Annex A. Case Studies Spain and UK: Interviews

This annex presents the results of the interviews we carried out to gather information about the state of implementation of governmental clouds for the selected use cases: Spain and UK. The results are presented according to the proposed security framework's PDCA structure.

A.1 PLAN Phase

	PLAN Phase	
	Risk Profiling	
Assessment Question	**UK**	**Spain**
Do you have a National Information Asset classification scheme? How do you classify government assets? How do you classify government assets and define the global risk profile?	The UK Government has adopted in April 2014 a new policy with regard to the security classification of information assets. The new policy is based on the categories: • Official • Secret • Top secret The G-Cloud 6 call for service proposal will be based according to this new asset classification. The classification system currently in use is a six categories classification: • 'Unclassified' • 'Protect' • 'Restricted',	Services are not *cloudified*, but are created directly in the Cloud. This is the result of a reformation of Public Administration to break the digital breach. Migration of current services to the Cloud could be possible, but it would be done upon request (the approach now is reactive, not proactive). Categorization of assets is described in the National Security Framework (ENS): There are three security levels (LOW, INTERMEDIATE, HIGH) in which systems can be classified, and those levels guide the selection of security controls and the kind of audits to be performed. When a system handles different types of information and provides different services, the system security level (i.e., global risk profile) will be the highest of those established for each type of information and each service.

	PLAN Phase	
	• ‘Confidential’ • ‘Secret’ • ‘Top Secret The service currently provided through the G-Cloud / CloudStore are categorised IL2 and 3. With the implementation of the new classification scheme the service provided through the G-Cloud framework will be those falling into the category: “OFFICIAL”. The category ‘OFFICIAL’ includes the majority of information related to public sector business, operations and services. Further details on the new classification can be found in the document: ’Government Security Classifications FAQ Sheet 1: Working with OFFICIAL Information v1.2 – April 2013’	
Which are the considered security dimensions? (e.g. Confidentiality, Integrity, …).	The security dimensions considered are: • Availability [A]. • Integrity [I]. Confidentiality [C].	In order to estimate this impact and establish the system category, five security dimensions are considered: • Availability [Av]. • Authenticity [A]. • Integrity [I]. • Confidentiality [C]. • Traceability [T].
Do you have impact levels for each dimension?	The impact of a security breach is categorized according to the Business Impact Level approach. This approach is currently in use,	According to the ENS, each security dimension affected will be included in one of the following levels: LOW, INTERMEDIATE or

	PLAN Phase	
How many categories or levels are considered for each dimension?	but with the introduction of the new classification the BIL won't be mandatory anymore. There's no impact level associated to each security dimension (CIA) even though a special attention is given to the 'Availability dimension. For instance the current Impact Level for the G-Cloud asset are often represented as follows: IL22x or IL33x where "x" represent the declared level of Availability In the context of the assessment of the 'Confidentiality' impact the UK Protective Marking was applied and there was a direct correlation between this classification and business impact level. The Protective Markings of PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET directly match to business impact levels 2, 3, 4, 5 and 6 respectively. The approach allows organizations to assess the BIL for compromises of the confidentiality integrity or availability of information and ICT systems. The business impact level scale ranges from 0 (no impact) to 6 (extreme impact). The business impact of a loss of confidentiality, integrity and availability is assessed as independent properties for any given asset or set of assets. A detailed description of the Impact Levels is provided in the document: 'Business Impact Level Tables' issued by CESG and the Cabinet Office.	HIGH. For determination of the level required in a security dimension, guidelines are provided in CCN-STIC-803. The security approach in the ENS is functional; it applies both to Cloud and non-Cloud services. Additional considerations should be made for the case of public Cloud, since the fulfilment of ENS requirements will depend on who is the proprietary of the data and the service (being defined in CCN-STIC-823. In this case, since the current situation is a private Cloud, i.e., both data and services belong to the Administration, so the ENS applies directly.
[Optional] Are security dimensions aggregated into a final risk category?	The BILs are the risk aggregation.	According to the ENS, when a system handles different types of information and provides different services, the system security

