadsheet in addition.

APPENDIX A INPUT DOCUMENTS – DETAILS

This Appendix includes the lists of identified input documents from the defined thematic domains: standards, national legal basis, European Union and international legal basis, technical and good practice documents and sector specific (banking sector) legislation and documents, and documents from other thematic domains.

The structure of the table has the following meaning:

Id	Identification number of the document
Abbreviation	Abbreviation of the document
Short name	Short name of the document (official where possible)
Title	Full title of the document
Year	Year when document was published
Status	Document type, from the list: Strategy, Policy, National law, Sub-national law, Regulation, Decree, Rules, Guidelines, Standard, EU / Regulation, EU / Directive, EU / Decision, EU / Strategy, EU / Guidelines, EU / Other type, In preparation, To be decided
Document description	Document description
URL	URL

A.1 STANDARDS

The standards are developed and adopted by different standardisation bodies and supported by several associations and organisations that contribute important information from the practice. The following overview provides a list of organisations that are working on standardisation in cloud computing: http://csc.etsi.org/phase2/snapshot2/StandardsOrganizations.html .

Selected standards for requirements collection:

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
ISO27017	ISO/IEC 27017	ISO/IEC 27017	Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services	2015	Standard	ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services.	https://www.iso.org/standard/43757.html
ISO27018	ISO/IEC 27018	ISO/IEC 27018	Information technology - Security techniques - Code of practice for PII protection in public clouds acting as PII processors	2014	Standard	ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.	https://www.iso.org/standard/61498.html

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
ISO27001	ISO/IEC 27001	ISO/IEC 27001	Information technology -- Security techniques -- Information security management systems -- Requirements				https://www.iso.org/standard/54534.html
SecNumCloud	SecNumCloud	SecNumCloud_2016	Prestataires de services d'informatique en nuage (SecNumCloud) référentiel d'exigences – niveau Essentiel, Version 3.0 du 8 décembre 2016 / Cloud Service Providers (SecNumCloud) Requirements - Essential Level, Version 3.0, 08.12.2016	2016	Standard	This framework covers cloud computing services and aims to qualify providers offering such services. Cloud computing can be defined as an IT management model that allows network access to shared and configurable computing resources. These resources are allocated to demand and sometimes self-service. Cloud service providers provide various services that are usually classified into three types of activity: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). This document is the repository of requirements for a cloud service provider (SecNumCloud), hereinafter referred to as the "provider". Secure Cloud became SecNumCloud.	http://www.ssi.gouv.fr/uploads/2014/12/secnumcloud_referentiel_v3.0_niveau_essentiel.pdf
C5-2016	C5-2016	BSI C5	BSI Cloud Computing Compliance Control Catalogue and Referencing Cloud Computing Compliance Controls Catalogue (C5) to International	2015	Standard	C5 is a standard published by German Federal Office for Information Security (BSI) and standardised the requirements on information security from existing and well-known international and national standards and regulations. C5 aims to provide customer a better cloud overview for a higher	https://www.bsi.bund.de/EN/Topics/Cloud-Compu-ting/Compliance_Controls_Catalogue/Compliance_Controls_Catalogue_node.html

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
			Standards (Refers to version 1.0 of C5), Version 1.0, 2016			level of security and avoiding redundant audits and unnecessary efforts. The C5 catalogue is divided into 17 thematic sections (e.g. organisation of information security, physical security). Here, the BSI makes use of recognised security standards such as 27001, the Cloud Controls Matrix of the Cloud Security Alliance as well as BSI publications and uses these requirements wherever appropriate. If these requirements had to be specified in more detail, they were put in concrete terms; if there were no requirements in other standards, new requirements were defined. In addition to these basic requirements, the catalogue also includes further requirements which either address confidentiality or availability, or both security objectives at the same time, for many requirements. The requirements were referenced to the standards mentioned above. This information provides a quick overview of where the requirements of the catalogue can be found in other standards and whether the requirements go beyond the standards or not.	and https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Cloud-Computing/ComplianceControlsCatalogue/Referencing_Cloud_Computing_Compliance_Controls_Catalogue.pdf;jsessionid=D3A3E72AB31B0B5B2249741B2F3EA333.2_cid341?__blob=publicationFile&v=2

A.2 NATIONAL LEGAL BASIS

SLOVENIA – LEGAL BASIS

The following national legislation, including national laws, rules, recommendations and guidelines, are identified as the input documents for the identification of requirements in the scope of the EU-SEC project.

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
SI-07	IVPJU	Recommendation - information security policy in PA	Recommendations of the information security policy of public administration	2010	Recommendation	The aim is to establish basic security platform to protect information assets from threats, whether internal or external, deliberate or accidental.	http://www.mpju.gov.si/fileadmin/mpju.gov.si/pageuploads/DIES/IVPJU_01.pdf
SI-09	GTZ		Generic Technological Requirements for Information Systems Development, V2.2.3, 2017	2017	Rules	The Rules include technical elements for the development of information systems and the required standards, requirements and rules for the installation of systems on a shared infrastructure, determine the system change management and information security. The document is used as an annex to the tender/contract documents for systems that are or will be placed on the shared infrastructure of the Ministry of Public Administration.	https://nio.gov.si/nio/asset/dokument+generic+tehnoloske+zahteve+gtz-743

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
SI-10	JNIT	Public procurement for IT solutions	Guidelines for the procurement of IT solutions, 2017	2017	Guidelines	The guidelines constitute a recommendation to subscribers of IT solutions in the public sector, recommend appropriate approaches in the preparation of public procurement and describe different domains of procurement in relation to the development and maintenance of information systems.	https://nio.gov.si/nio/asset/smernice+za+javno+narocanje+informacijskih+resitev

SPAIN – LEGAL BASIS

The following national legislation is identified as the input documents for the identification of requirements in the scope of the EU-SEC project.

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
ES-01	BOE-A-2010-1330	Royal Decree 3/2010, of 8 January	Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the field of Electronic Administration.	2010	National law	The purpose of the National Security Scheme is to create the necessary conditions of confidence in the use of electronic means, through measures to ensure the security of systems, data, communications, and electronic services, enabling Citizens and public Administrations, the exercise of rights and the fulfilment of duties through these means.	https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
ES-02	BOE-A-2011-7630	Law 8/2011, of 28 April	Law 8/2011, of 28 April, which establishes measures for the protection of critical infrastructures.	2011	National law	This law regulates the protection of critical infrastructures against deliberate attacks of all kinds (both physical and cybernetic) and, on the other hand, the definition of an organizational system for the protection of such infrastructures, The Public Administrations and affected private entities.	http://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf
ES-03	Law 56/2007	Law 56/2007, of 28 December	Law 56/2007, of 28 December, Measures to boost the information society	2007	National law	This Law establish a set of policy initiatives aimed at removing existing barriers to the expansion and use of information and communication technologies guarantying the rights of citizens in the new information society.	http://www.boe.es/boe/dias/2007/12/29/pdfs/A53701-53719.pdf
ES-04	Law 59/2003	Law 59/2003, of 19 December	Law 59/2003, of 19 December, of Electronic Signature	2003	National law	This law regulates electronic signature, its legal effectiveness and the provision of certification services.	http://boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

GERMANY – LEGAL BASIS

The selected legislation (sub-national) is identified as the input documents for the identification of requirements in the scope of the EU-SEC project.

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
BDSG	BDSG	BDSG German Federal Data Protection Act	BDSG German Federal Data Protection Act	2014	Sub-national law		
FAIT5	IDW RS FAIT 5	IDW RS FAIT 5	IDW Statement on Accounting: Principles of accounting in case of outsourcing of the accounting-relevant processes and functions, including Cloud computing	2015	Regulation		

A.3 TECHNICAL SPECIFICATIONS AND GOOD PRACTICES

The following guidelines, recommendations and good practice documents are identified as the input documents for the identification of requirements in the scope of the EU-SEC project.

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
TSC_2016	TSC	AICPA TSC	AICPA Trust Services Principles and Criteria	2016	Guidelines	This resource presents criteria for use when providing attestation or consulting services to evaluate controls relevant to the security, availability, and processing integrity of a system, and the confidentiality and privacy of the information processed by the system.	https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SOCGuidesandPublications.aspx
ENISA_MSM_DSP	ENISA_MSM_DSP	ENISA Minimum Security Measures for Digital Service Providers	Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, December 2016	2016	Guidelines	ENISA has issued this report to assist Member States and DSPs in providing a common approach regarding the security measures for DSPs. Although ENISA has already drafted a set of security objectives in the context of cloud security in 2014, this study goes further than that by broadening the scope of its work and by including security objectives for all three categories of digital service providers. This study lists 27 Security Objectives (SOs) for DSPs. In those 27 SOs, security measures that map to the NIS Directive requirements are also included. The SOs are mapped to diverse frameworks, including the CSA CCM. This report focuses only on the objectives which	https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
						are solely considered most relevant to the security element of the information systems and data maintained by the DSPs. However, some security measures described herein i.e. encryption, secure disposal of data, media access policy etc. are extensively used to address data protection requirements as well.	
PLA CoC	PLA CoC	The CSA CoC for GDPR Compliance	Cloud Security Alliance: Code of conduct for GDPR compliance	2018	Guidelines	The CSA CoC for GDPR Compliance aims to provide Cloud Service Providers (CSPs) and cloud consumers a solution for GDPR compliance and to provide transparency guidelines regarding the level of data protection offered by the CSP.	https://complexdiscovery.com/wp-content/uploads/2018/06/CSA-Code-of-Conduct-for-GDPR-Compliance.pdf

A.4 BANKING SECTOR DOCUMENTS

The following documents, mostly rules, guidelines and sector standards, applicable in the international context, are identified as the input documents for the identification of requirements in the scope of the EU-SEC project.

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
CBK-01	ENISA CCFS	ENISA Cloud in the Finance Sector	Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations (ENISA)	2015	EU / Guidelines	This study presents not just challenges and issues, but also some significant success stories that will be of good guidance and an example for those FIs, supervisory authorities and CSPs that are still at the beginning of their journey towards cloud. One conclusion we can derive from our surveys and analysis is that whenever the rules of the game are clear, more players are encouraged to participate.	https://www.enisa.europa.eu/publications/cloud-in-finance
CBK-02	PCI DSS	PCI DSS v3.2	Payment Card Industry Data Security Standard - Requirements and Security Assessment Procedures (version 3.2)	2016	Standard	The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.	https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf?agreement=true&time=1495807062413
CBK-03	EBA/GL/2017/05	ICT Risk Assessment SREP	Guidelines on ICT Risk Assessment under the Supervisory	2017	EU / Guidelines	These Guidelines are addressed to competent authorities and are in-	https://www.eba.europa.eu/docu-

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
			Review and Evaluation process (SREP)			tended to promote common procedures and methodologies for the assessment of the Information and Communication Technology (ICT) risk under the supervisory review and evaluation process (SREP), referred to in Article 97 of Directive 2013/36/EU1. These Guidelines drawn up pursuant to Article 107(3) of Directive 2013/36/EU, supplement and further specify criteria for the assessment of ICT risk as part of operational risk put forward in the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)2 (from here on 'EBA SREP Guidelines'). These Guidelines form an integral part of the EBA SREP Guidelines and should be read and applied along with it.	ments/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf
CBK-04	EBA/GL/2014/12-Rev1	SecurePay	Final Guidelines on the security of internet payments	2014	EU / Guidelines	Guidelines set out the EBA's view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in this area. The EBA therefore expects all competent authorities and financial institutions to whom guidelines are addressed to comply with guidelines.	https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1

Id	Abbreviation	Short name	Title	Year	Status	Document description	URL
CBK-05	EBA/CP/2017/06	EBA_REC_Outsourcing_Cloud	Draft recommendations on outsourcing to cloud service providers under Article 16 of Regulation (EU) No 1093/2010	2017	EU / Guidelines	These recommendations are intended to provide guidance on the outsourcing by institutions to cloud service providers.	http://www.eba.europa.eu/documents/10180/1848359/Draft+Recommendation+on+outsourcing+to+Cloud+Service++%28EBA-CP-2017-06%29.pdf
CBK-06	PCI PIN	Payment Card Industry PIN Security Requirements (version 2.0)	Payment Card Industry PIN Security Requirements (version 2.0)	2014	Rules	This document contains a complete set of requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.	https://www.pcisecuritystandards.org/document_library
CBK-07	PCI HSM	PCI HSM	Payment Card Industry Hardware Security Module - Security Requirements (version 1.0)	2009	Rules	This document contains a complete set of requirements for securing Hardware Security Modules (HSM). HSMs may support a variety payment processing and cardholder authentication applications and processes.	https://www.pcisecuritystandards.org/

APPENDIX B GDPR INTRODUCTION

The General Data Protection Regulation (GDPR) [10] has the highest importance for the protection of all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes were introduced to the regulatory policies; the key points of the GDPR, as well as information on the impacts it has on businesses, can be found below.

Increased Territorial Scope (extra-territorial applicability)

Arguably the biggest change to the regulatory landscape of data privacy came with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the organization's location. Previously, territorial applicability of the directive was ambiguous and referred to data processing 'in context of an establishment'. This topic has arisen in several high-profile court cases. GPDR makes its applicability very clear - it applies to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR also applies to processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing data of EU citizens have to appoint a representative in the EU.

Penalties

Under the GDPR, organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. violating the conditions for consent or violating the data subjects' rights. There is a tiered approach to fines e.g. an organization can be fined 2% for not following the Privacy by Design principles (Article 25). It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Conditions for consent were strengthened and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Breach Notification

Under the GDPR, breach notification is mandatory in all Member States, in cases where the breach of data is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customer organisations, the controllers, "without undue delay" after first becoming aware of the data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller a confirmation as to whether personal data concerning them is being processed and for what purpose, and other related information. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift towards data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to request the data controller to erase their personal data, including copies held by data processors. The conditions for erasure, as outlined in Article 17, include the data no longer being relevant to the original purposes for processing, or the data subject withdrawing consent.

Data Portability

GDPR introduced data portability - the right for a data subject to receive the personal data concerning them which they have previously provided, in a 'commonly used and machine-readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is now a requirement under the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically (Article 25) – "The controller

shall implement appropriate technical and organisational measures in an effective way to meet the requirements of this Regulation and protect the rights of data subjects". Article 5 calls for controllers to hold and process only the data that is necessary for the processing purposes (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Before the GDPR, controllers were required to notify their data processing activities to local DPAs, which, for multinationals, was challenging with most Member States having different notification requirements. Under the GDPR, it is not necessary to submit notifications / registrations to each local DPA of data processing activities, nor it is a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there are internal record keeping requirements, as further explained below, and data protection officer (DPO) appointment is mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

The General Data Protection Regulation implements the Article 8(1) in the Charter of Fundamental Rights of the European Union.

APPENDIX C REFERENCES

[AICPA] The American Institute of Certified Public Accountants, http://www.aicpa.org.

[CCM] Cloud Controls Matrix, Version 3.0.1, 10.06.2016, Cloud Security Alliance, https://cloudsecurityalliance.org/group/cloud-controls-matrix/.

[CCM mapping methodology] Standards mapping methodology, Cloud Security Alliance, available on request, https://cloudsecurityalliance.org/.

[Charter] The Charter of Fundamental Rights, http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[DoW] The European Security Certification Framework, Innovation Actions – Security Certification, DS-1-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components.

[ECHR] The European Convention of Human Rights, http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

[ENISA MSM-DSP] Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, December 2016, https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers.

[GDPR] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC.

[ISO/IEC 27000:2016] Information technology - Security techniques - Information security management systems - Overview and vocabulary, https://www.iso.org/standard/66435.html.

[ISO/IEC 27006] ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems, https://www.iso.org/standard/62313.html.

[NIS Directive] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.

[STAR] CSA Security, Trust & Assurance Registry, https://cloudsecurityalliance.org/star.

APPENDIX D COMBINED TABLE OF REQUIREMENTS AND MAPPING

The combined table of requirements includes all identified requirements from the selected input documents, details of their mapping to the CCM control domains and controls, justifications of mapping and created or proposed new controls or other information. The relationships between the requirements and the CCM controls could be analysed from diverse angles of interest; thus, this table was a useful tool for analysis, consolidation of requirements and transformation into the EU-SEC requirements and controls repository. The table is included in this appendix and available in Microsoft Excel format. Figure 14 displays the conceptual view of gathered information for the combined table of requirements.

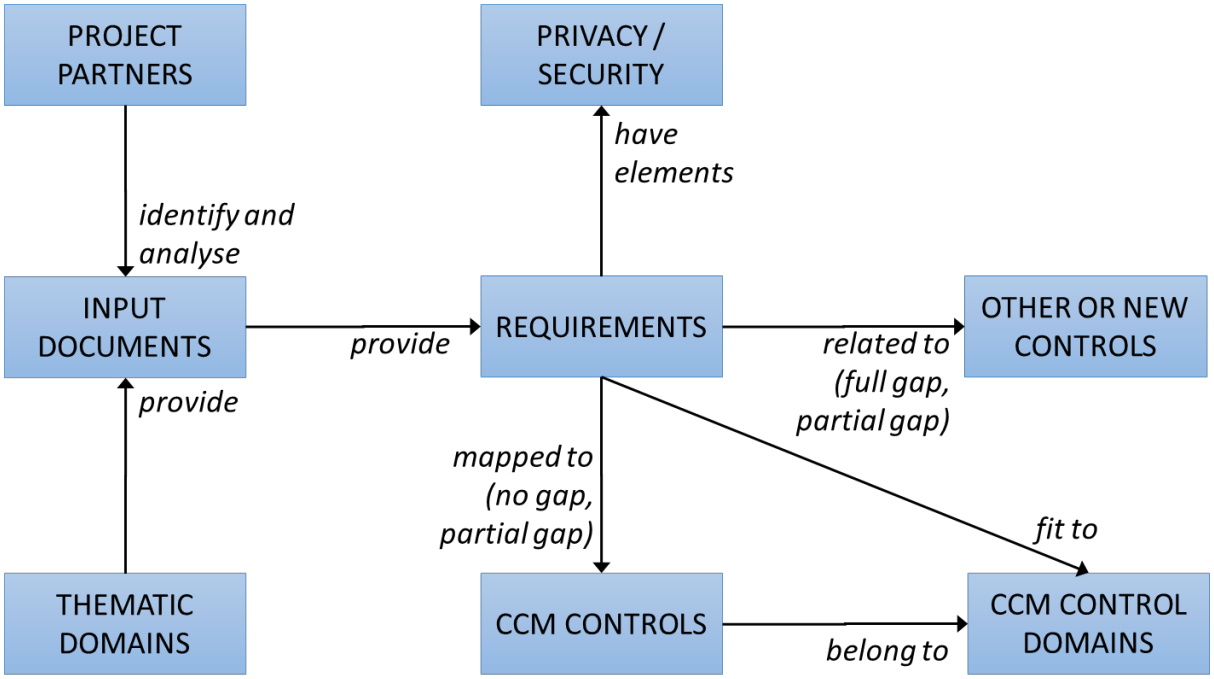

Figure 14: Information basis for the combined table of requirements

The combined table of requirements includes the following structure:

Source_document	Identification number of the input document The list of all input documents is in 3.1 and the details in AP-PENDIX A Input documents – details.
Req_Id	Identification number of the requirement
Req_title	Requirement title
Req_description	Requirement description
Type	Indicates the privacy or security elements which the requirement defines. The pre-defined values are: privacy, security, both, other.
Domain	CSA CCM control domains In addition, two values were used according to the methodology (2.4.4.4): "To be decided (Mapping exists)" and "To be decided (No mapping)".
Gap_level	Indicates the level of gap in the mapping between the require-ment and the CCM framework identified in gap analysis. The pre-defined values are: No gap, Partial gap, Full gap.
Details	Used in the case of no gap in mapping between the requirement and the CCM control(s). The mapping details provide information on fine tuning of the mapping and smaller differences in security objectives, if they occurred. The pre-defined values are: +, -, 0, To be decided. Explanation is in 2.4.4.22.4.4.4.
CCM_controls	The list of CCM controls to which the requirement is mapped. The acronym in the CCM control name indicates the CCM control do-main that is explained in 2.4.4.
Description	Explanation or justification of mapping between the requirement and the CCM control(s) It includes also the proposals of new controls in the case of full gap or partial gap.

