CSP CERT
Milestone 1
Security Requirements

Editor(s):	Leire Orue-Echevarria
Status-Version:	Final – v1.3
Date:	14.01.2019
Distribution level (CO, PU):	Public

Editor(s)	Leire Orue-Echevarria
Contributor(s)	Leire Orue-Echevarria (TECNALIA), Antonio Ramos (LEET Security), Aurelien Leteinturier (ANSSI), Bert Tuinsma (Zeker Online), Borja Larrumbide (BBVA), Hans Graux (time.lex), Helmut Fallmann (Fabasoft), James Mulhern (Amazon), Javier Cáceres (European Commission, DIGIT), Jesús Luna (Bosch), Linda Strick (CSA), Mike Edwards (IBM), Oliver Albl (Fabasoft), Patrick Gerte (BSI), Thomas Niessen (Trusted Cloud), Tom Vreeburg, Volkmar Lotz (SAP).
CSPCert Co-chairs	Borja Larrumbide (BBVA), Helmut Fallmann (Fabasoft)
Approved	All drafting members

Abstract:	The aim of this document is threefold. Firstly, it presents the methodology followed by the CSPCERT self-regulatory view to elicit the security objectives that the EU-wide cloud certification scheme should cover. Secondly, it presents the security requirements. Thirdly, it presents the high-level gap analysis between the following schemes: ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ANSSI SecNumCloud, BSI C5, and the ENISA Metaframework for cloud.
Keyword List:	Security requirements, cloud security certification scheme, ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ANSSI SecNumCloud, BSI C5.
Disclaimer	This document reflects only the authors' views and the Commission is not responsible for any use that may be made of the information contained therein

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	24.12.2018	TOC	Leire Orue-Echevarria
V0.2	26.12.2018	Section 1, Methodology (section 2) and contributions from all drafting members related to the security objectives integrated	Leire Orue-Echevarria
V0.3	28.12.2018	High level objectives reviewed and edited of all topics. Edited detailed objectives of information security policies.	Leire Orue-Echevarria
V0.4	31.12.2018	Edited detailed objectives: personnel and training, identity and access management, cryptography and key management	Leire Orue-Echevarria
V0.5	02.01.2019	Edited detailed objectives: asset management, physical infrastructure, communications security, procurement management, incidence management, compliance, security assessment.	Leire Orue-Echevarria
V0.6	03.01.2019	Edited detailed objectives: operational security, systems security and integrity, risk management, change and configuration management. Deleted device management and merged with asset management.	Leire Orue-Echevarria
V0.7	04.01.2019	Merged business continuity and disaster recovery and re-wrote completely the high level objective and the detailed objectives of business continuity. Edited detailed objectives of interoperability and portability. Modified section 2 to align it with the new categories. Deleted device management and merged with asset management.	Leire Orue-Echevarria
V0.8	07.01.2019	Rewritten text related to the categories of the controls in section 2. Incorporated the high level gap analysis as an annex	Leire Orue-Echevarria
V1.0	08.01.2019	Release of the document in the CSPCert Community	Leire Orue-Echevarria
V1.1	09.01.2019	Modified the logo, updated the text in the introduction	Borja Larrumbide

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v1.2	10.01.2019	Final version sent to the drafting members for comments and review	Leire Orue-Echevarria
V1.3	14.01.2019	Included modifications to answer the comments by the drafting members	Leire Orue-Echevarria

Table of Contents

List of Figures

List of Tables

Terms and abbreviations

ANSSI	Agence nationale de la sécurité des systèmes d'information
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Controls Catalogue
CCSM	Cloud Computing Schemes Metaframework
CSP	Cloud Service Provider
CSPCERT	Cloud Service Provider Certification self-regulatory group
EC	European Commission
EU	European Union
HSM	Hardware security module
ISO	International Standardization Organization
PII	Personal Identifiable Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security

1 Introduction

1.1 About this document

The aim of this document is threefold. Firstly, it presents the methodology followed by the CSPCERT self-regulatory view to elicit the security objectives or requirements that an EU-wide cloud security certification scheme should cover. Secondly, it presents the elicited security objectives. Thirdly, it presents the high-level gap analysis between the following schemes: ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ANSSI SecNumCloud, BSI C5, and the ENISA Metaframework schemes for the cloud. The previous standards and certifications were selected based on the objectives of the Cybersecurity act that targets existing European public certifications and the inclusion of ISO as a standard to be used.

1.2 Document structure

The rest of this document is structured as follows:

- Section 2 describes the methodology followed to extract the security objectives, that can also be used for requirements that can arise in the future,
- Section 3 describes the security requirements,
- Annex 1 contains the high-level gap analysis. This is done this way to ensure a better legibility of the document.

2 Methodology

The methodology followed for the definition of the security objectives is detailed below.

The following documents have been used as input sources:

- Study on Certification Schemes for Cloud Computing (SMART 2016 / 0029) [1]
- ISO 27002 [2], 27017 [3], 27018 [4]
- ENISA Cloud Computing Schemes Metaframework (CCSM) [5]
- BSI C5 [6]
- SecNumCloud [7]

First of all, all schemes have been analysed to seek for commonalities and families of controls. In this context, a 'family of controls', namely a domain, is a set of controls focused on a certain aspect, such as network security, operational security, or personnel. For simplification purposes, a family of controls is named as category (labelled as 'EC_Cloudcategory' in the spreadsheet that can be found in Annex 1).

The categories of security objectives are identified are as follows[1]:

1. **Information Security Policies:** ensure the definition of policies related to information security, aligned with the relevant laws, regulations, as well as with the business requirements of the organization. It also includes the definition of the appropriate roles and responsibilities to carry out the implementation of said policies.
2. **Personnel & Training:** Ensure that the employees and contractors are aware and understand their responsibilities towards the information security policies defined and implemented in the organization.
3. **Asset Management:** provide mechanisms for the identification and protection of organizational and information assets, also those coming from customers.
4. **Identity and Access Management:** Put in place the mechanisms to ensure the access to the information, information processing facilities and virtualized environments of only authorized users.
5. **Cryptography and Key management:** Ensure a secure operation of the cloud services with the definition and implementation of the appropriate cryptographic mechanisms.
6. **Physical Infrastructure Security:** Ensure the prevention of unauthorized access to the physical site so as to prevent any damage, loss, failure or theft of any of the business' assets that may hamper the organization's operations.
7. **Operational Security:** Ensure the secure and proper operations of the information security facilities so that the cloud service provider is always operational.
8. **Communications Security:** Ensure the protection of the information in networks, external and internal and in between systems.
9. **Procurement Management:** Define and implement mechanisms to manage the whole supply chain of the cloud service provider and ensure that these procurement activities maintain the appropriate security level.
10. **Incident Management:** Provide the means to manage, react to, and communicate security incidents.
11. **Business Continuity and disaster recovery**: Set out the activities needed to ensure the continuity of the operations of the cloud service recovery, including the disaster recovery ones while ensuring the integrity of the information at all times.
12. **Compliance**: Satisfy the legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

[1] These are the current categories available as of January 4th. However, as per discussions in the group and as result of the open consultation, some of these categories may be merged or change.

13. **Security Assessment:** To establish and maintain appropriate procedures for testing key network and information systems underpinning the cloud services and to establish and maintain appropriate procedures to perform security assessments of critical assets.
14. **Interoperability and Portability**: Provide means that allow customers to interface with other cloud services and/or if needed port to other providers offering similar services in a secure way.
15. **System Security and Integrity**: Put in place the appropriate measures to ensure that the system maintains an adequate level of security and integrity in its entire lifecycle, from development to operation, from internal developments to outsourced ones, using both commercial and open source software.
16. **Change and Configuration Management:** Establish and maintain change management procedures for network and information systems.
17. **Risk Management:** Provide the means to ensure an appropriate governance and risk management framework, as well as mechanisms to identify and address risks for the security of the cloud services

The second step has been the 1:1 matching of the controls of the selected certification schemes (ISO 27002, ISO 27017, ISO 27018, SecNumCloud, BSI C5 with ENISA CCSM as baseline) in each of the categories with the aim of analysing the gap of the existing schemes. It is important to note that while a control could be matched to several categories, this has been placed in the category that was most substantively fulfilled. The starting point for this gap analysis was the study SMART 2016 / 0029 and incremented with ISO 27017, ISO 27018 and SecNumCloud. The complete final mapping can be seen in Annex 1.