	PLAN Phase	
		level (i.e., global risk profile) will be the highest of those established for each type of information and each service.
[Optional] Do selection and evaluation of security dimensions comply with a security standard?	Each Public Administration ('Senior Information Risk Owner- SIRO) has to perform a risk assessment to identify the exposure to risk for the information asset. The IA Standard (IS) 1/2 is the risk assessment approach currently in use No. IS1/2 provides a common approach for information risk assessment, management and assurance activities. Further details on the definition of business impact are contained in the document issues by the Cabinet Office on 2 March 2014: 'Government Security Classifications FAQ Sheet 2: Managing Information Risk at OFFICIAL'.	Based on the Magerit Methodology for Risk Analysis, FIPS recommendations, and aligned with the Council of Europe regulations.
	Architectural Model	
What are the security criteria and functional criteria for selecting IaaS, PaaS or SaaS?	The UK Gov doesn't define functional and security requirements per se for IaaS, PaaS, SaaS. All the Cloud service model are allowed for the handling of the information and ICT assets categories as IL from 0 to 3 or 'OFFICIAL'. It a responsibility of the buyers (public organizations) as risk owners (Senior Information Risk Owner- SIRO) to determine which services can me moved into the Cloud, using which Cloud service model. It is also a responsibility of the risk owner to determine the specific set of security controls required to offer the necessarily level of the assurance.	Reactive model based on real needs.
What are the security criteria for selecting a	There are no specific criteria established for the selection of the Cloud deployment model.	So far, only Private.

	PLAN Phase	
Private, Public, Hybrid or Community Cloud?	In principle any Cloud deployments are allowed to be used.	Public adoption provisions: currently evaluating security aspects, and recommendations from the Spanish Cryptologic Center (CCN). In contact with public providers to know their security strategies.
Are the above criteria standard-based?	No	No
Under which conditions is subcontracting permitted?	There are not specific conditions applied to subcontracting. The suppliers allowed in the G-Cloud / CloudStore have to comply with the general requirements established in the G-Cloud framework (e.g. Cloud Security Principles) plus any further security requirements requested by the risk owners (service buyers).	All physical resources are private. The SARA Network is private. This is part of the risk analysis.
	Security and Privacy Requirements	
Assessment Question	**UK**	**Spain**
Which are the security requirements for the Cloud services? Is there a baseline or minimum?	The 14 Cloud Security Principles and associated security objectives are the defined security requirements. The Security Principles do not represent a minimum baseline since a CSP (suppliers) are allowed not to satisfy a certain Security Principle or some of the objectives established in the Security Principles. The CSP (suppliers) has anyway to state the reason why they do not satisfy a certain security objective and how they can assure that the risk associated with a information managed in the provision of a services is handled.	Related to the categorization in the ENS (Annex II).

	PLAN Phase	
Are there specific security requirements for IaaS, PaaS or SaaS?	NO	ENS plus the specific considerations that are being defined in CCN-STIC-823 [9]. This document, still in draft version, defines the concept of "communities". CSPs can provide services to different user communities depending on the security levels they support. The guide also includes recommendations to achieve adequate levels of logical and physical resources confinement.
Are there specific security requirements for a Private, Public, Hybrid or Community Cloud?	NO	Same as previous answer.
Are additional requirements contemplated?	Yes there additional requirements associated with: • Asset classified as 'OFFICIAL' and connected via Public Service Network (PSN), which will be Community Clouds, dedicated to services offered to the "PSN Community" or "PSN with Encrypted overlay Community". • Asset marked as 'OFFICIAL – SENSITIVE'	No
Are the requirements standard-based?	The requirements are not directly taken from standards, but they are loosely derived from ISO 27001 and CSA Cloud Control Matrix	The requirements are not directly taken from standards, but they are related to them. ENS requirements are being mapped to standard certifications: ISO 27001-27002, CSA CCM and NIST 800-53v3 (contained in CCN-STIC-825). Currently this guide explains how the ENS is fulfilled with an accreditation of norms ISO 27001-27002, remarking the differences and which additional issues should be considered for auditing).

	PLAN Phase	
Are requirements formalized in a policy document? Which format is used?	The requirements are formalized in the ‘Cloud Security Principles’.	Requirements are formalized in a document called “Statement of Applicability”. All decisions about security requirements and applicable security measures made by the Responsible of Security must be formally approved and documented in the Statement of Applicability, which has to be available for auditing purposes.
What are the privacy regulations/laws you took into account?	National Data Protection Legislation.	National data protection legislation.
Are there limitations for international transfer of data? Which ones?”	The limitations to international data transfer are those established in Privacy legislation as well as those associated to the ‘OFFICIAL – SENSITIVE’ category as defined in the document: ‘Government Security Classifications FAQ Sheet 1: Working with OFFICIAL Information v1.2 – April 2013’	Controls are based on applicable national, EU and international regulations e.g., European Data Protection, National data protection legislation.