Table 7: EU-SEC requirements and controls mapped to CCM framework

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
BDSG / 4f	BDSG-1	Data protection official	In so far as the structure of a public body requires, the appointment of one data protection official for several areas shall be sufficient. The required level of specialized knowledge is determined in particular according to the scope of data processing carried out by the controller concerned and the protection requirements of the personal data collected or used by the controller concerned.	Privacy	Data Security & Information Lifecycle Managem-ent	No gap	-	DSI-01	
BDSG / 5	BDSG-2	Confidentality	Persons employed in data processing shall not collect, process or use personal data without authorization (confidentiality). On taking up their duties such persons, in so far as they work for private bodies, shall be required to give an undertaking to maintain such confidentiality.	Privacy	Data Security & Information Lifecycle Managem-ent	No gap	-	DSI-01	
BDSG / 9	BDSG-3	Technical and organizational measures	Public and private bodies processing personal data either on their own behalf or on behalf of others shall take the technical and organizational measures necessary to ensure the implementation of the provisions of BDSG	Privacy	Data Security & Information Lifecycle Managem-ent	No gap	-	DSI-01	
BDSG / 9a	BDSG-4	Data protection audit	In order to improve data protection and data security, suppliers of data processing systems and programs and bodies conducting data processing may have their data protection strategies and their technical facilities examined and evaluated by independent and approved appraisers, and may publish the result of the audit.	Privacy	Audit Assurance & Compliance	No gap	-	AAC-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
BDSG / 10	BDSG-5	Establish-ment of automated retrieval procedures	An automated procedure for the retrieval of personal data may be established in so far as such procedure is appropriate, having due regard to the legitimate interests of the data subjects and to the duties or business purposes of the bodies involved. The provisions on the admissibility of retrieval in a particular case shall remain unaffected.	Privacy	Data Security & Information Lifecycle Manage-ment	No gap	-	DSI-01	
C5-2016	UP-01	Framework conditions of the cloud service (surrounding parameters for transparency) / System description	In their system description, the cloud provider provides comprehensible and transparent specifications regarding the cloud service, which allow an expert third party to assess the general suitability of the cloud service for the desired application. The system description describes the following aspects: • Type and scope of the cloud services rendered according to the service level agreement which is typically based on a contract concluded with the cloud customers, • Principles, procedures and safeguards for rendering (development and/or operation) the cloud service, including the controls established, • Description of the infrastructure, network and system components used for the development and operation of the cloud service, • Handling of significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document. The requirement is part of Framework conditions of the cloud service (surrounding parameters for transparency) that is not mapped to CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			IT systems, • Roles and responsibilities of the cloud provider and the cloud customer, including the duties to cooperate and corresponding controls at the cloud customer, • Functions assigned or outsourced to subcontractors.						
C5-2016	UP-02	Framework conditions of the cloud service (surrounding parameters for transparency) / Jurisdiction and data storage, processing and backup locations	In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding its jurisdiction as well as with respect to data storage, processing and backup locations, which allow an expert third party to assess the general suitability of the cloud service for the customer application. This also holds true if data of the cloud customer is processed, stored and backed up by subcontractors of the cloud provider. Data of the cloud customer shall only be processed, stored and backed up outside the contractually agreed locations only with the prior express written consent of the cloud customer.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document. The requirement is part of Framework conditions of the cloud service (surrounding parameters for transparency) that is not mapped to CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	UP-03	Framework conditions of the cloud service (surrounding parameters for transparency) / Jurisdiction and data storage, processing and backup locations	In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding applicable disclosure and investigatory powers of government agencies which allow access to data of the cloud customer. The specifications must allow an expert third party to assess the general suitability of the cloud service for the customer application. If the cloud provider accesses third-party services, the provider has obtained these specifications from them.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document. The requirement is part of Framework conditions of the cloud service (surrounding parameters for transparency) that is not mapped to CCM.
C5-2016	UP-04	Framework conditions of the cloud service (surrounding parameters for transparency) / Jurisdiction and data storage, processing and backup locations	In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding available and valid certifications and certificates of independent third parties, which allow an expert third party to assess the general suitability of the cloud service for the customer application.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document. The requirement is part of Framework conditions of the cloud service (surrounding parameters for transparency) that is not mapped to CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	OIS-01	Organisation of information security / Information security managem-ent system (ISMS)	The top management initiates, controls and monitors an information security management system (ISMS) which is based on ISO standards of the 2700x series. • The instruments and methods used allow acomprehensible control of the following tasks and activities to permanently maintain and ensure information security: Planning, implementing the plan and/or carrying out the project, • Performance review and/or monitoring the achievement of objectives • Eliminating discovered flaws and weaknesses and continuous improvement. The ISMS also includes the IT processes for the development and operation of the cloud service.		Governance and Risk Managem-ent	No gap	0	GRM-03, GRM-04	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	OIS-02	Organisat-ion of information security / Strategic targets regarding information security and responsibility of the top management	A security policy with security objectives and strategic parameters for achieving these objectives is documented. The security objectives are derived from the corporate objectives and business processes, relevant laws and regulations as well as the current and future expected threat environment with respect to information security. The strategic targets constitute essential framework conditions which in further policies and instructions are specified in more detail (see SA-01). The security policy is adopted by the top management and communicated to all		Governance and Risk Management	No gap	0	GRM-05, GRM-06	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			concerned internal and external parties of the cloud provider (e. g. cloud customers, subcontractors).						
C5-2016	OIS-03	Organisation of information security / Authorities and responsibilities in the framework of information security	Responsibilities shared between the cloud provider and cloud customers, duties to cooperate as well as interfaces for the reporting of security incidents and malfunctions are defined, documented, assigned depending on the respective cloud model (infrastructure, platform or software as a service) and the contractual duties and communicated to all concerned internal and external parties (e. g. cloud customers, subcontractors of the cloud provider). On the part of the cloud provider, at least the following roles (or comparable equivalents) are described in the security policy or associated policies and corresponding responsibilities assigned: • Head of IT (CIO) • IT Security Officer (CISO) • Representative for the handling of IT security incidents (e. g. Head of CERT) Changes to the responsibilities and interfaces are communicated internally and externally in such a timely manner that all internal and external parties concerned (e. g. cloud customers) are able to respond to them appropriately with organisational and technical		Business Continuity Management & Operational Resilience	Partial gap		BCR-10	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			safeguards, before the change becomes effective.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	OIS-04	Organisation of information security / Separation of functions	Organisational and technical controls are established in order to ensure the separation of roles and responsibilities (also referred to the "separation of duties") which are incompatible with respect to the confidentiality, integrity and availability of information of the cloud customers. Controls for the separation of functions are established in the following areas in particular: • Administration of roles, granting and assignment of access authorisations for users under the responsibility of the cloud provider, • Development and implementation of changes to the cloud service, • Maintenance of the physical and logical IT infrastructure relevant to the cloud service (networks, operating systems, databases) and the IT applications if they are in the cloud provider's area of responsibility according to the contractual agreements with the cloud customers. Operative and controlling functions should not be performed by one and the same person at the same time. If it is not possible to achieve a separation of duties for organisational or technical reasons, appropriate compensating controls are established in order to prevent or uncover improper activities.		Identity & Access Management	Partial gap		IAM-05	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	OIS-05	Organisation of information security / Contact with relevant government agencies and interest groups	Appropriate and relevant contacts of the cloud provider with government agencies and interest groups are established to be always informed about current threat scenarios and countermeasures.		To be decided (Mapping exists)	No gap	+	SEF-01, AIS-01	The CCM control leads to a higher security level as the requirement of C5 (exceeds).
C5-2016	OIS-06	Organisation of information security / Policy for the organisation of the risk management	Policies and instructions for the general procedure applicable to the identification, analysis, assessment and handling of risks and IT risks in particular are documented, communicated and provided according to SA-01.		Governance and Risk Management	Partial gap		GRM-01	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	OIS-07	Organisation of information security / Identification, analysis, assessment and handling of risks	The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the cloud service are done at least once a year in order to take internal and external changes and influencing factors into account. The identified risks are comprehensibly documented, assessed and provided with mitigating safeguards according to the safeguards of the risk management.		Governance and Risk Management	No gap	+	GRM-01, GRM-02, GRM-08, GRM-10, GRM-11	The CCM control leads to a higher security level as the requirement of C5 (exceeds).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	SA-01	Security policies and work instructions/ Documentation, communication and provision of policies and instructions	Policies and instructions for information security or related topics derived from the security policy are documented in an uniform structure. They are communicated and made available to all internal and external employees of the cloud provider properly and adequately. Policies are versioned and approved by top management of the cloud provider. The policies and instructions describe at least the following aspects: • Goals • Scopes of application • Roles and responsibilities, including requirements for the qualification of the personnel and the establishment of substitution arrangements, • Coordination of different company departments, • Security architecture and safeguards for the protection of data, IT applications and IT infrastructures which are managed by the cloud provider or third parties as well as • Safeguards for the compliance with legal and regulatory requirements (compliance).		Governance and Risk Management	No gap	0	GRM-06	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	SA-02	Security policies and work instructions / Review and approval of policies and instructions	The policies and instructions for information security are reviewed with respect to their appropriateness and effectiveness by specialists of the cloud provider who are familiar with the topic at least once a year. At least the following aspects are taken into account in the review: • Organisational changes at the cloud provider, • Current and future expected threat environment regarding information security as well as • Legal and technical changes in the cloud provider's environment. Revised policies and instructions are approved by committees or bodies of the cloud provider authorised to do so before they become valid.		Governance and Risk Management	No gap	0	GRM-08, GRM-09	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	SA-03	Security policies and work instructions / Deviations from existing policies and instructions	Exceptions of policies and instructions for information security are approved by committees or bodies of the cloud provider authorised to do so in a documented form. The appropriateness of approved exceptions and the assessment of the risks resulting from this are reviewed by specialists of the cloud provider who are familiar with the topic against the backdrop of the current and future expected threat environment regarding information security at least once a year.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	HR-01	Personnel / Security check of the background information	The background of all internal and external employees of the cloud provider with access to data of the cloud customers or of the shared IT infrastructure is checked according to the local legislation and regulation by the cloud provider prior to the start of the employment relationship. To the extent permitted by law, the security check includes the following areas: • Verification of the person by means of the identity card, • Verification of the curriculum vitae, • Verification of academic titles and degrees, • Request of a police clearance certificate for sensitive posts in the company		Human Resources	No gap	0	HRS-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	HR-02	Personnel / Employment Agreements	Employment agreements include the obligations of the cloud provider's internal and external employees to comply with relevant laws, regulations and provisions regarding information security (see KOS- 10). The security policy as well as the policies and instructions for information security derived from this are added to the employment agreement documents. Corresponding compliance is confirmed by the employee by a written statement before they can access the data of the cloud customers or the (shared) IT infrastructure.		Human Resources	No gap	0	HRS-03	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	HR-03	Personnel / Security training and awarenessraising programme	A security training and awareness-raising programme tailored to specific target groups on the topic of information security is available and mandatory for all internal and external employees of the cloud provider. The programme is updated at regular intervals with respect to the applicable policies and instructions, the assigned roles and responsibilities as well as the known threats and must then be run through again. The programme includes at least the following contents: • Regular and documented instruction on the secure configuration and secure operation of the IT applications and IT infrastructure required for the cloud service, including mobile terminal devices, • Appropriate handling of data of the cloudcustomers, • Regular and documented instruction on known basic threats, and • Regular and documented training on the behaviour in case of security-relevant events. • External service providers and suppliers of the cloud provider, who contribute to the development or operation of the cloud service, are obliged by contract to make their employees and subcontractors aware of the specific security requirements of the cloud		Human Resources	No gap	0	HRS-09	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			provider and train their employees generally in the subject of information security.						
C5-2016	HR-04	Personnel / Disciplinary Measures	A process for performing disciplinary measures is implemented and communicated to the employees in order to make the consequences of violations of the applicable policies and instructions as well as legal provisions and laws transparent.		Governance and Risk Management	No gap	0	GRM-07	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	HR-05	Personnel / Termination of the employment relationship or changes to the responsibilities	Internal as well as external employees are informed that the obligations to comply with relevant laws, regulations and provisions regarding information security remain valid even if the area of responsibility changes or the employment relationship is terminated.		Human Resources	No gap	0	HRS-04	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	AM-01	Asset management / Asset inventory	The assets (e. g. PCs, peripheral devices, telephones, network components, servers, installation documentation, process instructions, IT applications, tools) used to render the cloud service are identified and inventoried. By means of appropriate processes and safeguards, it is ensured that this inventory remains complete, correct, up-to-date and consistent. A history of the changes to the entries in the inventory is kept in a comprehensible manner. If no effective automatic procedures are established for this, this is ensured by a manual review of the inventory data of the assets which takes place at least once a month.		To be decided (Mapping exists)	No gap	0	DCS-01, GRM-02, MOS-09	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	AM-02	Asset management / Assignment of persons responsible for assets	All inventoried assets are assigned to a person responsible on the part of the cloud provider. The persons responsible of the cloud provider are responsible over the entire life cycle of the assets to ensure that they are inventoried completely and classified correctly.		To be decided (Mapping exists)	No gap	0	DCS-01, DSI-06, HRS-07	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	AM-03	Asset management / Instruction manuals for assets	Policies and instructions with technical and organisational safeguards for the proper handling of assets are documented, communicated and provided according to SA-01 in the respectively current version.		To be decided (Mapping exists)	No gap	0	DCS-01, HRS-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	AM-04	Asset management / Handing in and returning assets	All internal and external employees of the cloud provider are obliged to return or irrevocably delete all assets which were handed over to them in relation to the cloud service and/or for which they are responsible as soon as the employment relationship has been terminated.		Human Resources	No gap	0	HRS-01	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	AM-05	Asset management / Classification of information	The cloud provider uses a uniform classification of information and assets which are relevant to the development and rendering of the cloud service.		Data Security & Information Lifecycle Management	No gap	0	DSI-01	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	AM-06	Asset management / Labelling of information and handling of assets	Work instructions and processes for the implemented classification scheme of information and assets are in place in order to ensure the labeling of information as well as the corresponding handling of assets. This only refers to assets which store or process information.		Data Security & Information Lifecycle Management	No gap	0	DSI-04	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	AM-07	Asset management / Management of data media	Policies and instructions with technical and organisational safeguards for the secure handling of data media of any type are documented, communicated and provided according to SA-01. The targets establish a reference to the classification of information (see AM-05). They include the secure use, the secure transport as well as the irrevocable deletion and destruction of data media.		To be decided (Mapping exists)	No gap	0	BCR-11, DCS-05	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	AM-08	Asset management / Transfer and removal of assets	Devices, hardware, software or data may only be transferred to external premises after it has been approved by authorised committees or bodies of the cloud provider. The transfer takes place securely according to the type of the assets to be transferred.		Datacenter Security	No gap	0	DCS-04	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PS-01	Physical security / Perimeter protection	The perimeter of premises or buildings which house sensitive or critical information, information systems or other network infrastructure are protected in a physically solid manner and by means of appropriate security safeguards that conform to the current state of the art.		Datacenter Security	No gap	0	DCS-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PS-02	Physical security / Physical site access control	Access to the premises or buildings which house sensitive or critical information, information systems or other network infrastructure is secured and monitored by means of physical site access controls in order to avoid unauthorised site access.		Datacenter Security	No gap	+	DCS-07, DCS-08, DCS-09	The CCM control leads to a higher security level as the requirement of C5 (exceeds).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	PS-03	Physical security / Protection against threats from outside and from the environment	Structural, technical and organisational safeguards are taken to protect premises or buildings which house sensitive or critical information, information systems or other network infrastructure against fire, water, earthquakes, explosions, civil disturbances and other forms of natural threats and threats caused by humans. At two geo-redundant sites, at least the following safeguards are carried out: Structural safeguards: • Setup of a separate fire zone for the computer centre, • Use of fire-resistant materials according to DIN 4102-1 or EN 13501 (period of fire resistance of at least 90 minutes) Technical safeguards: • Sensors to monitor temperature and humidity, • Connecting the building to a fire alarm system with notification of the local fire department, • Early fire detection and extinguishing systems. Organisational safeguards: • Regular fire drills and fire safety inspections to check compliance with fire protection measures.		Business Continuity Management & Operational Resilience	No gap	0	BCR-05, BCR-06	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PS-04	Physical security / Protection against interruptions caused by power failures	Precautions against the failure of supply services such as power, cooling or network connections are taken by means of suitable safeguards and redundancies in coordination with safeguards for operational reliability. Power and telecommunication supply lines which transport data or supply information		Business Continuity Management & Operational Resilience	No gap	0	BCR-08	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		and other such risks	systems must be protected against interception and damage.						
C5-2016	PS-05	Physical security / Maintenance of infrastructure and devices	Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 which describe the maintenance (especially remote maintenance), deletion, updating and re-use of assets in information processing in outsourced premises or by external personnel.		To be decided (Mapping exists)	No gap	+	BCR-03, BCR-07, DCS-05	The CCM control leads to a higher security level as the requirement of C5 (exceeds).
C5-2016	RB-01	Safeguards for regular operations / Capacity management – planning	The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid capacity bottlenecks. The procedures include forecasts of future capacity requirements in order to identify use trends and master system overload risks.		Infrastructure & Virtualization Security	No gap	0	IVS-04	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	RB-02	Safeguards for regular operations / Capacity management – monitoring	Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the cloud provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.		To be decided (Mapping exists)	Partial gap		IVS-04, STA-03	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	RB-03	Safeguards for regular operations / Capacity management – data location	The cloud customer is able to determine the locations (city/country) of the data processing and storage including data backups.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document. Supplementary information for the basic requirement: This requirement supplements requirement UP-02 in which the locations are to be documented. If a cloud provider renders their services at several sites, this requirement demands the cloud provider to define precisely at which site the service is rendered and the data processed.
C5-2016	RB-04	Safeguards for regular operations / Capacity management – control of resources	In case of IaaS/PaaS, the cloud customer is able to control and monitor the distribution of the system resources assigned to them for administration/use (e. g. computing capacity or storage capacity) in order to prevent resources from being congested.		Infrastructure & Virtualization Security	No gap		IVS-04	
C5-2016	RB-05	Safeguards for regular operations / Protection against malware	The logical and physical IT systems which the cloud provider uses for the development and rendering of the cloud service as well as the network perimeters which are subject to the cloud provider's area of responsibility are equipped with anti-virus protection and repair programs which allow for a signature- and		Threat and Vulnerability Management	Partial gap		TVM-01	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			behaviour-based detection and removal of malware. The programs are updated according to the contractual agreements concluded with the manufacturer(s), but at least once a day.						
C5-2016	RB-06	Safeguards for regular operations / Data backup and restoration – concept	Policies and instructions with technical and organisational safeguards in order to avoid losing data are documented, communicated and provided according to SA-01. They provide reliable procedures for the regular backup (backup as well as snapshots, where applicable) and restoration of data. The scope, frequency and duration of the retention comply with the contractual agreements concluded with the cloud customers as well as the cloud provider's business requirements. Access to the data backed up is limited to authorised personnel. Restoration procedures include control mechanisms that ensure that restorations are carried out only after they have been approved by persons authorised to do so according to the contractual agreements with the cloud customers or the internal policies of the cloud provider.		Business Continuity Management & Operational Resilience	No gap	0	BCR-11	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	RB-07	Safeguards for regular operations / Data backup and restoration – monitoring	The process of backing up data is monitored by means of technical and organisational safeguards. Malfunctions are examined and eliminated promptly by qualified employees in order to ensure compliance with the contractual duties towards the cloud customers or the		Business Continuity Management & Operational Resilience	Partial gap		BCR-11	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			cloud provider's business requirements with respect to the scope, frequency and duration of the retention.						
C5-2016	RB-08	Safeguards for regular operations / Data backup and restoration - regular tests	Backup media and restoration procedures must be tested with dedicated test media by qualified employees at regular intervals. The tests are designed in such a way that the reliability of the backup media and the restoration time can be audited with sufficient certainty. The tests are carried out by qualified employees and the results documented comprehensibly. Any occurring errors are eliminated in a timely manner.		Business Continuity Management & Operational Resilience	Partial gap		BCR-11	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	RB-09	Safeguards for regular operations / Data backup and restoration – storage	The data to be backed up is transmitted to a remote site (e. g. another data centre of the cloud provider) or transported to a remote site on backup media. If the backup of the data is transmitted to the remote site via a network, this is carried out in an encrypted form that conforms to the state of the art. The distance to the main site should be large enough to ensure that catastrophes there do not lead to a loss of data at the remote site and, at the same time, short enough to be able to fulfill the contractual duties regarding the restoration times. The safeguards taken to ensure the physical and environment-related security at the remote site corresponds to the level at the main site.		Business Continuity Management & Operational Resilience	Partial gap		BCR-05, BCR-11	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	RB-10	Safeguards for regular operations / Logging and monitoring – concept	Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to log events on all assets which are used for the development or operation of the cloud service and to store them in a central place. The logging includes defined events which may impair the security and availability of the cloud service, including logging the activation, stopping and pausing of different logs. In case of unexpected or unusual events, the logs are checked by authorised personnel due to special events in order to allow for a timely examination of malfunctions and security incidents as well as for the initiation of suitable safeguards.		Infrastructure & Virtualization Security	No gap	0	IVS-01	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	RB-11	Safeguards for regular operations / Logging and monitoring – meta data	Policies and instructions with technical and organisational safeguards for the secure handling of meta data (user data) are documented, communicated and provided according to SA-01. The meta data is collected and used only for accounting and billing purposes, for eliminating malfunctions and errors (incident management) as well as for processing security incidents (security incident management). The meta data is not used for commercial purposes. Meta data must be deleted immediately once it is no longer required to fulfill the legitimate purpose		Infrastructure & Virtualization Security	Partial gap		IVS-01	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			according to this requirement. The period of time during which meta data is retained is determined by the cloud provider. It is reasonably related to the purposes pursued with the collection of meta data.						
C5-2016	RB-12	Safeguards for regular operations / Logging and monitoring - critical assets	The cloud provider maintains a list of all assets critical in terms of logging and monitoring and reviews this list for their currency and correctness at regular intervals. For these critical assets, advanced logging and monitoring safeguards were defined.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document.
C5-2016	RB-13	Safeguards for regular operations / Logging and monitoring – storage of the logs	The generated logs are stored on central logging servers on which they are protected against unauthorised access and changes. Logged data must be deleted immediately once they are no longer required to fulfill the purpose. Authentication takes place between the logging servers and the logged assets in order to protect the integrity and authenticity of the transmitted and stored information. The transmission is encrypted that conforms to the state of the art or via a separate administration network (out-of-band management).		To be decided (Mapping exists)	Partial gap		IVS-01, IAM-01	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	RB-14	Safeguards for regular operations / Logging and monitoring – accountability	The generated logs allow for a clear identification of user access to the tenant level in order to support (forensic) analyses in the case of a security incident.		Infrastructure & Virtualization Security	No gap	0	IVS-01	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	RB-15	Safeguards for regular operations / Logging and monitoring – configuration	The access and management of the logging and monitoring functionalities is limited to selected and authorised employees of the cloud provider. Changes to the logging and monitoring are checked by independent and authorised employees and approved beforehand.		Infrastructure & Virtualization Security	Partial gap		IVS-01	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	RB-16	Safeguards for regular operations / Logging and monitoring – availability of the monitoring software	The availability of the logging and monitoring software is monitored independently. In case the logging and monitoring software fails, the responsible employees are informed immediately.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document.
C5-2016	RB-17	Safeguards for regular operations / Handling of vulnerabilities, malfunctions and errors – concept	Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to ensure the prompt identification and addressing of vulnerabilities over all levels of the cloud service, for which they are responsible. The safeguards include among other things: • Regular identification and analysis of vulnerabilities, • Regular follow-up of safeguards in order to address identified safeguards (e. g. installation of security updates according to internal target specifications).		To be decided (Mapping exists)	No gap	0	TVM-02, AIS-01, GRM-10	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	RB-18	Safeguards for regular operations / Handling of vulnerabilities, malfunctions and errors – penetration tests	The cloud provider has penetration tests performed by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to documented test methods and include the infrastructure components defined to be critical to the secure operation of the cloud service, which were identified as such as part of a risk analysis. Type, scope, time/period of time and results are documented comprehensibly for an independent third party. Determinations from the penetration tests are assessed and, in case of medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, followed up and remedied. The assessment of the criticality and the mitigating safeguards for the individual determinations are documented.		Threat and Vulnerability Management	No gap	0	TVM-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	RB-19	Safeguards for regular operations / Handling of vulnerabilities, malfunctions and errors – integration with change and incident management	Policies and instructions with technical and organisational safeguards for the handling of critical vulnerabilities are documented, communicated and provided according to SA-01. The safeguards are coordinated with the activities of the change management and the incident management.		To be decided (Mapping exists)	No gap	0	CCC-03, TVM-02	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	RB-20	Safeguards for regular operations / Handling of vulnerabilities, malfunctions and errors – involvement of the cloud customer	The cloud customer is informed by the cloud provider of the status of the incidents affecting them in a regular and an appropriate form that corresponds to the contractual agreements or is involved into corresponding remedial actions. As soon as an incident was remedied from the cloud provider's point of view, the cloud customer is informed of the safeguards taken. This information is sufficiently detailed so that the cloud customer can use it in their security management.		To be decided (Mapping exists)	No gap	0	CCC-03, TVM-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	RB-21	Safeguards for regular operations / Handling of vulnerabilities, malfunctions and errors – check of open vulnerabilities	The IT systems which the cloud provider uses for the development and rendering of the cloud service are checked automatically for known vulnerabilities at least once a month. In the event of deviations from the expected configurations (for example, the expected patch level), the reasons for this are analysed in a timely manner and the deviations remedied or documented according to the exception process (see SA-03).		Threat and Vulnerability Management	Partial gap		TVM-02	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	RB-22	Safeguards for regular operations / Handling of vulnerabilities, malfunctions and errors –	System components which are used for the rendering of the cloud service are hardened according to generally established and accepted industry standards. The hardening instructions used are documented as well as the implementation status.		Infrastructure & Virtualization Security	No gap	0	IVS-07	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		system hardening							
C5-2016	RB-23	Safeguards for regular operations / Segregation of stored and processed data of the cloud customers in jointly used resources	Data is separated securely and strictly on jointly used virtual and physical resources (storage network, memory) according to a documented concept in order to guarantee the confidentiality and integrity of the stored and processed data.		Infrastructure & Virtualization Security	No gap	0	IVS-09	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	IDM-01	Identity and access management / Policy for system and data access authorisations	A role and rights concept based on the business and security requirements of the cloud provider as well as a policy for the management of system and data access authorisations are documented, communicated and provided according to SA-01 and address the following areas: • Granting and change (provisioning) of data access authorisations on the basis of the "least-privilege principle") and as is necessary for performing the required tasks ("need-to-know principle"), • Separation of functions between operative and controlling functions (also referred to as "separation of duties"), • Separation of functions in the administration of roles, approval and granting of data access		Identity & Access Management	No gap	+	IAM-02	The CCM control leads to a higher security level as the requirement of C5 (exceeds).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			authorisations, • Regular review of granted authorisations, • Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship, • Requirements for the approval and documentation of the management of system and data access authorisations.						
C5-2016	IDM-02	Identity and access management / User registration	System access authorisations for users under the responsibility of the cloud provider (internal and external employees) are granted in a formal procedure. Organisational and/or technical safeguards make sure that unique user IDs which clearly identify each user are granted.		Identity & Access Management	No gap	0	IAM-09	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	IDM-03	Identity and access management / Granting and change (provisioning) of data access authorisations	Granting and change of data access authorisations for users under the responsibility of the cloud provider comply with the policy for the management of system and data access authorisations. Organisational and/or technical safeguards make sure that the granted access authorisations meet the following requirements: • Data access authorisations comply with the "least- Privilege principle"). • When granting data access authorisations, only access authorisations necessary to perform the corresponding tasks should be granted ("need-toknow principle"). • Formal approval is given by an authorised person, before the data access authorisations		Identity & Access Management	Partial gap		IAM-05, IAM-09, IAM-11	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			are set up (i. e. before the user can access data of the cloud customers or components of the shared IT infrastructure) • Technically assigned data access authorisations which do not exceed the formal approval.						
C5-2016	IDM-04	Identity and access management / Withdrawal of authorisations (deprovisioning) in case of changes to the employment relationship	Data access authorisations of users under the cloud provider's responsibility (internal and external employees) are withdrawn in the case of changes to the employment relationship (dismissal, transfer, longer period of absence/sabbatical/parental leave) promptly, but 30 days after its coming into force at the latest and/or suspended temporarily. Any access is deactivated completely as soon as the employment relationship has expired.		Identity & Access Management	No gap	0	IAM-11	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	IDM-05	Identity and access management / Regular review of data access authorisations	Data access authorisations of users under the cloud provider's responsibility (internal and external employees) are reviewed at least once a year in order to adjust them promptly to changes to the employment relationship (dismissal, transfer, longer period of absence/sabbatical/parental leave). The review is performed by persons authorised to do so from corresponding part of the cloud provider, who are able to review the appropriateness of the granted authorisations due to their knowledge of the responsibilities. The review as well as the adjustments to the authorisations are documented comprehensibly.		Identity & Access Management	No gap	0	IAM-10	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	IDM-06	Identity and access management / Administrator authorisations	Granting and change of data access authorisations for internal and external users with administrative or extensive authorisations under the responsibility of the cloud provider comply with the policy or the management of system and data access authorisations (see IDM-01) or a separate policy. The authorisations are granted in a personalised manner and as is necessary for performing the corresponding tasks ("need-to-know principle"). Organisational and/or technical safeguards make sure that granting these authorisations does not result in undesired, critical combinations which violate the principle of the separation of duties (e. g. assigning authorisations for the administration		To be decided (Mapping exists)	Partial gap		IAM-02, IAM-05, IAM-08, IAM-10, IVS-11	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			of both the database and the operating system). If this is not possible in certain selected cases, appropriate, compensating controls are established in order to identify any misuse of these authorisations (e. g. logging and monitoring by an SIEM (security information and event management) solution).						
C5-2016	IDM-07	Identity and access management / Nondisclosure of authentication information	Secret authentication credentials (e. g. passwords, certificates, security token) is assigned to internal and external users of the cloud provider or cloud customer, provided that this is subject to organisational or technical procedures of the cloud provider, in a proper organised procedure which ensures the confidentiality of the information. If it is assigned initially, it is valid only temporarily, but not longer than 14 days. Moreover, users are forced to change it when using it for the first time. Access of the cloud provider to the authentication information of the cloud customer is strictly regulated, communicated		Identity & Access Management	No gap	0	IAM-12	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			with the cloud customer and only takes place if it is necessary to perform the corresponding tasks ("need-to-know principle"). Access is documented and reported to the cloud customer.						
C5-2016	IDM-08	Identity and access management / Secure login Methods	The confidentiality of the login information of internal and external users under the cloud provider's responsibility is protected by the following safeguards: • Identity check by trusted procedures, • Use of recognised industry standards for the authentication and authorisation (e. g. multifactor authentication, no use of jointly used authentication information, automatic expiry). • Multi-factor authentication for administrators of the cloud provider (e. g. using a smart card or biometric characteristics) is absolutely necessary.		Identity & Access Management	No gap	0	IAM-12	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	IDM-09	Identity and access management / Handling of emergency users	The use of emergency users (for activities which cannot be carried out with personalised, administrative users, see (IDM-06) is documented, to be justified and requires the approval by an authorised person, which takes the principle of the separation of functions into account. The emergency user is only activated as long as it is necessary to perform the corresponding tasks.		Identity & Access Management	Partial gap		IAM-13, IAM-02	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	IDM-10	Identity and access management / System-side access control	Access to information and application functions is limited by technical safeguards with which the role and rights concept is implemented.		Application & Interface Security	No gap	+	AIS-01, AIS-03, AIS-04	The CCM control leads to a higher security level as the requirement of C5 (exceeds).
C5-2016	IDM-11	Identity and access management / Password requirements and validation parameters	Security parameters on the network, operating system (host and guest), database and application level (where relevant to the cloud service) are configured appropriately to avoid unauthorised access. If no two-factor authentication or use of one-time passwords is possible, the use of secure passwords on all levels and devices (including mobile devices) under the cloud provider's responsibility is forced technically or must be ensured organisationally in a password policy. The targets must at least meet the following requirements: • Minimum password length of 8 characters, • At least two of the following character types must be included: Capital letters, minor letters,		Identity & Access Management	Partial gap		IAM-12	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			special characters and numbers, • Maximum validity of 90 days, minimum validity of 1 day • Password history of 6 • Transmission and storage of the passwords in an encrypted procedure that conforms to the state of the art.						
C5-2016	IDM-12	Identity and access management / Restriction and control of administrative software	The use of service programs and management consoles (e. g. for the management of the hypervisor or virtual machines), which allow extensive access to the data of the cloud customers, is restricted to authorised persons. Granting and changes to corresponding data access authorisations comply with the policy for the management of system and data access authorisations. Access is controlled by means of strong authentication techniques, including multi-factor authentication (see KOS-06).		To be decided (Mapping exists)	No gap	0	IAM-13, IVS-11	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	IDM-13	Identity and access management / Control of access to source code	Access to the source code and supplementary information that is relevant to the development of the cloud service (e. g. architecture documentation, test plans) is granted restrictively and monitored in order to prevent unauthorised functions from being introduced and unintended changes from being made.		Identity & Access Management	No gap	0	IAM-05, IAM-06	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	KRY-01	Cryptography and key management / Policy for the use of encryption procedures and key management	Policies and instructions with technical and organisational safeguards for encryption procedures and key management are documented, communicated and provided according to SA-01, in which the following aspects are described: • Using strong encryption procedures (e. g. AES) and the use of secure network protocols that correspond to the state of the art (e. g. TLS, IPsec, SSH), • Risk-based regulations for the use of encryption which are compared to schemes for the classification of information and take the communication channel, type, strength and quality of the encryption into account, • Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys, • Taking the relevant legal and regulatory obligations and requirements into consideration.		Encryption & Key Management	Partial gap		EKM-01, EKM-02, EKM-03, EKM-04	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	KRY-02	Cryptography and key management / Encryption of data for transmission (transport encryption)	Procedures and technical safeguards for strong encryption and authentication for the transmission of data of the cloud customers (e. g. electronic messages transported via public networks) are established.		Encryption & Key Management	No gap	0	EKM-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	KRY-03	Cryptography and key management / Encryption of sensitive data for storage	Procedures and technical safeguards for the encryption of sensitive data of the cloud customers for the storage are established. Exceptions apply to data that cannot be encrypted for the rendering of the cloud service for functional reasons. The private keys used for encryption are known only to the customer according to applicable legal and regulatory obligations and requirements. Exceptions (e. g. use of a master key by the cloud provider) are based on a controlled procedure and must be agreed upon jointly with the cloud customer.		Encryption & Key Management	No gap	0	EKM-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	KRY-04	Cryptography and key management / Secure key management	Procedures and technical safeguards for secure key management include at least the following aspects: • Generation of keys for different cryptographic systems and applications, • Issuing and obtaining public-key certificates, • Provisioning and activation of the keys for customers and third parties involved, • Secure storage of own keys (not those of the		Encryption & Key Management	Partial gap		EKM-01, EKM-02	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			cloud customers or other third parties) including the description as to how authorised users are granted access, • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised, • Handling of compromised keys, • Withdrawal and deletion of keys, for example in the case of compromising or staff changes, • Storage of the keys of the cloud users not at the cloud provider (i. e. at the cloud user or a trusted third party).						
C5-2016	KOS-01	Communication security / Technical safeguards	Based on the results of a risk analysis carried out according to OIS-05, the cloud provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns (e. g. by MAC spoofing and ARP poisoning attacks) and/or Distributed Denialof- Service (DDoS) attacks.		Infrastructure & Virtualization Security	No gap	0	IVS-01, IVS-13	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	KOS-02	Communication security / Monitoring of connections	Physical and virtualised network environments are designed and configured in such a way that the connections between trusted and untrusted networks must be restricted and monitored. At defined intervals, it is reviewed whether the use of all services, logs and ports serve a real commercial purpose. In addition, the review also includes the justifications for compensating		Infrastructure & Virtualization Security	No gap	0	IVS-06	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			controls for the use of logs which are considered to be insecure.						
C5-2016	KOS-03	Communication security / Cross-network access	Each network perimeter is controlled by security gateways. The system access authorisation for crossnetwork access is based on a security assessment on the basis of the customer requirements.		Infrastructure & Virtualization Security	Partial gap		IVS-06	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	KOS-04	Communication security / Networks for administration	There are separate networks for the administrative management of the infrastructure and for the operation of management consoles, which are separated logically or physically by the network of the cloud customers and are protected against unauthorised access by means of multi-factor authentication (see IDM-17). Networks which are used for the purposes of the migration or the generation of virtual machines must also be separated physically or logically by other networks.		Infrastructure & Virtualization Security	No gap	0	IVS-10, IVS-11	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	KOS-05	Communication security / Segregation of data traffic in jointly used network environments	The data traffic in jointly used network environments is segregated according to documented concept for the logical segmentation between the cloud customers on the network level in order to guarantee the confidentiality and integrity of the data transmitted.		Infrastructure & Virtualization Security	No gap	0	IVS-09, IVS-10	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	KOS-06	Communication security / Documentation of the network topology	The architecture of the network is documented comprehensibly and currently (e. g. in the form of diagrams) in order to avoid errors in the management during live operation and ensure timely restoration according to the contractual duties in the event of damage. Different environments (e. g. administration network and shared network segments) and data flows become apparent from the documentation. Furthermore, the geographical locations, in which the data is stored, are specified.		Infrastructure & Virtualization Security	No gap	0	IVS-13	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	KOS-07	Communication security / Policies for data transmission	Policies and instructions with technical and organisational safeguards in order to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction (e. g. use of encryption) are documented, communicated and provided according to SA-01. The policy and instructions establish a reference to the classification of information (see AM-05).		To be decided (Mapping exists)	No gap	0	DSI-02, HRS-03, EKM-03, STA-05	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	KOS-08	Communication security / Confidentiality agreement	The non-disclosure or confidentiality agreements to be concluded with internal employees, external service providers and suppliers of the cloud provider are based on the requirements of the cloud provider in order to protect confidential data and business details. The requirements must be identified, documented and reviewed at regular intervals (at least once a year). If the review shows that the requirements have to be adjusted, new non-disclosure or confidentiality agreements are concluded with the internal employees, the external service providers and the suppliers of the cloud provider. The non-disclosure or confidentiality agreements must be signed by internal employees, external service providers or suppliers of the cloud provider prior to the start of the contract relationship and/or before access to data of the cloud users is granted.		To be decided (Mapping exists)	No gap	0	HRS-06, HRS-03, STA-05	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PI-01	Portability and interoperability / Use of public	APIs and industry standards In order to guarantee the interoperability of cloud services, data regarding documented input and output interfaces and in recognised industry standards (e. g. the Open Virtualization Format for virtual appliances) is available in order to support the communication between different components and the migration of applications.		Interoperability & Portability	No gap	0	IPY-01, IPY-95	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	PI-02	Portability and interoperability / Export of data	At the end of the contract, the cloud customer can request the data to which they are entitled according to the contractual framework conditions, from the cloud provider and receives them in processable electronic standard formats such as CSV or XML.		Interoperability & Portability	No gap	0	IPY-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PI-03	Portability and interoperability / Policy for the portability and interoperability	If no individual agreements between the cloud provider and cloud customer regulate the interoperability and portability of the data, policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to ensure the respective requirements and duties of the cloud customer.		Interoperability & Portability	No gap	0	IPY-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PI-04	Portability and interoperability / Secure data import and export	The cloud provider uses secure network protocols for the import and export of information as well as for the management of the service in order to ensure the integrity, confidentiality and availability of the transported data.		Interoperability & Portability	No gap	0	IPY-04	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	PI-05	Portability and interoperability / Secure deletion of data	Both when changing the storage media for maintenance purposes and upon request of the cloud customer or the termination of the contract relationship, the content data of the cloud customer, including the data backups and the meta data (as soon as they are no longer required for the proper documentation of the accounting and billing), is deleted completely. The methods used for this (e. g. by overwriting data several times, deletion of the key) prevent		Data Security & Information Lifecycle Management	No gap	0	DSI-07	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			the data from being restored via forensic methods.						
C5-2016	BEI-01	Procurement, development and maintenance of information systems / Policies for the development / procurement of information systems	Policies and instructions with technical and organisational safeguards for the proper development and/or procurement of information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01. The policies and instructions describe at least the following aspects: • Security in software development methods in compliance with security standards established in the industry (e. g. OWASP for web applications), • Security of the development environment (e. g. separate development/test/production environments), • Programming policies for each programming language used (e. g. regarding buffer overflows, hiding internal object references towards users), • Security in version control.		To be decided (Mapping exists)	No gap	0	CCC-01, GRM-01, AIS-01	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	BEI-02	Procurement, development and maintenance of information systems / Outsourcing of the development	If the development of the cloud service (or parts thereof) is outsourced regarding the design, development, test and/or provision of source code of the cloud service, a high level of security is required. Therefore, at least the following aspects must be agreed upon contractually between the cloud provider and external service providers: • Requirements for a secure software development process (especially design, development and testing) • Provision of evidence demonstrating that adequate testing was carried out by the external service provider • Acceptance test of the quality of the services rendered according to the functional and nonfunctional requirements agreed upon • The right to subject the development process and controls to testing, also on a random basis		Change Control & Configuration Management	No gap	0	CCC-02	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	BEI-03	Procurement, development and maintenance of information systems / Policies for changes to information systems	Policies and instructions with technical and organisational safeguards for the proper management of changes to information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01. At least the following aspects are to be taken into account in this respect: • Criteria for the classification and prioritisation of changes and related requirements for the type and scope of tests to be carried out and permits to be obtained, • Requirements for the notification of affected cloud customers according to the contractual agreements, • Requirements for the documentation of tests as well as for the application and permit of changes, • Requirements for the documentation of changes to the system, operating and user documentation.		Change Control & Configuration Management	No gap	0	CCC-05	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	BEI-04	Procurement, development and maintenance of information systems / Risk	The principal of a change performs a risk assessment beforehand. All configuration objects which might be affected by the change are assessed with regard to potential impacts. The result of the risk assessment is documented appropriately and comprehensively.		Change Control & Configuration Management	Partial gap		CCC-05	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		assessment of changes							
C5-2016	BEI-05	Procurement, development and maintenance of information systems / Categorisation of changes	All changes are categorised on the basis of a risk assessment (e. g. as insignificant, significant or farreaching impacts) in order to obtain an appropriate authorisation prior to making the change available to the production environment.		Change Control & Configuration Management	Partial gap		CCC-05	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	BEI-06	Procurement, development and maintenance of information systems / Prioritisation of changes	All changes are prioritised on the basis of a risk assessment (e. g. as low, normal, high, emergency) in order to obtain an appropriate authorisation prior to making the change available to the production environment.		Change Control & Configuration Management	Partial gap		CCC-05	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	BEI-07	Procurement, development and maintenance of information systems /	All changes to the cloud service are subjected to tests (e. g. for integration, regression, security and user acceptance) during the development and before they are made available to the production environment. The tests are carried out by adequately qualified personnel of the cloud provider. According to the service level		Change Control & Configuration Management	No gap	+	CCC-03, CCC-05	The CCM control leads to a higher security level as the requirement of C5 (exceeds).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		Testing changes	agreement (SLA), changes are also tested by the customers (tenants) suitable for this.						
C5-2016	BEI-08	Procurement, development and maintenance of information systems / Rollback of changes	Processes are defined in order to be able to roll back required changes as a result of errors or security concerns and restore affected systems or services into its previous state.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document.
C5-2016	BEI-09	Procurement, development and maintenance of information systems / Review of proper testing and approval	Before a change is released to the production environment, it must be reviewed by an authorised body or a corresponding committee whether the planned tests have been completed successfully and the required approvals are granted.		Change Control & Configuration Management	No gap	0	CCC-05	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	BEI-10	Procurement, development and maintenance of information systems / Emergency changes	Emergency changes are to be classified as such by the change manager who creates the change documentation before applying the change to the production environment. Afterwards (e. g. within 5 working days), the change manager supplements the change documentation with a justification and the result of the application of the emergency change. This justification must show why the regular change process could not have been run through and what the consequences of a delay resulting from compliance with the regular process would have been. The change documentation is forwarded to the customers concerned and a subsequent release by authorised bodies is obtained according to the contractual agreements.		To be decided (No mapping)	Full gap			n/a - Not applicable, according to the source document.
C5-2016	BEI-11	Procurement, development and maintenance of information systems / System landscape	Production environments are separated physically or logically by non-production environments in order to avoid unauthorised access or changes to the production data. Production data is not replicated in test or development environments in order to maintain their confidentiality.		To be decided (Mapping exists)	No gap	0	DSI-05, IVS-08	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	BEI-12	Procurement, development and maintenance of information systems / Separation of functions	Change management procedures include role-based authorisations in order to ensure an appropriate separation of duties regarding the development, release and migration of changes between the environments.		Identity & Access Management	No gap	0	IAM-05	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	DLL-01	Control and monitoring of service providers and suppliers / Policies for the handling of and security requirements for service providers and suppliers of the cloud provider	Policies and instructions for ensuring the protection of information accessed by other third parties (e. g. service providers and/or suppliers of the cloud provider), who contribute significant parts to the development or operation of the cloud service, are documented, communicated and provided according to SA-01. The corresponding controls are used to mitigate risks which may result from the potential access to information of the cloud customers. The following aspects are at least to be taken into account for this: • Definition and description of minimum security requirements with regard to the information processed, which are based on recognised industry standards such as ISO/IEC 27001, • Legal and regulatory requirements, including data protection, intellectual property right, copyright, handling of meta data (see RB-11) as well as a description as to how they are ensured		Supply Chain Management, Transparency, and Accountability	No gap	+	STA-04, STA-05, STA-09	The CCM control leads to a higher security level as the requirement of C5 (exceeds).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			(e. g. site of data processing and liability, see surrounding parameters for transparency), • Requirements for incident and vulnerability management (especially notifications and collaborations when eliminating malfunctions), • Disclosure and contractual obligation to the minimum security requirements also to subcontractors if they do not only contribute insignificant parts to the development or operation of the cloud service (e. g. service provider of the computing centre). The definition of the requirements is integrated into the risk management of the cloud provider. According to requirement OIS-07, they are checked at regular intervals for their appropriateness.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	DLL-02	Control and monitoring of service providers and suppliers / Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider	Procedures for the regular monitoring and review of agreed services and security requirements of third parties (e.g. service providers and/or suppliers of the cloud provider) who contribute essential parts to the development or operation of the cloud service are established. The safeguards include at least the following aspects: • Regular review of service reports (e. g. SLA reports) if they are provided by third parties, • Review of security-relevant incidents, operational disruptions or failures and interruptions that are related to the service, • Unscheduled reviews after essential changes to the requirements or environment. The essentiality must be assessed by the cloud provider and documented comprehensibly for audits. Identified deviations are subjected to a risk analysis according to requirement OIS-07 in order to effectively address them by mitigating safeguards in a timely manner.		Supply Chain Management, Transparency, and Accountability	No gap	0	STA-02, STA-04, STA-07, STA-08	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	SIM-01	Security incident management / Responsibilities and procedural model	Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to ensure a fast, effective and proper response to all known security incidents. On the part of the cloud provider, at least the roles listed in OIS-01 must be filled, requirements for the classification, prioritisation and escalation of security incidents defined and interfaces with the incident management and the business continuity management created. In addition to this, the cloud provider has established a "computer emergency response team" (CERT), which contributes to the coordinated solution of specific security incidents. Customers affected by security incidents are informed in a timely manner and appropriate form.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap	0	SEF-01, SEF-02, SEF-03, SEF-05	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	SIM-02	Security incident management / Classification of customer systems	All customer systems are classified according to the agreements (SLA) between the cloud provider and cloud customer regarding the criticality for the rendering of services. The assignment of classifications is reviewed regularly as well as after essential changes / events for all customer systems. Deviations are followed up and eliminated in a timely manner. Moreover, the classification shows which parameters regarding the recovery of a system were agreed upon with the cloud customer.		Data Security & Information Lifecycle Management	Partial gap		DSI-01	The CCM control leads to a lower scurity level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	SIM-03	Security incident management / Processing of security incidents	Events which could represent a security incident are classified, prioritised and subjected to a cause analysis by qualified personnel of the cloud provider or in connection with external security service providers.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap	0	SEF-01, SEF-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	SIM-04	Security incident management / Documentation and reporting of security incidents	After a security incident has been processed, the solution is documented according to the contractual agreements and the report is forwarded for final information or, if necessary, as confirmation to the customers affected.		To be decided (Mapping exists)	No gap	0	SEF-03, SEF-04, STA-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	SIM-05	Security incident management / Security incident event management	Logged incidents are centrally aggregated and consolidated (event correlation). Rules for identifying relations between incidents and assessing them according to their criticality are implemented. These incidents are handled according to the security incident management process.		To be decided (Mapping exists)	Partial gap		AIS-04, IVS-06, SEF-02	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	SIM-06	Security incident management / Duty of the users to report security incident to a central body	The employees and external business partners are informed of their duties. If necessary, they agree to or commit themselves contractually to promptly report all security events to a previously specified central body. Furthermore, information is provided that "incorrect notifications" of events which have not turned out to be incidents afterwards, do not have any negative consequences for the employees.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap	0	SEF-03	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	SIM-07	Security incident management / Evaluation and learning process	Mechanisms are in place to be able to measure and monitor the type and scope of the security incidents as well as to report them to supporting bodies. The information gained from the evaluation is used to identify recurring incidents or incidents involving significant consequences and to determine the need for advanced safeguards.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap	0	SEF-04, SEF-05	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	BCM-01	Business continuity management / Top management responsibility	The top management (and/or a member of the top management) is specified as the process owner of the business continuity and contingency management and bears the responsibility for the establishment of the process in the company and compliance with the policies. They must ensure that adequate resources are made available for an effective process. Members of the top management and persons in other relevant leadership positions demonstrate leadership and commitment with respect to this topic, for example by asking and/or encouraging the employees to actively contribute to the effectiveness of the business continuity and contingency management.		Business Continuity Management & Operational Resilience	No gap	0	BCR-09	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	BCM-02	Business continuity management / Business impact analysis policies and procedures	Policies and instructions for determining impacts of possible malfunctions of the cloud service or company are documented, communicated and provided according to SA-01. At least the following aspects are taken into consideration: • Possible scenarios based on a risk analysis (e.		Business Continuity Management & Operational Resilience	No gap	0	BCR-09	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			g. loss of personnel, failure of building, infrastructure and service providers), • Identification of critical products and services, • Identification of dependencies, including the processes (incl. the resources required for this), applications, business partners and third parties, • Identification of threats to critical products and services, • Determination of consequences resulting from planned and unplanned malfunctions and changes over time, • Determination of the maximum acceptable duration of malfunctions, • Determination of the priorities for the restoration, • Determination of time-limited targets for the recovery of critical products and services within the maximum acceptable period of time (recovery time objective, RTO); • Determination of time-limited targets for the maximum acceptable period of time during which data is lost and cannot be restored (recovery point objective, RPO); • Estimation of the resources required for recovery.						
C5-2016	BCM-03	Business continuity management / Planning	Based on the business impact analysis, a uniform framework for planning the business continuity and business plan is introduced, documented and applied in order to ensure		Business Continuity Management	No gap	0	BCR-01	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		business continuity	that all plans (e. g. of the different sites of the cloud provider) are consistent. The planning depends on established standards which is documented comprehensibly in a "statement of applicability". Business continuity plans and contingency plans take the following aspects into consideration: • Defined purpose and scope by taking the relevant dependencies into account, • Accessibility and comprehensibility of the plans for persons who have to take action in line with these plans, • Ownership by at least one appointed person who is responsible for review, updating and approval, • Defined communication channels, roles and responsibilities including the notification of the customer, • Restoration procedures, manual temporary solutions and reference information (by taking the prioritisation into account for the recovery of cloud infrastructure components and services as well as orienting to customers), • Methods used for the implementation of the plans, • Continuous improvement process of the plans, • Interfaces with the security incident management.		& Operational Resilience				

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	BCM-04	Business continuity management / Verification, updating and testing of the business continuity	The business impact analysis as well as the business continuity plans and contingency plans are verified, updated and tested at regular intervals (at least once a year) or after essential organisational or environment-related changes. The tests also involve affected customers (tenants) and relevant third parties (e. g. critical suppliers). The tests are documented and results are taken into account for future business continuity safeguards.		Business Continuity Management & Operational Resilience	No gap	0	BCR-02, BCR-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	BCM-05	Business continuity management / Supply of the computing centres	The supply of the computing centres (e. g. water, electricity, temperature and moisture control, telecommunications and Internet connection) is secured, monitored and is maintained and tested at regular intervals in order to guarantee continuous effectiveness. It has been designed with automatic fail-safe mechanisms and other redundancies. Maintenance is performed in compliance with the maintenance intervals and targets recommended by the suppliers as well as only by personnel authorised to do so. Maintenance protocols including any suspected or detected deficiencies are stored for the duration of the period of time previously agreed upon. After this period of time has expired, the maintenance protocols are destroyed properly and permanently		Business Continuity Management & Operational Resilience	No gap	0	BCR-03, BCR-07	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	SPN-01	Security check and verification / Notification of the top management	The top management is informed of the status of the information security on the basis of security checks by means of regular reports and is responsible for the prompt elimination of determinations resulting from them.		Governance and Risk Management	Partial gap		GRM-05	The CCM control leads to a lower scurity level as the requirement of C5.
C5-2016	SPN-02	Security check and verification / Internal audits of the compliance of IT processes with internal security policies and standards	Qualified personnel (e. g. internal revision) of the cloud provider or expert third parties commissioned by the cloud provider audit the compliance of the internal IT processes with the corresponding internal policies and standards as well as the legal, regulatory and statutory prescribed requirements relevant to the cloud service on an annual basis. The deviations identified are prioritised and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.		Governance and Risk Management	No gap	+	GRM-03, GRM-05	The CCM control leads to a higher security level as the requirement of C5 (exceeds).
C5-2016	SPN-03	Security check and verification / Internal audits of the compliance of IT systems with internal security policies and standards	At least on an annual basis, qualified personnel (e. g. internal revision) of the cloud provider or expert third parties commissioned by the cloud provider audit the compliance of the IT systems, provided that they are completely or partially in the cloud provider's area of responsibility and are relevant to the development or operation of the cloud service, with the corresponding internal policies and standards as well as the legal, regulatory and statutory prescribed requirements relevant to the cloud service. The deviations identified are prioritised and, depending on their criticality, safeguards for		Governance and Risk Management	No gap	0	GRM-01, GRM-04	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			their elimination are defined, followed up and implemented in a timely manner.						
C5-2016	COM-01	Compliance and data protection / COM-01 Identification of applicable legal, contractual and data protection requirements	Legally, regulatory and statutory prescribed requirements, as well as the procedure to comply with these requirements and regulations must be identified, documented and updated regularly by the cloud provider for the cloud service related to the respective application.		Audit Assurance & Compliance	No gap	0	AAC-03	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	COM-02	Compliance and data protection / Planning independent, external audits	Independent audits and assessments of systems or components which contribute to the rendering of the cloud services are planned by the cloud provider in such a way that the following requirements are met: • There is only read access to software and data. • Activities which might impair the availability of the systems or components and thus result in a violation of the SLA are carried out outside regular business hours and/or not at load peak times. • The activities performed are logged and monitored.		Audit Assurance & Compliance	No gap	0	AAC-01	The CCM control leads to an equivalent security level as the requirement of C5.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
C5-2016	COM-03	Compliance and data protection / Carrying out independent, external audits	Audits and assessments of processes, IT systems and IT components, provided that they are completely or partially in the cloud provider's area of responsibility and are relevant to the development or operation of the cloud service, are carried out by independent third parties (e. g. certified public auditor) at least once a year in order to identify non-conformities with legally, regulatory and statutory prescribed requirements. The deviations identified are prioritised and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.		Audit Assurance & Compliance	No gap	0	AAC-02	The CCM control leads to an equivalent security level as the requirement of C5.
C5-2016	MDM-01	Mobile device management / Policies and procedures for the risk minimisation of access via the cloud provider's mobile terminal devices	Policies and instructions with technical and organisational safeguards for the proper use of mobile terminal devices in the cloud provider's area of responsibility, which allow access to IT systems for the development and operation of the cloud service, are documented, communicated and provided according to SA-01. These policies and instructions include at least the following aspects, insofar as they are applicable to the cloud provider's situation: • Encryption of the devices and data transmission, • Increased access protection, • Extended identity and authorisation management, • Ban on jailbreaking/rooting,		To be decided (Mapping exists)	No gap	+	HRS-05, MOS-02, MOS-03, MOS-04, MOS-09, MOS-10, MOS-11, MOS-12, MOS-15, MOS-16, MOS-17, MOS-18	The CCM control leads to a higher security level as the requirement of C5 (exceeds).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			• Installation only of approved applications from "App Stores" classified as trusted, • Bring your own device (BYOD) minimum requirements for private terminal devices.						
CBK-02 / Build and Maintain a Secure Network and Systems	CBK-02-01	Requirement 1: Install and maintain a firewall configuration to protect cardholder data	All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.	Both	Infrastructure & Virtualization Security	No gap		IVS-06, IVS-09	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections Workshop: Partial Gap, there are more PCI-DSS controls
CBK-02 / Build and Maintain a Secure Network and Systems	CBK-02-02	Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.	Both	To be decided (Mapping exists)	No gap		IVS-07, TVM-02	Any component of the network (HW & SW) shall be hardened to provide only necessary access and logging, this baseline must have passed previous vulnerability checks which shall prevent the use of default passwords and settings. Workshop: Partial Gap, there are more PCI-DSS controls

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
CBK-02 / Build and Maintain a Secure Network and Systems	CBK-02-04	Requirement 4: Encrypt transmission of cardholder data across open, public networks	Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.	Both	Encryption & Key Management	No gap		EKM-03, EKM-04, EKM-02, DSI-03	The requirement asks for policies and procedures for the use of encryption protocols for protection of sensitive data during transmission, which is covered by control EKM-03 Workshop: DSI-03 valid as well. Partial Gap, there are more PCI-DSS controls
CBK-02 / Build and Maintain a Secure Network and Systems	CBK-02-06	Requirement 6: Develop and maintain secure systems and applications	Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.	Both	Threat and Vulnerability Management	Partial gap		TVM-02, GRM-10, IVS-05	It is also necessary to define policies and procedures to detect vulnerabilities and manage patch installations Workshop: Adding GRM-10, IVS-05 make for full coverage
CBK-02 / Implement Strong Access Control Measures	CBK-02-07	Requirement 7: Restrict access to cardholder data by business need to know	To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.	Both	Identity & Access Management	No gap		IAM-08, IAM-02, IAM-05	User Access Management has to be limited in accordance to the job responsibilities, granting the least amount of data and privileges to perform a task

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
CBK-02 / Implement Strong Access Control Measures	CBK-02-08	Requirement 8: Identify and authenticate access to system components	Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.	Both	Identity & Access Management	No gap		IAM-12, IAM-04, IAM-09	The requirement is mainly mapped with the IAM-12 CCM Matrix, although there are other sub requirements which should be mapped with other controls of the IAM domain, mainly IAM-04 and IAM-09.
CBK-02 / Maintain a Vulnerability Management Program	CBK-02-05	Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs	Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.	Security	Threat and Vulnerability Management	No gap		IVS-07	Policies and procedures shall be established to prevent the execution of malicious software. Workshop: IVS07 - MoSCoW - Shall is not enough in PCI-DSS - Partial Gap, there are more PCI-DSS controls

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
CBK-02 / Maintain a Vulnerability Management Program	CBK-02-09	Requirement 9: Restrict physical access to cardholder data	Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.	Both	Datacenter Security	No gap		DCS-09, DCS-08	
CBK-02 / Maintain an Information Security Policy	CBK-02-012	Requirement 12: Maintain a policy that addresses information security for all personnel.	A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.	Both	Governance and Risk Management	No gap		GRM-06, GRM-03, GRM-08	Necessity to define a security Policy with its procedures, awareness shall be maintained throughout the entire organization

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
CBK-02 / Protect Carholder Data.	CBK-02-03	Requirement 3: Protect stored cardholder data	Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.	Both	Encryption & Key Management	No gap		EKM-03, EKM-04, EKM-02	The requirement asks for policies and procedures for the use of encryption protocols for protection of sensitive data in storage or in use. protocols shall be based on standards, keys shall not be stored in the cloud but maintained by the Cloud customer or trusted key management provider Workshop: Partial Gap, there are more PCI-DSS controls
CBK-02 / Regularly Monitor and Test Networks	CBK-02-10	Requirement 10: Track and monitor all access to network resources and cardholder data	Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.	Both	Infrastructure & Virtualization Security	No gap		IVS-01	Requirements and control in relation with the necessity of Audit Logging

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
CBK-02 / Regularly Monitor and Test Networks	CBK-02-11	Requirement 11: Regularly test security systems and processes	Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.	Both	Change Control & Configuration Management	No gap		CCC-03	Continuous testing is mandatory to assure security level in terms of Confidentiality, Integrity and Availability. Workshop: Partial Gap, there are more PCI-DSS controls
ENISA_MSM _DSP	ENISA-R-01	SO 01 - Information security policy	Level 1 - Basic: - Set a high level security policy, which is aligned with business objectives and addresses the security and continuity of the communication networks and/or services provided. - Make key personnel aware of the security policy. Level 2 - Industry standard: - Set detailed information security policies for critical assets and business processes. - Make all personnel aware of the security policy and what it entails for their work. - Review the security policy following incidents. Level 3 - State of the art: Review the information security policies periodically, and take into account significant system changes, violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	Security	Governance and Risk Management	No gap		GRM-01, GRM-03, GRM-04, GRM-05, GRM-06, GRM-07, GRM-08, GRM-09	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-02	SO 02 – Risk Management	Level 1 - Basic: - Create a list of the main risks for security and continuity of the provided communication networks, systems or services, taking into account the main threats for critical assets. - Consider risks which stem from data protection or other sector-specific reg-ulations or policies into the risk assess-ments. - Make key personnel aware of the main risks and how they are mitigated. Level 2 - Industry standard: - Set up a risk management methodol-ogy and/or tools based on industry standards. - Ensure that key personnel use the risk management methodology and tools. - Review the risk assessments following changes, security incidents or data breaches. - Ensure residual risks are accepted by management. Level 3 - State of the art: Review the risk management methodology and/or tools, periodically, taking into ac-count changes and past incidents.	Security	To be decided (Mapping exists)	No gap		GRM-02, GRM-04, GRM-08, GRM-10, GRM-11, STA-01, STA-04, STA-04, STA-05, STA-06	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-03	SO 03 – Security Roles	Level 1 - Basic: - Assign security roles and responsibilities to personnel. - Make sure the security roles are reachable in case of security incidents. Level 2 - Industry standard: - Personnel is formally appointed in security roles - Make personnel aware of the security roles in your organization and when they should be contacted. Level 3 - State of the art: Structure of security roles and responsibilities is regularly reviewed and revised, based on changes and/or past incidents.	Security	To be decided (Mapping exists)	No gap		BCR-10, CCC-01, DSI-06, GRM-06, HRS-03, HRS-07, IAM-02, IAM-05, IAM-09, IAM-10, SEF-01, SEF-02, SEF-03	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.
ENISA_MSM _DSP	ENISA-R-04	SO 04 – Third party management	Level 1 - Basic: - Contractual agreements when dealing with third parties and customers have been established. - Include security requirements and relevant tasks in contracts with third-parties and customers. - Communicate residual risks which might affect the offered services to the customers. - Retain the right to perform second party audits where it is deemed nec-essary from a risk perspective. - Responsibilities regarding the maintenance, operation and ownership of assets have been defined.	Security	To be decided (Mapping exists)	No gap		CCC-02, STA-01, STA-02, STA-03, STA-04, STA-05, STA-05, STA-06, STA-07, STA-08, STA-09	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			Level 2 - Industry standard: - Set a security policy for contracts with third-parties. - Ensure that all procurement of services/products from third-parties follows the policy. - Review security policy for third parties, following incidents or changes. - Perform risk analysis before entering any outsourcing agreement. - Mitigate residual risks that are not addressed by the third party. Level 3 - State of the art: - Keep track of security incidents related to or caused by third-parties. - Periodically review and update policy for third parties and reevaluate outsourcing agreements at regular intervals, taking into account past in-cidents, changes, etc.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-05	SO 05 – Background checks	Level 1 - Basic: Check professional references of key personnel (system admin-istrators, security officers, guards, et cetera). Level 2 - Industry standard: - Perform background checks/screening for key personnel and external contractors, when needed and legally permitted. - Set up a policy and procedure for background checks. - Individuals screening criteria is established and reviewed for organization's position. Level 3 - State of the art: - Review and update policy/procedures for background checks and reference checks at regular intervals, taking into account changes and past incidents. - The screening process is in line with the defined policies and regulations. - Individuals are rescreened based on a defined list of conditions.	Security	Human Resources	No gap		HRS-02	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.
ENISA_MSM _DSP	ENISA-R-06	SO 06 – Security knowledge and training	Level 1 - Basic: - Regularly provide key personnel with relevant training and material on security issues. - Ensure that third parties are trained and aware of security issues Level 2 - Industry standard: - Implement a program for training, making sure that key personnel have sufficient and up-to-date security knowledge.	Security	Human Resources	No gap		HRS-08, HRS-09	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			- The program is approved by the management. - Organize trainings and awareness sessions for personnel on security topics important for the organization. Level 3 - State of the art: - Contents of security training are based on assigned roles and responsibilities and specific requirements of the organization and the infor-mation system to which personnel have authorized access. - Review and update the training program periodically, taking into account changes and past incidents. - Test the security knowledge of personnel. - Contacts and communication channels with security groups and associations have been established in order to stay up to date with the lat-est recommended security practices, techniques, and technologies. - Provide to the organization personnel training sessions to obtain recognized security certifications.					