	A	B	C	E	G
1	EC-CLOUD CATEGORY	CCSM-ENISA	C5 GERMANY	SecNum FRANCE	ISO 27002
3	Information Security Policies	CCSM-ENISA SO 01 - Information security policy CCSM-ENISA SO 03 - Security roles	C5 OIS-01 Information security management system (ISMS) C5 SA-01 Documentation, communication and provision of policies and instructions C5 SA-02 Review and approval of policies and instructions C5 SA-03 Deviations from existing policies and instructions C5 OIS-03 Authorities and responsibilities s in the framework of information security C5 OIS-04 Separation of functions C5 OIS-05 Contact with relevant government agencies and interest groups C5 OIS-06 Policy for the organization of the risk management C5 OIS-02 Strategic targets regarding information security and responsibility of the top management C5 OIS-07 Identification, analysis, assessment and handling of risks	SecNum 5.1. Principles SecNum 5.2. Information security policy **SecNum 6.1. Functions and responsibilities linked to information security** **SecNum 6.2. Segregation of tasks** SecNum 6.3. Relations with the authorities SecNum 6.4. Relations with specialised work groups SecNum 6.5. Information security in project management HYG33: Adopt security policies dedicated to mobile devices	ISO 27002: 5.1.1 A set of policies for informat defined, approved by management, published employees and relevant external parties. ISO 27002: 5.1.2 The policies for information review at planned intervals or if significant cha their continuing suitability, adequacy and effec ISO 27002: 6.1.1 All information security resp defined and allocated. ISO 27002: 6.1.2 Conflicting duties and areas should be segregated to reduce opportunities unintentional modification or misuse of the org ISO 27002: 6.1.3 Appropriate contacts with r should be maintained. ISO 27002: 6.1.4 Appropriate contacts with s or other specialist security forums and profess should be maintained. ISO 27002: 6.1.5 Information security should project management, regardless of the type o ISO 27002: 6.2.1 A policy and supporting sec

Figure 1. High level gap analysis (mapping) – Excerpt.

The third step is the derivation of the security objectives that the EU-wide security certification scheme should cover. To this end, based on the gap analysis performed in the previous step, an in-depth analysis has been carried out and the security objectives have been extracted. The document distinguishes between high-level and detailed objectives. While the high-level is the overarching goal of the objective, the detailed objectives present more information of the different aspects that need to be fulfilled.

New security objectives can come into place as the technology progresses or as new sectors decide to include their own requirements in the EU-wide certification scheme. To this end, the current design allows for that. The process would be similar: identify under which category or categories the objective would fit in and define it.

In addition, current objectives may change. While for the time being, the version number of the objectives is not kept, this could be a field that could be added.

3 Security objectives

3.1 Information Security Policies

3.1.1 High level security objective

The Cloud Service Provider (CSP) must define, institutionalize and communicate, to internal and external stakeholders, the security policies, which must be approved by the top management. Roles and responsibilities related to such security policies must also be defined, assigned and communicated, also to internal and external stakeholders.

3.1.2 Detailed security objectives

ISP.1: The CSP must define and implement its information security policies. A well-defined information security policy shall include, among other aspects, baseline information security objectives, how these will be enforced, measured and its correctness evaluated so that appropriate corrective actions can be applied, threats as well as the policy sources (e.g. regulations, legislation, corporate strategy).

ISP.2: The CSP must complement the baseline information security policies with procedures related, among others, to the provisioning and usage of the cloud service, isolation, multi-tenancy, access rights, lifecycle management of a cloud service offering, lifecycle management of an account of a cloud service customer, compliance with applicable PII protection legislation, contractual agreements

ISP.3: The CSP must communicate all information security policies to both its internal and external stakeholders (e.g. cloud service customer).

ISP.4: The CSP must define, document and assign roles and responsibilities in the security policy, both at the cloud service provider's side and at the cloud customer's side, taking into consideration that:

a) The separation of roles and responsibilities must be ensured, so that operational and controlling functions are not performed by the same person at the same time. In the case it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be put in place.
b) Responsibilities for the protection of individual assets, for activities related to risk management and more specifically for the acceptance of residual risks, as well as for the implementation of certain security processes must be identified and defined.
c) No one can access, modify or use any asset without the proper authorization.
d) The cloud service customer data and applications custodied by the CSP must be considered for the allocation of roles and responsibilities.
e) Authorization levels must be identified and documented.

ISP.5: The CSP must communicate to all stakeholders, internal and external, any change occurred related to roles, responsibilities or contractual issues.

ISP.6: The CSP must document and implement the procedures that will have to be followed to report the corresponding authorities in a timely manner whenever a security incident has occurred.

ISP.7: The CSP must specify a point of contact regarding the processing of PII.

ISP.8: The CSP should maintain appropriate contacts with special interest groups, security fora, professional associations in order to improve the cooperation and coordination of security related aspects.

3.2 Personnel & Training

3.2.1 High level security objective

The CSP must ensure that employees and contractors are aware of, understand, and fulfil the information security responsibilities in the role for which they are considered, with the aim of protecting the organization's interests.

3.2.2 Detailed security objectives

PT.1: Prior to the employment contract, the cloud service provider must screen the background of the employee following a defined screening process and in accordance to the applicable laws and regulations. The background checks should be proportional to the business context, the sensitivity of the information that will be accessed by the employee and the associated risks.

PT.2: The contracts between employees and the CSP must state their role and responsibilities regarding the information security. Furthermore, the organization's policies in security matters such as access, confidentiality, ethics, management of the information and so on should be stated on the contract. A document containing the rules of behaviour with respect to how to deal with the information and data of the customers should be provided.

PT.3: The CSP as well as its external contractors and suppliers must make mandatory and available to all its employees a training programme in security such as information security in general (e.g. how to handle cloud data, threats, secure operation and management of data and information) and in security requirements. This training programme is to be tailored to the role and responsibility of each employee. Awareness raising campaigns and activities shall be launched as complement to the training programme.

PT.4: All CSPs employees and contractors must attend to the information security principles defined in accordance to the organization's policies and processes. This shall also be abided and monitored by the management.

PT.5: the CSP must have a disciplinary process define and communicated. This process shall be put in place against employees who have committed an information security breach.

PT.6; The CSP must inform internal and external employees that the security responsibilities and requirements remain valid even if there is a contract termination or a change in the role. The terminated employee will also be informed with the need to comply with the relevant legislation, regulations regarding information security whenever this situation occurs.

3.3 Asset[2] Management

3.3.1 High level security objective

The CSP keeps and achieves appropriate protection of all organizational and information assets, including those originating from the customers.

[2] In ISO 27000:2009 asset was defined as "anything that has value to the organization", including: a) information (2.18); b) software, such as a computer program; c) physical, such as computer; d) services; e) people, and their qualifications, skills, and experience; and f) intangibles, such as reputation and image.

In ISO 27000:2014 the definition of asset was removed from the standard but still, the term "asset" is used, but mostly in the sense of an "information asset".

In 2014, ISO published "ISO 55000:2014 - Asset management — Overview, principles and terminology" where asset is defined as "item, thing or entity that has potential or actual value to an organization". (Note 1 to entry: Value can

3.3.2 Detailed security objectives

AM.1: The CSP must define, establish, manage and update an inventory of assets associated with information and which are necessary for information processing.

AM.2: The CSP must assign roles and responsibilities for the ownership of the assets.

AM.3: The CSP must define, document, implement, put in place and monitor the rules to handle assets, including bringing in and returning assets by customers.

AM.4: The CSP must establish and maintain a classification of the information assets along with an appropriate labelling and handling mechanisms.

AM.5: The CSP must define, document, implement, and monitor procedures for the secure handling, transfer and disposal of media of any kind.

AM.6: The CSP must define, document, implement, and monitor procedures for the secure handling of physical assets of a customer (e.g. hard drives, hardware security module (HSM)). These procedures must be communicated to the customer.

3.4 Identity and Access Management

3.4.1 High level security objective

The CSP must secure the authorization and authentication of its own users as well as those coming from the cloud service customer in order to prevent unauthorized access and mitigate cyber security risks derived from the use of virtual environments.

3.4.2 Detailed security objectives

IAM.1: The CSP must restrict access both to the stored information and to the facilities where the information is located. To this end, an access control policy shall be defined, documented and implemented aligned with the organization's information security requirements.

IAM.2: The CSP must define, document and implement a user access management procedure, which shall include, among other aspects, a policy for providing and revoking permissions and privileges, a definition of the different access levels to read, write and delete information, policies to safeguard the non-disclosure of authentication and other sensitive information, and regular reviews.

IAM.3: The CSP must define and communicate to the whole organization the practices that must be followed in relation to the use of secret authentication information[3].

IAM.4: The CSP must define, document, implement, monitor and manage mechanisms such as multi-factor authentication, to prevent unauthorized access to virtualized environments, information systems, data and applications.

---

be tangible or intangible, financial or non-financial, and includes consideration of risks (3.1.21) and liabilities. It can be positive or negative at different stages of the asset life (3.2.2).