A.2 DO Phase

	DO Phase	
	Security Controls	
Assessment Question	**UK**	**Spain**
Do you have a security control framework / checklist to assess the fulfillment of your requirements? How are security requirements mapped to security controls?	UK: the document 'Implementing the Cloud Security Principles' suggests the possible best practices that can be used to satisfy the objectives defined under each of the 14 security principles. For each one of the objectives a reference to ISO 27001 and Cloud Security Alliance Cloud Control Matrix / STAR is provided.	Using the matrix in Annex 2 of ENS, which maps security levels to security measures.
Are security controls formalized in a policy document? Which format is used?	NO. See above	A "Statement of applicability" is defined per information system (no per service). Services are categorized according to the ENS scheme, and the highest required security level from all the services is the one considered.
Are security controls defined for the different security levels/risk profiles?	Additional security controls are required for 'OFFICIAL – SENSITIVE'. Additional security controls for OFFICIAL-SENSITIVE information are largely procedural rather than technical and designed to enforce particular need-to-know requirements. Examples could include:	Yes, according to the categorization in ENS.

	DO Phase	
	- Well communicated and understood handling processes - Clearly defined and bounded copy lists - More granular access controls within document stores or databases - Increased monitoring and compliance auditing	
Could please describe the structure of your security control framework? (e.g. are security controls categorized? Which are the considered categories?)	The security requirements are those mentioned in the PSN and Cloud Security Principles.	Security measures are categorized in three classes: - **Organisational framework**. This is constituted by the group of measures related to overall security organisation. - **Operational framework**. This is constituted by the measures to be taken to protect the system operation as an integral series of components for achieving a purpose. - **Protective measures**. These are focused on protecting specific assets, depending on their nature and the quality required by the security level of the dimensions that are affected.
Which are the specific security controls for each service model (IaaS, PaaS, SaaS)?	Not Applicable.	ENS Security Measures.

	DO Phase	
Which are the specific security controls for each deployment model (private, public, hybrid, community)?	Service accessible though the Public Service Network (PSN), are considered as Community Clouds (dedicated to services offered to the "PSN Community" or "PSN with Encrypted overlay Community"). The specific controls for the G-Cloud Community are those defined for the PSN.	ENS Security Measures.
Are the security controls compliant with any standard (e.g. NIST 800-53, CCM, ISO 27k)?	There's no standard mandated to comply with the Cloud Security Principles even though CSP / suppliers can demonstrate compliance by adopting ISO27001 and Cloud Security Alliance Cloud Control Matrix / STAR .	Yes, see above.
Are security controls formalized in a policy document? Which format is used?	No.	Yes, a questionnaire is distributed to clients to monitor the state of implementation of the ENS. From the compilation of these data, a common template is generated (performed every 3 months in years 2013, 2014). In the second semester of 2014 another process based on an IT tool is carried out to assess the state of ENS implementation in public administration. It is called "*Informe Nacional del Estado de la Seguridad*" or INES, and it is documented in CCN-STIC-824. Both processes (questionnaire and INES) are based on self-assessment. Regarding automation, The PILAR tool is used. It includes forms for each security measure in order to determine their maturity state (an auditor performs this evaluation).

	DO Phase	
		Thresholds are defined for the maturity levels and grouped in three qualitative levels: green (when the maturity level is ok), yellow (potential problems coming from slight deficiencies that need to be analyzed before they become serious), and red (for serious deficiencies that must be solved immediately).
	Implementation, Deployment and Accreditation	
Assessment Question	**UK**	**Spain**
How are security responsibilities defined and divided between the different parties (Gov Cloud, provider, customer, etc)? What are their roles and responsibilities? Does a contractual agreement designate the responsibilities of the parties (e.g. CSP, Cloud customer - local administration, etc) for the security of service provided via G-Cloud?	Security responsibility are allocated as follows: • Public Administration / Cloud Customer: responsible for the execution of the risk assessment, the identification of the specific controls necessary to offer the necessary level of assurance • CSP / Suppliers: responsible for the actual implementation of the security controls request by the Cloud Customers and those indicated in the G-Cloud framework. • CESG / Cabinet Office / G-Cloud: is the G-Cloud owners and are responsible for the definition of the framework and definition of the security principles and guidance for their implementation. The allocation of the responsibilities are included in the G-Cloud framework and in the service agreements.	When a public entity provides a cloud service to another one, both have to sign a Collaboration Agreement, a juridical instrument regulated by law, where conditions of the service provision are set. The roles of each actor are identified (client, provider), and the ENS is applied accordingly. The segregation of the roles in the scheme is decided by the stakeholders in collaboration, according to the law provisions