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-07	SO 07 – Personnel changes	Level 1 - Basic: Following changes in personnel re-voke access rights, badges, equip-ment, et cetera, if no longer neces-sary or permitted. Brief and educate new personnel on the policies and procedures in place. Level 2 - Industry standard: - Implement policy/procedures for personnel changes, taking into ac-count timely revocation access rights, badges, equipment. - Implement policy/procedures for education and training for person-nel in new roles. Level 3 - State of the art: - Periodically check that the pol-icy/procedures are effective. - Review and evaluate policy/proce-dures for personnel changes, taking into account changes or past inci-dents. - Automated process review access permissions that are initiated by personnel changes.	Security	Human Resources	No gap		HRS-04	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-08	SO 08 – Physical and environmental security	Level 1 - Basic: - Prevent unauthorized physical access to facilities and infrastructure and set up environmental controls, to protect against unauthorized access, burglary, fire, flooding, etc. - A list of personnel with authorized access to facilities containing information systems and appropriate au-thorization credentials (e.g., badges, identification cards) is maintained by the organization. - Visitors are authenticated before authorizing access to the facility. - Data center environmental conditions (e.g., water, power, temperature and humidity controls) shall be secured, monitored, maintained, and tested to ensure protection from unauthorized interception or damage. Level 2 - Industry standard: - Implement a policy for physical security measures and environmental controls. - Document procedure for emergency cases - A designated official within the organisation to review and approve the list of personnel with authorized access has been identified. - Visitors are escorted as required according to security policies and procedures. - Visitor's access records to the facility are maintained by the organisa-tion. - The Physical access to the premises is	Security	Datacenter Security	No gap		DCS-01, DCS-02, DCS-03, DCS-03, DCS-04, DCS-05, DCS-06, DCS-07, DCS-08, DCS-09, DCS-10, DCS-11	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			monitored by the organisation. - Industry standard implementation of physical and environmental controls. Level 3 - State of the art: - Evaluate the effectiveness of physical and environmental controls periodically. - Review and update the policy for physical security measures and environmental controls taking into account changes and past incidents. - Physical access records are kept and stored in case of an audit or investigation. - Physical access records are retained as dictated by applicable regulations or based on an organization-defined period by approved policy. - Separate facilities into different zones according to their contents						
ENISA_MSM _DSP	ENISA-R-09	SO 09 – Security of supporting utilities	Level 1 - Basic: Ensure security of supplies, such as electric power, fuel or HVC. Level 2 - Industry standard: - Implement a policy for security of critical supplies, such as electrical power, fuel, etc. - Implement industry standard security measures to protect supplies and supporting facilities. Level 3 - State of the art: - Advanced security measures to protect supplies.	Security	To be decided (Mapping exists)	No gap		BCR	Mapping to CCM is NOT DEFINED in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016. Workshop: Partial Gap, it looks to be fully covered in CCM - BCR - xxx but not xfref'd in Enisa because of a different level of detail

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			- Review and update policy and procedures to secure supplies regularly, taking into account changes and past incidents.						
ENISA_MSM _DSP	ENISA-R-10	SO 10 – Access control to network and information systems	Level 1 - Basic: - Users and systems have unique ID's and are authenticated before accessing services or systems. - Implement (logical) access control mechanism for network and information systems to allow only authorized use. Level 2 - Industry standard: - Implement policy for protecting ac-cess to network and information systems, addressing for example roles, rights, responsibilities and procedures for assigning and revoking access rights. - Based on the results of risk analysis, choose the relevant authentication mechanisms which are deemed relevant to different types of access. - Monitor access to network and information systems, have a process for approving exceptions and regis-tering access violations. - Security functions are restricted to the least amount of users necessary to ensure the security of the information system. - Track and monitor privileged accounts by validating their creation, use of specific authentication meth-ods and regular reviews. - Segment information access within network	Security	Encryption & Key Management	No gap		EKM-01, EKM-02, EKM-03, EKM-04	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			and information systems based on security requirements. Level 3 - State of the art: - Evaluate the effectiveness of access control policies and procedures and implement cross checks on access control mechanisms. - Access control policy and access control mechanisms are reviewed and when needed revised. - Restrictions in the number of concurrent sessions are defined and implemented by the organization.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-11	SO 11 – Integrity of network components and information systems	Level 1 - Basic: - Make sure software of network and information systems is not tam-pered with or altered, for instance by using input controls. - Protect security critical data (like passwords, shared secrets, private keys, etc.) from being disclosed or tampered with. - Take measures against malicious software on (internal) network and information systems. Level 2 - Industry standard: - Implement industry standard security measures, providing defense-in-depth and protection against tampering and altering of systems. - The malware protection mechanisms are centrally managed. - There are mechanisms which prevent users from circumventing malware protection capabilities. - Spam protection mechanisms are employed at system entry points such as workstations, servers, or mobile computing devices on the network. Level 3 - State of the art: - Sophisticated controls to protect integrity of systems. - Evaluate and review the effectiveness of measures to protect integrity of systems.	Security	To be decided (Mapping exists)	No gap		AIS, TVM	Mapping to CCM is NOT DEFINED in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016. Workshop: Partial Gap, it's partly covered in CCM - AIS, TVS, - xxx But not xfref'd in Enisa - Spam protection is not in CCM

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-12	SO 12 – Operating procedures	Level 1 - Basic: Set up operational procedures and as-sign responsibilities for operation of critical systems. Level 2 - Industry standard: Implement a policy for operation of systems to make sure all critical systems are operated and managed in line with predefined procedures. Level 3 - State of the art: Review and update the policy/proce-dures for operation of critical systems, taking into account incidents and/or changes.	Security	To be decided (Mapping exists)	No gap			Mapping to CCM is NOT DEFINED in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016. Workshop: No full Gap, it's fully covered in CCM - in differtent domains - xxx and it contains user reqs But not xfref'd in Enisa because of level of detail
ENISA_MSM _DSP	ENISA-R-13	SO 13 – Change management	Level 1 - Basic: - Follow predefined procedures when making changes to critical systems, according to licensing agreements - Inform the customer of significant changes to critical systems which affect the offered services. Level 2 - Industry standard: - Implement and test policy/proce-dures for change management, to make sure that changes of critical systems are always done following a predefined way. - Document change management procedures, and record for each change the steps of the followed procedure. Level 3 - State of the art: Review and update change management	Security	Change Control & Configuration Management	No gap		CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, CCC-06	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			procedures regularly, taking into ac-count changes and past incidents.						
ENISA_MSM _DSP	ENISA-R-14	SO 14 – Asset management	Level 1 - Basic: - A secure baseline configuration of components and information systems is developed, documented and maintained. - Manage critical assets e.g. software, hardware, information and configurations of critical systems. Level 2 - Industry standard: Implement policy/procedures for asset management and configuration control. Level 3 - State of the art: - Review and update the asset management policy regularly, based on changes and past incidents. - Review regularly the list with config-urations and the list with critical assets based, based on	Security	To be decided (Mapping exists)	No gap		DSI-01, HRS-01	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016. Mapping is related to asset management and asset returns.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			changes and past incidents. - A secure baseline configuration for development and test environments is managed separately from the operational baseline configuration.						
ENISA_MSM _DSP	ENISA-R-15	SO 15 – Security incident detection & Response	Level 1 - Basic: - Set up processes or systems for incident detection and response. - Make sure personnel is available and prepared to manage and handle incidents. Level 2 - Industry standard: - Implement industry standard systems and procedures for incident detection and response. - Implement systems and procedures for registering and forwarding incidents timely to the appropriate people. Level 3 - State of the art: - Investigate major incidents and draft final incident reports, including actions taken and recommendations to mitigate and reduce time to react to any future occurrence of this type of incident or data breach. - Review systems and processes for incident detection and response regularly and update them taking into account changes and past incidents. - Regular cyber exercises and related results to test the incident response effectiveness are scheduled and documented.	Security	Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-03, SEF-04, SEF-05	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-16	SO 16 – Security incident reporting	Level 1 - Basic: - Communicate and report about on-going or past incidents to third parties, customers, and/or government authorities, when necessary. Level 2 - Industry standard: - Implement policy and procedures for communicating and reporting about inci-dents. Level 3 - State of the art: - Evaluate past communications and reporting about incidents. - Review and update the reporting and communication plans, based on changes or past incidents.	Security	Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-01, SEF-02, SEF-04	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.
ENISA_MSM _DSP	ENISA-R-17	SO 17 – Business continuity	Level 1 - Basic: - Implement a service continuity strategy for the com-munications networks and/or services provided. Level 2 - Industry standard: - Implement contingency plans for critical systems. - Monitor activation and execution of contingency plans, registering successful and failed recovery times. Level 3 - State of the art: - Review and revise service continuity strategy peri-odically. - Review and revise contingency plans, based on past incidents and changes. - The continuity of operations plan is tested and	Security	Business Continuity Management & Operational Resilience	No gap		BCR-01, BCR-02, BCR-03, BCR-04-BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			up-dated on a regular basis. - Personnel involved in the continuity operations plan are trained in their roles and responsibilities with respect to the information system and re-ceive refresher training on an organization-de-fined frequency.						
ENISA_MSM _DSP	ENISA-R-18	SO 18 – Disaster recovery capabilities	Level 1 - Basic: - Prepare for recovery and restoration of services following disasters. Level 2 - Industry standard: - Implement policy/procedures for deploying disaster recovery capabilities. - Implement industry standard disaster recovery capabilities or be assured they are available from third parties (such as national emergency networks). Level 3 - State of the art: - Advanced implementation controls for disaster recovery capabilities to mitigate natural and/major disasters. - Review and update disaster recovery capabilities regularly, taking into account changes, past incidents, and results of tests and exercises.	Security	Business Continuity Management & Operational Resilience	No gap		BCR-09, BCR-11	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-19	SO 19 – Monitoring and logging	Level 1 - Basic: - Implement monitoring and logging of critical systems. Level 2 - Industry standard: - Implement policy for logging and monitoring of critical systems. - Set up tools for monitoring critical systems. - Set up tools to collect and store logs critical sys-tems. Level 3 - State of the art: - Set up tools for automated collection and analysis of monitoring data and logs. - Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.	Security	Infrastructure & Virtualization Security	No gap		IVS-01	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-20	SO 20 – System tests	Level 1 - Basic: - Test networks and information systems before using them or connecting them to existing systems. - The installation or de-installation of patches is done in an ad hoc manner. Level 2 - Industry standard: - Implement policy/procedures for testing net-work and information systems. - Implement tools for automated testing. - The installation or de-installation of patches is done periodically in an organized manner. Level 3 - State of the art: - Review and update the policy/procedures for testing, taking into account changes and past incidents. - The installation or de-installation of patches is reviewed to ensure the adequately implementation of the defined actions. - Exceptions to defined actions and approved mitigating actions are identified and documented.	Security	To be decided (Mapping exists)	No gap		AIS-01, TVM-02, other domains	Mapping to CCM is NOT DEFINED in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016. Workshop: No full Gap, it's fully covered in ENISA and CCM - AIS-01, TVS-02 and other domains - xxx But not xfref'd in Enisa because of level of detail

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-21	SO 21 – Security assessments	Level 1 - Basic: - Ensure critical systems undergo security scans and security testing regularly, particularly when new systems are introduced and following changes. - Vulnerabilities are monitored and assessed. Level 2 - Industry standard: - Implement policy/procedures for security assessments and security testing. - A single point of contact and communication channels for information security related issues with manufacturers or vendors have been identified. Level 3 - State of the art: - Evaluate the effectiveness of policy/procedures for security assessments and security testing. - Review and update policy/procedures for security assessments and security testing, taking into account changes and past incidents. - Information obtained from the vulnerability scanning process is shared with designated personnel throughout the organization and authorities to help eliminate similar vulnerabilities in other information systems.	Security	Audit Assurance & Compliance	No gap		AAC-02	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-22	SO 22 – Compliance	Level 1 - Basic: - Monitor compliance to standards and legal requirements. Level 2 - Industry standard: - Implement policy/procedures for compliance monitoring and auditing. Level 3 - State of the art: - Evaluate the policy/procedures for compliance and auditing. - Perform deviation root cause analysis. - Build remediation plans for critical assets. - Review and update the policy/procedures for compliance and auditing, taking into account changes and past incidents.	Security	Audit Assurance & Compliance	No gap		AAC-01, AAC-02, AAC-03	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-23	SO 23 – Security of data at rest	Level 1 - Basic: - Identify the most critical data taking into account relevant business needs and legal obligations (e.g. with regard to the processing of personal data). - Retain the critical data for a certain period depending on the type of data and its criticality - Implement cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas and in transit when moving within and between com-pany data locations. - Implement cryptographic mechanisms such as digital signatures and hashes to detect unauthorized changes to critical data at rest. - Implement mechanisms for the secure disposal of the data after their lawful use. Level 2 - Industry standard: - Classify all data according to a classification scheme which takes into account data's value, legal requirements, sensitivity, and criticality to the organization. - Use of removable media is prohibited unless strictly required. - Ensure the confidentiality and integrity of data at rest according to the classification scheme. - Establish a policy around confidentiality and integrity of data at rest and make all personnel	Security	Data Security & Information Lifecycle Management	No gap		DSI-01, DSI-02, DSI-03, DSI-04, DSI-05, DSI-06, DSI-07	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			to whom it is relevant, are aware of the policy and procedure and what it implies for their work. - Set detailed cryptographic key establishment and management policies and procedures for data at rest (only if cryptography has been implemented). - A set of best practice procedures are in place for the secure disposal of physical assets. Level 3 - State of the art: - Classify all assets according to the classification scheme. - Implement information labelling and handling procedures in accordance with the classification scheme - The data retention policy considers the value of data over time and the data retention laws the organization may be subject to. - Strong controls are in place surrounding connection of media devices. - Use automated key management mechanisms. - Review of confidentiality and integrity of data at rest policy. - Disposal of assets at the most opportune time in line with company objectives, strategy and the data retention policy, using the most ap-propriate methods.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-24	SO 24 – Interface security	Level 1 - Basic: - Set a high level security policy for keeping the cloud and online market interfaces secure - Make key personnel aware of the security policy. - Enable secure channels for data transmission (e.g. TLS2.0) - Use unique identifiers to identify users Level 2 - Industry standard: - Set detailed security policies for data security to include protection of customer administration interfaces (TLS2.0, 2-Factor authentication) etc. - Make all personnel aware of the security policy and what it implies for their work. - Review the security policy following incidents. - Implement 2-Factor authentication Level 3 - State of the art: Review the security policy periodically, and take into account violations, exceptions, past incidents, past tests/exercises, and incidents affecting other (similar) providers in the sector.	Security	Application & Interface Security	No gap		AIS-01, AIS-02, AIS-03, AIS -04	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-25	SO 25 – Software security	Level 1 - Basic: - Establish guidelines for maintaining software security Level 2 - Industry standard: - Implement a defined set of security measures to secure development environments, including measures for protecting test data. - Depending on the type of requirement include software testing methods (e.g. black-box, ad-hoc testing). - Keep separated environments for development purposes, testing purposes and production. Level 3 - State of the art: - Security by design is tested at various stages of the SDLC prior to Go-live utilizing independent tools and a self-service testing platform throughout SDLC. - Results of application assessments are used to regularly enhance developer training and the SDLC process.	Security	Application & Interface Security	No gap		AIS -04	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ENISA_MSM _DSP	ENISA-R-26	SO 26 – Interoperability and portability	Level 1 - Basic: - Implement processes and procedures which allow customers to interact with services and/or if needed to migrate to other providers offering similar services, in an easy and basic way Level 2 - Industry standard: - Implement industry standard security measures, which promote interoperability and portability, in-cluding fall-back procedures (for example in the case of cloud computing services). Level 3 - State of the art: - Set up state of the art controls to facilitate interoperability & portability. - Evaluate and review the effectiveness of interoperability & portability measures.	Security	Interoperability & Portability	No gap		IPY-01, IPY-02, IPY-03, IPY-04, IPY-05	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.
ENISA_MSM _DSP	ENISA-R-27	SO 27 – Customer Monitoring and log access	Level 1 - Basic: - Separate the logging information between the different customers. - Implement monitoring and logging of customer data. Level 2 - Industry standard: - Implement policy for logging and monitoring of customer data depending on the type of service. - Set up tools for customer to monitor this data - Set up tools to collect and store logs of cus-tomer data. Level 3 - State of the art:	Security	Infrastructure & Virtualization Security	No gap		IVS-01	Mapping to CCM is defined in the input document Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA, 2016.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			- Set up tools for automated collection and analysis of monitoring data and logs. - Review and update logging and monitoring policy/procedures, taking into account changes and past incidents.						
ES-01 / National Security Scheme	ES-01-002	Art. 6: Security management based on risks	Risk analysis and management is considered as essential principle of security. All risk should be reduced to accepted level implementing security controls.	Security	Governance and Risk Management	No gap		BCR-05, DSI-02, GRM-02, GRM-08, GRM-10, GRM-11	All selected controls are relationed with risk management.
ES-01 / National Security Scheme	ES-01-005	Art. 9: Periodic re-evaluation	Security controls should be periodicaly analyzed for its effectivness.	Security	Governance and Risk Management	No gap		GRM-01, GRM-09, GRM-08, STA-08	Security controls review is managed by annual requirements review, controls update to mitigate risk analysis results, and information security policy revision in CCM.
ES-01 / National Security Scheme	ES-01-006	Art. 10: Security as differentiated function	Different roles and responsibilities should be defined for: Responsible for information, Responsible for service and Responsible for security.	Security	To be decided (No mapping)	Partial gap		No control proposed. Verification needed	Verification needed: Full or partial Gap. Conflict of interest needs to be managed by implementing separation of duties. The mentioned CCM controls don't cover this, although RGM-06 could cover (part of) it. Is prevention of CoI important? Ask Caixa Bank

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ES-01 / National Security Scheme	ES-01-009	Art. 13: Risk analysis and management	Each organization using information systems should do risk identification, assesment, analysis and treatmen using recognized technology. Controls to mitigate or eliminate the risk should be justified and adecuate to the level of risk.	Security	Governance and Risk Management	No gap		GRM-02, GRM-10, GRM-11, STA-06	Controls covers the requierements of risk assesment and treatment.
ES-01 / National Security Scheme	ES-01-010	Art. 14: Personel management	All eployees working with information should be trained about information security and aply all security processes established within the organization and defined by security norms. All information access should be relationed unequivocally to the user.	Security	Human Resources	No gap		HRS-09, HRS-10, IAM-12, GRM-03	
ES-01 / National Security Scheme	ES-01-011	Art. 15: Professionality	Systems security is managed, reviewed and audited by professionals with suficient experiency. Organizations providing security services to Public Administrations should assure that are providing secure and mature services.	Security	Human Resources	No gap		HRS-09, STA-09	
ES-01 / National Security Scheme	ES-01-012	Art. 16: Authorization and access control	Information systems access should be controled and limited to users, processes, dispositives and others information systems that are properly authorized, restricting acces only to allowed functions.	Security	Identity & Access Management	No gap		DCS-02, DCS-06, DCS-09, EKM-01, IAM-02, IAM-04, IAM-08, IAM-09, MOS-06, MOS-20	Identity & Access Management domain is selected, because access control is the principal objective of this domain.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ES-01 / National Security Scheme	ES-01-013	Art. 17: Protection of facilities	Information systems will be instaled in separated areas with an access control system and protocol. Areas should be closed and have some keys control.	Security	Datacenter Security	No gap		DCS-02, DCS-06, DCS-09, DCS-08	
ES-01 / National Security Scheme	ES-01-014	Art. 18: Acquisition of security products	Acquisition of information security products will give competitive advantage solution with widely recognized and/or international security certification.	Security	Governance and Risk Management	No gap		GRM-01	
ES-01 / National Security Scheme	ES-01-015	Art. 19: Defauls Security	The system will provide the minimum functionality required for the organization to only achieve its objectives, and does not achieve any additional functionality.	Security	Infrastructure & Virtualization Security	No gap		GRM-01, IAM-13, IVS-01, IVS-07, IVS-02, IVS-11, MOS-07, IAM-03	Infrastructure & Virtualization Security domain was selected, because minumum functionality is required.
ES-01 / National Security Scheme	ES-01-018	Art. 22: Prevention against other interconnected information systems	The system must protect the perimeter, in particular, if it connects to public networks. In any case, the risks arising from the interconnection of the system, through networks, with other systems will be analyzed and their point of attachment will be controlled.	Security	Infrastructure & Virtualization Security	No gap		IVS-09	
ES-01 / National Security Scheme	ES-01-019	Art. 23: Activity register	Public or labor function, and other provisions that are applicable, will record the activities of users, retaining the information necessary to monitor, analyze, investigate and document undue or unauthorized activities, allowing to identify at any time the person acting.	Security	Identity & Access Management	No gap		IVS-01, IAM-13, IAM-07, IAM-04, IAM-01	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ES-01 / National Security Scheme	ES-01-020	Art. 24: Security Incidents	A system of detection and reaction against harmful code will be established. The security incidents that occur and the treatment actions to be taken shall be recorded. These records will be used for the continuous improvement of system security.	Security	Security Incident Management, E-Discovery, & Cloud Forensics	No gap		STA-02, SEF-02, SEF-03, SEF-04, SEF-05, TVM-01, TVM-03	
ES-01 / National Security Scheme	ES-01-021	Art. 25: Business continuity	The systems will have backup copies and will establish the necessary mechanisms to guarantee the continuity of the operations, in case of loss of the habitual means of work.	Security	Business Continuity Management & Operational Resilience	No gap		BCR-01, BCR-03, BCR-11	
ES-01 / National Security Scheme	ES-01-022	Art. 26: Continuous improvement of the security process	The integrated security process implemented must be updated and continuously improved. To this end, the criteria and methods recognized in national and international practice relating to the management of information technologies will be applied.	Security	Governance and Risk Management	Partial gap		GRM-04	Missing control. Workshop: It looks to be covered in ISO27001 (control 10), GRM-04 in CCM should tackle it. But it may be defined in more detail, especially the PDCA cycle
ES-01 / National Security Scheme	ES-01-026	Art. 34: Security Audit	Information systems will be audited el least every 2 years to verify compliance with ENS.	Security	Audit Assurance & Compliance	No gap		AAC-01, AAC-02, AAC-03, STA-09, STA-04	Audit domain was slected beacause objective of the requierement is to audit ENS.
ES-01 / National Security Scheme	ES-01-029	Art. 40: Control Mecanisms	Each body of the Public Administration or Entity of Public Law will establish its control mechanisms to guarantee in a real and effective way the fulfillment of the National Security Scheme.	Security	Governance and Risk Management	No gap		AAC-03, GRM-03	Governance and Risk management domain was selected because establishment ot controls to

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									guarantee fulfillment of ENS is requested.
FAIT5 / 19	FAIT5-1	IT-outsourcing	The legal requirements including the guidelines for proper accounting (§239 Abs. 4 HGB) and the related security requirements for IT-based accounting also fully apply in the case of IT-outsourcing. Third party service providers shall also be compliant with those requirements.	Other	Supply Chain Management, Transparency, and Accountability	No gap		STA-08	This requirement is from the CSC's perspective, the CSP is addressed as the third party Workshop: No Gap. No responsibility of CSP
FAIT5 / 21	FAIT5-2	Compliant IT-based accounting.	The use of internet based communication and the including of third party service providers result in cloud computing specific risks. Those Risks requires the adherence of the security requirements regarding accounting data as a condition for a compliant IT-based accounting.	Other	Supply Chain Management, Transparency, and Accountability	No gap		STA-08	This requirement is from the CSC's perspective, the CSP is addressed as the third party Workshop: No Gap. No responsibility of CSP
FAIT5 / 67.1	FAIT5-3	Distribution of data	Cloud distributed data has to be defined and classified for cloud based usage. This requirement applies to the distribution model in general and the data location and processing location in particular.	Both	Data Security & Information Lifecycle Management	Partial gap		Verification needed	Verification needed: is it really a partial gap and what is it?
FAIT5 / 67.2	FAIT5-4	Encryption of Data	The encrypted transition and storage of data by suitable encryption technologies is required. IaaS empowers the user to assure encryption but in PaaS and IaaS the CSP has to ensure proper measures are in place	Both	Encryption & Key Management	No gap	-	EKM-03,GRM-01	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
FAIT5 / 82	FAIT5-5	Appropriate access control procedures	According to the security requirements both, the CSP and the CSC, have to determine and declare appropriate access control procedures. Those have to cover the whole architecture stack (network, server, storage, virtualization, databases, and applications).	Both	Data Security & Information Lifecycle Management	No gap	-	DCS-07	
FAIT5 / 83	FAIT5-6	Key management	The usage of data encryption technologies requires the CSC to ensure an effective key management. This includes key generation transportation and storage.	Both	Encryption & Key Management	No gap	-	EKM-02, EKM-04	
FAIT5 / 85	FAIT5-7	Trusted IT architecture	Highly confidential or sensitive data requires the usage of a trusted IT architecture. Such an architecture requires the separation of trusted networks from untrusted. Access to trusted Network has to be limited by an administrator. The proper implementation is subject for auditing's.	Both	Infrastructure & Virtualization Security	Partial gap		IVS-13	Verification needed: is it really a partial gap and what is it? Proposed control: IVS-13. Verification needed
FAIT5 / 86	FAIT5-8	Administrative privileges	Administrative or privileged access to the IT infrastructure has to be managed by the CSP or the CSC and secure usage has to be assured. This applies especially to the access to the Hypervisor and Storage Systems. Proper roll assignment are subject to audit.	Both	Datacenter Security	Partial gap		DCS-01	Verification needed: is it really a partial gap and what is it? Proposed control: DCS-01. Verification needed

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	4.1	4 Context of the organisation / 4.1	4.1 Understanding the organisation and its context: The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.	Security	To be decided (Mapping exists)	Partial gap		BCR-09, BCR-05, BCR-10, AAC-03, DSI-02, AIS-04.	CCM presents itself with a significant partial gap with respect to 4.1. Both AAC-03 and BCR-05 succeed in -partially- addressing the external context requirements of 4.1., while BCR-09 partially internal context requirements, other, DSI-02, BCR-10, AIS-04, address -partially- both internal & external contexts. GRM-01 (baseline security) could be excluded as seems to be an "a posteriori" requirement to risk management, while 4.1. addresses requirements "a priori" to risk management.
ISO27001	4.2	4 Context of the organisation / 4.2	4.2 Understanding the needs and expectations of interested parties: The organisation shall determine: a) interested parties that are relevant to the ISMS, and b) the requirements of these interested parties relevant to information security. (The requirements may include legal and regulatory requirements and contracatual obligations.)	Both	To be decided (Mapping exists)	No gap		AAC-03, STA-05	AAC-03 fully covers both GRM-01 and GRM-09 with regards to legal/regulatory requirements as well as of also 4.2. Also, GRM-01 (i.e., baseline security reqs...) and GRM-09 (i.e. review policy in compliance with...) do not seem to address explicitly an "determine/understand" requirement as that required of 4.2.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									The requirements may be related to security, privacy or other.
ISO27001	4.2(a)	4 Context of the organisation / 4.2(a)	4.2 Understanding the needs and expectations of interested parties: a) interested parties that are relevant to the information security management system		To be decided (Mapping exists)	No gap		AAC-03, STA-05	AAC-03 fully covers both GRM-01 and GRM-09 with regards to legal/regulatory requirements as well as of also 4.2. Also, GRM-01 (i.e., baseline security reqs...) and GRM-09 (i.e. review policy in compliance with...) do not seem to address explicitly an "determine/understand" requirement as that required of 4.2.
ISO27001	4.2(b)	4 Context of the organisation / 4.2(b)	4.2 Understanding the needs and expectations of interested parties: b) the requirements of these interested parties relevant to the information security		To be decided (Mapping exists)	No gap		AAC-03, STA-05	AAC-03 fully covers both GRM-01 and GRM-09 regarding both legal and/or regulatory requirements at this point in time, as well as 4.2. GRM-01 (Baseline Security requirements) and GRM-09 (Review Policy regarding GRC/Governance, Risk & Compliance) and does not address similar requirements within

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									paragraph 4.2, at this point in time.
ISO27001	4.3	4 Context of the organisation / 4.3	4.3 Determining the scope of the information security management system. The scope shall be available as documented information.		To be decided (Mapping exists)	Partial gap		BCR-01/-05/-09/-10, AAC-03, DSI-02, AIS-04, STA-05.	There is no explicit reference in CCM about having a documented scope for an ISMS. STA-05 and BCR-01, however include such documentation requirements targeting the scoping of business relationships, dependencies and business continuity in the context of information security and thus can be considered as subsets of an ISMS documented scope. GRM-04 and GRM-06 (policy reviews) have no explicit reference to a "scope" of an information security system, and could be excluded.
ISO27001	4.3(a)	4 Context of the organisation / 4.3(a)	4.3 Determining the scope of the information security management system: a) external and internal issues		To be decided (Mapping exists)	Partial gap		BCR-09, BCR-05, BCR-10, AAC-03, DSI-02, AIS-04.	The "partial gap" notation is due to the missing requirement of a documented ISMS scope.Includes the requirements of 4.1.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	4.3(b)	4 Context of the organisation / 4.3(b)	4.3 Determining the scope of the information security management system: b) requirements (referred to 4.2 - interested parties		To be decided (Mapping exists)	Partial gap		AAC-03, STA-05	The "partial gap" notation is due to the missing requirement of a documented ISMS (Information Security Management Systems) scope, since part b) is covered by "no gap" found at 4.2. Proposal to change the CCM control domain name: Please Note: Change the following: "Governance and Risk Management" to GRC (Governance, Risk and Compliance).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	4.3(c)	4 Context of the organisation / 4.3(c)	4.3 Determining the scope of the information security management system: c) interfaces and dependencies between activities (in organisation, other organisations)	Both	To be decided (Mapping exists)	Partial gap		BCR-01, STA-05	The "partial gap" notation is due to the missing requirement of a documented ISMS scope. There is some relevance to scoping and business relationships with these two controls. Determining the scope of the Information Security Management System implementation construct: c) Interfaces and/or inter-dependencies supporting mutual activities (between organisations) must be; addressed, analyzed, documented and resolved prior to initiating an Audit Engagement. Privacy (i.e., transfer agreements) Comment: questionable if partial gap should be used in this methodology? There is no 'partial gap'. We have a gap in coverage or we don't have a gap, as in a gap is a gap and neither the twain shall meet.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	4.4	4 Context of the organisation / 4.4	4.4 Information security management system: The organisation shall establish, implement, maintain, and continually improve an information security management system, in accordance with the requirements of this International Standard (ISO 27001).		Governance and Risk Management	Partial gap		GRM-04	Agreed is a partial gap since there is no explicit reference to an ISMS. Policy review (GRM-09) is not explicitly referenced in 4.4. Comment: All organisations are required to; establish, implement, monitor, maintain, and continually improve (on a regular basis) an ISMS, as spelled out in the ISO 27001 Standard.
ISO27001	5.1	5 Leadership / 5.1	5.1 Leadership and Commitment: Top management shall demonstrate leadership and commitment with respect to the information security mangement system.	Both	Governance and Risk Management	No gap		GRM-05	General CCM control that defines management commitment. To consider also other areas: - human factors - a term eventually used within the airline industry to explain the multiple causes leading to airline disasters and victims. In addition to the human factor, there was also: - complacency (knowing a job too well) - lack of knowledge, training - lack of resources - short cuts to meet deadlines, - and so on and so on.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									So, where is our emphasis on these factors impacting 'Leadership and Commitment'...?
ISO27001	5.1(a)	5 Leadership / 5.1(a)	5.1 Leadership and commitment: a) information security policy and objectives		Governance and Risk Management	No gap		GRM-06	
ISO27001	5.1(b)	5 Leadership / 5.1(b)	5.1 Leadership and commitment: b) integration of ISMS requirements in the organisation's processes		Governance and Risk Management	Partial gap		GRM-01, GRM-04	Maybe reconsider GRM-03? It refers to awareness and compliance (i.e., existing policies procedures) not processes integration. Partial gap due to the explicit reference of an ISMS integration in 5.1.(b), eventhough GRM-01 and GRM-04 cover some of the requirements of an ISMS, these CCM controls do not refer to an ISMS.
ISO27001	5.1(c)	5 Leadership / 5.1(c)	5.1 Leadership and commitment: c) available resources		Infrastructure & Virtualization Security	Partial gap		IVS-04	GRM-04 does not explicitly refers to resources availability. IVS-04 refers partially to such a requirement, but at system level not at management level.
ISO27001	5.1(d)	5 Leadership / 5.1(d)	5.1 Leadership and commitment: d) communication		Governance and Risk Management	No gap		GRM-04, GRM-05, GRM-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	5.1(e)	5 Leadership / 5.1(e)	5.1 Leadership and commitment: e) achieving outcome		Governance and Risk Management	No gap		GRM-05	
ISO27001	5.1(f)	5 Leadership / 5.1(f)	5.1 Leadership and commitment: f) contribution to ISMS		To be decided (Mapping exists)	No gap		GRM-04, GRM-05, HRS-09, HRS-10	
ISO27001	5.1(g)	5 Leadership / 5.1(g)	5.1 Leadership and commitment: g) continual improvement		Governance and Risk Management	No gap		GRM-01, GRM-09	
ISO27001	5.1(h)	5 Leadership / 5.1(h)	5.1 Leadership and commitment: h) supporting other management roles		To be decided (Mapping exists)	No gap		GRM-06, STA-06, BCR-01, BCR-10	
ISO27001	5.2	5 Leadership / 5.2	5.2 Policy: Top management shall establish an information security policy	Security	Governance and Risk Management	No gap		GRM-06, GRM-05	GRM-06: Information security policies must be authorized by the organization's business leadership. GRM-05: Executive and line management shall take formal action to support information security. Security (Privacy *should* be addressed but not the core of an ISMS)
ISO27001	5.2(a)	5 Leadership / 5.2(a)	5.2 Policy: Top management shall establish an information security policy that: a) is appropriate to the purpose of organisation		Governance and Risk Management	No gap		GRM-06	GRM-06: Information security policies must be authorized by the organization's business leadership and supported by a strategic business plan.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	5.2(b)	5 Leadership / 5.2(b)	5.2 Policy: Top management shall establish an information security policy hat: b) includes information security objectives or provides the framework for setting information security objectives		To be decided (Mapping exists)	No gap		GRM-04, GRM-08, AIS-04	
ISO27001	5.2(c)	5 Leadership / 5.2(c)	5.2 Policy: Top management shall establish an information security policy that: c) includes commitment to satisfy applicable requirements related to information security		To be decided (Mapping exists)	No gap		GRM-05, GRM-06, BCR-01	
ISO27001	5.2(d)	5 Leadership / 5.2(d)	5.2 Policy: Top management shall establish an information security policy that: d) includes a commitment to continual improvement of the information security management system		Governance and Risk Management	No gap		GRM-01, GRM-09	
ISO27001	5.2(e)	5 Leadership / 5.2(e)	5.2 Policy: The information security policy shall: e) be available as documented information		To be decided (Mapping exists)	No gap		GRM-04, GRM-06, DSI-07, BCR-01	
ISO27001	5.2(f)	5 Leadership / 5.2(f)	5.2 Policy: The information security policy shall: f) be communicated within organisation		Governance and Risk Management	No gap		GRM-06	
ISO27001	5.2(g)	5 Leadership / 5.2(g)	5.2 Policy: The information security policy shall: g) be available to interested parties, as appropriate		Governance and Risk Management	No gap		GRM-05, GRM-06	
ISO27001	5.3	5 Leadership / 5.3	5.3 Organisational roles, responsibilities and authorities: Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated.	Security	To be decided (Mapping exists)	No gap		GRM-03, GRM-05, GRM-06, HRS-07, HRS-10	Security (Privacy *should* be addressed but not the core of an ISMS)