Note 2 to entry: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation or agreements.

Note 3 to entry: A grouping of assets referred to as an asset system (3.2.5) could also be considered as an asset.)

[3] Secret information: passwords, single sign-on procedures (SSO)

IAM.5: The CSP must define, document, implement, monitor and manage mechanisms to protect the separation of concerns in virtual environments, including customer data, applications, storage among others. This separation of concerns must include on one hand, the resources used by the cloud service customers through the CSP's offerings, and on the other hand, the administrative infrastructure that the CSP needs to run its business, which shall not be in contact with the customers' used and offered resources.

3.5 Cryptography and Key management

3.5.1 High level security objective

The CSP must define, select, dimension and implement appropriate cryptographic mechanisms supported by an adequate key management infrastructure, in order to ensure a secure operation of its cloud services.

The use of cryptography should be mandatory for the CSP in order to ensure the security of information (confidentiality, authenticity and integrity). That concerns data at rest as well as data flows.

3.5.2 Detailed security objectives

CKM.1: the CSP must define, implement and use appropriate cryptographic and protocol standards in order to provide efficient robustness against threats like crypto analysis. This implies that:

i) Proper authentication protocol and mechanisms must be implemented for entities and user request access to or transacting with cloud's equipment and resources.
ii) When appropriate or required by regulation, proper digital signature mechanisms must be used in order to ensure authenticity of electronic assets or transactions.

CKM.2: The CSP must protect properly with appropriate cryptographic mechanisms and protocols all data flows that are exposed to public networks or other customers.

CKM.3: The CSP must protect with appropriate cryptographic mechanisms the cloud customer's and sensitive data, which could be exposed during maintenance, transport, reallocation or disposal of media or equipment. As an example, only the hash values of the passwords of the users and of technical accounts should be stored.

CKM.4: All cryptographic mechanisms operated by the CSP shall be supported by a proper key management infrastructure and key management policy.

3.6 Physical Infrastructure Security

3.6.1 High level security objective

The CSP must provide means to prevent unauthorized access to its physical site as well as protection against theft, damage, loss and failure of assets in order to ensure a continuous operation.

3.6.2 Detailed security objectives

PI.1: The CSP must put in place physical perimeter protection in defined public, private and sensitive areas.

PI.2: The CSP must limit the access to private and sensitive areas only to authorized personnel.

PI.3: The CSP must maintain the needed infrastructure and devices to ensure the availability and the integrity of the information.

PI.4: The CSP must define and put in place the measures needed to protect the infrastructure from outside and environmental threats, and against the disruption of base services such as electric power.

3.7 Operational Security

3.7.1 High level security objective

The CSP must manage, define, document, implement, monitor and evaluate procedures related to its operation such as different environments needed, capacities, resources, information, data, protection of facilities, (user and system) activities, safeguards, incidents, failures, among others.

3.7.2 Detailed security objectives

OS.1: The CSP must define, document, communicate and distribute all operation procedures and the associated roles and responsibilities in a written form to all users and stakeholders that need to make use of them.

OS.2: The CSP must define, implement and maintain a segregation of environments (e.g. development, testing and operation) in order to diminish the risk of unauthorized access as well as changes that can occur to the environment in production. To this end, the following aspects should be planned and implemented: procedures and conditions to transfer software from one environment to the others (e.g. when a software is promoted to production environment and under which criterion, how testing is performed in each of the environments, roles and permissions of the users for all environments, and so on).

OS.3: The CSP must plan and control capacities and resources (personnel and cloud resources). The planning shall include forecasts to avoid, for instance, bottlenecks, overloads and other restrictions to be able to comply always with the agreed service level agreements (SLAs). For the monitoring aspect, safeguards shall be implemented that shall control that the provision of cloud resources is ensured under the agreed contractual agreements.

OS.4: The CSP must ensure that the information, data as well as the information facilities are protected against malware and malicious code. For that, the defined procedures should include the implementation of controls for malware prevention and detection, installation of patches, user awareness activities, regular reports that could be audited anytime, authorization levels to the different data and information hosted, and protective measures for data coming from external sources, among others.

OS.5: The CSP must plan, implement and test a backup procedure in agreement with a backup policy to ensure that no information is lost and that it can be restored at any time. The backup policy should define the retention and protection requirements as well as other aspects such as frequency of backups, location of where they are being performed, extent (incremental or full), restoration procedure, and access authorization.

OS.6: The CSP must record user activities, system activities, failures, information security events, files accessed, user privileges, alarms raised, among other aspects, in logging facilities of the CSP. The log information stored shall be protected from manipulation and unauthorized access. In order to ensure the synchronization of all these items, the CSP will have the clock synchronized to a single reference time source. The timestamp of this clock shall be visible in the log files so as to be able to correlate and analyse the different occurred events.

OS.7: The CSP must define, document, implement and control a process to manage vulnerabilities. To this end, specific information such as the assets of the company, the software

provider, their versions, the deployment status of the software, responsible people, and the risks among other should be recorded in different sources, namely logs.

OS.8 In order to maximize business continuity and therefore minimize disruptions, audit activities related to the evaluation of operational systems must be planned. The scope of the tests and the time in which they will be carried out need to be established and agreed. As a recommendation, they could be performed outside business hours.

3.8 Communications Security

3.8.1 High level security objective

The CSP must ensure an appropriate protection of communications in the networks, internal and external, and in between systems processing information.

3.8.2 Detailed security objectives

CS.1: The CSP must segregate the communications. The different parts of the network must be partitioned according to:

- the sensitivity of the information sent;
- the nature of the data flows (production, administration, supervision, etc.);
- the area that the data flows belong to (clients – with a distinction per client or set of clients, the service provider, third parties, etc.);
- the technical area (processing, storage, etc.);

in order to be able to apply the appropriate security measures on each partition.

CS.2: The CSP must define, document and regularly update and maintain a map of the information system and the network.

CS.3: The CSP must segregate the administration network from other networks (e.g. customers).

CS.4: The CSP must define, document, implement and monitor mechanisms, such as state of the art cryptographic standards (SSL/TLS) and their countermeasures, to protect the communication flows from and to the cloud infrastructure, between infrastructures, as well as between customers and infrastructures.

CS.5: The CSP must monitor, according to the regulations (e.g. like lawful interception) the communication flows within the cloud, internal and external, to respond appropriately and timely to threats.

3.9 Procurement Management (Supply chain management)

3.9.1 High level security objective

The CSP must establish, implement and maintain security procedures, policies and associated security requirements to manage its suppliers, in order to ensure that such procurement and outsource do not affect the security level of the cloud services. The CSP must ensure that these policies are also kept in its supply chain.

3.9.2 Detailed security objectives

PM.1: The CSPs must define, implement and maintain a procurement management procedure that defines the principles that ensure that security is part of the procurement process, including outsourced development and supporting utilities.

PM.2: The CSP must define, implement and maintain the mechanisms to ensure that security requirements for every third party that could affect the cloud service are put in place, according to the potential level of impact in the confidentiality, integrity and availability of the cloud service.

PM.3: The CSP must define, implement and maintain a procedure to identify third parties, to evaluate the impact / risk in the cloud service, and to supervise / monitor the implementation of the security requirements by the third parties.

PM.4: The CSPs must ensure that third parties also apply security controls to meet the applicable security requirements in their providers (fourth parties).

PM.5: The CSPs must define and implement a notification mechanism to ensure that information security incidents at their providers are considered also in their incident management procedure.

3.10 Incident Management

3.10.1 High level security objective

The CSP must define and implement an approach that manages information security incidents. This approach shall include, among other aspects, procedures, roles, responsibilities, communication mechanisms through the appropriate channels to the relevant stakeholders in a timely manner, evidence collection mechanisms and classification, and lessons learned.

3.10.2 Detailed security objectives

IM.1: The CSP must define and implement the responsibilities for incidence management.

IM.2: The CSP must define, document, implement, monitor and communicate a procedure to be able to respond to that information security incidents in a fast, efficient and orderly manner. This procedure shall include, among other aspects, incident planning and preparation, monitoring and logging of that information security incidents, handling of that information security incidents, and response management (e.g. escalation).

IM.3: The CSP must report information security events to the established stakeholders (e.g. CERTS) through the appropriate management channels as quickly as possible and in agreement with the documented procedures.

IM.4.: The CSP must define, document and implement the mechanisms to classify information security incidents and assess if an incident is to be qualified as an information security one.

IM.5: The employees and contractors using the organization’s information systems and services of a CSP must be required to note and report any observed or suspected information security weaknesses in services or systems.

IM.6: The CSP must define, document, implement and maintain a procedure for the collection, acquisition and preservation of information related to the information security incidents, which can serve as evidence.

IM.7: The CSP must collect, preserve and keep in an internal public repository the knowledge gained from analysing and resolving information security incidents, with the aim of reducing the likelihood or impact of future that information security incidents.

3.11 Business Continuity and disaster recovery

3.11.1 High level security objective

The CSP must define, implement and maintain plans for business continuity and disaster recover to ensure that the cloud service is always available but with the highest integrity.

3.11.2 Detailed security objectives

BC.1: The CSP must define, document and communicate all information security requirements, potential problematic situations (e.g. malfunctions), threats, metrics and their acceptable thresholds for those services not working properly (e.g. recovery time objective, mean time between failures, mean time to recover).

BC.2: the CSP must define, document, implement and monitor a business continuity plan, including contingency plans and recovery activities. This plan shall include issues such as the information security controls within business continuity and recover processes, compensation controls, steps on how to restore a cloud service, as well as prioritized list of the services to restore, roles and responsibilities, in order to ensure that the required degree of continuity of the cloud service is ensured at all times.

BC.3: The CSP must ensure the validity and effectiveness of its business continuity and recovery plans by executing drills and tests at regular intervals. The results of such drills and tests must be documented, and the plans updated accordingly.

BC.4: The CSP must ensure the availability of its services through the implementation of redundancy mechanisms (e.g. in components, in the architecture, …). The risks related to redundancy that can cause integrity and confidentiality issues must be considered.

3.12 Compliance

3.12.1 High level security objective

The CSP must ensure and provide the means to assure compliance with the applicable regulations, legislation as well as contractual and business requirements.

3.12.2 Detailed security objectives

C.1: The CSP must achieve a clear understanding of the applicable legal and contractual security requirements that it needs to comply with.

C.2: The CSP must safeguard the conformity with legal requirements such as Intellectual Property Rights, use of cryptographic controls and privacy requirements.

C.3: The CSP must ensure that its contract is aligned with legal and business requirements.

C.4: The CSP must ensure that its records are protected from destruction, forgery, non-authorized access or publications in agreement with the legislative, regulatory, contractual and business requirements in place.

C.5: The CSP must ensure that information security is managed and operated in agreement with the policies and procedures defined in the organization.

3.13 Security Assessment

3.13.1 High level security objective

The CSP must establish and maintain procedures to review the information security at planned intervals or when significant changes occur, and results are reported to the appropriate management levels and clients (where suitable). The review is conducted by qualified personnel (e. g. internal revision) of the cloud provider or expert third parties commissioned by the cloud provider.

3.13.2 Detailed security objectives

SA.1: The CSP must define, document, implement, monitor and maintain procedures to test the network and the information systems underpinning the cloud services.

SA.2: The top management of a CSP must be notified of regular compliance reviews.

SA.3: The CSP must conduct internal audits as well as independent reviews performed of IT systems and processes, including virtualized environments, networks and so on, to ensure the compliance with the organization's policies and standards (including technical compliance examination).

3.14 Interoperability and Portability[4]

3.14.1 High level security objective

The CSP must use standards and implement practices which allow customers to interface with other cloud services. The Cloud provider shall also implement practices that enable customers, if needed, to recover their data and migrate to other providers offering similar services.

3.14.2 Detailed security objectives

IP.1: The CSP must make available Information about APIs and formats to support interoperability and porting.

IP.2: The CSP must make available mechanisms for customers to be able to retrieve their data in a machine-readable format at the end of the contract.

IP.3: The CSP must define and implement procedures to facilitate the data transfer. These shall also be agreed with the customer of the cloud service.

IP.4: The CSP must make available measures to protect the porting of customer data and applications. This includes the use network controls to protect the information and the integrity of the network.

3.15 System Security and Integrity

This section aims at the definition of security objectives that ensure that best practices to achieve and maintain an adequate security level of software and systems and that these are systematically applied during development and deployment by the cloud service provider. The scope includes both software development conducted by the cloud service provider itself and the use and deployment of third party components including open source as well as – most common in practice – any blend of concepts in-between those.

[4] The objectives presented here are to be complementary to the Code of Conducts defined for IaaS and SaaS in the SWItching and POrtability self-regulatory group (SWIPO). Please refer to the Code of Conduct defined for IaaS and SaaS for more information.

In essence, the requirements defined here require the cloud provider to establish a secure development lifecycle, i.e. a set of principles and processes that ensure that security is considered to be an integral element during design and development and not brought in after-the-fact.

The objectives acknowledge the agility and speed of cloud development, deployment and operation ("DevOps"), the distributed nature of the software supply chain including open source libraries, as well as the varying nature of security contexts, e.g., the same microservice possibly used in different applications.

This section further acknowledges the need for integrating security into the lifecycle of a product or a service, leading to a focus on the processes applied during their lifecycle. In addition, this focus on the secure development and deployment life cycle facilitates the scalability of the approach by allowing to evaluate the processes themselves and their enforcement in a development project rather than the evaluation of the individual product characteristics. By doing so, for instance, a regular update of a software service can be evaluated (and certified) faster if the same processes have been applied. In turn, this leads to requirements on security functions of systems not being stated in this section but in related other sections of this document.

3.15.1 High level security objective

The CSP must manage, define, implement, and monitor the processes needed for the design, development and deployment[5] of all used software artefacts, software systems as well as their connectivity, necessary to provide the cloud service. Such processes shall cover the complete system lifecycle, from design to operation, including updates and patches, and both internal (from the CSP itself) and external (from outsourced parties, including third party components and open source software) developments.

[5] Example process elements for a secure development lifecycle as required by the detailed control objective include, for example:

- system/product/service description including the relevant security context and environment
- threat model and risk assessment following an established threat modelling approach
- statement of security objectives based on the threat and risk analysis
- statement of security functionality
- mapping between security objectives and security functionality
- state-of-the-art security analysis and testing of code (SAST, DAST, penetration testing), i.e., use of best-in-class tools and techniques and their combination
- security analysis of 3rd party components including open source, use of certified components
- secure deployment, integrity protection of software artefacts
- security response processes and patch processes

3rd party components also include applications of software providers that are deployed on a platform or infrastructure cloud offering. The cloud provider is required to perform a security analysis/risk assessment as part of a vetting/on boarding process for such deployments. The security analysis focuses on both legal compliance and also on the potential impact of the application's security characteristics (or lack thereof) on the infrastructure, platform or other tenants, respectively.

Regarding their own development efforts, organisations that are compliant with ISO 27034 are expected to meet many of the requirements of this section, having installed an Organization Normative Framework, providing an Organization ASC (Application Security Control) Library and having established process elements covering the assessment of the application security risk and the selection of ASCs to achieve a desired Level of Trust.

3.15.2 Detailed security objectives

SSI.1: The CSP must define, document, execute and control processes that ensure the security of software artefacts and software systems as well as their connectivity used to implement the cloud service. This includes:

- Process controls to ensure the correct and effective implementation of technical security measures (security functions) required in other sections of this document,
- The establishment of a secure development lifecycle for the cloud provider's own software and system developments.

For own developments of the cloud service provider, the secure development lifecycle shall include controls that:

1. allow the assessment of the security risk associated with each development effort,
2. facilitate the instantiation of the lifecycle process controls following the risk assessment and providing adequate security,
3. produce evidence for the control selection and the application of each selected control during the development effort,
4. include secure delivery and deployment processes maintaining system integrity
5. cover secure system update and patching, ensuring the timely application of security patches to fix known vulnerabilities,
6. include a security response process that manages the identification, reporting and fixing of vulnerabilities,
7. each control of the secure development lifecycle is required to include validation elements that produce and check evidence for their application. The application and execution of the controls is regularly checked based on the documents and artefacts produced by the processes.
8.

For the usage of 3rd party components and technical services, including open source software contributions, the secure development lifecycle shall include controls that:

1. define a vetting or on boarding process for 3rd party components, including security requirements following a risk assessment of the component and its environment,
2. include secure delivery and deployment processes maintaining system integrity,
3. include automated process for regular analysis of vulnerabilities of 3rd party components as well as the mitigation of such vulnerabilities,
4. each control of the secure development lifecycle is required to include validation elements that produce and check evidence for their application. The application and execution of the controls is regularly checked based on the documents and artefacts produced by the processes.

3.16 Change & Configuration Management

3.16.1 High level security objective

The CSP must define, document, implement, manage and monitor a process that controls the changes to the organization, business and development processes, software assets and information processing that can affect the information security.

3.16.2 Detailed security objectives

CCM.1: The CSP must define, implement and monitor a change and configuration management process that safeguards the changes performed to all information systems required for the development, deployment and operation of a cloud service.