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	5.3(a)	5 Leadership / 5.3(a)	5.3 Organisational roles, responsibilities and authorities: a) ensuring that ISMS conforms to this standard		Governance and Risk Management	Partial gap		GRM-05	
ISO27001	5.3(b)	5 Leadership / 5.3(b)	5.3 Organisational roles, responsibilities and authorities: b) reporting on the performance of ISMS to top management		Governance and Risk Management	Partial gap		GRM-09, GRM-10	A means of checking the performance is by reviewing policies and performing risk assessments, as defined in GRM-09 and GRM-10, nevertheless such requirement should be explicit in CCM.
ISO27001	6	6 Planning	6 Planning	Security	Governance and Risk Management	No gap		GRM-04	Information Security Management Program (ISMP). Security (Privacy *should* be addressed but not the core of an ISMS)
ISO27001	6.1.1	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.1	6.1.1 General: When planning for the ISMS, the organisation shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and detremine the risks and opportunities that need to be addressed.		To be decided (Mapping exists)	Partial gap		AAC-01, BCR-01, BCR-02, BCR-03, BCR-09, BCR-10, BCR-11, GRM-02, GRM-06, GRM-09, GRM-10, HRS-06, IAM-10,	Planning is provided in several CCM controls - for specific control domains.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
								IVS-04, STA-07	
ISO27001	6.1.1(a)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.1(a)	6.1.1 General: a) ensure the ISMS can achieve its intended outcome(s)		To be decided (Mapping exists)	No gap		GRM-04, GRM-06, BCR-10	
ISO27001	6.1.1(b)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.1(b)	6.1.1 General: b) prevent or reduce undesired effects		To be decided (Mapping exists)	No gap		GRM-02, GRM-04, AIS-04	
ISO27001	6.1.1(c)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.1(c)	6.1.1 General: c) achieve continual imrpovement		Governance and Risk Management	No gap		GRM-01, GRM-09	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.1(d)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.1(d)	6.1.1 General: d) to plan actions to address risks and opportunities		Governance and Risk Management	No gap		GRM-04, GRM-06	GRM-04: Risk management is included in ISMP, GRM-06: to establish ISMP. Other CCM controls in individual control domains include specific actions to address risks.
ISO27001	6.1.1(e)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.1(e)	6.1.1 General: e) how to 1) integrate and implement the actions into its ISMS processes, and 2) evaluate the effectiveness of the actions.		To be decided (Mapping exists)	No gap		GRM-08, GRM-10, GRM-11, AAC-01	GRM-08: use of risk assessment results, GRM-10: regular riks assessment to determine likelihood and impact of risks, GRM-11: risk mitigation. Other CCM controls in individual control domains include specific actions to address risks, AAC-01: Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations.
ISO27001	6.1.2	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2	6.1.2 Information security risk assessment: The organisation shall define and apply an information security risk assessment process.		Governance and Risk Management	No gap		GRM-02, GRM-08, GRM-10	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.2(a)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(a)	6.1.2 Information security risk assessment: a) information security risk criteria (risk acceptance criteria, criteria for performing information security risk assessments)		Governance and Risk Management	No gap		GRM-02, GRM-10, GRM-11	Not necessary to include all these controls, but only those that reference "criteria".
ISO27001	6.1.2(a)(1)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(a)(1)	6.1.2 Information security risk assessment: a) information security risk criteria - 1) risk acceptance criteria		Governance and Risk Management	No gap		GRM-02, GRM-10, GRM-11	
ISO27001	6.1.2(a)(2)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(a)(2)	6.1.2 Information security risk assessment: a) information security risk criteria - 2) criteria for perfoming security risk assessments		Governance and Risk Management	No gap		GRM-02, GRM-10, GRM-11	
ISO27001	6.1.2(b)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(b)	6.1.2 Information security risk assessment: b) repeated information security risk assessments produce consistent, valid and comparable results		Governance and Risk Management	Full gap			None of GRM 02/08/10 reflect the requirement of 6.1.2.b. for having repetitive and comparable results of risk assessments. Controls refer to the content and means of performing risk assessments not a consistency relationship between them, which is required by 6.1.2.b.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.2(c)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(c)	6.1.2 Information security risk assessment: c) identifies information security risks		To be decided (Mapping exists)	No gap		BCR-05, BCR-06, CCC-05, DSI-02, GRM-10, HRS-02, IAM-05, IAM-07, IVS-04, IVS-13, STA-01, STA-05, STA-06, TVM-02	Several CCM controls address idnetification of risks in diverse areas, what to consider and actiosn to take.
ISO27001	6.1.2(c)(1)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(c)(1)	6.1.2 Information security risk assessment: c) information security risks - 1) apply the information security risk assessment to identify risks associated with the loss of confidentiality, integrity and availability of information		Governance and Risk Management	Partial gap		GRM-02, GRM-04, GRM-10	GRM-02/4/10 reflect risks related to data's CIA. The rest of controls seem to be excessive.
ISO27001	6.1.2(c)(2)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(c)(2)	6.1.2 Information security risk assessment: c) information security risks - 2) identify risk owners		Governance and Risk Management	Full gap			The requirement of a risk owner is not found in CCM. "Risk ownership" requirement is not addressed in CCM and neither in GRM-02. Not close to awareness (GRM-02), has to be defined explicitly and assigned to managers.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.2(d)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(d)	6.1.2 Information security risk assessment: d) information security risk analysis		Governance and Risk Management	No gap		GRM-02, GRM-10	
ISO27001	6.1.2(d)(1)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(d)(1)	6.1.2 Information security risk assessment: d) information security risk analysis - 1) assess the potential consequences		Governance and Risk Management	No gap		GRM-02, GRM-10	
ISO27001	6.1.2(d)(2)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(d)(2)	6.1.2 Information security risk assessment: d) information security risk analysis - 2) lieklihood of occurence of risks identified		Governance and Risk Management	No gap		GRM-02, GRM-10	
ISO27001	6.1.2(d)(3)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(d)(3)	6.1.2 Information security risk assessment: d) information security risk analysis - 3) determine the level of risk		Governance and Risk Management	No gap		GRM-02, GRM-10	Risk levels estimation is part of the Risk Assessment process, made out of likelihood and impact estimations, hence, its covered by CCM.
ISO27001	6.1.2(e)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(e)	6.1.2 Information security risk assessment: e) evaluating information security risks		Governance and Risk Management	No gap		GRM-10, GRM-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.2(e)(1)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(e)(1)	6.1.2 Information security risk assessment: e) evaluating information security risks - 1) compare the results of risk analysis with the risk criteria		Governance and Risk Management	Full gap			There is no reference in CCM of such a comparison. GRM-10 does not define an evaluation of risk analysis results with preestablished risk criteria.
ISO27001	6.1.2(e)(2)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2(e)(2)	6.1.2 Information security risk assessment: e) evaluating information security risks - 2) prioritise the analysed risks for risk treatment		Governance and Risk Management	Full gap			There is no reference in CCM for risks prioritization. ISO control refers to prioritisation of risk analysis results for risk treatment. GRM-10 reflects Risk assessments, not risk management that involves risk treatment. CCM should be improved from this perspective.
ISO27001	6.1.2x	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.2x	The organisation shall retain documented information about the information security risk assessment process.		Governance and Risk Management	Partial gap		GRM-11	ISO27001 also includes this fundamental requirement that does not exist in this table: "The organization shall retain documented information about the information security risk assessment process". GRM-11 covers this requirement partially.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.3	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3	6.1.3 Information security risk treatment		Governance and Risk Management	No gap		GRM-04, GRM-11	
ISO27001	6.1.3(a)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(a)	6.1.3 Information security risk treatment: a) select appropriate information security risk treatment options, taking account of the risk assessment results		Governance and Risk Management	No gap		GRM-08, GRM-11	GRM-08 updates are part of the treatment process. GRM-11 is clearly about risk treatment in general, very general.
ISO27001	6.1.3(b)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(b)	6.1.3 Information security risk treatment: b) determine controls to implement the information security risk treatment		To be decided (No mapping)	Full gap			Not sure there exists such an explicit requirement stated in CCM, that is, to determine which controls to use.
ISO27001	6.1.3(c)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(c)	6.1.3 Information security risk treatment: c) compare the controls defined in 6.1.3.b with those in Annex A of this standard		To be decided (No mapping)	Full gap			Ok! It is similar to saying look for controls and compare them to EU-SEC repository, or CCM itself. Such CCM req. does not exist.
ISO27001	6.1.3(d)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(d)	6.1.3 Information security risk treatment: d) produce a Statement of Applicability that con- tains the necessary controls and justification of inclusions and the justification for exclusion		To be decided (No mapping)	Full gap			Ok! Statement of Applicability, no, nothing similar exists.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.1.3(e)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(e)	6.1.3 Information security risk treatment: e) formulate an information security risk treatment plan		To be decided (No mapping)	Full gap			Ok! No risk treatment planning exists as reference.
ISO27001	6.1.3(f)	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(f)	6.1.3 Information security risk treatment: f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.		To be decided (No mapping)	Full gap			The term risk owner is not used with CCM controls. A risk owner's approval and acceptance is not referenced as well. GRM-10 refers to determining the risk level of residual risk, not its approval or acceptance.
ISO27001	6.1.3(f)x	6 Planning / 6.1 Actions to address risks and opportunities / 6.1.3(f)x	6.1.3 Information security risk treatment: The organisation shall retain documented information about the information security risk treatment process.		Governance and Risk Management	Partial gap		GRM-11	Indeed, CCM includes GRM-11 that reflects a documentation requirement for risk ac-ceptance, which is part of the overall risk treatment that includes risk trans-fer/reduction/avoidance as well.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.2	6 Planning / 6.2	6.2 Information security objectives and planning to achieve them: The organisation shall establish information security objectives at relevant functions and levels. The organisation shall retain documented information on the information security objectives.	Security	To be decided (No mapping)	Full gap			The terms information security planning and objectives are not used in CCM, or any other meaning that points to objectives planning and establishment. There is no reference of a requirement for documenting information security objectives. Security (Privacy *should* be addressed but not the core of an ISMS)
ISO27001	6.2(a)	6 Planning / 6.2(a)	6.2 Information security objectives and planning to achieve them: a) be consistent with the information security policy		Governance and Risk Management	Partial gap		GRM-03	
ISO27001	6.2(b)	6 Planning / 6.2(b)	6.2 Information security objectives and planning to achieve them: b) be measurable (if practicable)		To be decided (No mapping)	Full gap			CCM doesn't directly include measurable information security objectives. Indirectly, this might be part of the information security policy.
ISO27001	6.2(c)	6 Planning / 6.2(c)	6.2 Information security objectives and planning to achieve them: c) take into account information security requirements and results from risk assessment and risk treatment		To be decided (Mapping exists)	Partial gap		GRM-01, GRM-08, GRM-11, STA-05, BCR-01	The requirements of 6.2.c. fall into the context of security objectives, which is a requirement not addressed by CCM. Also, the concept of Risk treatment is as well not fully addressed.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.2(d)	6 Planning / 6.2(d)	6.2 Information security objectives and planning to achieve them: d) be communicated		Governance and Risk Management	Partial gap		GRM-03, GRM-05, GRM-06	Partial gap notation reflects missing "security objectives" requirement, even though relevant CCM controls exist. Objectives are to be communicated, and such a concept does not exist in CCM.
ISO27001	6.2(e)	6 Planning / 6.2(e)	6.2 Information security objectives and planning to achieve them: e) be updated as appropriate		To be decided (Mapping exists)	Partial gap		GRM-09, BCR-01	
ISO27001	6.2(f)	6 Planning / 6.2(f)	6.2 Information security objectives and planning to achieve them: f) what will be done		To be decided (No mapping)	Full gap			Control is too generic and has a meaning only in the context of security objectives definition. We can literally map it using all CCM controls.
ISO27001	6.2(g)	6 Planning / 6.2(g)	6.2 Information security objectives and planning to achieve them: g) what resources will be required		Infrastructure & Virtualization Security	Partial gap		IVS-04	"resources shall be planned" it's close to what this require-ment is about, however not in the context of security objec-tives determination.
ISO27001	6.2(h)	6 Planning / 6.2(h)	6.2 Information security objectives and planning to achieve them: h) who will be responsible		To be decided (Mapping exists)	Partial gap		GRM-06, BCR-01, BCR-10, HRS-10	
ISO27001	6.2(i)	6 Planning / 6.2(i)	6.2 Information security objectives and planning to achieve them: i) when it will be completed		To be decided (No mapping)	Full gap			Difficult to map.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	6.2(j)	6 Planning / 6.2(j)	6.2 Information security objectives and planning to achieve them: j) how the results will be evaluated		To be decided (No mapping)	Full gap			Difficult to map.
ISO27001	7.1	7 Support / 7.1	7.1 Resources: The organisation shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the ISMS.	Security	To be decided (Mapping exists)	No gap		GRM-04, IVS-04	The ISO control is covered, nevertheless, the term of "continual improvement" should be added as wording. Security (Privacy *should* be addressed but not the core of an ISMS)
ISO27001	7.2	7 Support / 7.2	7.2 Competence: The organisation shall determine necessary competence of person(s) doing work under its control, ensure these persons are competent on the basis of appropriate education, training, or experience, take actions to acquire the necessary competence, where applicable, and evaluate the effectiveness of the actions taken, retain appropriate documented information as evidence of competence.		To be decided (Mapping exists)	Partial gap		GRM-04, HRS-02, HRS-09	HRS-02 (Background screening) or HRS-09 (training) are covering most competence verification and development requirements, nevertheless, still the requirements for evaluating actions of acquiring competence and for retaining documented evidences are missing.
ISO27001	7.2(a)	7 Support / 7.2(a)	7.2 Competence: a) competences		Human Resources	No gap		HRS-02	This CCM control determines the competence required based on the corresponding security requirements.
ISO27001	7.2(b)	7 Support / 7.2(b)	7.2 Competence: b) raising competences with education, training, experiences		Human Resources	No gap		HRS-02, HRS-09	CCM controls fully cover this ISO req. as well.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	7.2(c)	7 Support / 7.2(c)	7.2 Competence: c) where applicable, take actions to acquire the necessary competence		To be decided (No mapping)	Full gap			Competences or acquiring competences are not directly included in the CCM. Proposal: GRM-04 (ISMP) or HRS control domain might include this.
ISO27001	7.2(d)	7 Support / 7.2(d)	7.2 Competence: d) retain appropriate documented information as evidence of competence		To be decided (No mapping)	Full gap			Competences or acquiring competences are not directly included in the CCM. Proposal: GRM-04 (ISMP) or HRS control domain might include this.
ISO27001	7.3	7 Support / 7.3	7.3 Awareness: Persons doing work under the organisation's control shall be aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming with the ISMS requirements.	Security	To be decided (Mapping exists)	Partial gap		HRS-09, HRS-10, GRM-03, GRM-07	Note: all sections refer to Security, not (necessarily) Privacy; if then only to security aspects of privacy.
ISO27001	7.3(a)	7 Support / 7.3(a)	7.3 Awareness: a) of information security policy		To be decided (Mapping exists)	No gap		HRS-09, HRS-10, GRM-03	
ISO27001	7.3(b)	7 Support / 7.3(b)	7.3 Awareness: b) of their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance		To be decided (No mapping)	Full gap			This ISO control comes down to performance assessment and awareness of personnel in the context of information security. CCM does not address this requirement.
ISO27001	7.3(c)	7 Support / 7.3(c)	7.3 Awareness: c) the implications of not conforming with the ISMS requirements.		Governance and Risk Management	No gap		GRM-07	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	7.4	7 Support / 7.4	7.4 Communication: The organisation shall determine the need for internal and external communications relevant to the ISMS (what, when, with whom, who, processes).		To be decided (Mapping exists)	Partial gap		GRM-04, BCR-01, GRM-05, GRM-06, STA-05, SEF-03	ISO control is more generic in its content while CCM controls focus on certain areas of interest. CCM would benefit from a similar strategic managerial control.
ISO27001	7.5.1	7 Support / 7.5 Documented information / 7.5.1	7.5.1 General: The organisation's ISMS shall include documented information required by this standard and documented information determined by the organisation as being necessary for the effectiveness of the ISMS.		To be decided (Mapping exists)	Partial gap		BCR-01, BCR-04, BCR-09, DSI-02, DSI-05, DSI-06, GRM-04, GRM-05, GRM-11, HRS-04, HRS-06, HRS-07, IVS-06, IPY-04, IPY-05, MOS-02, MOS-03, MOS-05, MOS-07, MOS-16, DCS-01, SEF-01, AAC-03	Documentation is required by several more specific CCM controls in diverse control domains. Documentation in CCM is not necessary the same as documented information in ISO 27001. GRM-04 could include additional requirements, similar to ISO27001, to specify the need and details for documentation.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	7.5.2	7 Support / 7.5 Documented information / 7.5.2	7.5.2 Creating and updating: when creating and updating documented information the organisation shall ensure appropriate: identification and description, format, review and approval for suitability and adequacy.		To be decided (No mapping)	Full gap			CCM does not address documentation management, or templates formatting or review governance at any form.
ISO27001	7.5.2(a)	7 Support / 7.5 Documented information / 7.5.2(a)	7.5.2 Creating and updating: a) identification and description (e.g. a title, date, author, or reference number)		To be decided (No mapping)	Full gap			
ISO27001	7.5.2(b)	7 Support / 7.5 Documented information / 7.5.2(b)	7.5.2 Creating and updating: b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic)		To be decided (No mapping)	Full gap			
ISO27001	7.5.2(c)	7 Support / 7.5 Documented information / 7.5.2(c)	7.5.2 Creating and updating: c) review and approval for suitability and adequacy.		To be decided (No mapping)	Full gap			
ISO27001	7.5.3	7 Support / 7.5 Documented information / 7.5.3	7.5.3 Control of documented information: Documented information required by the ISMS and by this International Standard shall be controlled to ensure: availability and suitability, and that it is adequately protected. Needed activities: distribution, access, retrieval and use, storage and preservation, control of changes, retention and disposition.		Identity & Access Management	Partial gap		IAM-06	
ISO27001	7.5.3(a)	7 Support / 7.5 Documented information / 7.5.3(a)	7.5.3 Control of documented information: a) it is available and suitable for use, where and when its is needed		Interoperability & Portability	Partial gap		IPY-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	7.5.3(b)	7 Support / 7.5 Documented information / 7.5.3(b)	7.5.3 Control of documented information: b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity)		Encryption & Key Management	No gap		EKM-03	
ISO27001	7.5.3(c)	7 Support / 7.5 Documented information / 7.5.3(c)	7.5.3 Control of documented information: c) distribution, access, retrieval and use		To be decided (Mapping exists)	Partial gap		DCS-01, DCS-09, IAM-04	If documented data can be characterised as an organization's assets.
ISO27001	7.5.3(d)	7 Support / 7.5 Documented information / 7.5.3(d)	7.5.3 Control of documented information: d) storage and preservation, including the preservation of legibility		Business Continuity Management & Operational Resilience	Partial gap		BCR-11	
ISO27001	7.5.3(e)	7 Support / 7.5 Documented information / 7.5.3(e)	7.5.3 Control of documented information: e) control of changes (e.g. version control)		To be decided (No mapping)	Full gap			
ISO27001	7.5.3(f)	7 Support / 7.5 Documented information / 7.5.3(f)	7.5.3 Control of documented information: f) retention and disposition		Business Continuity Management & Operational Resilience	Partial gap		BCR-11	
ISO27001	8	8 Operation	8 Operation		Business Continuity Management & Operational Resilience	Partial gap		BCR-11	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	8.1	8 Operation / 8.1	8.1 Operational planning and control: The organisation shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1 (Actions to address risks and opportunities). The organisation shall also implement plans to achieve information security objectives determined in 6.2 (Information security objectives and planning to achieve them)		To be decided (Mapping exists)	No gap		AAC-01, BCR-01, BCR-02, BCR-03, BCR-09, BCR-10, BCR-11, GRM-02, GRM-06, GRM-09, GRM-10, HRS-06, IAM-10, IVS-04, STA-07, CCC-01, CCC-05, GRM-04, GRM-05	Policies, procedures and measures defined in CCM.
ISO27001	8.2	8 Operation / 8.2	8.2 Information security risk assessment: The organisation shall perform information security risk assessment at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2.a. The organisation shall retain documented information of the results of the information security risk assessments.		Governance and Risk Management	No gap		GRM-02, GRM-10	In addition, risk assessment, actions for reducing risks and risk management are defined in several specific CCM controls.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	8.3	8 Operation / 8.3	8.3 Information security risk treatment: The organisation shall implement the information security risk treatment plan. The organisation shall retain documented information of the results of the information security risk treatment.		To be decided (Mapping exists)	No gap		GRM-11, IVS-8, SEF-02	I would argue that the difference is in terminology only and that mapped control address the ISO requirement as GRM-11 is talking about risk treatment. Some of the domains drill deeper into this for specific operational aspects.
ISO27001	9.1	9 Performance evaluation / 9.1	9.1 Monitoring, measurement, analysis and evaluation: The organsiation shall evaluate the information security performance and the effectiveness of the ISMS.		Governance and Risk Management	No gap		GRM-09	CCM GRM-09 covers the Clause 9.1 requirement on high-level. However, some of the ISO requirements below are not specifically addressed in GRM-09.
ISO27001	9.1(a)	9 Performance evaluation / 9.1(a)	9.1 Monitoring, measurement, analysis and evaluation: a)		Governance and Risk Management	Partial gap		GRM-09	CCM GRM-09 covers the Clause 9.1 requirement on high-level. However, some of the ISO requirements below are not specifically addressed in GRM-09.
ISO27001	9.1(b)	9 Performance evaluation / 9.1(b)	9.1 Monitoring, measurement, analysis and evaluation: b)		Governance and Risk Management	Partial gap		GRM-09	CCM GRM-09 covers the Clause 9.1 requirement on high-level. However, some of the ISO requirements below are not specifically addressed in GRM-09.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	9.1(c)	9 Performance evaluation / 9.1(c)	9.1 Monitoring, measurement, analysis and evaluation: c)		Governance and Risk Management	Partial gap		GRM-09	CCM GRM-09 covers the Clause 9.1 requirement on high-level. However, some of the ISO requirements below are not specifically addressed in GRM-09.
ISO27001	9.1(d)	9 Performance evaluation / 9.1(d)	9.1 Monitoring, measurement, analysis and evaluation: d)		Governance and Risk Management	Partial gap		GRM-09	CCM GRM-09 covers the Clause 9.1 requirement on high-level. However, some of the ISO requirements below are not specifically addressed in GRM-09.
ISO27001	9.1(e)	9 Performance evaluation / 9.1(e)	9.1 Monitoring, measurement, analysis and evaluation: e)		Governance and Risk Management	No gap		GRM-08, GRM-09	
ISO27001	9.1(f)	9 Performance evaluation / 9.1(f)	9.1 Monitoring, measurement, analysis and evaluation: f)		Governance and Risk Management	Partial gap		GRM-09	CCM GRM-09 covers the Clause 9.1 requirement on high-level. However, some of the ISO requirements below are not specifically addressed in GRM-09.
ISO27001	9.2	9 Performance evaluation / 9.2	9.2 Internal audit: The organisation shall conduct internal audits at planned intervals to provide information whether the ISMS is conformant and is effectively implemented and maintained.		Audit Assurance & Compliance	Partial gap		AAC-01	CCM AAC-01 control is a high-level control related to Internal Audit which partially covers Clause 9.2 (but too high level to understand to which extent). Agreed with comment that more AAC

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									controls need to be created to cover 9.2 requirements.
ISO27001	9.2(a)	9 Performance evaluation / 9.2(a)	9.2 Internal audit: a)		Audit Assurance & Compliance	Full gap			
ISO27001	9.2(b)	9 Performance evaluation / 9.2(b)	9.2 Internal audit: b)		Audit Assurance & Compliance	No gap		AAC-01	
ISO27001	9.2(c)	9 Performance evaluation / 9.2(c)	9.2 Internal audit: c)		Audit Assurance & Compliance	Partial gap		AAC-01	CCM AAC-01 control is a high-level control related to Internal Audit which partially covers Clause 9.2 (but too high level to understand to which extent). Partial due to lack in AAC-01 of "plan, establish, implement and maintain an audit programme" requirements. AAC-01 refers to planning only. AAC-02, AAC-03 are not relevant here.
ISO27001	9.2(d)	9 Performance evaluation / 9.2(d)	9.2 Internal audit: d)		Audit Assurance & Compliance	Full gap			
ISO27001	9.2(e)	9 Performance evaluation / 9.2(e)	9.2 Internal audit: e)		Audit Assurance & Compliance	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	9.2(f)	9 Performance evaluation / 9.2(f)	9.2 Internal audit: f)		Audit Assurance & Compliance	Full gap			
ISO27001	9.2(g)	9 Performance evaluation / 9.2(g)	9.2 Internal audit: g)		Audit Assurance & Compliance	Full gap			
ISO27001	9.3(a)	9 Performance evaluation / 9.3(a)	9.3 Management review: a)		Governance and Risk Management	No gap		GRM-09, GRM-10	Risk management & assessments can provide information on the status of actions from previous reviews.
ISO27001	9.3(b)	9 Performance evaluation / 9.3(b)	9.3 Management review: b)		Governance and Risk Management	No gap		GRM-09, GRM-10	Risk management & assessments can provide information on changes in external and internal issues that are relevant to the ISMS
ISO27001	9.3(c)	9 Performance evaluation / 9.3(c)	9.3 Management review: c)		Governance and Risk Management	Partial gap		GRM-04, GRM-08, GRM-10, GRM-11, GRM-06, GRM-09	Risk management & assessments can provide feedback on the information security performance
ISO27001	9.3(c)(1)	9 Performance evaluation / 9.3(c)(1)	9.3 Management review: c) - 1)		Governance and Risk Management	No gap		GRM-09, GRM-10	Risk management & assessments can provide feedback on the information security performance
ISO27001	9.3(c)(2)	9 Performance evaluation / 9.3(c)(2)	9.3 Management review: c) - 2)		Governance and Risk Management	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	9.3(c)(3)	9 Performance evaluation / 9.3(c)(3)	9.3 Management review: c) - 3)		Governance and Risk Management	No gap		GRM-10	Risk management & assessments can provide feedback on the information security performance
ISO27001	9.3(d)	9 Performance evaluation / 9.3(d)	9.3 Management review: d)		Governance and Risk Management	Full gap			
ISO27001	9.3(e)	9 Performance evaluation / 9.3(e)	9.3 Management review: e)		Governance and Risk Management	No gap		GRM-04, GRM-08, GRM-10, GRM-11, GRM-06, GRM-09	
ISO27001	9.3(f)	9 Performance evaluation / 9.3(f)	9.3 Management review: f)		Governance and Risk Management	No gap		GRM-04, GRM-08, GRM-10, GRM-11, GRM-06, GRM-09	Risk management & assessments can lead to opportunities for continual improvement. Continual assessments and reviews address the continual improvement of 9.3(f)
ISO27001	10.1(a)	10 Improvement / 10.1(a)	10.1 Nonconformity and corrective action: a) react to nonconformity, and as applicable 1) take action to control and correct it; and 2) deal with the consequences		To be decided (No mapping)	Full gap			Managing nonconformity is not included in CCM
ISO27001	10.1(b)	10 Improvement / 10.1(b)	10.1 Nonconformity and corrective action: b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere		To be decided (No mapping)	Full gap			Managing the causes of nonconformity are not included in CCM

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	10.1(c)	10 Improvement / 10.1(c)	10.1 Nonconformity and corrective action: c) implement any action needed		To be decided (No mapping)	Full gap			GRM-01: Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.
ISO27001	10.1(d)	10 Improvement / 10.1(d)	10.1 Nonconformity and corrective action: d) review the effectiveness of any corrective action taken		To be decided (No mapping)	Full gap			review of effectiveness

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	10.1(e)	10 Improvement / 10.1(e)	10.1 Nonconformity and corrective action: e) make changes to the ISMS, if necessary		To be decided (No mapping)	Full gap			Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.
ISO27001	10.1(f)	10 Improvement / 10.1(f)	10.1 Nonconformity and corrective action: The organisation shall retain documented information as evidence of: f) the nature of the nonconformities and any subsequent actions taken		To be decided (No mapping)	Full gap			documented information about actions taken

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	10.1(g)	10 Improvement / 10.1(g)	10.1 Nonconformity and corrective action: The organisation shall retain documented information as evidence of: g) the results of any corrective action.		To be decided (No mapping)	Full gap			documented information about the results
ISO27001	10.2	10 Improvement / 10.2	10.2 Continual improvement: The organisation shall continually improve the suitability, adequacy and effectiveness of the ISMS.		To be decided (No mapping)	Full gap			Continual improvement of ISMS is not directly in CCM.
ISO27001	A.5.1.1	A.5 Information security policies / A.5.1 Management direction for information security / A.5.1.1	A.5.1.1 Policies for information security: A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.		Governance and Risk Management	No gap	To be decided	GRM-06	EU-SEC consortium mapping includes several controls that reflect policies towards specialized aspects of information security (while 5.1.1. refers to a requirement for having an information security policy by more general means), thus we could exclude those as excessive subsets of what is required by 5.1.1., and covered by GRM-06 alone.
ISO27001	A.5.1.2	A.5 Information security policies / A.5.1 Management direction for information security / A.5.1.2	A.5.1.2 Review of the policies for information security: The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.		Governance and Risk Management	No gap	To be decided	GRM-08, GRM-09, STA-06	STA-06 for external

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.6.1.1	A.6 Organisation of information security / A.6.1 Internal organisation / A.6.1.1	A.6.1.1 Information security roles and responsibilities: All information security responsibilities shall be defined and allocated.		To be decided (Mapping exists)	No gap	To be decided	BCR-10, DSI-06, DCS-01, GRM-06, HRS-07, HRS-10, SEF-03	
ISO27001	A.6.1.2	A.6 Organisation of information security / A.6.1 Internal organisation / A.6.1.2	A.6.1.2 Segregation of duties: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.		Identity & Access Management	No gap	0	IAM-05	
ISO27001	A.6.1.3	A.6 Organisation of information security / A.6.1 Internal organisation / A.6.1.3	A.6.1.3 Contact with authorities: Appropriate contacts with relevant authorities shall be maintained.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap	To be decided	SEF-01	contact with Data Privacy Authorities should be included
ISO27001	A.6.1.4	A.6 Organisation of information security / A.6.1 Internal organisation / A.6.1.4	A.6.1.4 Contact with special interest groups: Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap	To be decided	SEF-01	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.6.1.5	A.6 Organisation of information security / A.6.1 Internal organisation / A.6.1.5	A.6.1.5 Information security in project management: Information security shall be addressed in project management, regardless of the type of the project.		To be decided (No mapping)	Full gap			
ISO27001	A.6.2.1	A.6 Organisation of information security / A.6.2 Mobile devices and teleworking / A.6.2.1	A.6.2.1 Mobile device policy: A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.		To be decided (Mapping exists)	No gap	+	HRS-05, MOS-01, MOS-04, MOS-05, MOS-06, MOS-07, MOS-08, CCC-04	
ISO27001	A.6.2.2	A.6 Organisation of information security / A.6.2 Mobile devices and teleworking / A.6.2.2	A.6.2.2 Teleworking: A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.		Human Resources	No gap	-	HRS-05	
ISO27001	A.7.1.1	A.7 Human resource security / A.7.1 Prior to employment / A.7.1.1	A.7.1.1 Screening: Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the		Human Resources	No gap	0	HRS-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			classification of the information to be accessed and the perceived risks.						
ISO27001	A.7.1.2	A.7 Human resource security / A.7.1 Prior to employment / A.7.1.2	A.7.1.2 Terms and conditions of employment: The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.		Human Resources	No gap	0	HRS-03	
ISO27001	A.7.2.1	A.7 Human resource security / A.7.2 During employment / A.7.2.1	A.7.2.1 Management responsibilities: Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.		Governance and Risk Management	No gap	0	GRM-03, BCR-10, HRS-07	
ISO27001	A.7.2.2	A.7 Human resource security / A.7.2 During employment / A.7.2.2	A.7.2.2 Information security awareness, education and training: All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.		Human Resources	No gap	+	HRS-09. HRS-10, GRM-03, MOS-01, MOS-02	
ISO27001	A.7.2.3	A.7 Human resource security / A.7.2 During	A.7.2.3 Disciplinary process: There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.		Governance and Risk Management	No gap	0	GRM-07, HRS-04	Combination of HR and GRM

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		employment / A.7.2.3							
ISO27001	A.7.3.1	A.7 Human resource security / A.7.3 Termination and change of employment / A.7.3.1	A.7.3.1 Termination or change of employment responsibilities: Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.		Human Resources	No gap	0	HRS-01, HRS-04	
ISO27001	A.8.1.1	A.8 Asset management / A.8.1 Responsibility for assets / A.8.1.1	A.8.1.1 Inventory of assets: Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.		Datacenter Security	No gap	0	DCS-01, DCS-05, MOS-09	
ISO27001	A.8.1.2	A.8 Asset management / A.8.1 Responsibility for assets / A.8.1.2	A.8.1.2 Ownership of assets: Assets maintained in the inventory shall be owned.		Data Security & Information Lifecycle Management	No gap	0	DCS-01 DSI-06, MOS-09	
ISO27001	A.8.1.3	A.8 Asset management / A.8.1 Responsibility for assets / A.8.1.3	A.8.1.3 Acceptable use of assets: Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.		Human Resources	No gap	0	HRS-05, HRS-08, MOS-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.8.1.4	A.8 Asset management / A.8.1 Responsibility for assets / A.8.1.4	A.8.1.4 Return of assets: All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.		Human Resources	No gap	0	HRS-01	
ISO27001	A.8.2.1	A.8 Asset management / A.8.2 Information classification / A.8.2.1	A.8.2.1 Classification of information: Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.		Data Security & Information Lifecycle Management	No gap	0	DSI-01, DSI-03,	DSI-01: Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.
ISO27001	A.8.2.2	A.8 Asset management / A.8.2 Information classification / A.8.2.2	A.8.2.2 Labelling of information: An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.		Data Security & Information Lifecycle Management	No gap	0	DSI-04,	DSI-04: Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
ISO27001	A.8.2.3	A.8 Asset management / A.8.2 Information classification / A.8.2.3	A.8.2.3 Handling of assets: Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.		Data Security & Information Lifecycle Management	No gap	0	DSI-04, BCR-11	DSI-04: Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									act as aggregate containers for data.
ISO27001	A.8.3.1	A.8 Asset management / A.8.3. Media handling / A.8.3.1	A.8.3.1 Management of removable media: Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.		Data Security & Information Lifecycle Management	No gap	0	DSI-04, DSI-07	DSI-04: Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
ISO27001	A.8.3.2	A.8 Asset management / A.8.3. Media handling / A.8.3.2	A.8.3.2 Disposal of media: Media shall be disposed of securely when no longer required, using formal procedures.		Data Security & Information Lifecycle Management	No gap	0	DSI-07, DSI-05	DSI-05 for external management
ISO27001	A.8.3.3	A.8 Asset management / A.8.3. Media handling / A.8.3.3	A.8.3.3 Physical media transfer: Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.		To be decided (Mapping exists)	No gap		DSI-04, DCS-04, DCS-05	DSI-04 is a high-level control which could cover A.8.3. on high level. DCS-04 is prevent-ing unauthorized access. EKM-03 can be considered as com-pensating control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.1.1	A.9 Access control / A.9.1 Business requirements of access control / A.9.1.1	A.9.1.1 Access control policy		To be decided (Mapping exists)	No gap		IAM -04, DCS-07, EKM-02, GRM-04, HRS-05, IAM-02, IAM-05, IAM-01	IAM -04- Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access DCS-07- to secure areas shall be constrained and monitored by physical access control mechanisms, EKM-02 Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem, GRM-04-The security program shall include Security policy, Access control....,HRS-05-Policies and procedures shall be established, and supporting business processes and technical measures implemented, IAM-02 - User access policies and procedures shall be established for ensuring appropriate identity, entitlement, and access management for all internal

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									corporate and customer (tenant) users, IAM-05- User access policies and procedures shall be established, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.
ISO27001	A.9.1.2	A.9 Access control / A.9.1 Business requirements of access control / A.9.1.2	A.9.1.2 Access to networks and network services		Identity & Access Management	No gap		IAM-04, IAM-02	IAM-04-Policies shall also be developed to control access to network resources based on user identity.
ISO27001	A.9.2	A.9 Access control / A.9.2 User access management	A.9 Access control / A.9.2 User access management		Identity & Access Management	No gap		IAM-04	IAM-04- to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.2.1	A.9 Access control / A.9.2 User access management / A.9.2.1	A.9.2.1 User registration and de-registration		Identity & Access Management	No gap		IAM-09, IAM-10, IAM-11	IAM-09- infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures, IAM-10-User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, IAM-11 - shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.2.2	A.9 Access control / A.9.2 User access management / A.9.2.2	A.9.2.2 User access provisioning		Identity & Access Management	No gap		IAM-09, IAM-02, IAM-07	IAM-09- infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. IAM-02-for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally, IAM-07 - Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.2.3	A.9 Access control / A.9.2 User access management / A.9.2.3	A.9.2.3 Management of privileged access rights		Identity & Access Management	No gap		IAM-06, IAM-09, IAM-04	IAM-06- Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted , IAM-09-infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures, IAM-04 - Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.2.4	A.9 Access control / A.9.2 User access management / A.9.2.4	A.9.2.4 Management of secret authentication information of users		Identity & Access Management	No gap		IAM-08, IAM-12	IAM-08- Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities, IAM-12 -internal corporate or customer user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management
ISO27001	A.9.2.5	A.9 Access control / A.9.2 User access management / A.9.2.5	A.9.2.5 Review of users access rights		Identity & Access Management	No gap		IAM-02, IAM -04, IAM -08 IAM-10	IAM-02- User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components, IAM-04-Policies and

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access, IAM-08-Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary..IAM-10- User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.2.6	A.9 Access control / A.9.2 User access management / A.9.2.6	A.9.2.6 Removal of adjustment of access rights		Identity & Access Management	No gap		IAM-04, IAM-08, IAM-11	IAM-04-Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access, IAM-08-Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.IAM-11-(revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.3.1	A.9 Access control / A.9.3 User responsibilities / A.9.3.1	A.9.3.1 Use of secret authentication information		To be decided (Mapping exists)	No gap		IAM-08, HRS-11, HRS-10	IAM-08 - established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary. HRS-11 - to require that unattended workspaces do not have openly visible sensitive documents, HRS-10 - personnel shall be made aware of their roles and responsibilities
ISO27001	A.9.4.1	A.9 Access control / A.9.4 System and application access control / A.9.4.1	A.9.4.1 Information access restriction		Identity & Access Management	No gap		IAM-02, IAM-06, IAM-09	IAM-02-User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									interfaces and infrastructure network and systems components.IAM-06- Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted , IAM-09 - shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures.
ISO27001	A.9.4.2	A.9 Access control / A.9.4 System and application access control / A.9.4.2	A.9.4.2 Secure log-on procedure		Identity & Access Management	No gap		IAM-08, IAM-12	IAM-08 - established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary. IAM-12 - ensuring appropriate identity, entitlement, and access

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									management and in accordance with established policies and procedures:
ISO27001	A.9.4.3	A.9 Access control / A.9.4 System and application access control / A.9.4.3	A.9.4.3 Password management system		To be decided (Mapping exists)	No gap		MOS-16, IAM-08	MOS-16- Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, IAM-08- Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.
ISO27001	A.9.4.4	A.9 Access control / A.9.4 System and application access control / A.9.4.4	A.9.4.4 Use of privileged utility programs		Identity & Access Management	No gap		IAM-13	IAM-13- Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.,

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.9.4.5	A.9 Access control / A.9.4 System and application access control / A.9.4.5	A.9.4.5 Access control to program source code		To be decided (Mapping exists)	No gap		IAM-06, CCC-02	IAM-06- Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.CCC-02- External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.10.1	A.10 Cryptography / A.10.1 Cryptographic controls	A.10 Cryptography / A.10.1 Cryptographic controls		Encryption & Key Management	No gap		EKM-01, EKM-02, EKM-04	EKM-01-Keys must have identifiable owners (binding keys to identities) and there shall be key management policies, EKM-02-Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem, EKM-04-Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.10.1.1	A.10 Cryptography / A.10.1 Cryptographic controls / A.10.1.1	A.10.1.1 Policy on the use of cryptographic controls		To be decided (Mapping exists)	No gap		EKM-01, EKM-02, EKM-03, EKM-04, IVS-12	EKM-01-Keys must have identifiable owners (binding keys to identities) and there shall be key management policies, EKM-02-Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem,EKM-03-Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage, EKM-04 - Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required, IVS-12 - Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.10.1.2	A.10 Cryptography / A.10.1 Cryptographic controls / A.10.1.2	A.10.1.2 Key management		Encryption & Key Management	No gap		EKM-01, EKM-02, EKM-04	EKM-01-Keys must have identifiable owners (binding keys to identities) and there shall be key management policies, EKM-02-Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem, EKM-04 - Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required, IVS-12 - Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings)

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.1.1	A.11 Physical and environmental security / A.11.1 Secure areas / A.11.1.1	A.11.1.1 Physical security perimeter		Datacenter Security	No gap		DCS-02, DCS-06, DCS-07, DCS-09	DCS-02- Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.,DCS-06-Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information, DCS-07- Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access., DCS-09- Physical access to information assets and functions by users and support personnel shall be restricted.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.1.2	A.11 Physical and environmental security / A.11.1 Secure areas / A.11.1.2	A.11.1.2 Physical entry controls		Datacenter Security	No gap		DCS-02, DCS-06, DCS-07, GRM-04	DCS-02- Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems., DCS-06-Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information, DCS-07- Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.1.3	A.11 Physical and environmental security / A.11.1 Secure areas / A.11.1.3	A.11.1.3 Securing offices, rooms and facilities		Datacenter Security	No gap		DCS-06, DCS-07, GRM-04	DCS-06-Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information,

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.1.4	A.11 Physical and environmental security / A.11.1 Secure areas / A.11.1.4	A.11.1.4 Protecting against external environmental threats		Business Continuity Management & Operational Resilience	No gap		BCR-05, BCR-08, GRM-04	BCR-05- Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.GRM-04- The security program shall include Physical and environmental security BCR-08: Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.1.5	A.11 Physical and environmental security / A.11.1 Secure areas / A.11.1.5	A.11.1.5 Working in secure areas		Human Resources	No gap		HRS-10, HRS-11, DCS-07	HRS-10- Maintaining a safe and secure working environment, HRS-11- policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.
ISO27001	A.11.1.6	A.11 Physical and environmental security / A.11.1 Secure areas / A.11.1.6	A.11.1.6 Delivery and loading areas		Datacenter Security	No gap		DCS-07, DCS-08, GRM-04	DCS-07-Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access., DCS-08-Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									unauthorized data corruption, compromise, and loss.
ISO27001	A.11.2.1	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.1	A.11.2.1 Equipment siting and protection		To be decided (Mapping exists)	No gap		BCR-05, BCR-06, DCS-05, GRM-04	BCR-05 - Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, BCR-06- To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance., DCS-05- Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.2.2	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.2	A.11.2.2 Supporting utilities		Business Continuity Management & Operational Resilience	No gap		BCR-03, BCR-05, GRM-04	BCR-03- data centre utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, BCR-05- Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.2.3	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.3	A.11.2.3 Cabling security		Business Continuity Management & Operational Resilience	No gap		BCR-03, BCR-08, GRM-04	BCR-03- data centre utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at p, BCR-08- Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.
ISO27001	A.11.2.4	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.4	A.11.2.4 Equipment maintenance		Business Continuity Management & Operational Resilience	No gap		BCR-07, BCR-08	BCR-07- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel., BCR-08- Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									specific business impact assessment.
ISO27001	A.11.2.5	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.5	A.11.2.5 Removal of assets		Datacenter Security	No gap		DCS-04, DSI-07	DCS-04- Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises
ISO27001	A.11.2.6	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.6	A.11.2.6 Security of equipment and assets off-premises		Datacenter Security	Partial gap		DCS-04	DCS-04- Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises DCS-04 is partial match at best. A.11.2.6 is about operation of off-premises systems. Partial gap since there are no other CCM controls that define security safeguards for securely operating assets off-site.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.11.2.7	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.7	A.11.2.7 Secure disposal or re-use of equipment		To be decided (Mapping exists)	No gap		DSI-07, DCS-05	DSI-07- Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means., DCS-05- Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible.
ISO27001	A.11.2.8	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.8	A.11.2.8 Unattended user equipment		Human Resources	No gap		HRS-10, HRS-11	HRS-10- Maintaining a safe and secure working environment, HRS-11- Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									computing sessions are disabled
ISO27001	A.11.2.9	A.11 Physical and environmental security / A.11.2 Equipment / A.11.2.9	A.11.2.9 Clear desk and clear screen policy		Human Resources	No gap		HRS-11	HRS-11-Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.
ISO27001	A.12.1.1	A.12 Operations security / A.12.1 Operational procedures and responsibilities / A.12.1.1	A.12.1.1 Documented operating procedures		Business Continuity Management & Operational Resilience	No gap		BCR-04	BCR-04- Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.1.2	A.12 Operations security / A.12.1 Operational procedures and responsibilities / A.12.1.2	A.12.1.2 Change management		Change Control & Configuration Management	No gap		CCC-01, CCC-02, CCC-05	CCC-01- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities, CCC-02- External business partners shall adhere to the same policies and procedures for change management, CCC-05- Policies and procedures shall be established for managing the risks associated with applying changes to: business critical application and infrastructure networks and system components

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.1.3	A.12 Operations security / A.12.1 Operational procedures and responsibilities / A.12.1.3	A.12.1.3 Capacity management		Infrastructure & Virtualization Security	No gap		IVS-04	IVS-04-Projections of future capacity requirements shall be made to mitigate the risk of system overload.
ISO27001	A.12.1.4	A.12 Operations security / A.12.1 Operational procedures and responsibilities / A.12.1.4	A.12.1.4 Separation of development, testing and operational environments		To be decided (Mapping exists)	No gap		IVS-08, STA-01	IVS-08- Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets.STA-01- Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.2.1	A.12 Operations security / A.12.2 Protection from malware / A.12.2.1	A.12.2.1 Controls against malware		To be decided (Mapping exists)	No gap		TVM-01, MOS-01, MOS-17	TVM-01- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices, MOS-01- Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training, MOS-17- The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software
ISO27001	A.12.3.1	A.12 Operations security / A.12.3 Backup / A.12.3.1	A.12.3.1 Information backup		Business Continuity Management & Operational Resilience	No gap		BCR-11	BCR-11- Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.4	A.12 Operations security / A.12.4 Logging and monitoring	A.12 Operations security / A.12.4 Logging and monitoring		Infrastructure & Virtualization Security	No gap		IVS-02, IVS-07	IVS-02- Any changes made to virtual machine images must be logged and an alert raised regardless of their running state, IVS-07- Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.4.1	A.12 Operations security / A.12.4 Logging and monitoring / A.12.4.1	A.12.4.1 Event logging		Infrastructure & Virtualization Security	No gap		IVS-01, IVS-02, IVS-07	IVS-01- Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs,IVS-02- Any changes made to virtual machine images must be logged, IVS-07- Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.
ISO27001	A.12.4.2	A.12 Operations security / A.12.4 Logging and monitoring / A.12.4.2	A.12.4.2 Protection of log information		Identity & Access Management	No gap		IAM-01	IAM-01- Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.4.3	A.12 Operations security / A.12.4 Logging and monitoring / A.12.4.3	A.12.4.3 Administrator and operator logs		Infrastructure & Virtualization Security	No gap		IVS-01, IVS-02	IVS-01- Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviours and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach, IVS-02- Any changes made to virtual machine images must be logged and an alert raised regardless of their running state
ISO27001	A.12.4.4	A.12 Operations security / A.12.4 Logging and monitoring / A.12.4.4	A.12.4.4 Clock synchronisation		Infrastructure & Virtualization Security	No gap		IVS-03	IVS-03- A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.5.1	A.12 Operations security / A.12.5 Control of operational software / A.12.5.1	A.12.5.1 Installation of software on operational systems		Change Control & Configuration Management	No gap		CCC-02,CCC-03,CCC-04	CCC-02- External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization, CCC-03- Organizations shall follow a defined quality change control and testing process with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services. CCC-04- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.6.1	A.12 Operations security / A.12.6 Technical vulnerability management / A.12.6.1	A.12.6.1 Management of technical vulnerabilities		Threat and Vulnerability Management	No gap		TVM-02	TVM-02-Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (
ISO27001	A.12.6.2	A.12 Operations security / A.12.6 Technical vulnerability management / A.12.6.2	A.12.6.2 Restrictions on software installation		To be decided (Mapping exists)	No gap		IAM-06, CCC-04	IAM-06 -use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures., CCC-04- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.12.7.1	A.12 Operations security / A.12.7 Information systems audit considerations / A.12.7.1	A.12.7.1 Information systems audit controls		To be decided (Mapping exists)	No gap		AAC-01, IAM-01, IVS-01	AAC-01- Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits, IAM-01- Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits. IVS-01- Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									behaviours and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.
ISO27001	A.13.1.1	A.13 Communications security / A.13.1 Network security management / A.13.1.1	A.13.1.1 Network controls		To be decided (Mapping exists)	No gap		EKM-03, DSI-03, IVS-12	EKM-03- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations. DSI-03- Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									activity, IVS-12- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.13.1.2	A.13 Communications security / A.13.1 Network security management / A.13.1.2	A.13.1.2 Security of network services		To be decided (Mapping exists)	No gap		IVS-06, STA-03, IVS-12	IVS-06- Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections, STA-03- Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures, IVS-12- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.13.1.3	A.13 Communications security / A.13.1 Network security management / A.13.1.3	A.13.1.3 Segregation in networks		Infrastructure & Virtualization Security	No gap		IVS-06, IVS-08, IVS-09	IVS-06-Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. IVS-08- Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties., IVS-09- Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.13.2.1	A.13 Communications security / A.13.2 Information transfer / A.13.2.1	A.13.2.1 Information transfer policies and procedures		To be decided (Mapping exists)	No gap		AIS-03, AIS-04, DSI-04	AIS-03- Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.AIS-04- Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.DSI-04- Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.13.2.2	A.13 Communications security / A.13.2 Information transfer / A.13.2.2	A.13.2.2 Agreements on information transfer		To be decided (Mapping exists)	No gap		STA-05, AIS-03, AIS-04	STA-05- Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate, AIS-03- Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse. AIS-04 - Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.13.2.3	A.13 Communications security / A.13.2 Information transfer / A.13.2.3	A.13.2.3 Electronic messaging		Encryption & Key Management	No gap		EKM-03	EKM-03-Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.
ISO27001	A.13.2.4	A.13 Communications security / A.13.2 Information transfer / A.13.2.4	A.13.2.4 Confidentiality or non-disclosure agreements		Human Resources	No gap		HRS-06	HRS-06-Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.1.1	A.14 System acquisition, development and maintenance / A.14.1 Security requirements of information systems / A.14.1.1	A.14.1.1 Information security requirements analysis and specification		To be decided (Mapping exists)	No gap		GRM-01, BCR-01, STA-05, GRM-04	I would argue that the difference is in terminology only and that mapped control address the ISO control.
ISO27001	A.14.1.2	A.14 System acquisition, development and maintenance / A.14.1 Security requirements of information systems / A.14.1.2	A.14.1.2 Securing application services on public networks		To be decided (Mapping exists)	No gap		DSI-03, EKM-03, GRM-04	DSI-03- Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data, EKM-03- Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									contract dispute and compromise of data.
ISO27001	A.14.1.3	A.14 System acquisition, development and maintenance / A.14.1 Security requirements of information systems / A.14.1.3	A.14.1.3 Protecting application services transactions		To be decided (Mapping exists)	No gap		DSI-03, EKM-03, GRM-04	DSI-03- Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data, EKM-03- Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.2.1	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.1	A.14.2.1 Secure development policy		Identity & Access Management	No gap		IAM-06, GRM-04	IAM-06- Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.
ISO27001	A.14.2.2	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.2	A.14.2.2 System change control procedures		To be decided (Mapping exists)	No gap		CCC-02,CCC-03,CCC-05, TVM-02, GRM-09	CCC-02- External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization, CCC-03- Organizations shall follow a defined quality change control and testing , CCC-05- Policies and procedures shall be established for managing the risks associated with applying changes, TVM-02- Changes shall be managed through a change management process for all

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									vendor-supplied patches, configuration changes, or changes to the organization's internally developed software.
ISO27001	A.14.2.3	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.3	A.14.2.3 Technical review of applications after operating platform changes		To be decided (Mapping exists)	No gap		CCC-05, MOS-15, GRM-10	CCC-05- Policies and procedures shall be established for managing the risks associated with applying changes, MOS-15- Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes., GRM-10 - Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.2.4	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.4	A.14.2.4 Restrictions on changes to software packages		Change Control & Configuration Management	No gap		CCC-05	I understand A.14.2.4 as control over production changes which is additionally covered by CCM CCC-05.
ISO27001	A.14.2.5	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.5	A.14.2.5 Secure system engineering principles		To be decided (No mapping)	Full gap			Full gap - no relevant CCM control

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.2.6	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.6	A.14.2.6 Secure development environment		To be decided (Mapping exists)	No gap		CCC-01, CCC-02, GRM-04	CCC-01- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems com, CCC-02-External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization, GRM-04- The security program shall include the following areas insofar as they relate to the characteristics of the business: • Information systems acquisition, development, and maintenance

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.2.7	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.7	A.14.2.7 Outsourced development		To be decided (Mapping exists)	No gap		CCC-01, CCC-02, AIS-01, CCC-05	CCC-01- o ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data centre facilities have been pre-authorized by the organization's business leadership CCC-02- External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization,AIS-01- Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards and adhere to applicable legal, statutory, or regulatory compliance obligations.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.2.8	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.8	A.14.2.8 System security testing		Change Control & Configuration Management	No gap		CCC-03, TVM-02	CCC-03- Organizations shall follow a defined quality change control and testing process
ISO27001	A.14.2.9	A.14 System acquisition, development and maintenance / A.14.2 Security in development and support processes / A.14.2.9	A.14.2.9 System acceptance testing		Change Control & Configuration Management	No gap		CCC-02, CCC-03	CCC-02- External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization, CCC-03- Organizations shall follow a defined quality change control and testing