CCM.2: the CSP must define, implement and maintain a classification and a prioritization scale of changes.

CCM.3: The CSP must define, implement and maintain a strategy to test the performed changes in the integration (development) environment, before they are promoted to the production one.

CCM.4: The CSP must define, implement and maintain a risk assessment procedure that allows to analyse the impact of such change.

CCM.5: The CSP must implement mechanisms to record the performed changes, including reasons for the change, date, responsible, among other aspects, so as to ease the auditing procedures.

CCM.6: The CSP must define, implement and maintain a procedure to return to the situation previous to the performed change.

CCM.7: The CSP must define and implement a change approval process.

CCM.8: The CSP must define and implement a process to communicate all changes to the relevant stakeholders.

3.17 Risk Management

3.17.1 High level security objective

The CSP must define, establish, implement and maintain a governance and risk management process, covering the entire lifecycle of the provision of a cloud service.

3.17.2 Detailed security objectives

RM.1: The CSP must define, document and implement a risk management policy that covers the entire cloud service provision (including, where technically feasible, the whole cloud supply chain and underlying IaaS/PaaS/SaaS), as well as the whole cloud service life cycle.

RM.2: The CSP must periodically carry out its risk assessment by using a documented method that guarantees reproducibility and comparability of the approach.

RM.3: The CSP provider must take into account in the risk assessment:

- the cloud service customer's data classification/criticality;
- the current security posture provided by the implemented technical and organizational controls.
- Contextual information related to the cloud service, which may have effects on its attack surface (e.g., internet connectivity)

RM.4: The CSP must also consider other source of risks such as the ones derived from assessing threats to the organization associated with PII. For this purpose, it is recommended taking into account the organization's overall business strategy and objectives.

RM.5: When there are specific legal, regulatory or sector-specific requirements linked to the type of information entrusted by the cloud service customer to the cloud service provider, the latter must consider them for its risk assessment.

RM.6: The CSP must categorized the identified risks according to their criticality, and treated accordingly (e.g., by mitigating the risk through the implementation of the corresponding security controls, by transferring the risks, or by accepting the risk)

RM7: The risk owner of the CSP must formally accept the residual risks identified in the risk assessment, which were not feasible to mitigate in the risk treatment stage. However, it is not valid the acceptance of risks associated to requirements defined in this document and which were not implemented by the cloud service provider.

RM8: The CSP must update the risk assessment either given a defined frequency, or whenever there are significant changes affecting the security posture of the cloud service.

4 References

[1] L. Orue-Echevarria, C. Cortés, M. Álvarez, B. Sánchez and A. Ayerbe, “Certification Schemes for Cloud Computing,” EU Publications Office, 2018.

[2] ISO/IEC, “ISO /IEC 27002: 2013 - Information technology - Security techniques - Code of practice for information security management”.

[3] ISO / IEC, “ISO/IEC 27017: 2015 - Code of practice for information security controls based on ISO/IEC 27002 for cloud services”.

[4] ISO / IEC, “ISO / IEC 27018: 2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors”.

[5] ENISA, “Cloud Certification Schemes Metaframework,” 2014. [Online]. Available: https://resilience.enisa.europa.eu/cloud-computing-certification/cloud-certification-schemes-metaframework. [Accessed October 2018].

[6] BSI - German Federal Office for Information Security;, “Compliance Controls Catalogue (C5),” 2017. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.pdf;jsessionid=0A26465CAC7891AC14E23B835AB952BC.2_cid369?__blob=publicationFile&v=3.

[7] ANSSI, “Extract from Cloud IT service providers (SecNumCloud) – Requirements Reference Document – Essential level. Version 3.0,” 2017.

[8] Drafting Members of the CSPCert Group, “High Level Gap Analysis,” 2018. [Online]. Available: https://docs.google.com/spreadsheets/d/13dRIkcD7SlJ3FEPal7aLo0vHj8stlBQE82n_IJXXjpA/edit?usp=drive_web&ouid=116245655391871637992. [Accessed October 2018].

Annex 1 - High level Gap Analysis

This annex presents the current version of the high level gap analysis.

Table 1. High level Gap Analysis

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
Information Security Policies	CCSM-ENISA SO 01 - Information security policy CCSM-ENISA SO 03 - Security roles	C5 OIS-01 Information security management system (ISMS) C5 SA-01 Documentation, communication and provision of policies and instructions C5 SA-02 Review and approval of policies and instructions C5 SA-03 Deviations from existing policies and instructions C5 OIS-03 Authorities and responsibilities s in the framework of information security C5 OIS-04 Separation of functions C5 OIS-05 Contact with relevant government agencies and interest groups C5 OIS-06 Policy for the	SecNum 5.1. Principles SecNum 5.2. Information security policy SecNum 6.1. Functions and responsibilities linked to information security SecNum 6.2. Segregation of tasks SecNum 6.3. Relations with the authorities SecNum 6.4. Relations with specialised work groups SecNum 6.5. Information security in project management HYG33: Adopt security policies dedicated to mobile devices	ISO 27002: 5.1.1 A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties. ISO 27002: 5.1.2 The policies for information security should be review at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. ISO 27002: 6.1.1 All information security responsibilities should be defined and allocated. ISO 27002: 6.1.2 Conflicting duties and areas of responsibility should be segregated to	ISO 27017: CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment	ISO 27018: 5.1.1 A statement to achieving compliance with applicable PII protection legislation and the contractual terms. ISO 27018: 6.1.1 The public cloud PII processor should designate a point of contact regarding the processing of PII under the contract. ISO 27018 A.9.2 Retention period for administrative security policies and guidelines

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		organization of the risk management C5 OIS-02 Strategic targets regarding information security and responsibility of the top management C5 OIS-07 Identification, analysis, assessment and handling of risks		reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets ISO 27002: 6.1.3 Appropriate contacts with relevant authorities should be maintained. ISO 27002: 6.1.4 Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained. ISO 27002: 6.1.5 Information security should be addressed in project management, regardless of the type of the project. ISO 27002: 6.2.1 A policy and supporting security		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				measures should be adopted to manage the risks introduced by using mobile devices. ISO 27002: 6.2.2 A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.		
Personnel & Training	CCSM-ENISA SO 05 - Background checks CCSM-ENISA SO 06 - Security knowledge and training CCSM-ENISA SO 07 - Personnel changes	C5 HR-01 Security check of the background information C5 HR-02 Employment agreements C5 HR-03 Security training and awareness-raising programme C5 HR-04 Disciplinary measures C5 HR-05 Termination of the employment	SecNum 7.1. Selection of candidates SecNum 7.2. Conditions for hire SecNum 7.3. Awareness, learning and training on information security SecNum 7.4. Disciplinary process SecNum 7.5. Rupture, term or modification in the labour contract HYG1 Train the	ISO 27002: 7.1.1 Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be		ISO 27018: 7.2.2 Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor. ISO 27018: A.10.1 Confidentiality or

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		relationship or changes to the responsibilities	operational Team in Information System Security (which include not only technical but organizational and regulatory training) HYG2 Raise user awareness about basic information security (this target the end user on a system, here it shall be interpreted as an user of the Cloud Service offered) HYG24 Protect your professional email (beside technical protection, this rules emphasis on user awareness for the use of his email, which is more a matter of training) HYG39 Designate a point of contact in information system security and make	accessed and the perceived risks. ISO 27002: 7.1.2 The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security. ISO 27002: 7.2.1 Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. ISO 27002: 7.2.2 All employees of the organization and, where relevant, contractors should receive appropriate awareness		non-disclosure agreements

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			sure staff are aware of him or her	education and training and regular updates in organizational policies and procedures, as relevant for their job function. ISO 27002: 7.2.3 There should be a formal and communicated disciplinary process in place to take action against employees who have committed and information security breach. ISO 27002: 7.3.1 Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				employee or contractor and enforced.		
Asset Management	CCSM-ENISA SO 14 - Asset management	C5 AM-01 Asset inventory C5 AM-02 Assignment of persons responsible for assets C5 AM-03 Instruction manuals for assets C5 AM-04 Handing in and returning assets C5 AM-05 Classification of information C5 AM-06 Labelling of information and handling of assets C5 AM-07 Management of data media C5 AM-08 Transfer and removal of assets	SecNum 8.1. Inventory and property of assets SecNum 8.2. Restitution of assets SecNum 8.3. Identification of the information security needs SecNum 8.4. Marking and manipulating information SecNum 8.5. Management of removable media HYG4: Identify the most sensitive assets and maintain a network diagram (this diagram is a simple one, helping to locate where sensitive assets are localized)	ISO 27002: 8.1.1 Information, other assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained. ISO 27002: 8.1.2 Assets maintained in the inventory should be owned. ISO 27002: 8.1.3 Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented	ISO 27017: CLD.8.1.5 Removal of cloud service customer assets	ISO 27018: 8; Reference to ISO 27002, Section 8 ISO 27018: Annex 9.3: PII return, transfer and disposal