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.14.3.1	A.14 System acquisition, development and maintenance / A.14.3 Test data / A.14.3.1	A.14.3.1 protection of test data		To be decided (Mapping exists)	No gap		EKM-03, CCC-01, CCC-02, CCC-03, AIS-01	EKM-03- Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data , CCC-01- Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, CCC-02-External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization, CCC-03-Organizations shall follow a defined quality change control and testing process No gap since test data is addressed in the controls above even if not explicitly called out.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.15.1.1	A.15 Supplier relationships / A.15.1 Information security in supplier relationships / A.15.1.1	A.15.1.1 Information security policy for supplier relationships		To be decided (Mapping exists)	No gap		GRM-04, GRM-06,STA-05, STA-09, CCC-05	I would argue that the difference is in terminology only and that mapped control address the ISO control.
ISO27001	A.15.1.2	A.15 Supplier relationships / A.15.1 Information security in supplier relationships / A.15.1.2	A.15.1.2 Addressing security within supplier agreements		To be decided (Mapping exists)	No gap		STA-05, STA-09, CCC-02, CCC-05	I would argue that the difference is in terminology only and that mapped control address the ISO control. Maps to STA, CCC and GRM
ISO27001	A.15.1.3	A.15 Supplier relationships / A.15.1 Information security in supplier relationships / A.15.1.3	A.15.1.3 Information and communication technology supply chain		Supply Chain Management, Transparency, and Accountability	No gap		STA-03, STA-05, CCC-05	I would argue that the difference is in terminology only and that mapped control address the ISO control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.15.2.1	A.15 Supplier relationships / A.15.2 Supplier service delivery management / A.15.2.1	A.15.2.1 Monitoring and review of supplier services: Organisations shall regularly monitor, review and audit supplier service delivery.		Supply Chain Management, Transparency, and Accountability	No gap		STA-07, STA-08, STA-09, STA-06, CCC-05	STA refers to partners, service agreements (providers, tenants), annual review of information security across the information supply-chain, review of third-parties involved in the supply-chain.
ISO27001	A.15.2.2	A.15 Supplier relationships / A.15.2 Supplier service delivery management / A.15.2.2	A.15.2.2 Managing changes to supplier services		To be decided (Mapping exists)	No gap		GRM-08, STA-05, CCC-05	I would argue that the difference is in terminology only and that mapped control address the ISO control.
ISO27001	A.16.1.1	A.16 Information security incident management / A.16.1 Management of information security incidents and improvements / A.16.1.1	A.16.1.1 Responsibilities and procedures: Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-01, SEF-02	SEF-01 is more specific on contacting authorities.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.16.1.2	A.16 Information security incident management / A.16.1 Management of information security incidents and improvements / A.16.1.2	A.16.1.2 Reporting information security events: Information security events shall be reported through appropriate management channels as quickly as possible.		To be decided (Mapping exists)	No gap		SEF-01, SEF-03, STA-05, GRM-04	CCM controls are more specific. SEF-01: to ensure direct compliance liaisons with authorities. SEF-03: Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations. STA-05: timely notification of a security incident (or confirmed breach) to all customers and other business relationships impacted is included in service agreements GRM-04: communication is part of the ISMP
ISO27001	A.16.1.3	A.16 Information security incident management / A.16.1 Management of information security	A.16.1.3 Reporting information security weaknesses: Employees and contractors using the organisation/s information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.		To be decided (Mapping exists)	No gap		TVM-02, SEF-03	CCM provides more specific cases. TVM-02: timely detection of vulnerabilities and reporting. SEF-03: incident reporting, not weaknesses

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		incidents and improvements / A.16.1.3							
ISO27001	A.16.1.4	A.16 Information security incident management / A.16.1 Management of information security incidents and improvements / A.16.1.4	A.16.1.4 Assessment of and decision on information security events: Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-02	I would argue that the difference is in terminology only and that mapped control address the ISO control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.16.1.5	A.16 Information security incident management / A.16.1 Management of information security incidents and improvements / A.16.1.5	A.16.1.5 Response to information security incidents: Information security incidents shall be responded to in accordance with the documented procedures.		To be decided (Mapping exists)	No gap		SEF-02, SEF-04, BCR-02	The basic mapping is covered by SEF-02. SEF-04 is more specific on proper forensic procedures. BCR-02 is more specific to set incident response plans that must be tested in planned intervals or upon significant organisational or environmental changes.
ISO27001	A.16.1.6	A.16 Information security incident management / A.16.1 Management of information security incidents and improvements / A.16.1.6	A.16.1.6 Learning from information security incidents: Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-05	I would argue that the difference is in terminology only and that mapped control address the ISO control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.16.1.7	A.16 Information security incident management / A.16.1 Management of information security incidents and improvements / A.16.1.7	A.16.1.7 Collection of evidence: The organisation shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.		To be decided (Mapping exists)	No gap		SEF-04, IAM-01, IVS-01	Diverse CCM controls define more specific procedures or tools: forensic procedures, audit tools and procedures to protect log data or audit logs. ISO control is general, CCM controls are more specific in different control domains.
ISO27001	A.17.1.1	A.17 Information security aspects of business continuity management / A.17.1 Information security continuity / A.17.1.1	A.17.1.1 Planning information security continuity: The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.		Business Continuity Management & Operational Resilience	No gap		BCR-01, GRM-09	I would argue that the mapped BCR/GRM controls don't represent a gap to the ISO control. BCR-01 is including detailed recovery procedures.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.17.1.2	A.17 Information security aspects of business continuity management / A.17.1 Information security continuity / A.17.1.2	A.17.1.2 Implementing information security continuity: The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.		Business Continuity Management & Operational Resilience	No gap		BCR-01, BCR-02, BCR-03, BCR-04, BCR-05, BCR-06, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11	CCM includes controls that cover individual aspects which contribute to ensure the level of continuity for information security.
ISO27001	A.17.1.3	A.17 Information security aspects of business continuity management / A.17.1 Information security continuity / A.17.1.3	A.17.1.3 Verify, review and evaluate information security continuity: The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.		Business Continuity Management & Operational Resilience	No gap		BCR-01, BCR-02, BCR-03, BCR-05, BCR-07, BCR-08, BCR-09, BCR-10, BCR-11, GRM-01, GRM-08, GRM-09, GRM-10	I would argue that the mapped BCR/GRM controls don't represent a gap to the ISO control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.17.2.1	A.17 Information security aspects of business continuity management / A.17.2 Redundancies / A.17.2.1	A.17.2.1 Availability of information processing facilities: Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.		Business Continuity Management & Operational Resilience	No gap		BCR-03, BCR-06, IAM-02	I would argue that the difference is in terminology only and that mapped control address the availability requirements.
ISO27001	A.18.1.1	A.18 Compliance / A.18.1 Compliance with legal and contractual requirements / A.18.1.1	A.18.1.1 Identification of applicable legislation and contractual requirements		Governance and Risk Management	No gap		AAC-03, STA-05, BCR-11, EKM-03, GRM-01, GRM-02, GRM-09, IVS-01, IVS-04, IVS-09, IVS-13, SEF-01, SEF-03, AIS-01	The main CCM controls are AAC-03 (legislation, regulatory requirements) and STA-05 (contractual requirements) cover the ISO requirement. Other CCM controls cover more specific areas where information security applies.
ISO27001	A.18.1.2	A.18 Compliance / A.18.1 Compliance with legal and contractual	A.18.1.2 Intellectual property rights		Governance and Risk Management	Partial gap		GRM-09	PARTIAL GAP Confirmed. However, GRM-09 might cover the control if IPR is considered as part of ISMS.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		requirements / A.18.1.2							
ISO27001	A.18.1.3	A.18 Compliance / A.18.1 Compliance with legal and contractual requirements / A.18.1.3	A.18.1.3 Protection of records		Infrastructure & Virtualization Security	No gap		EKM-03, IAM-01, IAM-07, IVS-01, IVS-06, SEF-04, SEF-05	Protection of records (e.g. audit logs, monitoring results, sensitive data) is covered by CCM control in diverse control domains where the records are generated or stored.
ISO27001	A.18.1.4	A.18 Compliance / A.18.1 Compliance with legal and contractual requirements / A.18.1.4	A.18.1.4 Privacy and protection of personally identifiable information: Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.		To be decided (Mapping exists)	Partial gap		PLA-1.1., PLA-3.3., PLA-5.1., PLA-6.1.	PARTIAL GAP Confirmed. This control is addressed by PLA V3 CoC. However, GRM-09 might cover the control on high level.
ISO27001	A.18.1.5	A.18 Compliance / A.18.1 Compliance with legal and contractual requirements / A.18.1.5	A.18.1.5 Regulation of cryptographic controls: Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.		Encryption & Key Management	No gap		EKM-01, EKM-02, EKM-03, EKM-04, AAC-03, IVS-10, IVS-12, MOS-11, IAM-02	Several CCM controls in diverse control areas which cover policies, procedures and implementation of encryption. ISO control is general, CCM controls are more topic specific. Improvement: implementation of encryption controls could be added to STA to cover third parties and contractors.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.18.2.1	A.18 Compliance / A.18.2 Information security reviews / A.18.2.1	A.18.2.1 Independent review of information security		Governance and Risk Management	No gap		GRM-09, GRM-06, GRM-10, AAC-01, AAC-02, AAC-03, IVS-06, STA-06, STA-07, STA-08, STA-09	GRM-09 defines the regular review of the information security policies. Other controls are more specific about the planning, review or audit in individual control domains (e.g. auditing, control framework review, review in supply-chain and agreements, risk assessment review, network configuration review, etc.)
ISO27001	A.18.2.2	A.18 Compliance / A.18.2 Information security reviews / A.18.2.2	A.18.2.2 Compliance with security policies and standards: Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.		Governance and Risk Management	No gap		GRM-03, GRM-05, GRM-06, GRM-09, AIS-04, AAC-03, BCR-01, DSI-02, DCS-06, IVS-06, IPY-03, STA-07, STA-08, STA-09	The ISO control is an important control to ensure that all areas will be continuously checked and that new development in information security could enter into the organisation's policy. The main CCM control is GRM-03, but other CCM controls include maintenance or review of policies or procedures, too.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27001	A.18.2.3	A.18 Compliance / A.18.2 Information security reviews / A.18.2.3	A.18.2.3 Technical compliance review: Information systems shall be regularly reviewed for compliance with the organisation's information security policies and standards.		Governance and Risk Management	No gap		GRM-01, AAC-02, IVS-06, IPY-05	Information system = applications, services, information technology assets, or other information handling components (ISO 27000). The technical review is not directly expressed in CCM, but in general, it is included in the regular review (AAC-02) and in GRM-01 (baseline security requirements which are focused on technical part). Some CCM control domains include more specific controls on the review of technical components (IVS-06, IPY-05). Comment: Technical Compliance Review (TCR): Information systems shall be documented, posted and reviewed on a regular basis for compliance with the organization's information security policies and standards and shall be in compliance with all appropriate; regulatory agencies, laws and jurisdictions.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	5.1.1	5 Information Security Policies / 5.1 - Management direction for information security / 5.1.1 Policies for information security	A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.		To be decided (Mapping exists)	No gap		BCR-11, GRM-06	There is NO gap due to the following: BCR-11: Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness. GRM-06: Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	5.1.2	5 Information Security Policies / 5.1 - Management direction for information security / 5.1.2 Review of the policies for information security	The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.		Governance and Risk Management	No gap		GRM-08, GRM-09	There is NO gap due to the following: GRM-08: Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective. GRM-09: The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	6.1.1	6 Organisation of information security / 6.1 - Internal organization / 6.1.1 Information security roles and responsibilities	All information security responsibilities shall be defined and allocated. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		BCR-10, CCC-03, DSI-06, GRM-04, HRS-07, SEF-03	There is NO gap due to the following: BCR-10: [...] policies and procedures shall include defined roles and responsibilities supported by regular workforce training. SEF-03: Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner.[...] DSI-06: All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated. HRS-07: Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	6.1.2	6 Organisation of information security / 6.1 - Internal organization / 6.1.2 Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.		To be decided (Mapping exists)	No gap		IVS-08, IAM-05	There is NO gap due to the following: IAM-05: User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest. IVS-08: Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: [...] clear segregation of duties for personnel accessing these environments as part of their job duties.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	6.1.3	6 Organisation of information security / 6.1 - Internal organization / 6.1.3 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained. (Includes cloud sector-specific implementation guidance for cloud services.)		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-01	There is NO gap due to the following: SEF-01: Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.
ISO27017	6.1.4	6 Organisation of information security / 6.1 - Internal organization / 6.1.4 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.		To be decided (No mapping)	Full gap			CCM contains no references to special interest groups, specialist security forums or professional associations.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	6.1.5	6 Organisation of information security / 6.1 - Internal organization / 6.1.5 Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.		To be decided (No mapping)	Full gap			CCM contains no references to projects or project management.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	6.2.1	6 Organisation of information security / 6.2 - Mobile devices and teleworking / 6.2.1 / Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.		To be decided (Mapping exists)	Partial gap		CCC-04 HRS-05 HRS-06 HRS-08 HRS-10 MOS-01 MOS-02 MOS-03 MOS-04 MOS-05 MOS-06 MOS-07 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-16 MOS-17 MOS-18 MOS-19 MOS-20 TVM-01 TVM-03	There is no specific reference to physical security. Even though is within other controls my recommendation is to be specific, since should be in-cluded within security policy. Specially, should be a specific procedure taking into account legal, insurance another secu-rity requirements established for cases of theft or loss of mobile devices. MOS-04 Could add a refer-ence to web apps. MOS-17 Implement additional control to identify backup failure (may not be backed-up because of limited network bandwidth or because the mobile is not connected at the times when backups are scheduled).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	6.2.2	6 Organisation of information security / 6.2 - Mobile devices and teleworking / 6.2.2 / Teleworking	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.		To be decided (No mapping)	Full gap			"There is no reference for teleworking in CCM Mapping. Take into account that many control ID can be related, such us anti-virus protection and firewall requirements, but none of them specified this subject."
ISO27017	7.1.1	7 Human resource security / 7.1 - Prior to employment / 7.1.1 Screening	Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.		Human Resources	No gap		HRS-02	-
ISO27017	7.1.2	7 Human resource security / 7.1 - Prior to employment / 7.1.2 Terms and conditions of employment	The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.		Human Resources	No gap		HRS-03, HRS-04, HRS-07	-

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	7.2.1	7 Human resource security / A.7.2 - During employment / 7.2.1 Management responsibilities	Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.		Human Resources	Partial gap		HRS-06, HRS-07, HRS-09, HRS-10	Minor gap based on the recommendation of ISO27002 The employees or contractors should be provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing")
ISO27017	7.2.2	7 Human resource security / A.7.2 - During employment / 7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		HRS-09, HRS-10, HRS-11, GRM-06	-
ISO27017	7.2.3	7 Human resource security / 7.2 - During employment / 7.2.3 Disciplinary process	There shall be a formal and communicated disciplinary process in place to take action against employees who have committed na information security breach.		Governance and Risk Management	No gap		GRM-07	-

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	7.3.1	7 Human resource security / 7.3 - Termination and change of employment / 7.3.1 Termination or change of employment responsibilities	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.		Human Resources	Partial gap		HRS-04	Must be specified that information security responsibilities and duties remain valid after termination or change of employment.
ISO27017	8.1.1	8 Asset management / 8.1 - Responsibility for assets / 8.1.1 Inventory of assets	Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		DCS-01, GRM-04	
ISO27017	8.1.2	8 Asset management / 8.1 - Responsibility for assets / 8.1.2 Ownership of assets	Assets maintained in the inventory shall be owned. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		DCS-01, DSI-06	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	8.1.3	8 Asset management / 8.1 - Responsibility for assets / 8.1.3 Acceptable use of assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.		To be decided (Mapping exists)	No gap		DCS-01, HRS-03, HRS-05, HRS-08, MOS-05	
ISO27017	8.1.4	8 Asset management / 8.1 - Responsibility for assets / 8.1.4 Return of assets	All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.		Human Resources	No gap		HRS-01	
ISO27017	8.2.1	8 Asset management / 8.2 - Information classification / 8.2.1 Classification of information	Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.		To be decided (Mapping exists)	No gap		DSI-01, DSI-03, GRM-02	
ISO27017	8.2.2	8 Asset management / 8.2 - Information classification /	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization. (Includes cloud sector-specific implementation guidance for cloud services.)		Data Security & Information Lifecycle Management	No gap		DSI-04	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		8.2.2 Labelling of information							
ISO27017	8.2.3	8 Asset management / 8.2 - Information classification / 8.2.3 Handling of assets	Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organisation.		Data Security & Information Lifecycle Management	No gap		DSI-04	
ISO27017	8.3.1	8 Asset management / 8.3 - Media handling / 8.3.1 Management of removable media	Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.		Data Security & Information Lifecycle Management	No gap		DSI-07	
ISO27017	8.3.2	8 Asset management / 8.3 - Media handling / 8.3.2 Disposal of media	Media shall be disposed of securely when no longer required, using formal procedures.		To be decided (Mapping exists)	No gap		DSI-07, DCS-05, GRM-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	8.3.3	8 Asset management / 8.3 - Media handling / 8.3.3 Physical media transfer	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.		Datacenter Security	Partial gap		DCS-04	While in CCM this control is oriented to getting authorization and just in the context of datacentre, in the ISO it is more oriented as a general term focusing on the security aspects to consider for media transfer. Suggestion would be to have a control under DSI section for the implementation of policies/procedures especially for "physical media transfer"
ISO27017	9.1.1	9 Access control / 9.1 - Business requirements of access control / 9.1.1 Access control policy	An access control policy shall be established, documented and reviewed based on business and information security requirements.		To be decided (Mapping exists)	No gap		IAM-02, AIS-02, CCC-01, CCC-02, HRS-05, GRM-06	
ISO27017	9.1.2	9 Access control / 9.1 Business requirements of access control / 9.1.2 Access to networks and	Users shall only be provided with access to the network and network services that they have been specifically authorized to use. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		IAM-02, IAM-03, IAM-04, IAM-06, IAM-08, IAM-09, IAM-13, IVS-06	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		network services							
ISO27017	9.2.1	9 Access control / 9.2 User access management / 9.2.1 User registration and de-registration	A formal user registration and de-registration process shall be implemented to enable assignment of access rights. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		IAM-02, IAM-04, IAM-07, IAM-09, IAM-11, IAM-12, IVS-12, MOS-20	(includes implementation guidance for cloud services)
ISO27017	9.2.2	9 Access control / 9.2 User access management / 9.2.2 User access provisioning	A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		IAM-02, IAM-04, IAM-07, IAM-09, IAM-11, IAM-12, IVS-12, MOS-20	(includes implementation guidance for cloud services)

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	9.2.3	9 Access control / 9.2 User access management / 9.2.3 Management of privileged access rights	The allocation and use of privileged access rights shall be restricted and controlled. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		IAM-04, IAM-08, IAM-09, IAM-11, IVS-01	(includes implementation guidance for cloud services)
ISO27017	9.2.4	9 Access control / 9.2 User access management / 9.2.4 Management of secret authentication information of users	The allocation of secret authentication information shall be controlled through a formal management process. (Includes cloud sector-specific implementation guidance for cloud services.)		Identity & Access Management	No gap		IAM-04, IAM-08, IAM-12	(includes implementation guidance for cloud services)
ISO27017	9.2.5	9 Access control / 9.2 User access management / 9.2.5 Review of user access rights	Asset owners shall review users' access rights at regular intervals.		To be decided (Mapping exists)	No gap		AIS-02, IAM-02, IAM-04, IAM-07, IAM-09, IAM-11, IAM-12, IVS-12, MOS-20	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	9.2.6	9 Access control / 9.2 User access management / 9.2.6 Removal or adjustment of access rights	The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.		To be decided (Mapping exists)	No gap		AIS-02, HRS-04, IAM-02, IAM-04, IAM-07, IAM-09, IAM-11, IAM-12, IVS-12, MOS-20	
ISO27017	9.3.1	9 Access control / 9.3 User responsibilities / 9.3.1 Use of secret authentication information	Users shall be required to follow the organization's practices in the use of secret authentication information.		To be decided (Mapping exists)	No gap		IAM-02, EKM-03	
ISO27017	9.4.1	9 Access control / 9.4 System and application access control / 9.4.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		AIS-02, IAM-08	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	9.4.2	9 Access control / 9.4 System and application access control / 9.4.2 Secure log-on procedures	Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.		Infrastructure & Virtualization Security	Partial gap		IVS-11	CCM needs to specify that credentials should be protected in storage, transit, and use. Authentication repositories should be protected at all times from various threat vectors. Authentication session timeouts should be kept to a minimum at all times.
ISO27017	9.4.3	9 Access control / 9.4 System and application access control / 9.4.3 Password management system	Password management systems shall be interactive and shall ensure quality passwords.		To be decided (No mapping)	Full gap			Password management systems shall be interactive and shall ensure quality passwords.
ISO27017	9.4.4	9 Access control / 9.4 System and application access control / 9.4.4 Use of privileged utility programs	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		CCC-04, IAM-03, IAM-13, IVS-01	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	9.4.5	9 Access control / 9.4 System and application access control / 9.4.5 Access control to program source code	Access to program source code shall be restricted.		Identity & Access Management	No gap		IAM-06	
ISO27017	10.1.1	10 Cryptography / 10.1 Cryptographic controls / 10.1.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.		Encryption & Key Management	No gap		EKM-01, EKM-02, EKM-03, EKM-04	
ISO27017	10.1.2	10 Cryptography / 10.1 Cryptographic controls / 10.1.2 Key management	A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.		Encryption & Key Management	Partial gap		EKM-02	Update EKKM-02 to cover: 27002-10.1.2 (f) Dealing with key compromise 27002-10.1.2 (h) Recovering keys that are lost or corrupted 27002-10.1.2 (j) Destroying keys 27002-10.1.2 (k) Logging and auditing of key management related activities

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	11.1.1	11 Physical and environmental security / 11.1 Secure areas / 11.1.1 Physical security perimeter	Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.		Datacenter Security	No gap		DCS-02	
ISO27017	11.1.2	11 Physical and environmental security / 11.1 Secure areas / 11.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.		Datacenter Security	No gap		DCS-07	
ISO27017	11.1.3	11 Physical and environmental security / 11.1 Secure areas / 11.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.		Datacenter Security	No gap		DCS-02	
ISO27017	11.1.4	11 Physical and environmental security / 11.1 Secure areas / 11.1.4 Protecting against external and	Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.		Business Continuity Management & Operational Resilience	No gap		BCR-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		environmental threats							
ISO27017	11.1.5	11 Physical and environmental security / 11.1 Secure areas / 11.1.5 Working in secure areas	Procedures for working in secure areas shall be designed and applied.		To be decided (Mapping exists)	No gap		DCS-06 HRS-11	Error: DCS-06 instead of BCS-06?
ISO27017	11.1.6	11 Physical and environmental security / 11.1 Secure areas / 11.1.6 Delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.		Datacenter Security	No gap		DCS-08	
ISO27017	11.2.1	11 Physical and environmental security / 11.2 Equipment / 11.2.1 Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.		To be decided (Mapping exists)	No gap		DCS-02, DCS-07, DCS-08, BCR-05, BCR-06, BCR-08	
ISO27017	11.2.2	11 Physical and environmental security / 11.2 Equipment / 11.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.		Business Continuity Management & Operational Resilience	No gap		BCR-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	11.2.3	11 Physical and environmental security / 11.2 Equipment / 11.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.		Business Continuity Management & Operational Resilience	No gap		BCR-07	
ISO27017	11.2.4	11 Physical and environmental security / 11.2 Equipment / 11.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.		Business Continuity Management & Operational Resilience	No gap		BCR-06, BCR-07, BCR-08	
ISO27017	11.2.5	11 Physical and environmental security / 11.2 Equipment / 11.2.5 Removal of assets	Equipment, information or software shall not be taken off-site without prior authorization.		Datacenter Security	No gap		DCS-04, DCS-08	
ISO27017	11.2.6	11 Physical and environmental security / 11.2 Equipment / 11.2.6 Security of equipment and assets off-premises	Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.		To be decided (Mapping exists)	No gap		DCS-04, HRS-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	11.2.7	11 Physical and environmental security / 11.2 Equipment / 11.2.7 Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		DSI-07, DCS-05	Error: DSI-07 instead of DCI-07?
ISO27017	11.2.8	11 Physical and environmental security / 11.2 Equipment / 11.2.8 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.		Human Resources	No gap		HRS-11, HRS-10	
ISO27017	11.2.9	11 Physical and environmental security / 11.2 Equipment / 11.2.9 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.		To be decided (Mapping exists)	Partial gap		DCS-06, HRS-11	27002-11.2.9 is more explicit.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	12.1.1	12 Operations security / 12.1 Operational procedures and responsibilities / 12.1.1 Documented operating procedures	Operating procedures shall be documented and made available to all users who need them.		To be decided (Mapping exists)	No gap		GRM-04 (closest), GRM-06 The following are highly related as well: IVS-01, IAM-13, HRS-07, HRS-08, IVS-07, CCC-03, DSI-04, DSI-07, AIS-02, BCR-01, BCR-04, BCR-09, BCR-11, CCC-01, CCC-02, DSI-02, DSI-06, GRM-05, HRS-06, HRS-07,	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
								HRS-11, IAM-06, IAM-09, IVS-04, IVS-06, IPY-04, IPY-05, MOS-02, MOS-03, MOS-05, MOS-07, MOS-16	
ISO27017	12.1.2	12 Operations security / 12.1 Operational procedures and responsibilities / 12.1.2 Change management	Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.		To be decided (Mapping exists)	No gap		CCC-01, CCC-02, CCC-03, CCC-04, CCC-05, GRM-01, GRM-10, BCR-09, IVS-02, GRM-08, STA-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	12.1.3	12 Operations security / 12.1 Operational procedures and responsibilities / 12.1.3 Capacity management	The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.		To be decided (Mapping exists)	No gap		IVS-04, STA-03	
ISO27017	12.1.4	12 Operations security / 12.1 Operational procedures and responsibilities / 12.1.4 Separation of development, testing and operational environments	Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.		To be decided (Mapping exists)	No gap		IVS-08, CCC-02, CCC-03, DSI-05	
ISO27017	12.2.1	12 Operations security / 12.2 Protection from malware / 12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.		To be decided (Mapping exists)	No gap		TVM-01, MOS-01, MOS-17, CCC-04, IVS-07, TVM-03, MOS-04, MOS-03, MOS-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	12.3.1	12 Operations security / 12.3 Backup / 12.3.1 Information backup	Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		BCR-09, BCR-10, BCR-11, BCR-02, BCR-06, AIS-04, STA-05	Individual jurisdictions may impose specific requirements regarding the frequency of reviews of backup and recovery procedures. Organizations operating in these jurisdictions should ensure that they comply with these requirements. (AIS-04 and STA-05 closely align with this requirement from 27018. It may require discussion among the group to determine if the CCM controls fully meet the requirement).
ISO27017	12.4.1	12 Operations security / 12.4 - Logging and monitoring / 12.4.1 Event logging	Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		IVS-01, BCR-03, DSI-03, IAM-01, SEF-02, SEF-03, IVS-02, IVS-07, IVS-09, IVS-12, IVS-06, IVS-07, CCC-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	12.4.2	12 Operations security / 12.4 - Logging and monitoring / 12.4.2 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.		To be decided (Mapping exists)	No gap		IVS-01, IVS-02, IVS-07, IAM-01, IPY-03, STA-01, STA-05, AIS-03, AIS-04, CCC-03 IVS-04, CCC-02	
ISO27017	12.4.3	12 Operations security / 12.4 - Logging and monitoring / 12.4.3 Administrator and operator logs	System administrator and system operator activities shall be logged and the logs protected and regularly reviewed. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		IVS-01, IVS-02, IAM-07, CCC-04, HRS-08, IAM-02, IAM-05	
ISO27017	12.4.4	12 Operations security / 12.4 - Logging and monitoring / 12.4.4 Clock synchronisation	The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source. (Includes cloud sector-specific implementation guidance for cloud services.)		Infrastructure & Virtualization Security	No gap		IVS-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	12.5.1	12 Operations security / 12.5 Control of operational software / 12.5.1 Installation of software on operational systems	Procedures shall be implemented to control the installation of software on operational systems.		To be decided (Mapping exists)	No gap		CCC-04, IVS-08, CCC-03, MOS-02, MOS-03, MOS-04, MOS-15, MOS-17	
ISO27017	12.6.1	12 Operations security / 12.6 Technical vulnerability management / 12.6.1 Management of technical vulnerabilities	Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		GRM-10, GRM-11, TVM-02, IVS-05, STA-01, IVS-04	
ISO27017	12.6.2	12 Operations security / 12.6 Technical vulnerability management / 12.6.2 Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.		To be decided (Mapping exists)	No gap		CCC-04, MOS-03, TVM-03, IAM-13	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	12.7.1	12 Operations security / 12.7 Information systems audit considerations / 12.7.1 Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.		To be decided (Mapping exists)	No gap		AAC-01, IAM-01	
ISO27017	13.1.1	13 Communications security / 13.1 Network security management / 13.1.1 Network controls	Networks shall be managed and controlled to protect information in systems and applications.		Infrastructure & Virtualization Security	No gap		IVS-06, IVS-09, IVS-12	
ISO27017	13.1.2	13 Communications security / 13.1 Network security management / 13.1.2 Security of network services	Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.		Infrastructure & Virtualization Security	No gap		IVS-06, IVS-09, IVS-12	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	13.1.3	13 Communications security / 13.1 Network security management / 13.1.3 Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.		Infrastructure & Virtualization Security	No gap		IVS-06, IVS-09, IVS-12	
ISO27017	13.2.1	13 Communications security / 13.2 Information transfer / 13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.		To be decided (Mapping exists)	No gap		IVS-06, IVS-09, TVM-03	
ISO27017	13.2.2	13 Communications security / 13.2 Information transfer / 13.2.2 Agreements on information transfer	Agreements shall address the secure transfer of business information between the organization and external parties.		To be decided (Mapping exists)	No gap		HRS-06, IVS-06, IVS-09, TVM-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	13.2.3	13 Communications security / 13.2 Information transfer / 13.2.3 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.		To be decided (Mapping exists)	No gap		EKM-03, IVS-06, IVS-09	
ISO27017	13.2.4	13 Communications security / 13.2 Information transfer / 13.2.4 Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.		Human Resources	No gap		HRS-06	
ISO27017	14.1.1	14 System acquisition, development and maintenance / 14.1 Security requirements of information systems / 14.1.1 Information security requirements	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		CCC-01, CCC-02, CCC-03, CCC-05, GRM-01	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		analysis and specification							
ISO27017	14.1.2	14 System acquisition, development and maintenance / 14.1 Security requirements of information systems / 14.1.2 Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.		To be decided (No mapping)	Full gap			
ISO27017	14.1.3	14 System acquisition, development and maintenance / 14.1 Security requirements of information systems / 14.1.3 Protecting application services transactions	Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	14.2.1	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.1 Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		AIS-01, CCC-01, CCC-02, IAM-06, TVM-02	
ISO27017	14.2.2	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.2 System change control procedures	Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.		To be decided (Mapping exists)	No gap		CCC-05, TVM-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	14.2.3	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.3 Technical review of applications after operating platform changes	When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.		To be decided (Mapping exists)	No gap		CCC-03, CCC-05, TVM-02	
ISO27017	14.2.4	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.4 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.		To be decided (Mapping exists)	Partial gap		CCC-05, TVM-02	More specific and explicit guidelines should be added in the CCM to strictly control the changes to software packages

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	14.2.5	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.5 Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.		To be decided (Mapping exists)	No gap		IVS-02, IVS-03, IVS-04, IVS-11, IVS-10, MOS-15	
ISO27017	14.2.6	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.6 Secure development environment	Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.		To be decided (Mapping exists)	No gap		IVS-08, IAM-06, DSI-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	14.2.7	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.7 Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.		Change Control & Configuration Management	No gap		CCC-02	
ISO27017	14.2.8	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.8 System security testing	Testing of security functionality shall be carried out during development.		To be decided (Mapping exists)	No gap		AIS-01, CCC-03, MOS-07	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	14.2.9	14 System acquisition, development and maintenance / 14.2 Security in development and support processes / 14.2.9 System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.		To be decided (Mapping exists)	Partial gap		AIS-01, CCC-03, MOS-07	CCM controls include security testing but don't explicitly mention specifically the acceptance testing
ISO27017	14.3.1	14 System acquisition, development and maintenance / 14.3 Test data / 14.3.1 Protection of test data	Test data shall be selected carefully, protected and controlled.		Data Security & Information Lifecycle Management	Partial gap		DSI-05, DSI-06	Explicit requirements to protect (via authorisation, access control, logging and destruction) the use of operational (confidential and PII) as test data.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	15.1.1	15 Supplier relationships / 15.1 Information security in supplier relationships / 15.1.1 Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.		To be decided (Mapping exists)	No gap		BCR-10, BCR-11, CCC-01 to CCC-05, DCS-01, DCS-05, DCS-06, DCS-09, GRM-01, GRM-04, GRM-06, GRM-07, GRM-08, GRM-09, GRM-10, GRM-11, IAM-02, IAM-09, STA-01, STA-07, STA-08, TVM-01, TVM-02, TVM-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	15.1.2	15 Supplier relationships / 15.1 Information security in supplier relationships / 15.1.2 Addressing security within supplier agreements	All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information		To be decided (Mapping exists)	No gap		CCC-02, IAM-02, IAM-09, STA-03, STA-05,STA-09	
ISO27017	15.1.3	15 Supplier relationships / 15.1 Information security in supplier relationships / 15.1.3 Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.		To be decided (Mapping exists)	No gap		BCR-10, BCR-11, CCC-01 to CCC-05, DCS-01, DCS-05, DCS-06, DCS-09, GRM-01, GRM-04, GRM-06, GRM-07, GRM-08, GRM-09, GRM-11, IAM-02, IAM-	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
								09, STA-07, STA-08, TVM-01, TVM-02, TVM-03	
ISO27017	15.2.1	15 Supplier relationships / 15.2 Supplier service delivery management / 15.2.1 Monitoring and review of supplier services	Organizations shall regularly monitor, review and audit supplier service delivery.		To be decided (Mapping exists)	No gap		IAM-02, IAM-09, STA-01, STA-02, STA-04, STA-05, STA-06, STA-07, STA-08	
ISO27017	15.2.2	15 Supplier relationships / 15.2 Supplier service delivery management / 15.2.2 Managing changes to supplier services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.		Supply Chain Management, Transparency, and Accountability	Partial gap		STA-01, STA-02, STA-04, STA-05, STA-06, STA-07, STA-08	Explicit information about handling changes to the provision of services.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	16.1.1	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	Partial gap		SEF-01, SEF-03, IVS-01, IVS-02	No CCM control specifies the scope of security incidents the provider will report or the level of disclosure. Ref: The cloud service provider should provide the cloud service customer with documentation covering: — the scope of information security incidents that the cloud service provider will report to the cloud service customer; — the level of disclosure of the detection of information security incidents and the associated responses;
ISO27017	16.1.2	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.2 Reporting	Information security events shall be reported through appropriate management channels as quickly as possible. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		SEF-02, SEF-03, IVS-01, IVS-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		information security events							
ISO27017	16.1.3	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.3 Reporting information security weaknesses	Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.		To be decided (Mapping exists)	No gap		SEF-02, SEF-03, CCC-02, IVS-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	16.1.4	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.4 Assessment of and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.		To be decided (Mapping exists)	No gap		SEF-02, IVS-02	
ISO27017	16.1.5	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.5 Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.		To be decided (Mapping exists)	No gap		SEF-02, SEF-03, IVS-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	16.1.6	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.6 Learning from information security incidents	Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-05	
ISO27017	16.1.7	16 Information security incident management / 16.1 - Management of information security incidents and improvements / 16.1.7 Collection of evidence	The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-04	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	17.1.1	17 Information security aspects of business continuity management / 17.1 Information security continuity / 17.1.1 Planning information security continuity	The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.		To be decided (Mapping exists)	No gap		BCR-09, GRM-11	
ISO27017	17.1.2	17 Information security aspects of business continuity management / 17.1 Information security continuity / 17.1.2 Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.		Business Continuity Management & Operational Resilience	No gap		BCR-01, BCR-09	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	17.1.3	17 Information security aspects of business continuity management / 17.1 Information security continuity / 17.1.3 Verify, review and evaluate information security continuity	The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.		To be decided (Mapping exists)	No gap		BCR-02, CCC-03, GRM-09	
ISO27017	17.2.1	17 Information security aspects of business continuity management / 17.2 Redundancies / 17.2.1 Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.		To be decided (Mapping exists)	No gap		BCR-03, BCR-05, BCR-06, STA-03, STA-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	18.1.1	18 Compliance / 18.1 Compliance with legal and contractual requirements / 18.1.1 Identification of applicable legislation and contractual requirements	All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization. (Includes cloud sector-specific implementation guidance for cloud services.)		Audit Assurance & Compliance	No gap		AAC-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	18.1.2	18 Compliance / 18.1 Compliance with legal and contractual requirements / 18.1.2 Intellectual property rights	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products. (Includes cloud sector-specific implementation guidance for cloud services.)		Change Control & Configuration Management	Partial gap		CCC-01, CCC-04	Edit CCC-01 to read: Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data centre facilities have been pre-authorized by the organization's business leadership or other accountable business role or function. All new acquisitions must comply with legislative, regulatory, and contractual requirements related to intellectual property rights and use of proprietary software products.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	18.1.3	18 Compliance / 18.1 Compliance with legal and contractual requirements / 18.1.3 Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	Partial gap		EKM-03, GRM-02, IVS-01	No new controls needed. This is covered, but spread over multiple CCM controls.
ISO27017	18.1.4	18 Compliance / 18.1 Compliance with legal and contractual requirements / 18.1.4 Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.		To be decided (No mapping)	Full gap			New control matching the ISO language (AIS-05?): Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.
ISO27017	18.1.5	18 Compliance / 18.1 Compliance with legal and contractual requirements / 18.1.5 Regulation of	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations. (Includes cloud sector-specific implementation guidance for cloud services.)		Encryption & Key Management	No gap		EKM-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
		cryptographic controls							
ISO27017	18.2.1	18 Compliance / 18.2 Information security reviews / 18.2.1 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		GRM-06, GRM-02, GRM-09, CCC-02, AAC-02, AAC-03, STA-01, STA-07	GRM-06 (27017 CSP-specific guidance: The cloud service provider should provide documented evidence to the cloud service customer to substantiate its claim of implementing information security controls), GRM-02, GRM-09 (27017 CSP-specific guidance: In lieu of independent audit, at minimum a self-assessment will be performed), CCC-02, AAC-02, AAC-03, STA-01 (27017 CSP-specific guidance: In lieu of independent audit, at minimum a self-assessment will be performed), STA-07.
ISO27017	18.2.2	18 Compliance / 18.2 Information security reviews / 18.2.2 Compliance with security policies and standards	Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.		Governance and Risk Management	No gap		GRM-09	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	18.2.3	18 Compliance / 18.2 Information security reviews / 18.2.3 Technical compliance review	Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.		Governance and Risk Management	No gap		GRM-09	
ISO27017	CLD.6.3.1	Annex A - Cloud service extended control set / CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment	Responsibilities for shared information security roles in the use of the cloud service should be allocated to identified parties, documented, communicated and implemented by both the cloud service customer and cloud service provider. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		HRS-07, HRS-10, STA-05, DSI-06, SEF-03	
ISO27017	CLD.8.1.5	Annex A - Cloud service extended control set / CLD.8.1.5 Removal of cloud service customer assets	Assets of the cloud service customer that are on the cloud service provider's premises should be removed, and returned if necessary, in a timely manner upon termination of the cloud service agreement. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		STA-05, DSI-07	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	CLD.9.5.1	Annex A - Cloud service extended control set / CLD.9.5.1 Segregation in virtual computing environment	A cloud service customer's virtual environment running on a cloud service should be protected from other cloud service customers and unauthorized persons. (Includes cloud sector-specific implementation guidance for cloud services.)		Infrastructure & Virtualization Security	No gap		IVS-01, IVS-09, IVS-11	
ISO27017	CLD.9.5.2	Annex A - Cloud service extended control set / CLD.9.5.2 Virtual machine hardening	Virtual machines in a cloud computing environment should be hardened to meet business needs. (Includes cloud sector-specific implementation guidance for cloud services.)		Infrastructure & Virtualization Security	No gap		IVS-06, IVS-07, IVS-11	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	CLD.12.1.5	Annex A - Cloud service extended control set / CLD.12.1.5 Administrator's operational security	Procedures for administrative operations of a cloud computing environment should be defined, documented and monitored. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	No gap		AIS-04, AAC-02, BCR-01, BCR-07, BCR-10, AIS-04, BCR-10, BCR-11, CCC-01, CCC-04, DSI-07, DCS-05, DCS-06, EKM-02, EKM-03, HRS-08, IAM-02, IAM-04, IAM-05, IAM-08, IVS-12, IPY-03, SEF-02, TVM-01, TVM-02, GRM-06	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27017	CLD.12.4.5	Annex A - Cloud service extended control set / CLD.12.4.5 Monitoring of cloud services	The cloud service customer should have the capability to monitor specified aspects of the operation of the cloud services that the cloud service customer uses. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	Partial gap		SEF-05, IAM-07, IVS-01, IVS-07	The monitoring controls are quite covered by the controls included in CCM. However, these controls do not specifically mention that the monitoring capability should be at the disposal of the cloud customer which is an important attribute in the control
ISO27017	CLD.13.1.4	Annex A - Cloud service extended control set / CLD.13.1.4 Alignment of security management for virtual and physical networks	Upon configuration of virtual networks, consistency of configurations between virtual and physical networks should be verified based on the cloud service provider's network security policy. (Includes cloud sector-specific implementation guidance for cloud services.)		To be decided (Mapping exists)	Partial gap		IVS-01, IVS-04, IVS-05, IVS-09, IVS-06	The monitoring controls are quite covered by the controls included in CCM. However, these controls do not specifically mention the consistency between the virtual and physical networks which is an important attribute in the control