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				and implemented. ISO 27002: 8.1.4 All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement. ISO 27002: 8.2.1 Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. ISO 27002: 8.2.2 An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				classification scheme adopted by the organization. ISO 27002: 8.2.3 Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by the organization. ISO 27002: 8.3.1 Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by the organization. ISO 27002: 8.3.2 Media should be disposed of securely when no longer		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				required, using formal procedures. ISO 27002: 8.3.3 Media containing information should be protected against unauthorized access, misuse or corruption during transportation.		
Identity & Access Management	CCSM-ENISA SO 10 - Access control to network and information systems	C5 IDM-01 Policy for system and data access authorisations C5 IDM-02 User registration C5 IDM-03 Granting and change (provisioning) of data access authorisations C5 IDM-09 Handling of emergency users C5 IDM-07 Non-disclosure of authentication information	SecNum 9.1. Policies and access control SecNum 9.2. Registering and deregistering users SecNum 9.3. Management of access rights SecNum 9.4. Review of user access rights SecNum 9.5. Management of user authentications SecNum 9.6. Access to administration interfaces SecNum 9.7. Restriction of access to information HYG5: have an exhaustive	ISO 27002: 9.1.1 An access control policy should be established, documented and reviewed based on business and information security requirements. ISO 27002: 9.1.2 Users should only be provided with access to the network and network services that they have been specifically authorized to use.	ISO 27017: CLD.9.5.1 Segregation in virtual computing environments ISO 27017: CLD.9.5.2 Virtual Machine Hardening	ISO 27018: 9.2 Public cloud PII processor should enable the cloud service customer to manage access by cloud service users under the cloud service customer's control ISO 2018: 9.2.1 Procedures for user registration and de-registration should address the

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		C5 IDM-06 Administrator authorisations C5 IDM-05 Regular review of data access authorisations C5 IDM-04 Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship C5 IDM-08 Secure login methods C5 IDM-10 System-side access control C5 IDM-11 Password requirements and validation parameters C5 IDM-12 Restriction and control of administrative software C5 IDM-13 Control of access to source code	inventory of privileged account and keep it updated (not only administrator but include user with extended privileges) HYG8: Identify each individual accessing the system by name and distinguish the user/administrator role (this control applies to both end user and personnel. It shall be further refined between these two categories) HYG9: Allows the appropriate rights to the information system's sensitive resources. HYG29: Reduce administration rights on workstations to strictly operational needs	ISO 27002: 9.2.1 A formal registration and de-registration process should be implemented to enable assignment of access rights. ISO 27002: 9.2.2 A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services. ISO 27002: 9.2.3 The allocation and use of privileged access rights should be restricted and controlled. ISO 27002: 9.2.4 The allocation of secret authentication information should be controlled through a formal management		situation where user access control is compromised ISO 2018: 9.4.2 Public cloud PII processor should provide secure log-on procedures ISO 27018:Annex A.10.8 Unique Use of User IDs ISO 27018: Annex A.10.9 Records of Authorized Users ISO 27018: Annex A.10.10 User ID Management ISO 27018: A.10.13 Access to data on pre-used data storage space

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				process. ISO 27002: 9.2.5 Asset owners should review users' access rights at regular intervals. ISO 27002: 9.2.6 The access rights of all employees and external party users to information and information processing facilitating should be removed upon termination of their employment, contract or agreement, or adjusted upon change. ISO 27002: 9.3.1 Users should be required to follow the organization's practices in the use of secret authentication information. ISO 27002: 9.4.1 Access to information and		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				application system functions should be restricted in accordance with the access control policy. ISO 27002: 9.4.2 Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure. ISO 27002: 9.4.3 Password management systems should be interactive and should ensure quality passwords. ISO 27002: 9.4.4 The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled. ISO 27002: 9.4.5 Access		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				to program source code should be restricted.		
Cryptography & Key management		C5 KRY-01 Policy for the use of encryption procedures and key management C5 KRY-02 Encryption of data for transmission (transport encryption) C5 KRY-03 Encryption of sensitive data for storage C5 KRY-04 Secure key management	SecNum 10.1. Encryption of the data stored SecNum 10.2. Flow encryption SecNum 10.3. Password hashing SecNum 10.4. Non-repudiation SecNum 10.5. Management of secrets HYG10: Set and verify the rules for the choice and size of password (determines in fine the real strength of cryptography key used for encryption) HYG13: prefer a two-factor authentication when possible HYG31: Encrypt sensitive data, in particular on	ISO 27002: 10.1.1 A policy on the use of cryptographic controls for protection of information should be developed and implemented. ISO 27002: 10.1.2 A policy on the use, protection and lifetime of cryptographic keys should be developed and implemented through their whole lifecycle.		ISO 27018: 10 Reference to ISO 27002; Sections 10.1.1, 10.1.2 ISO 27018 Annex A 10.6.: Encryption of PII transmitted over public data-transmission networks

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			hardware that can potentially be lost			
Physical Infrastructure Security	CCSM-ENISA SO 08 - Physical and environmental security	C5 PS-01 Perimeter protection C5 PS-02 Physical site access control C5 PS-03 Protection against threats from outside and from the environment C5 PS-04 Protection against interruptions caused by power failures and other such risks C5 PS-05 Maintenance of infrastructure and devices	SecNum 11.1.1. Physical security perimeters: Public areas SecNum 11.1.2. Physical security perimeters: Private areas SecNum 11.1.3. Physical security perimeters: Sensitive areas SecNum 11.2.1. Physical access control: Private areas SecNum 11.2.2. Physical access control: Sensitive areas SecNum 11.3. Protection against outside and environmental threats SecNum 11.4. Working in private and sensitive areas SecNum 11.5. Delivery and loading areas	ISO 27002: 11.1.1 Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. ISO 27002: 11.1.2 Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. ISO 27002: 11.1.3 Physical security for officers, rooms and facilities should be designed and applied. ISO 27002: 11.1.4		ISO 27018: 11; reference to ISO 27002; Sections 11.1, 11.2 ISO 27018: A.10.7 Secure disposal of hardcopy materials

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			SecNum 11.6. Wiring security SecNum 11.7. Hardware maintenance SecNum 11.8. Disposal of assets SecNum 11.9. Secured recycling of hardware SecNum 11.10. Hardware on hold for use HYG26: Control and protect the access to the server rooms and technical areas	Physical protection against disasters, malicious attack or accidents should be designed and applied. ISO 27002: 11.1.5 Procedures for working in secure areas should be designed and applied. ISO 27002: 11.1.6 Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. ISO 27002: 11.2.1 Equipment should be sited and protected to reduce the risks from		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				environmental threats and hazards, and opportunities for unauthorized access. ISO 27002: 11.2.2 Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. ISO 27002: 11.2.3 Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage. ISO 27002: 11.2.4 Equipment should be correctly maintained to ensure its continued availability and integrity. ISO 27002: 11.2.5		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				Equipment, information or software should not be taken off-site without prior authorization. ISO 27002: 11.2.6 Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises. ISO 27002: 11.2.7 All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. ISO 27002: 11.2.8 Users should ensure that unattended equipment		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				has appropriate protection. ISO 27002: 11.2.9 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.		
Operational Security	CCSM-ENISA SO 12 - Operating procedures	C5 RB-02 Capacity management – monitoring C5 RB-04 Capacity management – control of resources C5 RB-05 Protection against malware C5 RB-08 Data backup and restoration - regular tests C5 RB-13 Logging and monitoring - storage of the logs C5 RB-15 Logging and	SecNum 12.1. Documented operating procedures SecNum 12.2. Managing change SecNum 12.3. Segregation of the development, test and operating environments SecNum 12.4. Measures against malicious code SecNum 12.5. Information backup SecNum 12.6. Logging of	ISO 27002: 12.1.1 Operating procedures should be documented and made available to all users who need them. ISO 27002: 12.1.2 Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled. ISO 27002: 12.1.3 The	ISO 27017: CLD.12.1.5 Administrator's operational security ISO 27017: CLD.12.4.5 Monitoring of Cloud Services	ISO 27018: 12, reference to ISO 27002 Section 12 ISO 27018: 12.4.1 Cloud PII processor should define procedures regarding if, when and how log informaton can be made availabel to or usable by customer ISO 27018: 12.4.2