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.1.1	Public cloud PII processor extended control set for PII protection - A.1 Consent and choice / A.1.1 Obligation to co-operate regarding PII principals' rights	Control The public cloud PII processor should provide the cloud service customer with the means to enable them to fulfil their obligation to facilitate the exercise of PII principals' rights to access, correct and/or erase PII pertaining to them. Public cloud PII protection implementation guidance The PII controller's obligations in this respect may be defined by law, by regulations or by contract. These obligations may include matters where the cloud service customer uses the services of the public cloud PII processor for implementation. For example, this could include the correction or deletion of PII in a timely fashion. Where the PII controller depends on the public cloud PII processor for information or technical measures to facilitate the exercise of PII principals' rights, the relevant information or technical measures should be specified in the contract.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.2.1	Public cloud PII processor extended control set for PII protection - A.2 Purpose legitimacy and specifications / A.2.1 Public cloud PII processor's purpose	Control PII to be processed under a contract should not be processed for any purpose independent of the instructions of the cloud service customer. Public cloud PII protection implementation guidance Instructions may be contained in the contract between the public cloud PII processor and the cloud service customer including, e.g., the objective and time frame to be achieved by the service. In order to achieve the cloud service customer's purpose, there may be technical reasons why it is appropriate for a public cloud PII processor to determine the method for processing PII, consistent with the general instructions of the cloud service customer but without the cloud service customer's express instruction. For example, in order to efficiently utilize network or processing capacity it may be necessary to allocate specific processing resources depending on certain characteristics of the PII principal. In circumstances where the public cloud PII processor's determination of the processing method involves the collection and use of PII, the public cloud PII processor should adhere to the relevant privacy principles set forth in ISO/IEC 29100. The public cloud PII processor should provide		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			the cloud service customer with all relevant information, in a timely fashion, to allow the cloud service customer to ensure the public cloud PII processor's compliance with purpose specification and limitation principles and ensure that no PII is processed by the public cloud PII processor or any of its sub-contractors for further purposes independent of the instructions of the cloud service customer.						
ISO27018	A.2.2	Public cloud PII processor extended control set for PII protection - A.2 Purpose legitimacy and specifications / A.2.2 Public cloud PII processor's commercial use	Control PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service. NOTE This control is an addition to the more general control in A.2.1 and does not replace or otherwise supersede it.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.4.1	Public cloud PII processor extended control set for PII protection - A.4 Data minimisation / A.4.1 Secure erasure of temporary files	Control Temporary files and documents should be erased or destroyed within a specified, documented period. Public cloud PII protection implementation guidance Implementation guidance on PII erasure is provided in A.10.11. Information systems may create temporary files in the normal course of their operation. Such files are specific to the system or application, but may include file system roll-back journals and temporary files associated with the updating of databases and the operation of other application software. Temporary files are not needed after the related information processing task has completed but there are circumstances in which they may not be deleted. The length of time for which these files remain in use is not always deterministic but a "garbage collection" procedure should identify the relevant files and determine how long it has been since they were last used. PII processing information systems should implement a periodic check that unused temporary files above a specified age are deleted.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.5.1	Public cloud PII processor extended control set for PII protection - A.5 Use, retention and disclosure limitation / A.5.1 PII disclosure notification Control	The contract between the public cloud PII processor and the cloud service customer should require the public cloud PII processor to notify the cloud service customer, in accordance with any procedure and time periods agreed in the contract, of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited. Public cloud PII protection implementation guidance The public cloud PII processor should provide contractual guarantees that it will reject any requests for PII disclosure that are not legally binding, consult the corresponding cloud service customer where legally permissible before making any PII disclosure and accept any contractually agreed requests for PII disclosures that are authorized by the corresponding cloud service customer. An example of a possible prohibition on disclosure would be a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.5.2	Public cloud PII processor extended control set for PII protection - A.5 Use, retention and disclosure limitation / A.5.2 Recording of PII disclosures	Control Disclosures of PII to third parties should be recorded, including what PII has been disclosed, to whom and at what time. Public cloud PII protection implementation guidance PII may be disclosed during the course of normal operations. These disclosures should be recorded (see 12.4.1). Any additional disclosures to third parties, such as those arising from lawful investigations or external audits, should also be recorded. The records should include the source of the disclosure and the source of the authority to make the disclosure.		To be decided (No mapping)	Full gap			
ISO27018	A.7.1	Public cloud PII processor extended control set for PII protection - A.7 Openness, transparency and notice / A.7.1 Disclosure of sub-contracted PII processing	Control The use of sub-contractors by the public cloud PII processor to process PII should be disclosed to the relevant cloud service customers before their use. Public cloud PII protection implementation guidance Provisions for the use of sub-contractors to process PII should be transparent in the contract between the public cloud PII processor and the cloud service customer. The contract should specify that sub-contractors may only be commissioned on the basis of a consent that can generally be given by the cloud service		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			customer at the beginning of the service. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract. Information disclosed should cover the fact that sub-contracting is used and the names of relevant sub- contractors, but not any business-specific details. The information disclosed should also include the countries in which sub-contractors may process data (see A.11.1) and the means by which sub-contractors are obliged to meet or exceed the obligations of the public cloud PII processor (see A.10.12). Where public disclosure of sub-contractor information is assessed to increase security risk beyond acceptable limits, disclosure should be made under a non-disclosure agreement and/or on the request of the cloud service customer. The cloud service customer should be made aware that the information is available.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.9.1	Public cloud PII processor extended control set for PII protection - A.9 Accountability / A.9.1 Notification of a data breach involving PII	Control The public cloud PII processor should promptly notify the relevant cloud service customer in the event of any unauthorized access to PII or unauthorized access to processing equipment or facilities resulting in loss, disclosure or alteration of PII. Public cloud PII protection implementation guidance Provisions covering the notification of a data breach involving PII should form part of the contract between the public cloud PII processor and the cloud service customer. The contract should specify how the public cloud PII processor will provide the information necessary for the cloud service customer to fulfil his obligation to notify relevant authorities. This notification obligation does not extend to a data breach caused by the cloud service customer or PII principal or within system components for which they are responsible. The contract should also define the maximum delay in notification of a data breach involving PII. In the event that a data breach involving PII has occurred, a record should be maintained with a description of the incident, the time period, the consequences of the incident, the name of the reporter, to whom the incident was reported, the steps taken to resolve the incident		To be decided (Mapping exists)	No gap		IAM-07, IAM-11, IAM-12, IVS-06	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			(including the person in charge and the data recovered) and the fact that the incident resulted in loss, disclosure or alteration of PII. In the event that a data breach involving PII has occurred, the record should also include a description of the data compromised, if known; and if notifications were performed, the steps taken to notify the cloud service customer and/or regulatory agencies. In some jurisdictions, relevant legislation or regulations may require the public cloud PII processor to directly notify appropriate regulatory authorities (e.g., a PII protection authority) of a data breach involving PII. NOTE There may be other breaches requiring notification that are not covered here, e.g., collection without consent or other authorization, use for unauthorized purposes, etc.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.9.2	A.9 Accountability / A.9.2 Retention period for administrative security policies and guidelines	Control Copies of security policies and operating procedures should be retained for a specified, documented period upon replacement (including updating). Public cloud PII protection implementation guidance Review of current and historical policies and procedures may be required, e.g., in the cases of customer dispute resolution and investigation by a PII protection authority. A minimum retention period of five years is recommended in the absence of a specific legal or contractual requirement.		To be decided (Mapping exists)	No gap		IAM-04, IAM-07, IAM-08, IAM-10, IAM-11, IAM-12, IVS-01	
ISO27018	A.9.3	A.9 Accountability / A.9.3 PII return, transfer and disposal	Control The public cloud PII processor should have a policy in respect of the return, transfer and/or disposal of PII and should make this policy available to the cloud service customer. Public cloud PII protection implementation guidance At some point in time, PII may need to be disposed of in some manner. This may involve returning the PII to the cloud service customer, transferring it to another public cloud PII processor or to a PII controller (e.g., as a result of a merger), securely deleting or otherwise destroying it, anonymizing it or archiving it.		Identity & Access Management	Partial gap		IAM-08	IAM-08 covers the principle of least privilege to identities. All other aspects of this control are not covered.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			The public cloud PII processor should provide the information necessary to allow the cloud service customer to ensure that PII processed under a contract is erased (by the public cloud PII processor and any of its sub- contractors) from wherever they are stored, including for the purposes of backup and business continuity, as soon as they are no longer necessary for the specific purposes of the cloud service customer. The nature of the disposition mechanisms (de-linking, overwriting, demagnetization, destruction or other forms of erasure) and/or the applicable commercial standards should be provided for contractually. The public cloud PII processor should develop and implement a policy in respect of the disposition of PII and should make this policy available to cloud service customer. The policy should cover the retention period for PII before its destruction after termination of a contract, to protect the cloud service customer from losing PII through an accidental lapse of the contract. NOTE This control and guidance is also relevant under the retention element of the "Use, retention and disclosure limitation" principle (see A.5).						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.10.1	A.10 Information security / A.10.1 Confidentiality or non-disclosure agreements	Control Individuals under the public cloud PII processor's control with access to PII should be subject to a confidentiality obligation. Public cloud PII protection implementation guidance A confidentiality agreement, in whatever form, between the public cloud PII processor, its employees and its agents should ensure that employees and agents do not disclose PII for purposes independent of the instructions of the cloud service customer (see A.2.1). The obligations of the confidentiality agreement should survive termination of any relevant contract. A.10.2 Restriction of the creation of hardcopy material ControlThe creation of hardcopy material displaying PII should be restricted. Public cloud PII protection implementation guidanceHardcopy material includes material created by printing.		Human Resources	Partial gap		HRS-03	HRS-03 covers standard company NDA obligations.
ISO27018	A.10.2	A.10 Information security / A.10.2 Restriction of the creation of hardcopy material	The creation of hardcopy material displaying PII should be restricted. Public cloud PII protection implementation guidance Hardcopy material includes material created by printing.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.10.3	A.10 Information security / A.10.3 Control and logging of data restoration	Control There should be a procedure for, and a log of, data restoration efforts. Public cloud PII protection implementation guidance NOTE The above control makes generic the following requirement which applies in certain legal jurisdictions. The log of data restoration efforts should contain: the person responsible, a description of the restored data, and the data that were restored manually.		To be decided (No mapping)	Full gap			
ISO27018	A.10.4	A.10 Information security / A.10.4 Protecting data on storage media leaving the premises	Control PII on media leaving the organization's premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g., by encrypting the data concerned).		To be decided (Mapping exists)	No gap		DCS-04, DCS-05, MOS-11, EKM-03	
ISO27018	A.10.5	A.10 Information security / A.10.5 Use of unencrypted portable storage media and devices	Control Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.		Encryption & Key Management	Partial gap		EKM-03	EKM-03 lacks specific mention of portable physical media and portal devices.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.10.6	A.10 Information security / A.10.6 Encryption of PII transmitted over public data-transmission networks	Control PII that is transmitted over public data-transmission networks should be encrypted prior to transmission. Public cloud PII protection implementation guidance In some cases, e.g., the exchange of e-mail, the inherent characteristics of public data-transmission network systems might require that some header or traffic data be exposed for effective transmission. Where multiple service providers are involved in providing service from different service categories of the cloud computing reference architecture, there may be varied or shared roles in implementing this guidance.		To be decided (No mapping)	Full gap			
ISO27018	A.10.7	A.10 Information security / A.10.7 Secure disposal of hardcopy materials	Control Where hardcopy materials are destroyed, they should be destroyed securely using mechanisms such as cross-cutting, shredding, incinerating, pulping, etc.		To be decided (No mapping)	Full gap			DSI-07 covers secure disposal of electronic data.
ISO27018	A.10.8	A.10 Information security / A.10.8 Unique use of user IDs	Control If more than one individual has access to stored PII, then they should each have a distinct user ID for identification, authentication and authorization purposes.		To be decided (No mapping)	Full gap			IAM-02, IAM-04, though not specific to PII.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.10.9	A.10 Information security / A.10.9 Records of authorized users Control	An up-to-date record of the users or profiles of users who have authorized access to the information system should be maintained. Public cloud PII protection implementation guidance A user profile should be maintained for all users whose access is authorized by the public cloud PII processor. The profile of a user comprises the set of data about that user, including user ID, necessary to implement the technical controls providing authorized access to the information system.		Identity & Access Management	No gap		IAM-04	
ISO27018	A.10.10	A.10 Information security / A.10.10 User ID management	Control De-activated or expired user IDs should not be granted to other individuals. Public cloud PII protection implementation guidance In the context of the whole cloud computing reference architecture, the cloud service customer may be responsible for some or all aspects of user ID management for cloud service users under its control.		Identity & Access Management	No gap		IAM-12	
ISO27018	A.10.11	A.10 Information security / A.10.11 Contract measures	Control Contracts between the cloud service customer and the public cloud PII processor should specify minimum technical and organizational measures to ensure that the contracted security arrangements are in place and that data is not		To be decided (No mapping)	Full gap			No other control. Required to be more specific about PII information, because STA-05 is generic and don't have PII restrictions.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			processed for any purpose independent of the instructions of the controller. Such measures should not be subject to unilateral reduction by the public cloud PII processor. Public cloud PII protection implementation guidance Information security and PII protection obligations relevant to the public cloud PII processor may arise directly from applicable law. Where this is not the case, PII protection obligations relevant to the public cloud PII processor should be covered in the contract. The controls in this International Standard, together with the controls in ISO/IEC 27002, are intended as a reference catalogue of measures to assist in entering into an information processing contract in respect of PII. The public cloud PII processor should inform a prospective cloud service customer, before entering into a contract, about the aspects of its services material to the protection of PII. The public cloud PII processor should be transparent about its capabilities during the process of entering into a contract. However, it is ultimately the cloud service customer's responsibility to ensure that the measures implemented by the public cloud PII processor meet its obligations.						

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.10.12	A.10 Information security / A.10.12 Sub-contracted PII processing	Control Contracts between the public cloud PII processor and any sub-contractors that process PII should specify minimum technical and organizational measures that meet the information security and PII protection obligations of the public cloud PII processor. Such measures should not be subject to unilateral reduction by the sub-contractor. Public cloud PII protection implementation guidance The use of sub-contractors to store backup copies is covered by this control (see A.7.1).		To be decided (No mapping)	Full gap			No other control. Required to be more specific about PII information, because STA-05 is generic and don't have PII restrictions.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.10.13	A.10 Information security / A.10.13 Access to data on pre-used data storage space	Control The public cloud PII processor should ensure that whenever data storage space is assigned to a cloud service customer, any data previously residing on that storage space is not visible to that cloud service customer. Public cloud PII protection implementation guidance Upon deletion by a cloud service user of data held in an information system, performance issues may mean that explicit erasure of that data is impractical. This creates the risk that another user may be able to read the data. Such risk should be avoided by specific technical measures. No specific guidance is especially appropriate for dealing with all cases in implementing this control. However, as an example, some cloud infrastructure, platforms or applications will return zeroes if a cloud service user attempts to read storage space which has not been overwritten by that user's own data.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
ISO27018	A.11.1	A.11 Privacy compliance / A.11.1 Geographical location of PII	Control The public cloud PII processor should specify and document the countries in which PII might possibly be stored. Public cloud PII protection implementation guidance The identities of the countries where PII might possibly be stored should be made available to cloud service customers. The identities of the countries arising from the use of sub-contracted PII processing should be included. Where specific contractual agreements apply to the international transfer of data, such as Model Contract Clauses, Binding Corporate Rules or Cross Border Privacy Rules, the agreements and the countries or circumstances in which such agreements apply should also be identified. The public cloud PII processor should inform the cloud service customer in a timely fashion of any intended changes in this regard so that the cloud service customer has the ability to object to such changes or to terminate the contract.		To be decided (No mapping)	Full gap			STA-05 covers supply chain agreements between providers and customers.
ISO27018	A.11.2	A.11 Privacy compliance / A.11.2 Intended destination of PII	Control PII transmitted using a data-transmission network should be subject to appropriate controls designed to ensure that data reaches its intended destination.		To be decided (No mapping)	Full gap			EKM-03 demands policy and controls about data in transi-tion, but not in detail about PII and "intended destination", so it must be detailed in addi-tional control

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	5.1.a	5. Information security policies and Risk Management Principles / 5.1.a	5.1.a. Provider must use stable software that is monitored by security patches and configured in such a way as to obtain an optimum level of security.	Security	To be decided (Mapping exists)	No gap		TVM-02, CCC-03, GRM-01	CCM is much more specific
SecNumCloud	5.2.a	5. Information security policy / 5.2.a	5.2.a. The service provider must document and implement a service information security policy.	Both	Governance and Risk Management	No gap		GRM-06	CCM is much more specific
SecNumCloud	5.2.b	5. Information security policy / 5.2.b	5.2.b. The information security policy must identify the obligations of the provider as to compliance with the national legislation and regulations in force according to the nature of the information that could be entrusted by the client to the provider; on the other hand, the client must ensure that the legal and regulatory constraints applicable to the data he actually confers on the provider are met.	Both	To be decided (Mapping exists)	No gap		GRM-06, GRM-09, STA-05	
SecNumCloud	5.2.d	5. Information security policy / 5.2.d	5.2.d. The provider's management must formally approve the information security policy.	Security	Governance and Risk Management	No gap		GRM-06	
SecNumCloud	5.2.e	5. Information security policy / 5.2.e	5.2.e. The provider must review the information security policy annually and any major changes that may have an impact on the service.	Both	Governance and Risk Management	No gap		GRM-09	CCM mentions 'planned intervals' SecNumCloud specifies timeframe as annually

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	5.3.1	5. Risk assessment / 5.3.1	5.3.1 The service provider must document a risk assessment covering the entire scope of the service.	Both	Governance and Risk Management	Partial gap		GRM-10	Could not detect a relevant CCM requirement. 5.3.1. addresses risk assessment documentation when full scope of service is covered. This requirement is inherent to GRM-10, the control to be updated in order to cover "documented" risk assessment.
SecNumCloud	5.3.2	5. Risk assessment / 5.3.2	5.3.2 The contractor must carry out the risk assessment using a documented method ensuring the reproducibility and comparability of the approach	Both	To be decided (No mapping)	Full gap			Could not detect a relevant CCM requirement, ensuring a formalized method for repro-ducibility of risk assessment results.
SecNumCloud	5.3.3	5. Risk assessment / 5.3.3	5.3.3 The provider must take into account in the risk assessment: - management of customer information with different security needs; - the risks of failure of the partitioning mechanisms of resources of the technical infrastructure (memory, calculation, storage, network) shared between the customers; - the risks associated with the incomplete or insecure erasure of the data stored on the shared memory or storage spaces between clients, in particular during the reallocations of memory and storage spaces;	Both	Governance and Risk Management	Partial gap		GRM-02	GRM-02 can be further enhanced by the list of requirements of 5.3.3.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			- risks related to the exposure of the administration interfaces on a public network.						
SecNumCloud	5.3.4	5. Risk assessment / 5.3.4	5.3.4 Where there are specific legal, regulatory or sectoral requirements related to the types of information that the client has given to the provider, the latter must take them into account in its assessment of the risks by ensuring that all the requirements are met, and not to lower the level of safety established by compliance with the requirements of this standard. The management of the service provider must formally accept the residual risks identified in the risk assessment.	Both	To be decided (Mapping exists)	No gap		GRM-10, GRM-11, STA-05	
SecNumCloud	5.3.5	5. Risk assessment / 5.3.5	5.3.5 Provider's management must formally accept residual risks	Both	Governance and Risk Management	No gap		GRM-10	
SecNumCloud	5.3.6	5. Risk assessment / 5.3.6	5.3.6 The provider must annually review the risk assessment and each major change that may have an impact on the service.	Both	To be decided (Mapping exists)	No gap		CCC-05, GRM-10	
SecNumCloud	6.1.a	6. Information security organization / 6.1.a	6.1.a Information Security roles and responsibilities The service provider must document and implement an internal security organization to ensure the definition, implementation and monitoring of the operational functioning of information security within its organization.	Both	Governance and Risk Management	No gap		GRM-04	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	6.1.b	6. Information security organization / 6.1.b	6.1.b The service provider must designate an information systems security officer and a physical security officer.	Both	To be decided (No mapping)	Full gap			Both requirements not addressed in CCM.
SecNumCloud	6.1.c	6. Information security organization / 6.1.c	6.1.c The service provider must define and assign information security responsibilities for the personnel involved in the provision of the service.	Both	To be decided (Mapping exists)	No gap		HRS-10, BCR-10	
SecNumCloud	6.1.d	6. Information security organization / 6.1.d	6.1.d The Service Provider must ensure after all major changes that may have an impact on service that the assignment of responsibilities for information security is still relevant.	Both	To be decided (Mapping exists)	No gap		GRM-01, GRM-09, BCR-02	CCM mentions planned intervals, not a review after major changes in IAM.
SecNumCloud	6.2.a	6. Information security organization / 6.2	6.2.a Separation of duties. The provider must identify the risks associated with accumulated responsibilities or tasks, take them into account in the assessment of risks and implement measures to reduce these risks.	Both	Identity & Access Management	No gap		IAM-05	SecNumCloud specifically mentions risks associated with an accumulation of responsibilities and tasks.
SecNumCloud	6.3.a	6. Information security organization / 6.3.a	6.3.a Relations with authorities. Relations with the authorities It is recommended that the provider establish appropriate relationships with the authorities responsible for information security and personal data and, where appropriate, with the sectoral authorities, depending on the nature of the information entrusted by the client to the provider.	Both	Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-01	CCM mentions authorities in the context of forensics only; SecNumCloud recommends keeping relations with all applicable bodies.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	6.4.a	6. Information security organization / 6.4.a	6.4.a Relationship with specialized working groups It is recommended that the provider maintain appropriate contacts with expert groups or recognized sources, in particular to take account of new threats and the appropriate security measures to counter them.	Both	To be decided (No mapping)	Full gap			Contacts with outside world in order to keep a high level of being informed isn't mentioned in CCM as an asset. The notion of an expert party/group is not addressed in CCM.
SecNumCloud	6.5.a	6. Information security organization / 6.5.a	6.5.a Information Security in Project Management The provider must document a risk estimate prior to any project that may have an impact on the service, regardless of the nature of the project.	Both	To be decided (Mapping exists)	No gap		CCC-05, GRM-10, GRM-11	Project management isn't mentioned in CCM
SecNumCloud	6.5.b	6. Information security organization / 6.5.b	6.5.b Information Security in project management. To the extent that a project affects or is likely to affect the level of security of the service, the service provider must notify the customer and inform the customer in writing of the potential impacts, measures implemented to reduce these impacts and residual risks concerning him.	Both	To be decided (Mapping exists)	No gap		STA-03, STA-05, BCR-09, GRM-05	Project management isn't mentioned in CCM
SecNumCloud	7.1.a	7. Human resources security / 7.1.a	7.1.a Selection of human resources. The service provider must document and implement a procedure for verifying the information concerning its personnel in compliance with the laws and regulations in force. These checks apply to all persons involved in the provision of the service and must be proportional to the	Both	Human Resources	No gap		HRS-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			sensitivity of the client information entrusted to the service provider and the risks identified.						
SecNumCloud	7.2.a	7. Human resources security / 7.2. a	7.2.a Conditions of employment The service provider must have an ethics charter integrated into the internal rules, in particular providing that: - the services are carried out with loyalty, discretion and impartiality; - staff only use methods, tools and techniques validated by the service provider; - the personnel undertake not to disclose information to a third party, even if they are anonymized and decontextualised, obtained or generated within the framework of the service, unless the client has given written authorization; - the personnel undertake to inform the service provider of any manifestly illicit content discovered during the service; - staff undertake to comply with current national legislation and regulations and good practices related to their activities.	Both	Human Resources	Partial gap		HRS-03, HRS-10	Partial gap due to missing requirements from CCM controls., and specifically an ethics charter (and its 4 out of 5 points). Most HRS controls address service provider requirements, not of personnel. Additionally, controls inserted by SIMPA, e.g. HRS-08,HRS-11, address personnel requirements but are not included in 7.2.a. These would be useful to map when performing a CCM->SecNumCloud mapping, which is not the case here. Code of ethics could be part of the HRS-10 but the CCM control does not explicitly mention it as it is addressing policies and procedures.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	7.2.b	7. Human resources security / 7.2.b	7.2.b Conditions of Employment. The service provider must have the ethics charter signed by all persons involved in the provision of the service.	Both	Human Resources	Partial gap		HRS-03	An ethics charter is missing in CCM. It's only mentioned in the context of background screening; not in the context of an organizational ethics charter employees should commit to and sign. To be discussed; this should be wise to add to CCM. Partial gap due to ethics charter requirement.
SecNumCloud	7.2.c	7. Human resources security / 7.2.c	7.2.c The service provider must, at the request of a client, make the rules of procedure and the ethics charter accessible to the client.	Both	Governance and Risk Management	Partial gap		GRM-06	Partial gap due to ethics charter requirement. See also comment in SecNumCloud/7.2.b.
SecNumCloud	7.3.a	7. Awareness, learning and information security training / 7.3.a	7.3.a The service provider must make all persons involved in the provision of the service aware of the security of the information. They should be provided with updates on relevant policies and procedures as part of their missions.	Both	Human Resources	No gap		HRS-09, HRS-10	
SecNumCloud	7.3.b	7. Awareness, learning and information security training / 7.3.b	7.3.b The service provider must document and implement an information security training plan adapted to the service and the tasks of the personnel.	Both	To be decided (Mapping exists)	No gap		HRS-09, GRM-04	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	7.3.c	7. Awareness, learning and information security training / 7.3.c	7.3.c The provider's information systems security officer must formally validate the information security training plan.	Security	To be decided (Mapping exists)	Partial gap		HRS-09, GRM-03	Partial gap due to missing validation requirement of training program, e.g., in HRS-09, for instance gap could be addressed: "A security awareness training program shall be approved by top management and established..."
SecNumCloud	7.4.a	7. Security of human resources / 7.4.a	7.4.a Disciplinary Process. The provider must document and implement a disciplinary process applicable to all persons involved in the provision of the service that has violated the security policy.	Both	Governance and Risk Management	No gap		GRM-07	
SecNumCloud	7.4.b	7. Security of human resources / 7.4.b	7.4.b Disciplinary Process. The service provider must, at the request of a client, make available to it the penalties incurred in the event of breach of the security policy.	Both	Governance and Risk Management	No gap		GRM-07	
SecNumCloud	7.5.a	7. Security of human resources / 7.5.a	7.5.a Breach, termination or modification of the employment contract The Contractor shall define and assign the roles and responsibilities for termination or modification of any contract with a person involved in the provision of the Service.	Both	Human Resources	No gap		HRS-04	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	8.1.a	8. Asset management / 8.1.a	8.1.a Inventory and ownership of assets The service provider must keep an up-to-date inventory of all the equipment implementing the service. This inventory must specify for each equipment: - equipment identification information (name, IP address, MAC address, etc.); - the function of the equipment; - the equipment model; - the location of the equipment; - the owner of the equipment; - the need for information security (as defined in Chapter 8.3).	Both	Datacenter Security	No gap		DCS-01	DCS-01 is set at a more high-level but addresses all the specific equipment inventorying requirements of 8.1.a. The auditor should be careful to include all the requirements of 8.1.a as the control is more detailed.
SecNumCloud	8.1.b	8. Asset management / 8.1.b	8.1.b The service provider must keep an up-to-date inventory of all the software implementing the service. This inventory must identify for each software, its version and the equipment on which the software is installed.	Both	Datacenter Security	No gap		DCS-01	DCS-01 can be enhanced to include in parentheses some examples of assets (software, hardware equipment, removable media, etc.) and means of inventorying (licence, version, storage or location of use, etc.)
SecNumCloud	8.1.c	8. Asset management / 8.1.c	8.1.c The service provider must ensure the validity of software licenses throughout the service.	Both	To be decided (No mapping)	Full gap			Software license validity requirements not detected in CCM.
SecNumCloud	8.2.a	8. Asset management / 8.2.a	8.2.a Return of assets The service provider must document and implement an asset recovery procedure to ensure that each person involved in the provision of the service returns all the assets in	Both	To be decided (Mapping exists)	No gap		HRS-01, DCS-01	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			his possession at the end of his period of employment or contract.						
SecNumCloud	8.3.a	8. Asset management / 8.3.a	8.3.a Identification of information security requirements The service provider must identify the different security needs of the service information.	Both	Governance and Risk Management	No gap		GRM-01, GRM-04	
SecNumCloud	8.3.b	8. Asset management / 8.3.b	8.3.b When the customer entrusts the provider with data subject to specific legal, regulatory or sectoral constraints, the service provider must identify the specific security needs associated with these constraints.	Both	To be decided (Mapping exists)	No gap		GRM-01, DSI-02, AAC-03, STA-05	
SecNumCloud	8.4.a	8. Asset management / 8.4.a	8.4.a Marking and manipulation of information It is recommended that the service provider document and implement a procedure for the marking and handling of all the information involved in the delivery of the service, in accordance with its need for security defined in Chapter 8.3.	Both	Data Security & Information Lifecycle Management	No gap		DSI-04	
SecNumCloud	8.5.a	8. Asset management / 8.5.a	8.5.a Removable Media Management The service provider shall document and implement a procedure for the management of removable media in accordance with the security requirement defined in Chapter 8.3.	Both	To be decided (No mapping)	Full gap			Policy or procedure for removable media management does not exist as a requirement in CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	8.5.b	8. Asset management / 8.5.b	8.5.b Removable media management. When removable media is used on the technical infrastructure or for administrative tasks, these media must be dedicated for use.	Both	Datacenter Security	Partial gap		DCS-01	SecNumCloud is more specific. I'm not sure I understand the translation: "When removable media is used...these media must be dedicated for use"!? Partial because CCM lacks a management policy control for removable media in general. Could be fixed here.
SecNumCloud	9.1.a	9. Identity and Access management / 9.1.a	9.1.a Policies and Access Control The service provider must document and implement an access control policy on the basis of the result of its risk assessment and the sharing of responsibilities.	Both	Identity & Access Management	No gap		IAM-02, IAM-04	
SecNumCloud	9.1.b	9. Identity and Access management / 9.1.b	9.1.b The provider must annually review the access control policy and any major changes that may have an impact on the service.	Both	To be decided (Mapping exists)	No gap		IAM-10, GRM-09	SecNumCloud has a specific interval annually. CCM mentions interval.
SecNumCloud	9.2.a	9. Identity and Access management / 9.2.a	9.2.a Registration and unsubscription of users The service provider must document and implement a procedure for registering and de-subscribing users using an account management and access rights interface. This procedure should indicate which data should be deleted from a user.	Both	Identity & Access Management	No gap		IAM-02, IAM-11, IAM-12	
SecNumCloud	9.2.b	9. Identity and Access management / 9.2.b	9.2.b The service provider must assign registered accounts when registering the users under his responsibility.	Both	Identity & Access Management	No gap		IAM-02, IAM-08, IAM-12	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	9.2.c	9. Identity and Access management / 9.2.c	9.2.c The service provider shall implement means to ensure that the unsubscription of a user entails the elimination of all access to the resources of the service information system and the deletion of its data in accordance with the procedure of the user, registration and de-registration (see Requirement 9.2 (a)).	Both	Identity & Access Management	No gap		IAM-11, IAM-12	
SecNumCloud	9.3.a	9. Identity and Access management / 9.3.a	9.3.a Management of access rights The service provider must document and implement a procedure to ensure the allocation, modification and withdrawal of access rights to the resources of the service information system.	Both	Identity & Access Management	No gap		IAM-02, IAM-04, IAM-10, IAM-11	
SecNumCloud	9.3.b	9. Identity and Access management / 9.3.b	9.3.b The service provider must make available to its customers the tools and means that allow a differentiation of the roles of users of the service, for example according to their functional role.	Both	Identity & Access Management	No gap		IAM-02, IAM-06	
SecNumCloud	9.3.c	9. Identity and Access management / 9.3.c	9.3.c The service provider must keep up to date the inventory of users under his responsibility who have administrative rights over the resources of the service information system.	Both	Identity & Access Management	No gap		IAM-04	
SecNumCloud	9.3.d	9. Identity and Access management / 9.3.d	9.3.d The provider must be able to provide, for a given resource implementing the service, a list of all users having access to it, whether they are under the responsibility of the service provider or the customer and the access rights have been awarded.	Both	Identity & Access Management	No gap		IAM-09	IAM-09 covers this control at a higher level. This SecNumCloud control is about the provision of an Access Control List (ACL) w.r.t. the access rights of all users to a given single resource.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	9.3.e	9. Identity and Access management / 9.3.e	9.3.e The provider must be able to provide, for a given user, that they are under the responsibility of the service provider or the client, a list of all access rights on the various elements of the service information system.	Both	Identity & Access Management	No gap		IAM-09	IAM-09 covers this control at a higher level. This SecNumCloud control is about the provision of an ACL w.r.t. the access rights of a user over multiple resources.
SecNumCloud	9.3.f	9. Identity and Access management / 9.3.f	9.3.f The provider must define a list of access rights incompatible with each other. It must ensure, when granting access rights to a user, that it does not have access rights that are incompatible with each other under the previously established list.	Both	Identity & Access Management	No gap		IAM-04, IAM-05, IAM-09	This is a requirement of an ACL that has no overlapping of users access rights - which is a function of segregation of duties.
SecNumCloud	9.3.g	9. Identity and Access management / 9.3.g	9.3.g The provider must include in the procedure of management of the rights of access the actions of revocation or suspension of the rights of any user.	Both	Identity & Access Management	No gap		IAM-11	
SecNumCloud	9.4 a	9. Identity and Access management / 9.4.a	9.4.a. Access rights review. The service provider must annually review user access rights within its scope of responsibility.	Both	Identity & Access Management	No gap		IAM-10	SecNumCloud mentions annually; CCM mentions planned intervals
SecNumCloud	9.4.b	9. Identity and Access management / 9.4.b	9.4.b. Access rights review. The service provider must make available to the client a tool facilitating the review of the access rights of the users placed under the responsibility of the latter.	Both	Identity & Access Management	Partial gap		IAM-02, IAM-10	CCM doesn't mention specifically that a tool must be made available to third parties. Gap due to missing tool reference for review.
SecNumCloud	9.4.c	9. Identity and Access management / 9.4.c	9.4.c The service provider must review the list of users on a quarterly basis, which can use the technical accounts mentioned in requirement 9.2 b).	Both	To be decided (No mapping)	Full gap			Not specified in CCM

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	9.5.a	9. Identity and Access management / 9.5.a	9.5.a The service provider must formalize and implement procedures for managing user authentication. In accordance with the requirements of Chapter 10, these shall include: - the management of the means of authentication (issuing and resetting the password, updating the CRLs and importing the root certificates when using certificates, etc.). - the implementation of means allowing multiple-factor authentication in order to respond to the different cases of use of the repository. - systems that generate passwords or verify their robustness when password authentication is used. They must follow the recommendations of [NT_MDP].	Both	Identity & Access Management	Partial gap		IAM-02, IAM-12	Partial gap due to unknown requirements of NT-MDP. Also, a control for password man-agement policy (not adhering specifically to mobile devices) is missing from CCM.
SecNumCloud	9.5.b	9. Identity and Access management / 9.5.b	9.5.b Any authentication mechanism must provide for the blocking of an account after a limited number of unsuccessful attempts.	Both	Identity & Access Management	Partial gap		IAM-02	This SecNumCloud control is low level not addressed ex-plicitly by CCM. It is however directly related to an "Access Policy", i.e., IAM-02, w.r.t. au-thentication technical controls. Can be covered in a parenthe-sis by using a "limited authen-tication attempts policy" term..

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	9.5.c	9. Identity and Access management / 9.5.c	9.5.c. As part of a SaaS service, the service provider must offer its customers multiple means of authentication for end-user access.	Both	Identity & Access Management	No gap		IAM-02	CCM contains a cloud service delivery model applicability column for designating adherence of controls to I/P/SaaS models. IAM-02 applies to SaaS.
SecNumCloud	9.5.d	9. Identity and Access management / 9.5.d	9.5.d Where non-nominal technical accounts are required, the service provider must put in place measures requiring users to authenticate with their registered account before accessing these technical accounts.	Both	Identity & Access Management	No gap		IAM-02, IAM-08, IAM-12	SecNumCloud is more specific
SecNumCloud	9.6.a	9. Identity and Access management / 9.6.a	9.6.a Access to Administration Interfaces Administration accounts under the responsibility of the service provider must be managed using tools and directories separate from those used for the management of user accounts under the responsibility of the client.	Both	To be decided (Mapping exists)	No gap		AIS-02, IAM-02, IAM-05, IAM-13, IVS-11	
SecNumCloud	9.6.b	9. Identity and Access management / 9.6.b	9.6.b The administrative interfaces available to clients must be separate from the administrative interfaces used by the provider.	Both	To be decided (Mapping exists)	No gap		IAM-02, IAM-05, IVS-11, IVS-09	
SecNumCloud	9.6.c	9. Identity and Access management / 9.6.c	9.6.c The administration interfaces provided to the clients must not allow any connection with accounts of administrators under the responsibility of the service provider.	Both	To be decided (Mapping exists)	No gap		AIS-04, IAM-02, IAM-05, IVS-09, IVS-11	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	9.6.d	9. Identity and Access management / 9.6.d	9.6.d. The administration interfaces used by the service provider must not be accessible from a public network and thus must not allow any connection of users under the responsibility of the customer.	Both	To be decided (Mapping exists)	Partial gap		IAM-09, IVS-11	There is no clear reference in CCM of a public network, and also that access from such networks to administrative interfaces used by CSP is forbidden.
SecNumCloud	9.6.e	9. Identity and Access management / 9.6.e	9.6.e If administration interfaces are made available to clients with access via a public network, the administrative flows must be authenticated and encrypted with means consistent with the requirements of Chapter 10.2.	Both	To be decided (Mapping exists)	No gap		IAM-02, IVS-11, EKM-03	
secNumCloud	9.6.f	9. Identity and Access management / 9.6.f	9.6.f The service provider must establish a double-factor authentication system for access: to the administrative interfaces used by the service provider; - the administration interfaces used by the service provider; - the administration interfaces dedicated to customers.	Both	To be decided (Mapping exists)	No gap		IAM-02, IAM-12, IVS-11	
SecNumCloud	9.6.g	9. Identity and Access management / 9.6.g	9.6.g As part of a SaaS service, the administration interfaces available to the clients must be differentiated from the interfaces allowing the access of the end users.	Both	To be decided (Mapping exists)	No gap		IAM-02, IVS-09	
SecNumCloud	9.6.h	9. Identity and Access management / 9.6.h	9.6.h Once an administration interface is accessible from a public network, the authentication process must take place before any interaction between the user and the interface in question.	Both	Identity & Access Management	No gap		IAM-02, IAM-09, IAM-12	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	9.6.i	9. Identity and Access management / 9.6.i	9.6.i When the service provider uses an IaaS service as a base for another type of service (PaaS or SaaS), the resources allocated for the use of the service provider must in no case be accessible via the public interface made available to other customers of the IaaS service.	Both	To be decided (Mapping exists)	No gap		IAM-02, IAM-07, IAM-09, IVS-09	SecNumCloud is more specific
SecNumCloud	9.6.j	9. Identity and Access management / 9.6.j	9.6.j When the service provider uses a PaaS service as a base for another type of service (typically SaaS), the resources allocated for the use of the service provider must in no case be accessible via the public interface provided to the other clients of the PaaS service.	Both	To be decided (Mapping exists)	No gap		IAM-02, IAM-07, IAM-09, IVS-09	SecNumCloud is more specific
SecNumCloud	9.7.a	9. Identity and Access management / 9.7.a	9.7.a Restricting Access to Information The service provider must implement appropriate segregation measures between its customers.	Both	Identity & Access Management	No gap		IAM-02, IAM-05	
SecNumCloud	9.7.b	9. Identity and Access management / 9.7.b	9.7.b The service provider must implement appropriate segregation measures between the information system of the service and its other information systems (office automation, management information systems, technical building management, physical access control, etc.).	Both	To be decided (Mapping exists)	No gap		IAM-02, IVS-09	
secNumCloud	9.7.c	9. Identity and Access management / 9.7.c	9.7.c The service provider must design, develop, configure and deploy the information system of the service by ensuring at least a partitioning between the technical infrastructure and the equipment necessary for the administration of the services and resources she hosts.	Both	To be decided (Mapping exists)	No gap		IAM-02, IVS-09	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	10.1.a	10. Cryptology / 10.1.a	10.1.a Encrypting stored data a) The provider must define and implement an encryption mechanism that prevents the recovery of client data in the event of reallocation of a resource or recovery of the physical medium. - in the case of an IaaS service, this objective may be achieved, for example: - by encrypting the disk or the file system, when the file-mode access protocol guarantees that only empty blocks can be allocated (for example NAS-type storage in which a physical block is actually assigned only to time of writing), - by volume encryption in the case of block access (e.g. SAN-type storage or local storage), with at least one key per client; - in the case of a PaaS or SaaS service, this objective can be achieved by using application encryption in the perimeter of the service provider, with at least one key per client.	Both	To be decided (Mapping exists)	Partial gap		EKM-03, EKM-04, IAM-02	CCM relative controls can be enhanced to refer to the use of encryption for disposal of digital storage media & non-recoverable (destruction of key), address cloud model specific storage encryption (I/P/S-aaS).
SecNumCloud	10.1.d	10. Cryptology / 10.1.d	10.1.d The service provider shall implement encryption of data on removable media and backup media that are required to leave the physical security perimeter of the service information system (as defined in Chapter 11), depending on the need for data security (see Chapter 8.3).	Both	Encryption & Key Management	No gap		EKM-03	Encryption in storage.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	10.3.a	10. Cryptology / 10.3.a	10.3.a Hashing passwords (a) The service provider shall store only the user's passwords and technical accounts.	Both	Identity & Access Management	No gap		IAM-12	A user password/technical account is considered an ID credential.
SecNumCloud	10.3.b.c.d	10. Cryptology / 10.3.b.c.d	10.3.b.c.d b) The provider must implement a hash function that complies with the rules of [CRYPTO_B1]. c) It is recommended that the provider perform a hash function that complies with the recommendations of [CRYPTO_B1]. d) The provider must generate the password fingerprints with a hash function associated with the use of a cryptographic salt complying with the rules of [CRYPTO_B1].	Both	To be decided (No mapping)	Full gap			SecNumCloud specific rules for France. No reference of hashes/hash functions and related rules used in CCM. Potential control: GRM-04.
SecNumCloud	10.4.a.b	10. Cryptology / 10.4.a.b	10.4.a.b Non-repudiation a) When the service provider implements an electronic signature mechanism, the provider must comply with the rules of [CRYPTO_B1]. b) When the service provider implements an electronic signature mechanism, it is recommended that the service provider comply with the recommendations of [CRYPTO_B1].	Both	To be decided (No mapping)	Full gap			SecNumCloud specific rules for France. No reference of electronic/digital signature and related rules used in CCM
SecNumCloud	11,1	11. Physical and environmental security / 11.1. Physical security perimeters	Physical security perimeters: a) The service provider must document and implement safety perimeters, including the marking of the zones and the various means of limitation and access control. b) The provider must distinguish between public areas, private areas and sensitive areas.		Datacenter Security	No gap		DCS-02, DCS-07, DCS-08	CCM makes a distinction over private/sensitive/public with the terms non-production/production/service areas of unauthorized access, respectively.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	11.1.1	11. Physical and environmental security / 11.1. Physical security perimeters / 11.1.1. Public areas	Public areas: a) Public areas are accessible to all within the limits of the provider's property. The service provider must not host any resources devoted to the service or allowing access to components of the service in public areas.		Datacenter Security	No gap		DCS-08	
SecNumCloud	11.1.2	11. Physical and environmental security / 11.1. Physical security perimeters / 11.1.2. Private areas	Private areas: a) Private areas can host: - platforms and means of service development; - administrative, operational and supervisory positions; - the premises from which the service provider operates.		Infrastructure & Virtualization Security	Partial gap		IVS-08	Partial gap can be closed in CCM with a designation of type of separation (logical, physical, crypto-based) and type of services hosted in the non-production environment that need to be protected, possibly affecting IVS-08.
SecNumCloud	11.1.3	11. Physical and environmental security / 11.1. Physical security perimeters / 11.1.3. Sensitive areas	Sensitive areas: a) Sensitive areas are reserved for the hosting of the production information system of the non-administrative, operational and supervisory service.		Infrastructure & Virtualization Security	Partial gap		IVS-08	Partial gap can be closed in CCM with a designation of type of separation (logical, physical, crypto-based) and type of services hosted in the production environment that need to be protected, possibly affecting IVS-08.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	11.2.1	11. Physical and environmental security / 11.2. Physical access control / 11.2.1. Private areas	Private areas a) The provider must protect private areas against unauthorized access. To do this, he must implement a physical access control based at least on a personal factor: the knowledge of a secret, the possession of an object or biometrics. b) It is recommended that the provider comply with [G_SANSCONTACT] 's recommendations to implement physical access control. c) The service provider must define and document derogatory physical access measures in case of emergency. d) The service provider must display at the entry of private zones a warning concerning the limits and conditions of access to these zones. e) The service provider must define and document the time slots and access conditions to the private zones according to the profiles of the workers. f) The provider must document and implement the means to ensure that visitors are systematically accompanied by the provider during their access and stay in private area. The service provider must keep a record of the identity of the visitors in accordance with the laws and regulations in force. g) The service provider must document and implement mechanisms to monitor and detect unauthorized access to private areas.		To be decided (Mapping exists)	Partial gap		DCS-02, DCS-07, DCS-09, IAM-02, IAM-04, IAM-09.	Difference between 11.2.1 and 11.2.2. is requirement with respect to the terms "sensitive" and "private" areas (term private not met in CCM). 11.2.1. lacks points h) and i) of 11.2.2. In this case CCM control DCS-08, which reflects requirement 11.2.2.i), is left out here, but used in 11.2.2. Partial gap exists due to 12.2.1.b),d),f),h) as below.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	11.2.2	11. Physical and environmental security / 11.2. Physical access control / 11.2.2. Sensitive areas	Sensitive areas: a) The provider must protect sensitive areas against unauthorized access. To do this, he must implement a physical access control based at least on two personal factors: the knowledge of a secret, the possession of an object or biometrics. b) It is recommended that the provider respect the recommendations of [G_SANSCONTACT] for the implementation of the physical access control. c) The service provider must define and document derogatory physical access measures in case of emergency. d) The service provider must display at the entrance of sensitive areas a warning concerning the limits and conditions of access to these zones. e) The service provider must define and document the time slots and access conditions to the sensitive areas according to the profiles of the workers. f) The provider must document and implement the means to ensure that visitors are systematically accompanied by the provider during their access and stay in sensitive areas. The service provider must keep a record of the identity of the visitors in accordance with the laws and regulations in force.		To be decided (Mapping exists)	Partial gap		DCS-02, DCS-07, DCS-08, DCS-09, IAM-02, IAM-04, IAM-09.	Partial gap due to 11.2.2.b),d),f),h).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			g) The service provider must document and implement mechanisms for monitoring and detecting unauthorized access to sensitive areas. h) The service provider must set up logging of physical access to sensitive areas. He must review these newspapers at least monthly. i) The provider must implement means ensuring that no direct access exists between a public area and a sensitive area.						
SecNumCloud	11.3	11. Physical and environmental security / 11.3. Protection from external and environmental threats	a) The service provider must document and implement the means to minimize the risks inherent to physical (fire, water damage, etc.) and natural (climate risks, floods, earthquakes, etc.). b) The service provider must document and implement measures to limit the risk of fire starting and spreading and the risk of water damage. c) The service provider must document and implement measures to prevent and limit the consequences of a power failure and to allow service to be resumed in accordance with the service availability requirements defined in the service agreement. d) The service provider must document and implement the means to maintain appropriate temperature and humidity conditions for the equipment. In addition, it must implement measures to prevent air conditioning failures		Business Continuity Management & Operational Resilience	No gap		BCR-05, BCR-08, BCR-03, BCR-06	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			and limit the consequences. e) The service provider must document and implement regular checks and tests of detection and physical protection equipment.						
SecNumCloud	11.4	11. Physical and environmental security / 11.4. Work in private and sensitive areas	a) The service provider must integrate the physical security elements into the security policy and the risk assessment in accordance with the level of security required by the category of the zone. b) The provider must document and implement procedures for work in private and sensitive areas. He must communicate these procedures to the relevant stakeholders.		Datacenter Security	No gap		DCS-06	
SecNumCloud	11.5	11. Physical and environmental security / 11.5. Delivery and loading areas	Delivery and loading areas and other points through which unauthorized persons may enter the premises unaccompanied are considered as public areas. a) The service provider must isolate the access points of these zones to the private and sensitive areas, so as to avoid unauthorized access or, failing this, implement countervailing measures to ensure the same level of security.		Datacenter Security	No gap		DCS-07, DCS-08	
SecNumCloud	11.6	11. Physical and environmental security / 11.6. Wiring Safety	a) The service provider must document and implement measures to protect the electrical and telecommunication wiring from physical damage and the possibility of interception. b) The service provider must establish and maintain a wiring plan. c) It is recommended that the service provider		To be decided (Mapping exists)	Partial gap		BCR-03, BCR-04, BCR-05, DSI-04, DCS-01	Cabling labelling is not in CCM. Partial gap due to 11.6.b. requirement (i.e., wiring plan) not covered by CCM controls.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			implement measures to identify the cables (e.g. colour code, label, etc.) in order to facilitate their operation and limit handling errors.						
SecNumCloud	11.7	11. Physical and environmental security / 11.7. Maintenance of equipment	a) The service provider must document and implement measures to ensure that the installation, maintenance and servicing conditions for the service information system equipment in the private and sensitive areas are compatible with the requirements the confidentiality and availability of the service defined in the service agreement. b) The service provider must take out maintenance contracts to have software security updates installed on the equipment of the service information system. c) The service provider must ensure that media can only be returned to a third party if the customer's data is stored encrypted in accordance with Chapter 10.1 or has been previously destroyed using a secure deletion mechanism. rewriting random patterns. d) The service provider must document and implement measures to ensure that the conditions of installation, maintenance and maintenance of ancillary technical equipment (power supply, air conditioning, fire, etc.) are compatible with the requirements service availability defined in the service agreement.		To be decided (Mapping exists)	No gap		DCS-01, DCS-05, BCR-03, BCR-07, BCR-08, STA-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	11.8	11. Physical and environmental security / 11.8. Exit of assets	a) The service provider must document and implement a procedure for off-site transfer of customer data, equipment and software. This procedure must require the provider's management to give its written authorization. In all cases, the service provider must implement the means to ensure that the level of protection in terms of confidentiality and integrity of the assets during their transport is equivalent to that on the site.		Datacenter Security	Partial gap		DCS-04, DCS-05	Partial due to missing policy or procedure-based safeguard for physical transport security of assets.
SecNumCloud	11.9	11. Physical and environmental security / 11.9. Secure Material Recycling	a) The service provider must document and implement means to securely erase by random rewriting any data medium made available to a customer. If the storage space is encrypted as per requirement 10.1 a), erasure can be achieved by securely erasing the encryption key.		To be decided (Mapping exists)	No gap		DSI-07, DCS-05, EKM-02	
SecNumCloud	11.10	11. Physical and environmental security / 11.10. Materials awaiting use	a) The service provider must document and implement a procedure for the protection of equipment awaiting use.		To be decided (Mapping exists)	No gap		BCR-01, BCR-06, BCR-07, DCS-09	
SecNumCloud	12.1	12. Operational safety / 12.1. Documented Operating Procedures	a) The service provider must document the operating procedures, keep them up-to-date and make them accessible to the personnel concerned.		To be decided (Mapping exists)	No gap		BCR-10, BCR-04, GRM-06	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.2	12. Operational safety / 12.2. Change management	a) The provider must document and implement a procedure for managing changes to information processing systems and means. b) The service provider must document and implement a procedure allowing, in the event of operations carried out by the service provider and having an impact on the security or the availability of the service, to communicate as soon as possible to all its customers the following information: - the scheduled date and time of the start and end of operations; - the nature of the operations; - the impacts on the security or the availability of the service; - the contact within the service provider. c) In the context of a PaaS service, the service provider must inform the customer as soon as possible of any future changes to software elements under his responsibility as long as full compatibility cannot be ensured. d) As part of a SaaS service, the service provider must inform the customer as soon as possible of any future changes to the elements of the service if it is likely to cause a loss of functionality for the customer.		To be decided (Mapping exists)	No gap		CCC-02, CCC-03, CCC-05, TVM-02, GRM-01	CCC controls cover fully 12.2.c & d "authorization by, the customer (tenant) as per agreement (SLA) prior to deployment" and IaaS, PaaS, SaaS models (See cloud service delivery model applicability column).

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.3	12. Operational safety / 12.3. Separation of development, test and operating environments	a) The service provider must document and implement measures to physically separate service-related environments from other environments, including development environments.		Infrastructure & Virtualization Security	No gap		IVS-08	
SecNumCloud	12.4	12. Operational safety / 12.4. Measures against malicious code	a) The provider must document and implement detection, prevention and remediation measures to protect against malicious code. The scope of application of this requirement on the service information system must necessarily contain the user stations under the responsibility of the provider and the incoming flows on the same information system. b) The provider must document and implement employee awareness of the risks of malware and good practices to reduce the impact of an infection.		To be decided (Mapping exists)	No gap		TVM-01, MOS-01	Unauthorized code/software installation does not necessarily make such code/software malicious (i.e., TVM-03, CCC-04)

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.5	12. Operational safety / 12.5. Saving information	a) The service provider must document and implement a data backup and restoration policy under his responsibility as part of the service. This policy must provide for a daily backup of all data (information, software, configurations, etc.) under the responsibility of the provider as part of the service. b) The provider must document and implement safeguarding safeguards in accordance with the access control policy (see Chapter 9). This policy must provide for a monthly review of the traces of access to backups. c) The service provider must document and implement a procedure to regularly test the restoration of backups. d) The service provider must locate the backups at a sufficient distance from the main equipment in line with the results of the risk assessment and to deal with major incidents. Backups are subject to the same localization requirements as operational data. The backup site (s) are subject to the same security requirements as the primary site, in particular those listed in Chapters 8 and 11. Communications between the primary site and the backup site must be encrypted, in accordance with the requirements of Chapter 10.		To be decided (Mapping exists)	No gap		BCR-06, BCR-11, IVS-10	No gap, but the SecNumCloud has more detail

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.6	12. Operational safety / 12.6. Event Logging	a) The service provider must document and implement a logging policy that includes at least the following elements: - the list of sources of collection; - the list of events to be logged by source; - the purpose of logging by event; - frequency of collection and time base used; - the local and centralized retention period; - log protection measures (including encryption and duplication); - the location of newspapers. b) The provider must generate and collect the following events: - user activities related to information security; - the modification of access rights within the scope of its responsibility; - events stemming from the mechanisms for combating malicious codes (see 12.4); - the exceptions; - failures; - any other event related to information security. c) The service provider must keep logging events for at least six months subject to compliance with legal and regulatory requirements. d) The service provider must provide, at the request of a client, all the events concerning him.		To be decided (Mapping exists)	Partial gap		IVS-01, BCR-11, IPY-02, SEF-03	The SecNumCloud controls appears to be highly granular with respect to logging requirements, case not met in CCM. Partial gaps in CCM of: - 12.6.a. missing logging policy requirement - 12.6.b. - 12.6.c. (covered partially at high level by BCR-11) - 12.6.e.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			e) It is recommended that the logging system implemented by the provider comply with the recommendations of [NT_JOURNAL].						
SecNumCloud	12.7	12. Operational safety / 12.7. Protection of the logged information	a) The service provider must protect the logging equipment and journaled events against breaches of their availability, integrity or confidentiality, in accordance with chapter 3.2 of [NT_JOURNAL]. b) The service provider must manage the sizing of the storage space of all the equipment hosting one or more collection sources in order to allow the local preservation of the logged events provided for by the event logging policy. This dimensioning management must take into account changes in the information system. c) The provider must transfer the logged events with confidentiality and integrity protection to one or more dedicated central servers and store them on a separate physical machine from the one that generated them. d) The service provider must set up a backup of the events collected according to a suitable policy. e) The service provider must perform the logging and event collection processes with accounts that have sufficient and sufficient privileges and must limit access to logged events in accordance with the access control policy (see Chapter 8).		Infrastructure & Virtualization Security	Partial gap		IVS-01	IVS-01 is far too high level defined, SecNumCloud control 12.7 requirements are not met in CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.8	12. Operational safety / 12.8. Synchronization of clocks	a) The service provider must document and implement synchronization of the clocks of all the equipment on one or more internally coherent sources of time between them. These sources can themselves be synchronized to several reliable external sources, except for isolated networks. b) The service provider must set the timestamp of each event logged.		Infrastructure & Virtualization Security	No gap		IVS-03, IVS-01	IVS-01 related to 12.8.b.
SecNumCloud	12.9	12. Operational safety / 12.9. Analysis and correlation of events	a) The service provider shall document and implement an infrastructure for the analysis and correlation of events recorded by the logging system to detect events that may affect the security of the service information system, in real time or a posteriori for events up to six months. b) It is recommended that the security incident detection provider (PDIS) requirements repository be used for the establishment and operation of the event analysis and correlation infrastructure. c) The service provider must acknowledge the alarms reported by the event analysis and correlation infrastructure at least daily.		Security Incident Management, E-Discovery, & Cloud Forensics	Partial gap		SEF-02, SEF-03, SEF-05	Partial gap due to 12.9.b. requirement not found in CCM. The wording in 12.9.a: "analysis and correlation of events" is covered by the sentence "to triage security-related events" included in SEF-02 requirement of CCM control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.10	12. Operational safety / 12.10. Installing Software on Operational Systems	a) The service provider must document and implement a procedure to control the installation of software on the equipment of the service information system. b) The service provider must document and implement a procedure for managing the configuration of the software environments available to the client, in particular for keeping them in a safe state.		To be decided (Mapping exists)	No gap		CCC-04, GRM-01, MOS-03, IVS-06	
SecNumCloud	12.11	12. Operational safety / 12.11. Management of technical vulnerabilities	a) The service provider must document and implement a monitoring process to manage the technical vulnerabilities of the software and systems used in the service information system. b) The provider must assess its exposure to these vulnerabilities by including them in the risk assessment and applying the appropriate risk-management measures.		Threat and Vulnerability Management	No gap		TVM-02	Not sure if should include the MOS-section

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	12.12	12. Operational safety / 12.12. Administration	a) The service provider must document and implement a procedure obliging the administrators under his responsibility to use dedicated terminals for the exclusive performance of administrative tasks, in accordance with Chapter 4.1 entitled "Post and administrative network" of [NT_admin]. He must control them and keep them up to date. b) The service provider must implement measures to harden the configuration of the terminals used for administration tasks, in particular those of chapter 4.2 entitled "Securing the base" of [NT_ADMIN]. c) When the provider authorizes a mobility situation for the directors under his responsibility, he must frame it by a documented policy. The implemented solution must ensure that the security level of this mobility situation is at least equivalent to the level of security outside the mobility situation (see Chapters 9.6 and 9.7). This solution must include: - the use of an encrypted, non-disengageable and non-circumventable tunnel for all flows (see Chapter 10.2); - full disk encryption (see chapter 10.1).		To be decided (Mapping exists)	Partial gap		IVS-07, MOS-11,EKM-03	Partial gap due to 12.12.a. and 12.12.c. encrypted tunnelling reqs. missing in CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	13.1	13. Security of communications / 13.1. Mapping of the information system	a) The service provider must establish and maintain a map of the service information system in relation to the asset inventory (see chapter 8.1 a), including at least the following elements: - the list of material or virtualized resources; - the names and functions of the applications, supporting the service; - the network architecture scheme at level 3 of the OSI model on which the hotspots are identified: - the interconnection points, in particular with third-party and public networks, - networks, subnetworks, including administrative networks, - equipment providing security functions (filtering, authentication, encryption, etc.), - servers hosting data or performing sensitive functions; - matrix of authorized network flows, specifying: - their technical description (services, protocols and ports); - business or infrastructure justification; - where appropriate, when services, protocols or ports deemed unsafe are used, the compensatory measures put in place, in the defence-in-depth logic. b) The provider must review the mapping at least once a year.		To be decided (Mapping exists)	No gap		DCS-01, BCR-04, IVS-13, DSI-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	13.2	13. Security of communications / 13.2. Network partitioning	a) The service provider must document and implement, for the service information system, partitioning measures (logical, physical or encryption) to separate the network flows according to: - the sensitivity of the information transmitted; - the nature of the flows (production, administration, supervision, etc.); - the domain belonging to the flows (customers - with distinction by customer or set of customers, the provider, third parties, etc.); - the technical field (processing, storage, etc.). b) The provider must partition, physically or by encryption, all data flows internal to the information system of the service vis-à-vis any other information system. When this partitioning is done by encryption, it is performed in accordance with the requirements of chapter 10.2. c) In cases where the technical infrastructure administration network is not physically partitioned, the administration flows must pass through an encrypted tunnel, in accordance with the requirements of Chapter 10.2. d) The service provider must set up and configure an application firewall to protect the administration interfaces intended for its clients and exposed on a public network. e) The service provider must implement a		Infrastructure & Virtualization Security	Partial gap		IVS-08, IVS-09, IVS-11	Partial due to statement 13.2.c., i.e., using cryptographic partitioning in the absence of physical separation. In addition, the terms "physical", "logical", "cryptographic" separation/partitioning are fundamental to cyber security and not met in any CCM controls.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			filtering mechanism on all the administration and supervision interfaces of the service's technical infrastructure that only allows the legitimate connections identified in the matrix of authorized flows.						
SecNumCloud	13.3	13. Security of communications / 13.3. Network Monitoring	a) The service provider must have one or more security incident detection probes on the service information system. These probes must in particular allow the supervision of each of the interconnections of the service information system with third party information systems and public networks. These probes must be collection sources for the event analysis and correlation infrastructure (see Chapter 12.9).		To be decided (Mapping exists)	No gap		IVS-01, IVS-06, IVS-07, SEF-05	
SecNumCloud	14.1	14. Acquisition, development and maintenance of information systems / 14.1. Secure Development Policy	a) The service provider must document and implement rules for the secure development of software and systems, and apply them to internal developments. b) The service provider must document and implement appropriate training in secure development for the employees concerned.		To be decided (No mapping)	Full gap		-	This SecNumCloud control is about secure software development and an organisation maintaining a Secure Software Development Life Cycle (SSDLC) framework & policy. Training targets here software engineers in need to applying security rules during development. Could not detect in CCM a relevant control.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	14.2	14. Acquisition, development and maintenance of information systems / 14.2. System Change Control Procedures	a) The service provider must document and implement a procedure for controlling changes to the service information system. b) The service provider must document and implement a procedure to validate changes to the service information system on a pre-production environment before they go into production. c) The service provider must keep a history of software and system versions (internal or external developments, commercial products) implemented to enable the reconstitution, if necessary in a test environment, of a complete environment as it was implemented. implemented on a given date. The retention period of this history must be consistent with that of the backups (see Chapter 12.5).		To be decided (Mapping exists)	No gap		CCC-02, CCC-03, GRM-01, DCS-01, BCR-11	Error: BRC-11 > BCR-11 is assigned.
SecNumCloud	14.3	14. Acquisition, development and maintenance of information systems / 14.3. Technical review of applications after change to the operating platform	a) The service provider must document and implement a procedure to test, prior to their production, all applications to verify the absence of any undesirable effect on the activity or on the security of the service.		Change Control & Configuration Management	No gap		CCC-03	No, but CCM does not make distinction between change of application and change of platform/OS

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	14.4	14. Acquisition, development and maintenance of information systems / 14.4. Secure development environment	a) The service provider must implement a secure development environment to manage the entire development cycle of the service information system. b) The service provider must take development environments into account in the assessment of risks and ensure their protection in accordance with this standard.		Governance and Risk Management	Partial gap		GRM-04, GRM-10	CCM may close the gap by referencing in these CCM controls the terms SSDLC and risk assessment in SSDLC, or create related control w.r.t. security in non-production environments during software development and testing.
SecNumCloud	14.5	14. Acquisition, development and maintenance of information systems / 14.5. Outsourced development	a) The service provider must document and implement a procedure to supervise and control the outsourced development activity of software and systems. This procedure must ensure that the outsourced development activity complies with the provider's secure development policy and achieves an external development security level equivalent to that of an internal development (see requirement 14.1 a).		Change Control & Configuration Management	No gap		CCC-02	
SecNumCloud	14.6	14. Acquisition, development and maintenance of information systems / 14.6. Safety testing and system compliance	a) The service provider must submit new or updated information systems for compliance and security functionality testing during development. It must document and implement a test procedure that identifies: - the tasks to be performed; - the input data; - the results expected at the exit.		Change Control & Configuration Management	No gap		CCC-01, CCC-03	CCM has no controls regarding development environment

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	14.7	14. Acquisition, development and maintenance of information systems / 14.7. Protection of test data	a) The service provider must document and implement a procedure to ensure the integrity of the test data used in pre-production. b) If the service provider wishes to use customer data from production to perform tests, the service provider must first obtain the customer's consent and anonymize them. The provider must ensure the confidentiality of the data during their anonymisation.		To be decided (Mapping exists)	No gap		DSI-05, CCC-03	CCM is more generic
SecNumCloud	15.1	15. Relations with third parties / 15.1. Identification of third parties	a) The service provider must keep up to date a list of all the third parties involved in the implementation of the service (host, developer, integrator, archiver, sub-contractor operating on site or at a distance, air conditioning suppliers, etc.). This list must be exhaustive, specify the contribution of the third party to the service and take into account the cases of subcontracting at several levels.		To be decided (Mapping exists)	No gap		HRS-07, STA-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	15.2	15. Relations with third parties / 15.2. Security in agreements with third parties	a) The service provider must demand from third parties participating in the implementation of the service, in their contribution to the service, a level of security at least equivalent to that which he undertakes to maintain in his own security policy. It must do so through requirements, adapted to each third party and its contribution to the service, in the specifications or in the security clauses of the partnership agreements. The service provider must include these requirements in contracts with third parties. b) The service provider must contract, with each of the third parties involved in the implementation of the service, audit clauses allowing a qualification organization to verify that these third parties comply with the requirements of these standards. c) The service provider must define and assign the roles and responsibilities relating to the modification or termination of the contract linking it to a third party involved in the implementation of the service.		To be decided (Mapping exists)	No gap		STA-06, STA-09, STA-05, HRS-04	
SecNumCloud	15.3	15. Relations with third parties / 15.3. Monitoring and review of third party services	a) The service provider must document and implement a procedure to regularly check the measures put in place by the third parties involved in the implementation of the service to meet the requirements of this standard, in accordance with Chapter 18.3.		Supply Chain Management, Transparency, and Accountability	No gap		STA-08, STA-09	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	15.4	15. Relations with third parties / 15.4. Management of changes in third party services	a) The service provider must document and implement a procedure for monitoring changes made by third parties involved in the implementation of the service that may affect the security level of the service information system. b) Insofar as a change of third party involved in the implementation of the service affects the level of security of the service, the service provider must inform all customers without delay in accordance with Chapter 12.2 and implement measures to restore the previous level of security.		To be decided (Mapping exists)	Partial gap		CCC-02, CCC-05, IVS-02	Partial gap due to 15.4.b. IVS-02 covers such a requirement but regarding VM images. CCM would need a more generic requirement addressing 15.4.b., existing in CCC.
SecNumCloud	15.5	15. Relations with third parties / 15.5. Confidentiality Commitments	a) The service provider must document and implement a procedure to review at least annually the requirements of confidentiality or non-disclosure commitments vis-à-vis third parties involved in the implementation of the service.		Human Resources	No gap		HRS-06	
SecNumCloud	16.1	16. Management of incidents related to information security / 16.1. Responsibilities and Procedures	a) The service provider must document and implement a procedure to provide quick and effective responses to security incidents. These procedures must define the means and deadlines for communication of security incidents to all concerned customers as well as the level of confidentiality required for this communication. b) The service provider must inform its		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-02, SEF-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			employees and all third parties involved in the implementation of the service of this procedure.						
SecNumCloud	16.2	16. Management of incidents related to information security / 16.2. Reporting related to information security	a) The service provider must document and implement a procedure requiring its employees and third parties involved in the implementation of the service to report to it any security incidents, known or suspected, as well as any security breaches. b) The service provider must document and implement a procedure allowing all customers to report any security incidents, known or suspected, and any security breaches. c) The service provider must promptly communicate to customers the security incidents and the associated recommendations to limit their impact. It must allow the client to choose the severity levels of the incidents for which he wishes to be informed. d) The service provider must communicate the security incidents to the competent authorities in accordance with the legal and regulatory requirements in force.		To be decided (Mapping exists)	No gap		SEF-01, SEF-02, SEF-03, SEF-04, STA-02, STA-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	16.3	16. Management of information security incidents / 16.3. Assessment of events related to information security and decision-making	a) The provider must assess events related to information security and decide whether to qualify them as security incidents. For the assessment, it must be based on one or more scales (estimation, evaluation, etc.) shared with the client. b) The service provider must use a classification that clearly identifies security incidents affecting customer data, in accordance with the results of the risk assessment.		Security Incident Management, E-Discovery, & Cloud Forensics	No gap		SEF-02, SEF-05	No Gap, however CCM would benefit from having basic quotes from this SecNumCloud control integrated at its relevant controls, could be in parentheses. E.g., what triage of security-related events actually means.
SecNumCloud	16.4	16. Management of incidents related to information security / 16.4. Responding to information security incidents	a) The service provider must handle security incidents until they are resolved and must inform the clients in accordance with the procedures. b) The service provider must archive documents detailing security incidents. c) It is recommended that the service provider use a security incident response provider [PRIS] qualified to handle security incidents requiring additional expertise.		To be decided (Mapping exists)	Partial gap		SEF-02, SEF-03, SEF-05, STA-02	Could not detect and equivalent CCM control to requirement 16.4.c.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	16.5	16. Management of incidents related to information security / 16.5. Learning from incidents related to information security 16.5. Learn from information security incidents	a) The service provider must document and implement a continuous improvement process to reduce the occurrence and impact of types of security incidents already addressed.		To be decided (No mapping)	Full gap		-	Incident re-occurrence and its estimated impact management is not addressed currently by CCM
SecNumCloud	16.6	16. Management of incidents related to information security / 16.6. Collection of evidence	a) The service provider must document and implement a procedure to record information about security incidents that can be used as evidence.		To be decided (Mapping exists)	No gap		SEF-04, SEF-05, STA-02	
SecNumCloud	17.1	17. Continuity of activity / 17.1. Organization of business continuity	a) The service provider must document and implement a business continuity plan that takes into account the security of information. b) The service provider must annually review the service's business continuity plan and any		To be decided (Mapping exists)	No gap		BCR-01, BCR-02, AAC-03	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			major changes that may have an impact on the service.						
SecNumCloud	17.2	17. Continuity of activity / 17.2. Implementation of business continuity	(a) The service provider must document and implement procedures to maintain or restore the operation of the service and to ensure the availability of information at the level and within the timeframe for which the service provider has committed to of the customer in the service agreement.		To be decided (Mapping exists)	No gap		BCR-01, BCR-07, BCR-11, DCS-01	
SecNumCloud	17.3	17. Continuity of activity / 17.3. Verify, review and evaluate business continuity	a) Provider must document and implement a procedure to test the business continuity plan to ensure that it is relevant and effective in a crisis situation		Business Continuity Management & Operational Resilience	No gap		BCR-01, BCR-02, BCR-10	
SecNumCloud	17.4	17. Continuity of activity / 17.4. Availability of information processing facilities	a) The service provider must document and implement measures that enable him to respond to the need for availability of the service defined in the service agreement (see Chapter 19.1).		To be decided (Mapping exists)	No gap		BCR-07, IVS-04	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	18.1	18. Compliance / 18.1. Identification of legislation and applicable contractual requirements	a) The service provider must identify the legal, regulatory and contractual requirements applicable to the service. In France, the service provider must consider at least the following texts: - the personal data [LOI_IL]; - professional secrecy [CP_ART_226-13], where applicable without prejudice to the application of Article 40 paragraph 2 of the Code of Criminal Procedure relating to the reporting to a judicial authority; - breach of trust [CP_ART_314-1]; - the secret of private correspondence [CP_ART_226-15]; - invasion of privacy [CP_ART_226-1]; - fraudulent access or retention to an information system [CP_ART_323-1]. b) The service provider must document and implement procedures to comply with applicable legal, regulatory and contractual requirements applicable to the service, as well as specific security requirements (see requirement 8.3b)). c) The service provider must, at the request of a client, make all of these procedures available to them. d) The service provider must document and implement an active monitoring process of the legal, regulatory and contractual requirements applicable to the service.		To be decided (Mapping exists)	No gap		AAC-03, STA-07, HRS-10, GRM-09, DSI-02	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	18.2	18. Compliance / 18.2. Independent Review of Information Security	a) The service provider must document and implement a three-year audit program defining the scope and frequency of audits in line with change management, policies, and risk assessment results. b) The service provider must include in the audit program a qualified audit per year by a qualified information system audit [PASSI] auditor. The overall audit program should include: - the audit of the configuration of the servers and network equipment included in the scope of the service. This audit is performed by sampling and must include all types of equipment and servers present in the service information system; - the intrusion test of external access to the service; - if the service benefits from internal developments, the source code audit of the implemented security features.		To be decided (Mapping exists)	Partial gap		STA-08, AAC-01, AAC-02, TVM-02, IVS-06, GRM-10	AAC-02 covers fully at high level the SecNumControl, however there are gaps of low level defined requirements of the latter. These are, partial gaps with respect to part a) 3 yrs audit program with defined scope/frequency of audits, and part b) source code auditing.
SecNumCloud	18.3	18. Compliance / 18.3. Compliance with safety policies and standards	a) The service provider via the information security officer must regularly ensure the correct execution of all the security procedures under his responsibility in order to ensure their compliance with the security policies and standards.		To be decided (Mapping exists)	No gap		AAC-02, STA-03, STA-04, BCR-10, GRM-03	Control aims at ensuring procedures' implementation in conformance to corresponsing policy and standards.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	18.4	18. Compliance / 18.4. Technical Compliance Review	a) The service provider must document and implement a policy to verify the technical compliance of the service with the requirements of these standards. This policy must define the objectives, methods, frequencies, expected results and corrective measures.		To be decided (Mapping exists)	Partial gap		AAC-02, STA-07	This control requires the documentation and implementation of a policy that dictates service technical reviews for compliance against the standard itself. AAC-02 and STA-07 partially cover this requirement. STA-07 is closer semantically, however it refers to service agreements compliance, & not explicitly to a generic scope of service technical requirements (which can also exist in an SLA). Missing reqs to CCM are the terms: technical requirements compliance policy, documentation of such a policy & policy definitions (i.e., objectives, methods, etc..)
SecNumCloud	19.1.a	19. Additional requirements / 19.1. Service agreement / a)	a) The service provider must establish a service agreement with each customer of the service. Any modification of the service agreement must be subject to customer acceptance		Supply Chain Management, Transparency, and Accountability	No gap		STA-05	

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	19.1.b	19. Additional requirements / 19.1. Service agreement / b)	b) The service provider must identify in the service agreement: - the responsibilities of each party: provider and third parties involved in the provision of the service, customers, etc.; - the elements explicitly excluded from the provider's responsibilities; - the location of the service. The location of the support must be specified when it is carried out from a State outside the European Union, as required by requirement 19.2 d).		Supply Chain Management, Transparency, and Accountability	No gap		STA-05	
SecNumCloud	19.1.c	19. Additional requirements / 19.1. Service agreement / c)	c) The service provider must propose a service agreement applying the law of a Member State of the European Union. The applicable law must be identified in the service agreement.		Supply Chain Management, Transparency, and Accountability	No gap		STA-05	
SecNumCloud	19.1.d	19. Additional requirements / 19.1. Service agreement / d)	d) The service provider must describe in the service agreement the technical and organizational means it implements to ensure compliance with the applicable law.		Supply Chain Management, Transparency, and Accountability	No gap		STA-05	
SecNumCloud	19.1.e	19. Additional requirements / 19.1. Service agreement / e)	e) The service provider must include in the service agreement a clause of revision of the agreement providing in particular for a cancellation without penalty for the customer in case of loss of the qualification granted to the service.		Supply Chain Management, Transparency, and Accountability	Partial gap		STA-05, STA-07	Partial gap due to no explicit statement of "agreement cancellation with no penalty" at any CCM control. STA-07 covers the review of agreements and detection of inconsistencies at the customer or provider side.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	19.1.f.g	19. Additional requirements / 19.1. Service agreement / f) g)	f) The service provider must include in the service agreement a reversibility clause allowing the customer to recover all of his data (provided directly by the customer or produced as part of the service based on the customer's data or actions). g) The service provider must ensure this reversibility via one of the following technical methods: - the provision of files in one or more formats that are documented and exploitable outside the service provided by the service provider; - the implementation of technical interfaces allowing access to data in a documented and exploitable scheme (API, pivot format, etc.). The technical terms of reversibility appear in the service agreement.		To be decided (Mapping exists)	Partial gap		STA-03, STA-05, BCR-11, AIS-01, IPY-02, IPY-03	CCM controls mostly cover this control requirement. Par-tial gap notation is given due to the lack of references of these requirements in the con-text of a service agreement.
SecNumCloud	19.1.h	19. Additional requirements / 19.1. Service agreement / h)	h) The service provider must indicate in the service agreement the level of availability of the service.		To be decided (Mapping exists)	Partial gap		STA-05, IVS-04	Again, here service agreement related requirements are covered by CCM but there is no reference of a "service level availability".
SecNumCloud	19.1.i	19. Additional requirements / 19.1. Service agreement / i)	i) The service provider must indicate in the service agreement that he cannot claim ownership of the data transmitted and generated by the customer. These data are the property of the customer.		Supply Chain Management, Transparency, and Accountability	Partial gap		STA-05	STA-05 covers SLAs but there is no explicit reference to data ownership by customer.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	19.1.j	19. Additional requirements / 19.1. Service agreement / j)	j) The service provider must indicate in the service agreement that it does not disclose any information relating to the service to third parties, except with the express written authorization of the customer.		Human Resources	No gap		HRS-06	
SecNumCloud	19.1.k	19. Additional requirements / 19.1. Service agreement / k)	k) The service provider must indicate in the service agreement whether it allows remote access for administration or support actions to the service information system.		To be decided (Mapping exists)	Partial gap		STA-05, IAM-02	There is no explicit reference in CCM of "remote access" provision to be included in a service agreement hence the partial gap.
SecNumCloud	19.1.l	19. Additional requirements / 19.1. Service agreement / l)	l) The service provider must specify in the service agreement that: - the service is qualified and include the certificate of qualification; - the customer can lodge a complaint concerning the qualified service with ANSSI; - the client authorizes the ANSSI and the qualification body to audit the service and its service information system in order to verify that they comply with the requirements of these standards.		To be decided (Mapping exists)	Partial gap		STA-05, STA-07, AAC-02	CCM covers 3rd bullet only
SecNumCloud	19.1.m	19. Additional requirements / 19.1. Service agreement / m)	m) The service provider must specify in the service agreement that the customer authorizes, in accordance with this standard (see requirement 18.2 b), a qualified information system audit [PASSI] service provider mandated by the service provider to be audited. the service and its information system as part of the control plan.		To be decided (Mapping exists)	Partial gap		STA-04, STA-05, STA-08, AAC-01, AAC-02, TVM-02, IVS-06	Partial gap due to 18.2.b missing reqs that are referenced in this control e.g., source code audits and "in accordance to this standard" reference. Remaining reqs are covered by CCM.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	19.2	19. Additional Requirements / 19.2. Location of data	a) The service provider must document and communicate to the client the location of storage and data processing. b) The service provider must store and process customer data within the European Union. c) The administration and supervision of the service must be carried out from the European Union. d) The service provider may perform support operations to clients from a State outside the European Union. It must document the list of operations that can be performed by the customer support from a state outside the European Union, and the mechanisms to ensure access control and supervision from the European Union.		To be decided (Mapping exists)	Partial gap		STA-05, IAM-09, DSI-02, DCS-01	Partial gap selection is made on the missing explicit requirement from CCM with respect to the storage/processing/administration within EU
SecNumCloud	19.3	19. Additional requirements / 19.3. Regionalization	a) The service provider must ensure that the service interfaces accessible to the customer are at least available in French. b) The provider must provide first level support in French.		To be decided (No mapping)	Full gap			

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	19.4	19. Additional requirements / 19.4. End of contract	a) At the end of the contract between the service provider and the customer, whether the contract has come to an end or for any other reason, the service provider must ensure a secure deletion of all the customer data. This deletion can be carried out according to one of the following methods, and within a period specified in the service agreement: - erasure by complete rewriting of any medium that hosted these data; - erasure of the keys used for the encryption of the client's storage spaces described in chapter 10.1; - safe recycling, under the conditions set out in chapter 11.9. b) At the end of the contract, the service provider must delete the technical data relating to the customer (directory, certificates, access configuration, etc.).		To be decided (Mapping exists)	No gap		EKM-02, IAM-02, IAM-11, IAM-12, DCS-05, DSI-07	
SI-07 / Article: 10	SI-07-05	Information security policy of public administration (IVPJU) / Adoption of a common risk assessment methodology	The Minister responsible for public administration approves the methodology for a risk assessment on a proposal from the inter-ministerial working group on information security.	Both	Governance and Risk Management	Partial gap		GRM-02, GRM-10	In order to fill the gap the control GRM 02 (or GRM 10) should be changed and the following should be added: Risk Assessment Methodology should be defined and approved by the senior management.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SI-07 / Article: 122	SI-07-65	The policy for development and maintenance of information systems and change management / Production environment (system)	Production: There shall be the documented procedures for any change in the information system in a production environment allowing return to the state before the change.	Security	Change Control & Configuration Management	No gap		CCC-03, CCC-05	NO GAPS: covered in CCC-03 and CCC-05 even if doesn't cover "roll back" reference, which it might be added to the CCC-05 control as an example.
SI-07 / Article: 145	SI-07-78	Information systems management policy / Data processing of log files	Processing of the data in the logs: Logs containing sensitive data are stored, processed and transmitted in accordance with the provisions of the Act (Law), any access to such records or other form of processing of data in the logs must be recorded. Any exceptions must be explained in writing and must include the risk assessment.	Privacy	Datacenter Security	No gap		IAM-02, DCS-07, DCS-08, DCS-09	NO GAPS: covered in IAM-02, DCS-07, DCS-08, DCS-09. This is duplicate control, see SI-07-44.
SI-07 / Article: 34	SI-07-23	The policy for appropriate use of information systems and protection of sensitive data / Controlled information systems / Sensitive data / Log files	In the case that the log files (logs) contain sensitive information, the insights and other procedures on the system must be recordered.	Both	Infrastructure & Virtualization Security	No gap		IVS-01	NO GAPS: this control is mapped by IVS-01

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SI-07 / Article: 52	SI-07-34	The policy for appropriate use of information systems and protection of sensitive data / Remote access	Remote Access: Remote access to the information system shall be permitted only on the basis of approved methods with the appropriate level of security, for those users who need access to perform tasks, but only to a limited extent. It should also take into account the principle of a blank screen. After work it is necessary to sign out of the system and to ensure that sensitive data and traces do not remain on the workstation.	Security	Identity & Access Management	No gap		HRS-11, IAM-02	NO GAPS: this is covered by HRS-011 and IAM-02
SI-07 / Article: 58	SI-07-37	The policy for appropriate use of information systems and protection of sensitive data / Access to WWW and web services	Access to Internet and WWW services: Inside the network of public administration, the user access to web sites and related information on their assigned internal IP numbers, time allocation of the internal IP numbers and information on the connection between internal and a public IP address can be recorded for the purpose of investigation of suspected illegal acts. The Managers can communicate these data on a reasoned request by the Authority that on the basis of statutory powers deal with alleged illegal acts. Different data processing from the first sentence is not allowed. The retention period of the synthesized data is three months, and then the data is destroyed or anonymised. Anonymised data can be used to operate the system.	Both	Human Resources	No gap		HRS-08	NO GAPS: covered in HRS-08

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SI-07 / Article: 7	SI-07-02	Information security policy of public administration (IVPJU) / Jurisdiction, adoption and mandatory use	Recommendations IVPJU on the basis of Article 80 of the Regulation on Administrative Operations (OG RS, No. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07 and 31/08) is adopted by the Ministry of public administration, and public authorities are obliged to consider it as an overarching information security policy.	Both	Governance and Risk Management	No gap		GRM-04, GRM-06, DCS-05, DCS-06	NO GAPS: the relevant mapping in CCM are GRM 04, GRM 06, DCS 05 and DCS 06. NOTE: Only applicable to the Slovenian Gov Cloud managed by the Ministry of PA.
SI-07 / Article: 85	SI-07-44	The policy for appropriate use of information systems and protection of sensitive data / Data access - sensitive data	Access to Data - Sensitive data: (85) The collection of sensitive data (electronic and paper) must have adequate insights logs, which register: who, when and why made a view, in accordance with the relevant legislation. All service and maintenance work on the server, database, application, or service must be recorded.	Both	Identity & Access Management	No gap		IAM-02, DCS-07, DCS-08, DCS-09	NO GAPS: covered in IAM-02, DCS-07, DCS-08, DCS-09
SI-07 / Article: 9	SI-07-04	Information security policy in public administration (IVPJU) / Review and changes by the authorised working group	The Ministry, responsible for public administration is the guardian of the policy IVPJU. At least once a year, the inter-ministerial working group on information security, appointed by the Minister responsible for public administration, reviews and proposes amendments to the policy.	Both	Governance and Risk Management	No gap		GRM-09	NO GAPS: GRM 09

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SI-07 / Articles: 132 - 133	SI-07-69	Information systems management policy / Change management in the production environment (system) and network	Managing changes in the production environment and network: With changes in the information system it must be ensured its confidentiality, integrity and maximized availability. Before any change in the information system, a rollback plan must be provided. The users of the information system shall be properly informed about the changes in the information system, which could lead to the changes in the daily work of the users of the system.	Both	Change Control & Configuration Management	No gap		CCC-03, CCC-05	NO GAPS: covered in CCC-03 and CCC-05 even if doesn't cover "roll back" reference, which it might be added to the CCC-05 control as an example.
SI-07 / Articles: 36 - 39	SI-07-25	The policy for appropriate use of information systems and protection of sensitive data / Using removable media	Management of removable media: (36) Adequate protection and security in the management of removable media must be provided. (37) A loss or theft of removable media should be reported to the responsible person. (38) The removable media of unknown or suspect origin may not be used. Before using the contents, the removable media should always be checked against the possible infection with malware. (39) The user must give all removable media that are no longer needed or are useless to the responsible person.	Security	Human Resources	Partial gap		HRM or DCS	A control should be added in CCM (either in HRM or DCS domain) to address the issue of "removable media lifecycle". The requirement from SI-07 / Articles: 36 - 39 could be taken "as is".