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		monitoring - configuration C5 RB-21 Handling of vulnerabilities, malfunctions and errors - check of open vulnerabilities C5 RB-01 Capacity management – planning C5 RB-03 Capacity management – data location C5 RB-06 Data backup and restoration - concept C5 RB-07 Data backup and restoration - monitoring C5 RB-09 Data backup and restoration - storage C5 RB-10 Logging and monitoring - concept C5 RB-11 Logging and monitoring - meta data	events SecNum 12.7 Protection for logged information SecNum 12.8 Clock synchronization SecNum 12.9. Analysis and correlation of events SecNum 12.11. Technical vulnerability management SecNum 12.12. Administration. HYG6: Organize the procedure relating to user joining, departing and changing positions (include personnel, but can be interpreted to customer subscribing any offers for joining and departing) HYG11: protect password on stored system (avoid post-it, and use electronic safe solution instead. Protection of password	use of resources should be monitored, turned and projections made of future capacity requirements to ensure the required system performance. ISO 27002: 12.1.4 Development, testing, and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment. ISO 27002: 12.2.1 Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness. ISO 27002: 12.3.1		Log information recorded may contain PII. Measures should be put in place to ensure only use for its inteded purposes ISO 27018: A.10.2 Restriction of the creation of hardcopy material ISO 27108: A.10.3 Control and logging of data restoration

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		C5 RB-12 Logging and monitoring - critical assets C5 RB-14 Logging and monitoring - accountability C5 RB-16 Logging and monitoring - availability of the monitoring software C5 RB-17 Handling of vulnerabilities, malfunctions and errors - concept C5 RB-18 Handling of vulnerabilities, malfunctions and errors - penetration tests C5 RB-19 Handling of vulnerabilities, malfunctions and errors - integration with change and incident management C5 RB-20 Handling of	should be part of the operational procedures) HYG16: use a centralized management tool to standardize security policies (backing security operation by a standardized and automated tool)	Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. ISO 27002: 12.4.1 Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. ISO 27002: 12.4.2 Logging facilities and log information should be protected against tampering and unauthorized access. ISO 27002: 12.4.3 System administrator and system operator activities should be logged and the logs		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		vulnerabilities, malfunctions and errors - involvement of the cloud customer C5 RB-22 Handling of vulnerabilities, malfunctions and errors - system hardening C5 RB-23 Segregation of stored and processed data of the cloud customers in jointly used resources		protected and regularly reviewed. ISO 27002: 12.4.4 The clocks of all relevant information processing systems within and organization or security domain should be synchronised to a single reference time source. ISO 27002: 12.5.1 Procedures should be implemented to control the installation of software on operational systems. ISO 27002: 12.6.1 Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				evaluated and appropriate measures taken to address the associated risk. ISO 27002: 12.6.2 Rules governing the installation of software by users should be established and implemented. ISO 27002: 12.7.1 Audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruptions to business processes.		
Communications Security		C5 KOS-03 Cross-network access C5 KOS-02 Monitoring of connections C5 KOS-04 Networks	SecNum 10.2. Flow encryption SecNum 13.1. Map of the information system. SecNum 13.2. Network	ISO 27002: 13.1.1 Networks should be managed and controlled to protect information in systems and	ISO 27017: CLD.13.1.4 Alignment if security management for	ISO 27018: 13; Reference to ISO 27002 Section 13 ISO 27018 Annex A

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		for administration C5 KOS-05 Segregation of data traffic in jointly used network environments C5 KOS-08 Confidentiality agreement C5 KOS-07 Policies for data transmission C5 KOS-01 Technical safeguards C5 KOS-06 Documentation of the network topology	partitioning SecNum 13.3. Network monitoring HYG18: Encrypt sensitive data sent through the internet (apply to end user connection, data link for replication/redundancy, remote administration link etc..) HYG19: Segment the network and implement a partitioning between these areas HYG20: ensure the security of WiFi access network and that uses are separated HYG21: use secure network protocol when they exists HYG22: implements a secure gateway to the internet (this implies all access to Internet are	applications. ISO 27002: 13.1.2 Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced. ISO 27002: 13.1.3 Groups of information services, users and information systems should be segregated on networks. ISO 27002: 13.2.1 Formal transfer policies, procedures and controls should be in place to protect the transfer of information through the	virtual and physical networks	10.6.: Encryption of PII transmitted over public data-transmission networks

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			known and secured) HYG23: Segregate the services visible from the Internet from the rest of the Information System HYG25: Secure the dedicated network interconnections with partners HYG28: use a dedicated and separated network for information system administration HYG32: Secure the network connection of devices used in a mobile working situation	use of all types of communication facilities. ISO 27002: 13.2.2 Agreements should address the secure transfer of business information between the organization and external parties. ISO 27002: 13.2.3 Information involved in electronic messaging should be appropriately protected. ISO 27002: 13.2.4 Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, regularly reviewed and documented.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
Procurement Management (Supply change management)	CCSM-ENISA SO 04 - Security in Supplier relationships CCSM-ENISA SO 09 - Security of supporting utilities	C5 BEI-01 Policies for the development / procurement of information systems C5 BEI-03 Policies for changes to information systems C5 BEI-09 Review of proper testing and approval C5 BEI-11 System landscape C5 BEI-02 Outsourcing of the development C5 DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider C5 DLL-02 Monitoring of the rendering of services and security requirements for service providers and	SecNum 14. Acquisition, development and maintenance of information systems SecNum 14.1. Secure development policy SecNum 14.2. Procedures for controlling changes to the system SecNum 14.3. Technical review of the applications after a change made to the operating platform SecNum 14.4. Secure development environment SecNum 14.5. Outsourced development SecNum 14.6. System security and compliance test SecNum 14.7. Protection of test data SecNum 15. Relations with third parties	ISO 27002: 14.1.1 The information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems. ISO 27002: 14.1.2 Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification. ISO 27002: 14.1.3 Information involved in application service transactions should be protected to prevent incomplete		ISO 27018: 14; reference to ISO 27002 Section 14 ISO 27018: 15; reference to ISO 27002 Section 15 ISO 27018: Annex A7.1: Disclosure of Sub-Contracted PII Processing ISO 27018: A.10.11 Data processing contract measures ISO 27018: Annex A 10.12 Sub-contracted PII processing

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		suppliers of the cloud provider C5 BEI-12 Separation of functions	SecNum 15.1. Identification of third parties SecNum 15.2. Security in the agreements made with third parties SecNum 15.3. Monitoring and review of third party services SecNum 15.4. Managing changes made in the services of third parties SecNum 15.5. Confidentiality undertakings HYG3 Control Outsourced Service (studying offer, impose some requirements like contract reversibility, prefer standard and open format to proprietary solutions) HYG42 Favor the use of products and services qualified by ANSSI. This	transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay. ISO 27002: 14.2.1 Rules for the development of software and systems should be established and applied to developments within the organization. ISO 27002: 14.2.6 Organizations should establish and appropriately protect secure developments environments for system development and integration efforts that cover the entire system development lifecycle. ISO 27002: 14.2.7 The organization should		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			could be translated as « favor products and service that have been formally certified under the European Cyber Certification Scheme »	supervise and monitor the activity of outsourced system development. ISO 27002: 14.2.8 Testing of security functionality should be carried out during development. ISO 27002: 14.2.9 Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions. ISO 27002: 14.3.1 Test data should be selected carefully, protected and controlled. ISO 27002: 15.1.1 Information security requirements for mitigating the risks		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				associated with supplier's access to the organization's assets should be agreed with the supplier and documented. ISO 27002: 15.1.2 All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information. ISO 27002: 15.1.3 Agreements with suppliers should include requirements to address the information security risks associated with information and		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				communications technology services and product supply chain. ISO 27002: 15.2.1 Organizations should regularly monitor, review and audit supplier service delivery. ISO 27002: 15.2.2 Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
Incident Management	CCSM-ENISA SO 15 – Security incident detection and response CCSM-ENISA SO 16 – Security incident reporting	C5 SIM-01 Responsibilities and procedural model C5 SIM-03 Processing of security incidents C5 SIM-04 Documentation and reporting of security incidents C5 SIM-05 Security incident event management C5 SIM-07 Evaluation and learning process C5 SIM-02 Classification of customer systems C5 SIM-06 Duty of the users to report security incident to a central body	SecNum 16. Managing incidents linked to information security SecNum 16.1. Responsibilities and procedures SecNum 16.2. Reporting linked to information security SecNum 16.3. Assessment of events linked to information security and decision making SecNum 16.4. Response to incidents linked to information security SecNum 16.5. Learning from incidents linked to information security SecNum 16.6. Collecting proof HYG40 Define a security incident management procedure	ISO 27002: 16.1.1 Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. ISO 27002: 16.1.2 Information security events should be reported through appropriate management channels as quickly as possible. ISO 27002: 16.1.3 Employees and contractors using the organization's information systems and services should be required to note and report any observed or suspected information		ISO 27018: 16, Reference to ISO 27002, Section 16 ISO 27018: Annex A.9.1 Notification of a data breach involving PII