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SI-07 / Articles: 92 - 94	SI-07-48	The policy for procurement of equipment and services (external customers) / Preparing public procurement	Preparation of public procurement: (92) In preparing the specifications for the public procurement for the purchase of components or maintenance of information systems it is needed to anticipate and define security features that meet the requirements of information security policy of public administration and the relevant legislation. (93) Where appropriate, the public procurement contracting authority must adequately classify the sensitive documents and sensitive data against disclosure before publishing. It is necessary to respect the provisions of the relevant legislation. (94) The preparation of the public procurement should determine the technical, economic and human resources conditions and criteria for selecting suppliers in terms of providing security policy objectives.	Both	Supply Chain Management, Transparency, and Accountability	Partial gap		STA or STA-05	Partial GAP in CCM. It shall be compensated by either amending the STA-05 or by including a new control in STA Domain. The new control could re-use the wording of the SI-07-48 requirement. It shall be noted that the SI-07-48 requirement could be made widely applicable by removing the reference to the "public procurement" and referring to "procurement" in general terms. It shall be also noted SI-10-01 (which is marked as FULL GAP this this analysis) is also referring to "procurement" therefore it makes sense to add a new control in STA Domain and that would address both the partial gap in SI-07-48 and SI-10-01. Other options: customer requirements (might not be relevant)

SI-09 / 1.18	SI-09-04	Audit trail / GTZ-NADZOR-REVIZIJA-10	IT solution which is the subject of the contract must provide adequate audit trails (logs / Journal) for the areas where personal or financial data or security schema are processed. Audit trail must be relevant by the content, retention and control system (including the security plan and related procedures), so that they last as evidence before a judicial authority.	Both	Infrastructure & Virtualization Security	No gap		IVS-01	The relevant mapping with IVS-01. There is a minor gap in IVS-01, once the SI-09-04 refers to: "so that they last as evidence before a judicial authority." IVS-01 refers to "and to support forensic investigative capabilities in the event of a security breach." So, to fill the gap the CCM control should be supplemented with the reference to the "the possible use of logs in judicial cases". In addition, during an audit engagement, incorporating requisite best practices (e.g. Audit Charters), protocols and standards as required by many government regulatory agencies such as the following; SEC, PCAOB, ISACA, FASB and similar global regulatory agencies. Comment: IT solution which is the subject of the contract must provide: end-to-end, secure, GRC compliant, easily accessible, shared and searchable Audit Trail (logs / Journal) for all types of audits, including forensic audits in areas where personal,

									financial, and/or data security schemas are processed . Audit trails must be relevant as determined by the content, provenance, retention, archival, and control system protocols in-plaice and maintained, (including the security plan and related procedures such as a bullet proof Chain of Custody), as they may eventually be offered as supporting evidence before the appropriate judicial authority. Req_type should be "Both"; Privacy is limited to access of information of a person. This requirement also applies to financial data, which may not relate to a person. Comment: Data collection and data retention should be aligned with GDPR. Thus, supporting deletion or masking of personal data.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SI-10 / 3.6.1	SI-10-01	Technical and professional capacity	Technical conditions contain evidences that the provider understands the public procurement orders and has competencies related to the required technologies, as evidenced in particular by expert evidences and track records of the company. References and certificates must be valid on the date of submission of the bid. Staff conditions may contain in particular experts' experiences, references and certifications. In some cases, the support of principals must be demonstrably ensured.	Other	To be decided (No mapping)	Full gap		STA-01 or GRM-04 or STA	Req_type should be "Both"; Privacy is limited to access of information of a person. This requirement also applies to financial data, which may not relate to a person
TSC_2016	CC1.1	Common Criteria Related to Organization and Management	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	To be decided (Mapping exists)	No gap	To be decided		there is no CCM controls regarding the definition of organizational structures and reporting lines. Comment: workshop consolidation showed no gap.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC1.2	Common Criteria Related to Organization and Management	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy or any combination thereof].	Both	Governance and Risk Management	No gap	0	GRM-03 GRM-05 GRM-06	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC1.3	Common Criteria Related to Organization and Management	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] and provides resources necessary for personnel to fulfil their responsibilities.	Both	Human Resources	No gap	0	HRS-02 HRS-09	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC1.4	Common Criteria Related to Organization and Management	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	Human Resources	No gap	0	HRS-02 HRS-07 HRS-09 HRS-10	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC2.1	Common Criteria Related to Communications	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	Both	Business Continuity Management & Operational Resilience	No gap	0	BCR-04	n/a
TSC_2016	CC2.2	Common Criteria Related to Communications	The entity's [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Both	To be decided (Mapping exists)	No gap	0	HRS-03 HRS-09 STA-03 STA-05 STA-09	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC2.3	Common Criteria Related to Communications	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Both	To be decided (Mapping exists)	No gap	+	DSI-06 GRM-06 HRS-03 HRS-09 SEF-03 STA-03 STA-05 STA-09	n/a
TSC_2016	CC2.4	Common Criteria Related to Communications	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] of the system, is provided to personnel to carry out their responsibilities.	Both	Business Continuity Management & Operational Resilience	No gap	-	BCR-04	Other than responsibilities and roles, there are other information relevant to designing, developing, implementing, operating, maintaining and monitoring controls. They shall all be make available for responsible person. BCR-04 only mentioned for administrators about system documentation, other parts shall also be considered. / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC2.5	Common Criteria Related to Communications	Internal and external users have been provided with information on how to report [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] failures, incidents, concerns, and other complaints to appropriate personnel.	Both	Security Incident Management, E-Discovery, & Cloud Forensics	No gap	0	SEF-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC2.6	Common Criteria Related to Communications	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] are communicated to those users in a timely manner.	Both	Security Incident Management, E-Discovery, & Cloud Forensics	No gap	+	SEF-04	SEF-04 includes both notifications and opportunity to participate in forensic investigation. / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC3.1	Common Criteria Related to Risk Management and Design and Implementation of Controls	The entity (1) identifies potential threats that could impair system [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyses the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	Both	To be decided (Mapping exists)	No gap	+	AAC-03 BCR-01 BCR-05 BCR-06 BCR-09 DSI-01 DSI-06 GRM-02 GRM-10 GRM-11 IAM-07	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC3.2	Common Criteria Related to Risk Management and Design and Implementation of Controls	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	Both	To be decided (Mapping exists)	No gap	+	AAC-03 BCR-10 GRM-01 GRM-03 GRM-06 GRM-08 GRM-09 HRS-08 HRS-10	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC4.1	Common Criteria Related to Monitoring of Controls	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof], and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	Both	Audit Assurance & Compliance	No gap	0	AAC-01 AAC-02	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC5.1	Common Criteria Related to Logical and Physical Access Controls	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	Identity & Access Management	No gap	0	AIS-02 IAM-01 IAM-03 IAM-04 IAM-05 IAM-08 IAM-09 IAM-13	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC5.2	Common Criteria Related to Logical and Physical Access Controls	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof]. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Both	Identity & Access Management	No gap	+	IAM-02 IAM-09 IAM-10 IAM-11	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC5.3	Common Criteria Related to Logical and Physical Access Controls	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	Identity & Access Management	No gap	+	IAM-12	n/a
TSC_2016	CC5.4	Common Criteria Related to Logical and Physical Access Controls	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	To be decided (Mapping exists)	No gap	To be decided		n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014. Comment: workshop consolidation showed no gap.
TSC_2016	CC5.5	Common Criteria Related to Logical and Physical Access Controls	Physical access to facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	Datacenter Security	No gap	0	DCS-07 DCS-08 DCS-09	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC5.6	Common Criteria Related to Logical and Physical Access Controls	Logical access security measures have been implemented to protect against [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Both	To be decided (Mapping exists)	No gap	+	AIS-04 DSI-05 DSI-07 EKM-02 EKM-03 HRS-01 HRS-05 HRS-11 IVS-06 IVS-08 IVS-09 IVS-10 IVS-11 IVS-12 TVM-03	There are lots of requirements in CCM actually related to logical access. Here are only typical listed. / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC5.7	Common Criteria Related to Logical and Physical Access Controls	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	To be decided (Mapping exists)	No gap	0	DSI-03 DCS-04 DCS-05 EKM-02 EKM-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC5.8	Common Criteria Related to Logical and Physical Access Controls	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	To be decided (Mapping exists)	No gap	0	CCC-04 MOS-03 MOS-04 MOS-05 TVM-01	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC6.1	Common Criteria Related to System Operations	Vulnerabilities of system components to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	Threat and Vulnerability Management	No gap	0	TVM-01 TVM-02 TVM-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC6.2	Common Criteria Related to System Operations	[Insert the principle(s)addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and	Both	Security Incident Management, E-Discovery, & Cloud Forensics	No gap	0	SEF-02 SEF-03 SEF-04 SEF-05	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.						
TSC_2016	CC7.1	Common Criteria Related to Change Management	The entity's commitments and system requirements, as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof], are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	Both	To be decided (Mapping exists)	No gap	-	AIS-01 CCC-01 CCC-02 CCC-03 CCC-04 CCC-05 TVM-01 TVM-02 TVM-03	Maintenance and management of system components are not included in CCM. / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	CC7.2	Common Criteria Related to Change Management	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	To be decided (Mapping exists)	No gap	-	CCC-01 CCC-05 DCS-01 GRM-08 MOS-19	Policies and procedures updates are not requested in CCM. Regular update check on infrastructure, data and software are not requested directly in CCM. / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	CC7.3	Common Criteria Related to Change Management	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof].	Both	To be decided (Mapping exists)	No gap	To be decided		There is no CCM controls regarding the monitoring and testing the change management process. Comment: workshop consolidation showed no gap.
TSC_2016	CC7.4	Common Criteria Related to Change Management	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's [insert the principle(s) addressed by the engagement: security, availability, processing integrity, confidentiality, or privacy, or any combination thereof] commitments and system requirements.	Both	Change Control & Configuration Management	No gap	0	CCC-01 CCC-02 CCC-03 CCC-04 CCC-05 IAM-06	n/a
TSC_2016	A1.1	Additional Criteria for Availability	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	AIS-04 BCR-03 BCR-05 BCR-06 BCR-07 BCR-08 IVS-04	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	A1.2	Additional Criteria for Availability	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	BCR-01 BCR-02 BCR-03 BCR-05 BCR-06 BCR-07 BCR-08 BCR-09 BCR-11 IVS-04	n/a
TSC_2016	A1.3	Additional Criteria for Availability	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	Other	Business Continuity Management & Operational Resilience	No gap	0	BCR-01 BCR-02 BCR-03 BCR-09 BCR-11	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	PI1.1	Additional Criteria for Processing Integrity	Procedures exist to prevent, or detect and correct, processing errors to meet the entity's processing integrity commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	AIS-03 AIS-04 IVS-02 IVS-03 IVS-07 IPY-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	PI1.2	Additional Criteria for Processing Integrity	System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	AIS-03 AIS-04 IVS-02 IVS-03 IVS-07 IPY-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	PI1.3	Additional Criteria for Processing Integrity	Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	AIS-03 AIS-04 IVS-02 IVS-03 IVS-07 IPY-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	PI1.4	Additional Criteria for Processing Integrity	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the entity's processing integrity commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	AIS-03 AIS-04 IVS-02 IVS-03 IVS-07 IPY-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	PI1.5	Additional Criteria for Processing Integrity	System output is complete, accurate, distributed, and retained to meet the entity's processing integrity commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	AIS-03 AIS-04 IVS-02 IVS-03 IVS-07 IPY-03	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	PI1.6	Additional Criteria for Processing Integrity	Modification of data, other than routine transaction processing, is authorized and processed to meet the entity's processing integrity commitments and system requirements.	Other	To be decided (No mapping)	Full gap	-	IAM-09	CCM specifies no requirements on authorization on modification of data. Only access to such systems, where people may have the right to modify customer data has mentioned in IAM-09. / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	C1.1	Additional Criteria for Confidentiality	Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	DCS-02 DCS-06 DSI-03 DSI-05 EKM-03 IAM-02 IAM-04 IVS-08 HRS-11	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	C1.2	Additional Criteria for Confidentiality	Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	0	DCS-02 DCS-06 DSI-05 EKM-03 IAM-02 IAM-04 IVS-08 HRS-11	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	C1.3	Additional Criteria for Confidentiality	Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.	Other	To be decided (Mapping exists)	No gap	-	DCS-01, DCS-02 ,DCS-06, HRS-04, HRS-06	DCS-01, DCS-02, DCS-06, HRS-04, HRS-06 / Requirement is relevant
TSC_2016	C1.4	Additional Criteria for Confidentiality	The entity obtains confidentiality commitments that are consistent with the entity's confidentiality system requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.	Both	To be decided (Mapping exists)	No gap	+	HRS-02 SEF-03 STA-01 STA-05 STA-06 STA-08 STA-09	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	C1.5	Additional Criteria for Confidentiality	Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.	Both	Supply Chain Management, Transparency, and Accountability	No gap	0	STA-05 STA-09	n/a / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	C1.6	Additional Criteria for Confidentiality	Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.	Both	Supply Chain Management, Transparency, and Accountability	No gap	-	STA-05	There is no specified infor-mation in STA-05 about com-mitments changes, only "notifi-cation of any changes" is men-tioned here. Suggest adding commitments and system re-quirements changes into STA-05. / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	C1.7	Additional Criteria for Confidentiality	The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.	Both	Supply Chain Management, Transparency, and Accountability	No gap	To be decided		Suggest to 1. add data retain requirements in SLA 2. handle to retain data according to SLA Comment: workshop consolidation showed no gap.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	C1.8	Additional Criteria for Confidentiality	The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.	Both	Data Security & Information Lifecycle Management	No gap	-	DSI-07	Data disposes procedures exist, however, no specific requirements on customer data disposes. Shall align on customer data disposes requirements in contract or SLA. / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	P1.1	Additional Criteria for Privacy	The entity provides notice to data subjects about its privacy practices to meet the entity's privacy commitments and system requirements. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Extraordinary workshop group 2 29.8.2017: FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED first clause "Provide details on:" points from (i) to (xii)
TSC_2016	P1.2	Additional Criteria for Privacy	The entity's privacy commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Extraordinary workshop group 2 29.8.2017: FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 1.CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY and 3. WAYS IN WHICH THE DATA WILL BE PROCESSED point 3b

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P2.1	Privacy Criteria Related to Choice and Consent	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from the data subject or other authorized person, if required, and such consent is obtained only for the purpose for which the information is intended consistent with the entity's privacy commitments and system requirements. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Extraordinary workshop group 2 29.8.2017: FULL GAP Confirmed. This control is partially addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED first clause "Provide details on:" points (vii). Guidelines on providing consent will be due by WP29 by end of the year, and PLA will be updated. Then this requirement is to be revisited.
TSC_2016	P3.1	Privacy Criteria Related to Collection	Personal information is collected consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No Mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Extraordinary workshop group 2 29.8.2017: FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 1.CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P3.2	Privacy Criteria Related to Collection	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Extraordinary workshop group 2 29.8.2017: FULL GAP Confirmed. This control is partially addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED first clause "Provide details on:" points (vii). Guidelines on providing consent will be due by WP29 by end of the year, and PLA will be updated. Then this requirement is to be revisited.
TSC_2016	P4.1	Privacy Criteria Related to Use, Retention, and Disposal	The entity limits the use of personal information to the purposes identified in the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Extraordinary workshop group 2 29.8.2017: FULL GAP Confirmed. This control is fully addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED first clause "Provide details on:" point (ii) and 3.d in full, 4. RECORD KEEPING point (b) and 6. DATA SECURITY MEASURES first clause.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P4.2	Privacy Criteria Related to Use, Retention, and Disposal	The entity retains personal information consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 11. DATA RETENTION, RESTITUTION AND DELETION.
TSC_2016	P4.3	Privacy Criteria Related to Use, Retention, and Disposal	The entity securely disposes of personal information consistent with the entity's privacy commitments and system requirements.	Privacy	Data Security & Information Lifecycle Management	No gap	To be decided	DSI-07	Data disposes procedures exist, however, no specific requirements on customer data disposes. Shall align on customer data disposes requirements in contract or SLA. / Different mapping in TSC_2016 than in old mapping of TSC_2014
TSC_2016	P5.1	Privacy Criteria Related to Access	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to the data subject consistent with the entity's privacy commitments and system requirements. If access is denied, the data subject is informed of the denial and reason for such denial, as required, consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 6. DATA SECURITY MEASURES (Intervenability) and 12. COOPERATION.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P5.2	Privacy Criteria Related to Access	The entity corrects, amends, or appends personal information based on information provided by the data subjects and communicates such information to third parties, as committed or required, consistent with the entity's privacy commitments and system requirements. If a request for correction is denied, the data subject is informed of the denial and reason for such denial consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 6. DATA SECURITY MEASURES (Intervenability) and 12. COOPERATION.
TSC_2016	P6.1	Privacy Criteria Related to Disclosure and Notification	The entity discloses personal information to third parties with the explicit consent of the data subject to meet the entity's privacy commitments and system requirements, and such consent is obtained prior to disclosure.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED (see 3b and 3.d.d.).
TSC_2016	P6.2	Privacy Criteria Related to Disclosure and Notification	The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is partially addressed by PLA V3 CoC and specifically: 13. LEGALLY REQUIRED DISCLOSURE.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P6.3	Privacy Criteria Related to Disclosure and Notification	The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures of personal information, including breaches, consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (Mapping exists)	Partial gap	To be decided	IVS-01, SEF-04, other parts addresse d by PLA, Code of Conduct	PARTIAL GAP: this control is partially addressed by CCM IVS-01 and SEF-04 while the remaining portion of this control is addressed in PLA V3 CoC, and particularly in 8. PERSONAL DATA BREACH. (please note that this PLA requirement will be updated in January2018 after the final version of the WP29 Guidelines on Data Breach Notification will be published).
TSC_2016	P6.4	Privacy Criteria Related to Disclosure and Notification	The entity obtains privacy commitments from vendors and other third parties whose products and services are part of the system and who have access to personal information processed by the system that are consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED (see 3b)
TSC_2016	P6.5	Privacy Criteria Related to Disclosure and Notification	Compliance with the entity's privacy commitments and system requirements by vendors and others third parties whose products and services are part of the system and who have access to personal information processed by the system is assessed on a periodic and as-needed basis and corrective action is taken, if necessary.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC and specifically: 1.CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY. (The PLA V3 CoC doesn't refer to the periodical assessment of the system, which is is a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
									specification that could be added somewhere).
TSC_2016	P6.6	Privacy Criteria Related to Disclosure and Notification	The entity obtains commitments from vendors and other third parties that may have access to personal information processed by the system, to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on to meet the entity's established incident response procedures, privacy commitments, and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED (see 3b) and 8. PERSONAL DATA BREACH.
TSC_2016	P6.7	Privacy Criteria Related to Disclosure and Notification	The entity provides notification of breaches and incidents to affected data subjects, regulators, and others consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed: his control is addressed by PLA V3 CoC, and specifically in 8. PERSONAL DATA BREACH and 12. COOPERATION.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P6.8	Privacy Criteria Related to Disclosure and Notification	The entity provides to the data subjects an accounting of the personal information held and disclosure of a data subject's personal information, upon the data subject's request, consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC, and specifically in 3. WAYS IN WHICH THE DATA WILL BE PROCESSED, and in 4. RECORD KEEPING and in 12. COOPERATION.
TSC_2016	P7.1	Privacy Criteria Related to Quality	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information consistent with the entity's privacy commitments and system requirements.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	FULL GAP Confirmed. This control is addressed by PLA V3 CoC and specifically: 1.CSP DECLARATION OF COMPLIANCE AND ACCOUNTABILITY.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
TSC_2016	P8.1	Privacy Criteria Related to Monitoring and Enforcement	The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance with the entity's privacy commitments and system requirements; corrections and other necessary actions related to identify deficiencies are taken in a timely manner.	Privacy	To be decided (No mapping)	Full gap	To be decided	Control addresse d by PLA, Code of Conduct	Full gap confirmed. This could be compensated by the PLA V3 CoC requirement 6 Data Security Measures ('- Intervenability: describe how the CSP enables data subjects' rights of access, rectification, erasure ('right to be forgotten'), blocking, objection, restriction of processing [please refer to Section 10 'Restriction of processing'], portability [please refer to Section 9 'Data portability, migration, and transfer back'], in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further processed by subcontractors; (this is also relevant for Section 9 'Data portability, migration, and transfer back');)

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
SecNumCloud	5.1.b	5. Information security policies and Risk Management Principles / 5.1.b.	5.1.b The provider must apply the ANSSI [HYGIENE] computer health guide to the service information system.	Security					Mapping and gap analysis: mapping not possible currently. SecNumCloud specific for France based on ANSSI. ANSSI [HYGIENE]?
SecNumCloud	10.1.b	10. Cryptology / 10.1.b	10.1.b The service provider must use a data encryption method complying with the rules of [CRYPTO_B1].	Both					Mapping and gap analysis: mapping not possible currently. Potential controls: GRM-04
SecNumCloud	10.1.c	10. Cryptology / 10.1.c	10.1.c It is recommended to use a data encryption method that complies with [CRYPTO_B1].	Both					Mapping and gap analysis: mapping not possible currently. Potential controls: GRM-04
SecNumCloud	10.2.a.b.c .d.e	10. Cryptology / 10.2.a.b.c.d.e	10.2.a.b.c.d.e Stream encryption a) When the provider implements a network stream encryption mechanism, it must respect the rules of [CRYPTO_B1]. b) When the service provider implements a network flow encryption mechanism, it is recommended that the service provider comply with the recommendations of [CRYPTO_B1]. c) If the TLS protocol is implemented, the provider must implement the recommendations of [NT_TLS]. d) If the IPsec protocol is implemented, the provider must implement the recommendations of [NT_IPSEC]. e) If the SSH protocol is implemented, the	Both					Mapping and gap analysis: mapping not possible currently. Unknown gap due to unknown rules and recommendations in crypto_b1 and NT_XXX. Potential controls: EKM-02, EKM-03, EKM-04, IPY-04

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			provider must implement the recommendations of [NT_SSH].						
SecNumCloud	10.5.a.b.c.d	10. Cryptology / 10.5.a.b.c.d	10.5.a.b.c.d Management of Secrets a) The service provider must implement cryptographic keys complying with the rules of [CRYPTO_B2]. b) It is recommended that the service provider implement cryptographic keys that comply with the recommendations of [CRYPTO_B2]. c) The service provider must protect the access to the cryptographic keys and other secrets used for the encryption of the data by an appropriate means: security container (software or hardware) or disjoint support. d) The service provider shall protect access to cryptographic keys and other secrets used for administrative tasks by a suitable security, software or hardware container.	Both					Mapping and gap analysis: mapping not possible currently. No gap between CCM and 10.5.c),d). Unknown what is in crypto_b2. If the latter is not made known this gap cannot be closed. Eventually break down 10.5. into 4 sub-controls and 2 are no gap and two are not possible to map Potential controls: EKM-01, EKM-02, EKM-03, EKM-04.

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	DCA-1.1	Declaration of compliance and accountability	1. Declare and ensure to comply with the applicable EU data protection law and with the terms of this Code of Conduct, also with respect to technical and organisational security measures, and to safeguard the protection of the rights of the data subject. Where there is a material change in applicable EU data protection law which may imply new or conflicting obligations regarding the terms of this Code of Conduct, the CSP commits to complying with the terms of the applicable EU data protection law. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	DCA-1.2	Declaration of compliance and accountability	2. Declare and ensure to be able to demonstrate compliance with the applicable EU data protection law and with the terms of this Code of Conduct (accountability). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	DCA-1.3	Declaration of compliance and accountability	3. Describe what policies and procedures the CSP has in place to ensure and demonstrate compliance by the CSP itself and its subcontractors (see also Controls no. WWP-3.1 to 3.5, below) or business associates, with the applicable EU data protection law and with the Terms of this Code of Conduct.	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;						
PLA CoC	DCA-1.4	Declaration of compliance and accountability	4. Identify the elements that can be produced as evidence to demonstrate such compliance. Evidence elements can take different forms, such as self-certification/attestation, third-party audits (e.g., certifications, attestations, and seals), logs, audit trails, system maintenance records, or more general system reports and documentary evidence of all processing operations under its responsibility. These elements need to be provided at the following levels: (i) organisational policies level to demonstrate that policies are correct and appropriate; (ii) IT controls level, to demonstrate that appropriate controls have been deployed; and (iii) operations level, to demonstrate that systems are behaving (or not) as planned. Examples of evidence elements pertaining to different levels are data protection certifications, seals and marks. **[C & P] the requirement is applicable both to**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			the situation in which the CSP is a controller and one in which the CSP is a processor;						
PLA CoC	CAR-1.1	CSP relevant contacts and its role	1. Specify CSP's identity and contact details (e.g., name, address, email address, telephone number and place of establishment); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	CAR-1.2	CSP relevant contacts and its role	2. Specify the identity and contact details (e.g., name, address, email address, telephone number and place of establishment) of the CSP's local representative(s) (e.g., a local representative in the EU); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	CAR-1.3	CSP relevant contacts and its role	3. Specify the CSP's data protection role for each of the relevant processing activities inherent to the services (i.e., controller, joint-controller, processor or subprocessor); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	CAR-1.4	CSP relevant contacts and its role	4. Specify the contact details of the CSP's Data Protection Officer (DPO) or, if there is no DPO, the contact details of the individual in charge of privacy matters to whom the customer may address requests; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	CAR-1.5	CSP relevant contacts and its role	5. Specify the contact details of the CSP's Information Security Officer (ISO) or, if there is no ISO, the contact details of the individual in charge of security matters to whom the customer may address requests. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.1	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 1. categories of personal data concerned in the processing; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.2	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 2. purposes of the processing for which data are intended and the necessary legal basis to carry out such processing in a lawful way; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-1.3	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 3. recipients or categories of recipients of the data; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.4	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 4. existence of the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing, as well as the right to data portability; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.5	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 5. where applicable, the fact that the CSP intends to transfer personal data to a third country or international organisation and the absence of an adequacy decision by the European Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-1.6	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 6. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.7	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 7. where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.8	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 8. the right to lodge a complaint with a supervisory authority (as defined in Article 4 (21) GDPR); **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-1.9	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 9. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.10	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 10. the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.11	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 11. where the CSP intends to further process the personal data for a purpose other than that for which the personal data is being collected, information on that other purpose, prior to the relevant further processing;	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-1.12	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 12. where personal data has not been obtained from the data subject, from which source the personal data originated, and if applicable, whether the data came from publicly accessible sources; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.13	Ways in which the data will be processed	CSPs that are controllers must provide details to cloud customers regarding: 13. activities that are conducted to provide the agreed cloud service(s) (e.g., data storage), activities conducted at the customer's request (e.g., report production) and those conducted at the CSP's initiative (e.g., backup, disaster recovery, fraud monitoring). **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-1.14	Ways in which the data will be processed	CSPs that are processors must provide to cloud customers details on: 14. the extent and modalities in which the customer-data controller can issue its binding instructions to the CSP-data processor (General Information - applicable to CSPs that are processors). **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-1.15	Ways in which the data will be processed	CSPs that are processors must 15. Specify how the cloud customers will be informed about relevant changes concerning relevant cloud service(s), such as the implementation or removal of functions (General Information - applicable to both CSPs that are controllers and CSPs that are processors). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-2.1	Personal data location	1. Specify the location(s) of all data centres or other data processing locations (by country) where personal data may be processed, and in particular, where and how data may be stored, mirrored, backed up, and recovered (this may include both digital and non-digital means). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-2.2	Personal data location	2. Notify cloud customers of any intended changes to these locations once a contract has been entered into, in order to allow the cloud customer to acknowledge or object. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-2.3	Personal data location	3. Allow cloud customers to terminate the contract in the event that an objection cannot be satisfactorily resolved between the CSP and the cloud customer, and afford the cloud customer sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-3.1	Subcontractors	1. Identify subcontractors and subprocessors that participate in the data processing, along with the chain of accountabilities and responsibilities used to ensure that data protection requirements are fulfilled. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-3.2	Subcontractors	2. Declare to cloud customers and further ensure that the CSP will not engage another processor without prior specific or general written authorisation of the cloud customer. **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-3.3	Subcontractors	3. Declare to cloud customers and further ensure that the CSP imposes on other processors the same data protection obligations stipulated between the CSP and the cloud customer, by way of a contract (or other binding legal act), in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of EU applicable law; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-3.4	Subcontractors	4. Declare to cloud customers and further ensure that the CSP remains fully liable to the cloud customer for the performance of other processors' obligations, in case the other processors fail to fulfil their data protection obligations. **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-3.5	Subcontractors	5. Identify the procedures used to inform the cloud customer of any intended changes concerning the addition or replacement of subcontractors or subprocessors with customers retaining at all times the possibility to object to such changes or terminate the contract. In the event of termination by the cloud customer, the cloud customer must be afforded sufficient time to procure an alternative CSP or solution (by establishing a transition period during which an agreed-upon level of services will continue to be provided to the cloud customer, under the contract). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-4.1	Installation of software on cloud customer's system	1. Indicate to cloud customers whether the provision of the service requires the installation of software on the cloud customer's system (e.g., browser plug-ins). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-4.2	Installation of software on cloud customer's system	2. Indicate to cloud customers the software's implications from a data protection and data security point of view. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-5.1	Data processing contract (or other binding legal act)	1. Share with the cloud customers the model data processing contract (or other binding legal act) which will govern the processing carried out by the CSP on behalf of the cloud customer and set out the subject matter and duration of the processing, the type of personal data and categories of data subjects and the obligations and rights of the cloud customer. **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-5.2	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 2. process personal data only upon documented instructions from the cloud customer, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the CSP is subject; in such a case, the CSP will inform the cloud customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-5.3	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 3. ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they do not process personal data except upon instructions from the cloud customer, unless otherwise required by Union or Member State law; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-5.4	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 4. implement all technical and organizational security measures which the CSP deems adequate, in light of the available technology, the state of the art, the costs in implementing those measures and the processing activities inherent to the services provided, to ensure that the CSP's services are covered by a level of security which is appropriate, considering the potential risks to the interests, rights and freedoms of data subjects; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	WWP-5.5	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 5. Respect the conditions for engaging another processor (see Controls no. WWP-3.1 to 3.5, above). **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-5.6	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 6. taking into account the nature of the processing, assist the cloud customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the cloud customer's obligation to respond to requests for exercising the data subject's rights; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-5.7	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 7. assist the cloud customer in ensuring compliance with obligations related to security of processing, notification of a personal data breach to the supervisory authority; communication of a personal data breach to the data subject, and data protection impact assessment; taking into account the nature of processing and the information available to the processor;	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			[P] the requirement is applicable only to the situation in which the CSP is a processor.						
PLA CoC	WWP-5.8	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 8. at the choice of the cloud customer, delete or return all personal data to customer after end of the provision of services relating to processing; and delete existing copies unless Union or Member State law requires storage of the personal data (see Controls no. RRD-1.1 to 4.5, below).	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	WWP-5.9	Data processing contract (or other binding legal act)	The contract or other legal act must stipulate, that the CSP will do the following: 9. make available to the cloud customer all information necessary to demonstrate compliance with relevant data protection obligations; and allow for and contribute to audits, including inspections, conducted by the cloud customer or another auditor mandated by the customer. **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	REC-1.1	Recordkeeping for CSP-controller	1. CSP controller confirms to cloud customers and commits to maintain a record of processing activities under CSP responsibility and make it available to the supervisory authority on request. **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-1.2	Recordkeeping for CSP-controller	Record contains: 2. name and contact details of controller and, where applicable, the joint controller, the controller's representative and the data protection officer; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-1.3	Recordkeeping for CSP-controller	Record contains: 3. the purposes of the processing; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-1.4	Recordkeeping for CSP-controller	Record contains: 4. a description of the categories of data subjects and of the categories of personal data; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-1.5	Recordkeeping for CSP-controller	Record contains: 5. categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			[C] the requirement is applicable only to the situation in which the CSP is a controller;						
PLA CoC	REC-1.6	Recordkeeping for CSP-controller	Record contains: 6. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-1.7	Recordkeeping for CSP-controller	Record contains: 7. where possible, the envisaged time limits for erasure of different categories of data or, if that is not possible, the criteria used to determine that period; **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-1.8	Recordkeeping for CSP-controller	Record contains: 8. a description of technical and organisational security measures in place (see also Controls no. SEC-1.1 to 1.3.xxvii, below). **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-2.1	Recordkeeping for CSP-processor	1. CSP processor confirms to cloud customers and commits to maintain a record of all categories of processing activities carried out on behalf of a controller and make it available to the supervisory authority upon request.	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			[P] the requirement is applicable only to the situation in which the CSP is a processor.						
PLA CoC	REC-2.2	Recordkeeping for CSP-processor	Record contains: 2. name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-2.3	Recordkeeping for CSP-processor	Record contains: 3. categories of processing carried out on behalf of each controller; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-2.4	Recordkeeping for CSP-processor	Record contains: 4. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards; **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	REC-2.5	Recordkeeping for CSP-processor	Record contains: 5. a description of technical and organisational security measures in place (see also Controls no. SEC-1.1 to 1.3.xxvii, below). **[P] the requirement is applicable only to the situation in which the CSP is a processor.**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	DTR-1-1	Data transfer	1. Clearly indicate whether data is to be transferred, backed up and/or recovered across borders, in the regular course of operations or in an emergency. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	DTR-1-2	Data transfer	If transfer restricted under applicable EU law: 2. Clearly identify the legal ground for the transfer (including onward transfers through several layers of subcontractors), e.g., European Commission adequacy decision, model contracts/standard data protection clauses, approved codes of conduct or certification mechanisms, binding corporate rules (BCRs), and Privacy Shield. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.1	Data security measures	1. Specify to cloud customers the technical, physical and organisational measures that are in place to protect personal data against accidental or unlawful destruction; or accidental loss, alteration, unauthorized use, unauthorised modification, disclosure or access; and against all other unlawful forms of processing; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.2	Data security measures	2. Describe to cloud customers the concrete technical, physical, and organisational measures (protective, detective and corrective) that are in place to ensure the following safeguards: **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.2.i	Data security measures	(i) availability - processes and measures in place to manage risk of disruption and to prevent, detect and react to incidents, such as backup Internet network links, redundant storage and effective data backup, restore mechanisms and patch management; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.2.ii	Data security measures	(ii) integrity: - methods by which the CSP ensures integrity (e.g., detecting alterations to personal data by cryptographic mechanisms such as message authentication codes or signatures, error-correction, hashing, hardware radiation/ionization protection, physical access/compromise/destruction, software bugs, design flaws and human error, etc.); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.2.iii	Data security measures	(iii) confidentiality - methods by which the CSP ensures confidentiality from a technical point of view in order to assure that only authorised persons have access to data; including, inter alia as appropriate, pseudonymisation and encryption of personal data 'in transit' and 'at rest,' authorisation mechanism and strong authentication; and from a contractual point of view, such as confidentiality agreements, confidentiality clauses, company policies and procedures binding upon the CSP and any of its employees (full time, part time and contract employees), and subcontractors who may be able to access data; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.2.iv	Data security measures	(iv) transparency - technical, physical and organisational measures the CSP has in place to support transparency and to allow review by customers (see, e.g., Control no. MON-1.1, below); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.2.v	Data security measures	(v) isolation (purpose limitation) - How the CSP provides appropriate isolation to personal data (e.g., adequate governance of the rights and roles for accessing personal data (reviewed on a regular basis), access management based on the "least privilege" principle; hardening of hypervisors; and proper management of shared resources wherever virtual machines are used to share physical resources among cloud customers); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.2.vi	Data security measures	(vi) intervenability - methods by which the CSP enables data subjects' rights of access, rectification, erasure ('right to be forgotten'), blocking, objection, restriction of processing (see Control no. ROP-1.1, below), portability (see Controls no. PMT-1.1 to 1.2, below) in order to demonstrate the absence of technical and organisational obstacles to these requirements, including cases when data are further processed by subcontractors (this is also relevant for Section 9, 'Data portability, migration and transfer back'); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.2.vii	Data security measures	(vii) portability - refer to Controls no. PMT-1.1 to 1.2., below; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.2.viii	Data security measures	(viii) accountability: refer to Controls no. DCA-1.1 to 1.4, above. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3	Data security measures	3. As a minimum acceptable baseline, this CoC requires CSPs to comply with the controls set out in ENISA's Technical Guidelines for the implementation of minimum security measures for Digital Service Providers; for each control, the tables on sophistication levels within security measures provided in the ENISA's Technical Guidelines will apply, and the CSP must indicate the appropriate sophistication level complied with per each control (1 to 3), taking into account the state of the art, costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. It shall be noted that not all the minimum security measures listed in the ENISA's Technical Guidelines are directly applicable to all the CSPs. For instance, the requirements SO08 or SO09 cannot be directly implemented by a PaaS or SaaS provider. In any case, if some of the below mentioned security measures cannot be directly implemented by a CSP, the CSP in question shall nonetheless guarantee their implementation through their providers. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3.i	Data security measures	i. (SO 01) – Information security policy: The CSP establishes and maintains an information security policy. The document details information on main assets and processes, strategic security objectives. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.ii	Data security measures	ii. (SO 02) – Risk Management: The CSP establishes and maintains an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risks management procedures can include (but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools and Risk Assessment (RA) tools etc. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.iii	Data security measures	iii. (SO 03) – Security Roles: The CSP assigns appropriate security roles and security responsibilities to designated personnel. (i.e. CSO, CISO, CTO etc.). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3.iv	Data security measures	iv. (SO 04) – Third party management: The CSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, security requirements in contracts, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.v	Data security measures	v. (SO 05) – Background checks: The CSP performs appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory framework. Background checks may include checking past jobs, checking professional references, etc. [**C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.vi	Data security measures	vi. (SO 06) – Security knowledge and training: The CSP verifies and ensures that personnel have sufficient security knowledge and that they are provided with regular security training. This is achieved through for example, security awareness raising, security education, security training etc.	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;						
PLA CoC	SEC-1.3.vii	Data security measures	vii. (SO 07) – Personnel changes: The CSP establishes and maintains an appropriate process for managing changes in personnel or changes in their roles and responsibilities. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.viii	Data security measures	viii. (SO 08) – Physical and environmental security: The CSP establishes and maintains policies and measures for physical and environmental security of datacentres such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3.ix	Data security measures	ix. (SO 09) – Security of supporting utilities: The CSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.x	Data security measures	x. (SO 10) – Access control to network and information systems: The CSP established and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xi	Data security measures	xi. (SO 11) – Integrity of network components and information systems: The CSP establishes, protects, and maintains the integrity of its own network, platforms and services by taking steps to prevent successful security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information.	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;						
PLA CoC	SEC-1.3.xii	Data security measures	xii. (SO 12) – Operating procedures: The CSP establishes and maintains procedures for the operation of key network and information systems by personnel. (i.e. operating procedures, user manual, administration procedures for critical systems etc.). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xiii	Data security measures	xiii. (SO 13) – Change management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3.xiv	Data security measures	xiv. (SO 14) – Asset management: The CSP establishes and maintains change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xv	Data security measures	xv. (SO 15) – Security incident detection & Response: The CSP establishes and maintains procedures for detecting and responding to security incidents appropriately. These should consider detection, response, mitigation, recovery and remediation from a security incident. Lessons learned should also be adopted by the service provider. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xvi	Data security measures	xvi. (SO 16) – Security incident reporting: The CSP establishes and maintains appropriate procedures for reporting and communicating about security incidents. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3.xvii	Data security measures	xvii. (SO 17) – Business continuity: The CSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xviii	Data security measures	xviii. (SO 18) – Disaster recovery capabilities: The CSP establishes and maintains an appropriate disaster recovery capability for restoring the offered services in case of natural and/or major disasters. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xix	Data security measures	xix. (SO 19) – Monitoring and logging: The CSP establishes and maintains procedures and systems for monitoring and logging of the offered services (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xx	Data security measures	xx. (SO 20) – System test: The CSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services. **[C & P] the requirement is applicable both to**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			the situation in which the CSP is a controller and one in which the CSP is a processor;						
PLA CoC	SEC-1.3.xxi	Data security measures	xxi. (SO 21) – Security assessments: The CSP establishes and maintains appropriate procedures for performing security assessments of critical assets. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xxii	Data security measures	xxii. (SO 22) – Compliance: The CSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xxiii	Data security measures	xxiii. (SO 23) – Security of data at rest: The CSP establishes and maintains appropriate mechanisms for the protection of the data at rest. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	SEC-1.3.xxiv	Data security measures	xxiv. (SO 24) – Interface security: The CSP should establish and maintain an appropriate policy for keeping secure the interfaces of services which use personal data. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xxv	Data security measures	xxv. (SO 25) – Software security: The CSP establishes and maintains a policy which ensures that the software is developed in a manner which respects security. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xxvi	Data security measures	xxvi. (SO 26) – Interoperability and portability: The CSP uses standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	SEC-1.3.xxvii	Data security measures	xxvii. (SO 27) – Customer Monitoring and log access: The CSP grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed.	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	MON-1.1	Monitoring	1. Indicate to cloud customers the options that the CSP has in place to allow the customer to monitor and/or audit in order to ensure appropriate privacy and security measures described in the PLA are met on an on-going basis (e.g., logging, reporting, first- and/or third-party auditing of relevant processing operations performed by the CSP or subcontractors). Any audits carried out which imply that an auditor will have access to personal data stored on the systems used by the CSP to provide the services will require that auditor to accept a confidentiality agreement. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	PDB-1.1	Explain to cloud customers the procedures in place to collect and disclose the following information:	Specify to cloud customers: 1. How the customer will be informed of personal data breaches affecting the customer's data processed by the CSP and/or its subcontractors, without undue delay and, where feasible, no later than 72 hours from the moment on which the CSP is made aware of the personal data breach in question. A CSP will be considered as "aware" of a personal data breach on the moment that it detects (e.g., directly, or due to a notification received from a subcontractor/sub-processor) an incident which qualifies as a personal data breach and establishes that that incident has affected data processed by the CSP and/or its subcontractors on behalf of a given customer. Should it not be feasible to inform a given customer of a personal data breach within the 72-hour deadline, the CSP will inform that customer of the personal data breach as soon as possible and accompany this communication to the customer with reasons for the delay. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	PDB-1.2	Personal Data Breach	Explain to cloud customers the procedures in place to collect and disclose the following information: 2. the nature of the personal data breach including, where possible, the categories and approximate number of personal data records concerned; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PDB-1.3	Personal Data Breach	Explain to cloud customers the procedures in place to collect and disclose the following information: 3. the name and contact details of the data protection officer or other contact point where more information can be obtained (see Section 2 'CSP relevant contacts and its role', above); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PDB-1.4	Personal Data Breach	Explain to cloud customers the procedures in place to collect and disclose the following information: 4. the likely consequences of the personal data breach; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	PDB-1.5	Personal Data Breach	Explain to cloud customers the procedures in place to collect and disclose the following information: 5. the measures taken (or propose to be taken) to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PDB-1.6	Personal Data Breach	Explain to cloud customers the procedures in place to collect and disclose the following information: 6. Where it is not feasible to provide all of the above information in an initial notification, the CSP must provide as much information to the customer as possible on the reported incident, and provide any further details needed to meet the above requirement as soon as possible (i.e., provision of information in phases). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PDB-1.7	Personal Data Breach	Specify to cloud customers: 7. How the competent supervisory authority/ies will be informed of personal data security breaches, in less than 72 hours of becoming aware of a personal data breach); **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	PDB-1.8	Personal Data Breach	Specify to cloud customers: 8. How data subjects will be informed, without undue delay, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. **[C] the requirement is applicable only to the situation in which the CSP is a controller;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PMT-1.1	Data portability, migration and transfer back	Specify to cloud customers: 1.How the CSP assures data portability, in terms of the capability to transmit personal data in a structured, commonly used, machine-readable and interoperable format: **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PMT-1.1.i	Data portability, migration and transfer back	(i) to the cloud customer ('transfer back', e.g., to an in-house IT environment); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PMT-1.1.ii	Data portability, migration and transfer back	(ii) directly to the data subjects; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	PMT-1.1.iii	Data portability, migration and transfer back	(iii) to another service provider ('migration'), e.g., by means of download tools or Application Programming Interfaces, or APIs). **[C & P] the requirement is applicable both to**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
			the situation in which the CSP is a controller and one in which the CSP is a processor;						
PLA CoC	PMT-1.2	Data portability, migration and transfer back	2. how and at what cost the CSP will assist customers in the possible migration of data to another provider or back to an in-house IT environment. Whatever the procedure implemented, the CSP must cooperate in good faith with cloud customers, by providing a reasonable solution. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	ROP-1.1	Restriction of processing	1. Explain to cloud customers how the possibility of restricting the processing of personal data is granted; considering that where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	RRD-1.1	Data Retention, Restitution and Deletion policies	1. Describe to cloud customers the CSP's data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-1.2	Data Retention, Restitution and Deletion policies	2. Describe to cloud customers CSP's subcontractors' data retention policies, timelines and conditions for returning personal data or deleting data once the service is terminated. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-2.1	Data Retention	1. Indicate and commit to complying with the time period for which the personal data will or may be retained, or if that is not possible, the criteria used to determine such a period. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	RRD-2.2	Data Retention	2. Take into consideration the following criteria, when defining retention periods: Necessity – Personal data is retained for as long as necessary in order to achieve the purpose for which it was collected, so long as it remains necessary to achieve that purpose (e.g., to perform the services); Legal Obligation – Personal data is retained for as long as necessary in order to comply with an applicable legal obligation of retention (e.g., as defined in applicable labour or tax law), for the period of time defined by that obligation; Opportunity – Personal data is retained for as long as permitted by the applicable law (e.g., processing based on consent, processing for the purpose of establishing, exercising or defending against legal claims – based on applicable statutes of limitations regarding legal claims related to the performance of the services). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-3.1	Data retention for compliance with sector-specific legal requirements	1. Indicate whether and how the cloud customer can request the CSP to comply with specific sector laws and regulations. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	RRD-4.1	Data restitution and/or deletion	1. indicate the procedure for returning to the cloud customers the personal data in a format allowing data portability (see also Controls no. PMT-1.1 to 1.2, above); **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-4.2	Data restitution and/or deletion	2. the methods available or used to delete data; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-4.3	Data restitution and/or deletion	3. whether data may be retained after the cloud customer has deleted (or requested deletion of) the data, or after the termination of the contract; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-4.4	Data restitution and/or deletion	4. the specific reason for retaining the data; **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RRD-4.5	Data restitution and/or deletion	5. the period during which the CSP will retain the data. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	CPC-1.1	Cooperation with the cloud customers	1. Specify how the CSP will cooperate with the cloud customers in order to ensure compliance with applicable data protection provisions, e.g., to enable the customer to effectively guarantee the exercise of data subjects' rights: rights of access, rectification, erasure ('right to be forgotten'), restriction of processing, portability), to manage incidents including forensic analysis in case of security/data breach. See also Controls no. SEC-1.1 to 1.3.xxvii and PDB-1.1 to 1.8, above. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	CPC-1.2	Cooperation with the cloud customers	2. Make available to the cloud customer and the competent supervisory authorities the information necessary to demonstrate compliance (see also Controls no. DCA-1.1 to 1.4, above). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	LRD-1.1	Legally required disclosure	1. Describe the process in place to manage and respond to requests for disclosure of personal data by Law Enforcement Authorities, including to verify the legal grounds upon which such requests are based prior to responding to them, with special attention to the notification procedure to interested customers, unless otherwise prohibited, such as a prohibition under criminal law to preserve confidentiality of a law enforcement investigation. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a
PLA CoC	RMD-1.1	Remedies for customer	1. Indicate what remedies the CSP makes available to the cloud customer in the event the CSP – and/or the CSP's subcontractors (see Controls no. WWP-1.1 to 5.9, above and, more specifically, Controls no. WWP-3.1 to 3.5, above) – breach the obligations under the PLA. Remedies could include service credits for the cloud customer and/or contractual penalties for the CSP. **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a

REQUIREMENTS					Mapping to CSA Cloud Controls Matrix (CCM)				
Source_ document	Req_Id	Req_title	Req_description	Type	Domain	Gap_ level	Details	CCM_ controls	Description
PLA CoC	INS-1.1	CSP insurance policy	1. Describe the scope of the CSP's relevant insurance policy/ies (e.g., data protection compliance-insurance, including coverage for sub-processors that fail to fulfil their data protection obligations and cyber-insurance, including insurance regarding security/data breaches). **[C & P] the requirement is applicable both to the situation in which the CSP is a controller and one in which the CSP is a processor;**	Privacy	n/a	Full gap	n/a	n/a	n/a