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				security weaknesses in systems or services. ISO 27002: 16.1.4 Information security events should be assessed and it should be decided if they are to be classified as information security incidents. ISO 27002: 16.1.5 Information security incidents should be responded to in accordance with the documented procedures. ISO 27002: 16.1.6 Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents. ISO 27002: 16.1.7 The		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				organization should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.		
Business Continuity	CCSM-ENISA SO 17 –Business continuity CCSM-ENISA SO 18 - Disaster recovery capabilities	C5 BCM-01 Top management responsibility C5 BCM-02 Business impact analysis policies and procedures C5 BCM-04 Verification, updating and testing of the business continuity C5 BCM-03 Planning business continuity C5 BCM-05 Supply of the computing centres	SecNum 17. Continuity of activity SecNum 17.1. Organization of the continuity of activity SecNum 17.2. Implementing continuity of activity SecNum 17.3. Check, review and evaluate the continuity of activity SecNum 17.4. Availability of the means for information processing HYG37: Define and apply a backup policy for critical	ISO 27002: 17.1.1 The organization should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. ISO 27002: 17.1.2 The organization should establish, document, implement and maintain processes, procedures and controls to ensure		ISO 27018:12.3.1 Information backup ISO 27018: 17 Reference to ISO 27002, Section 17

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			components (applicable equally for disaster recovery) There is no explicit requirement toward disaster recovery in SecNumCloud. However, some requirements are close to a disaster recovery, thus they're referenced here. SecNum 12.5. Information backup SecNum 11.3. Protection against outside and environmental threats (more preventing than recovering) HYG37: Define and apply a backup policy for critical components (applicable equally for business continuity) SecNum 19.1 Service	the required level of continuity for information security during and adverse situation. ISO 27002: 17.1.3 The organization should verify the established information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations. ISO 27002: 17.2.1 Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			Agreement h) (service availability)			
Compliance	CCSM-ENISA SO 22 – Checking compliance CCSM-ENISA SO 27 - Cloud monitoring and log access CCSM-ENISA SO 19 - Monitoring and logging policies	C5 COM-01 Identification of applicable legal, contractual and data protection requirements C5 COM-02 Planning independent, external audits C5 COM-03 Carrying out independent, external audits	SecNum 5.3 Risk assessment. Clause 4 SecNum 18.1 Identification of the legislation and the contractual requirements that apply SecNum 18.2 Independent review of information security SecNum 18.3 Compliance with security policies and standards SecNum 18.4 Technical compliance examination SecNum 19.1 Service agreement SecNum 19.2 Location of data SecNum 19.3 Regionalization	ISO 27002: 18.1.1 All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organization. ISO 27002: 18.1.2 Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property		ISO 27018: 18; Reference to ISO 27002, Section 18 with an extension in 18.2.1: Independent reviews serving as compliance instrument for the cloud customer ISO 27018: Annex A 11.1: Disclosure of geographical location of PII ISO 27018: Annex A 11.2 Intended destination of PII

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			SecNum 19.4 End of contract	rights and use of proprietary software products. ISO 27002: 18.1.3 Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements. ISO 27002: 18.1.4 Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. ISO 27002: 18.1.5 Cryptographic controls should be used in compliance with all		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				relevant agreements, legislation and regulations. ISO 27002: 18.2.1 The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur. ISO 27002: 18.2.2 Managers should regularly review the compliance of information processing and procedures within their area of		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				responsibility with the appropriate security policies, standards and any other security requirements. ISO 27002: 18.2.3 Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.		
Security Assessment	CCSM-ENISA SO 21 - Security assessments CCSM-ENISA SO 20 - System tests	C5 SPN-01 Notification of the top management C5 SPN-02 Internal audits of the compliance of IT processes with internal security policies and standards C5 SPN-03 Internal audits of the compliance of IT systems with internal	SecNum 18.2 Independent review of information security HYG38: Undertake regular controls and security audits then apply the associated corrective actions HYG41: (for strengthening HYG38) Carry out a formal risk assessment			ISO 27018: 18.2.2; 18.2.3; Reference to ISO 27002 18.2.2; 18.2.3

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		security policies and standards				
Interoperability & Portability	CCSM-ENISA SO 26 - Cloud interoperability and portability	C5 PI-01 Use of public APIs and industry standards C5 PI-02 Export of data C5 PI-03 Policy for the portability and inter-operability C5 PI-04 Secure data import and export C5 PI-05 Secure deletion of data				
System Security & Integrity	CCSM-ENISA SO 11 - Integrity of network and information systems CCSM-ENISA SO 23 - Cloud data security CCSM-ENISA SO 24 - Cloud interface security CCSM-		SecNum 11.8 Disposal of assets SecNum 14.7 Protection of test data HYG14: Implement a minimum of security across the whole IT stock HYG15: Protect against threat relating to the use			ISO 27018: 9.4; reference to ISO 27002 9.4

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
	ENISA SO 25 - Cloud software security		of removable media (include USB device, CD-ROM but our reflexion have to take into account any other way used to populate data on the cloud infrastructure in our context) HYG17: Activate and configure the firewall on workstations (this should be considered for an IAAS infrastructure, workstation won't make as much sense in a cloud infrastructure as in a regular IT system) HYG36: Activate and configure the most important component logs			
Change & Configuration Management	CCSM-ENISA SO 13 - Change management	BEI-03 Policies for changes to information systems BEI-04 Risk assessment	SecNum 12.2 Managing change SecNum 14.2. Procedures for controlling changes to	14.2.2 Changes to systems within the development lifecycle should be controlled by		ISO 27018: 12.1.2; reference to ISO 27002 12.1.2

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
		of changes BEI-05 Categorisation of changes BEI-06 Prioritisation of changes BEI-07 Test the changes BEI-08 Rollback of changes BEI-09 Review of proper testing and approval BEI-10 Emergency changes	the system SecNum 14.3. Technical review of the applications after a change made to the operating platform HYG34: Define an update policy for the components of the information system HYG35: Anticipate the software and system end of life/maintenance and limit software reliance (e.g. dependancy to proprietary software/solution)	the use of formal change control procedures. 14.2.3 When operating platforms are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security. 14.2.4 Modifications to software packages should be discouraged, limited to necessary changes and all changes should be strictly controlled		
Risk / Threat / Vulnerability Management	CCSM-ENISA SO 02 - Risk management		SecNum 5.3 Risk assessment SecNum 12.11 Technical vulnerability management			ISO 27018: 0.3 PII protection requirements ISO 27018: 0.4 Selecting and implementing

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
						controls in a cloud computing environment
Personnel & Training	CCSM-ENISA SO 05 - Background checks CCSM-ENISA SO 06 - Security knowledge and training CCSM-ENISA SO 07 - Personnel changes	C5 HR-01 Security check of the background information C5 HR-02 Employment agreements C5 HR-03 Security training and awareness-raising programme C5 HR-04 Disciplinary measures C5 HR-05 Termination of the employment relationship or changes to the responsibilities	SecNum 7.1. Selection of candidates SecNum 7.2. Conditions for hire SecNum 7.3. Awareness, learning and training on information security SecNum 7.4. Disciplinary process SecNum 7.5. Rupture, term or modification in the labour contract HYG1 Train the operational Team in Information System Security (which include not only technical but organizational and regulatory training) HYG2 Raise user awareness about basic	ISO 27002: 7.1.1 Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. ISO 27002: 7.1.2 The contractual agreements with employees and contractors should state their and the organization's		ISO 27018: 7.2.2 Measures should be put in place to make relevant staff aware of the possible consequences on the public cloud PII processor. ISO 27018: A.10.1 Confidentiality or non-disclosure agreements

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
			information security (this target the end user on a system, here it shall be interpreted as en user of the Cloud Service offered) HYG24 Protect your professional email (beside technical protection, this rules emphasis on user awareness for the use of his email, which is more a matter of training) HYG39 Designate a point of contact in information system security and make sure staff are aware of him or her	responsibilities for information security. ISO 27002: 7.2.1 Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization. ISO 27002: 7.2.2 All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function. ISO 27002: 7.2.3 There should be a formal and		

EC-CLOUD CATEGORY	**CCSM-ENISA** [5]	**C5 GERMANY** [6]	**SecNum FRANCE** [7]	**ISO 27002** [2]	**ISO 27017 (Only deltas included)** [3]	**ISO 27018 (Reference plus deltas included)** [4]
				communicated disciplinary process in place to take action against employees who have committed and information security breach. ISO 27002: 7.3.1 Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.		