	DO Phase	
[if reply above is contract]How is the contract established?	The framework contract is the defined in the G-Cloud tender.	The Collaboration Agreement is not a contract
Do you define a set of standard SLA, and in particular Security SLAs? Could you give us an example of SLAs or SLOs in use? Is it possible to negotiate the security contents of the SLA?	No.	No, just service related parameters. In regard to security, the agreement contains two clauses specifying: 1) that the ENS must fulfilled;2) that the national privacy law and data protection laws must be fulfilled. An example of Collaboration Agreement available shows the Agreement that the Spanish Ministry of Finance and Public Administration offers as service provider to a regional Public Administration for the Cloud service called ORVE[1], which is a Virtual Registry Office.
How do you assess / verify ex ante the suitability of a Cloud service to provide a sufficient level of assurance? Do you have in place a formal authorization and accreditation system? How does it work? It is directly managed by a National Agency (e.g. similar to US FedRamp)? It relies on commercially available certifications (which ones)? It is based on self-attestation /assessment?	Suppliers assert how they meet the Cloud Security Principles by selecting a predefined answer for a range of questions that meet the Cloud Security Principles. Suppliers will then be required to provide evidence and documentation to support their assertion. In the document: "Implementing Cloud security principles" are mentioned various approaches that cab be used to show compliance to G-Cloud requirements: • Service provider assertion • Contractual commitment • Independent validation of assertions • Independent testing of implementation	Self-assessment.

[1] http://www.fmmadrid.es/index.php/14-sample-data-articles/140-sistema-orve

	DO Phase	
	- Assurance in the service design - Assured components If the supplier want to use a 'independent validation of the assertion' the following option are available: - An independent third party has reviewed and confirmed the service provider's assertions. The third party certifies that the service meets the objectives associated with the given principle - A certificate of compliance with a recognized standard is presented by the service provider. - A certificate of compliance with a recognized standard is presented by the service provider. Additionally, the scope of certification and implementation of controls are also reviewed by a suitably qualified individual, such as a CCP certified 'Accreditor' or 'IA Auditor' at the Senior or Lead level or a recognised subject matter expert. If the supplier wants to use an "independent testing of implementation" a security assessment / penetration testing performed by organization registered under the CREST, CHECK, Tiger schemes.	
Is there any procedure for verifying that the initial deployment (when the service is just launched and starts running) is SLA-conformant?	n/a	Before moving to production environment, the correct operation of the application must be checked:

	DO Phase	
		BASIC systems require acceptance testing; and verification that the security of other service components is not affected. MEDIUM systems, apart from the same tests as BASIC systems, require vulnerability analysis and penetration testing. HIGH systems, apart from the same tests as MEDIUM systems, require consistency analysis in process integration and considering the possibility of a source code audit.
[Optional] Are the deployment and verification procedures automatic or manual?	n/a	n/a

A.3 CHECK Phase

	CHECK Phase	
	Log/Monitoring	
Assessment Question	**UK**	**Spain**
Do you periodically check that the security requirements are met? How? Do you monitor the execution of the agreements (e.g. monitoring SLAs, audit the 3rd party, etc)? Which are the objects of monitoring?	There's no specific requirement for monitoring service execution in the G-Cloud, but each Cloud Customer can specify additional monitoring requirement (e.g. real time security monitoring).	Monitoring of the fulfillment of ENS requirements is performed by means of the INES, via a self-assessment procedure. The objects of monitoring are the applicable ENS requirements and associated security measures. Regarding audits, the minimum elements to include in the audit, in accordance with Annex 2 of ENS, are: 1.Risk analysis (methodological basis) 2.Organizational framework (policy and procedures documentation, through interviews) 3. Operational framework (incident management, access control mechanisms, etc.) 4. Applicability Statement (strength of security measures) 5. Procedures for continuous improvement of security, (maturity cycle of the information system) For each of these 5 points, guide CCN-STIC-802 points out the kind of tests to be performed. For incident management, there is a centralized incident correlation system in SARA.

	CHECK Phase	
Which evidences are registered for analysis and documentation?	N/A They analyze the traffic monitoring on server level, e.g. if it has terminated unexpectedly.	Describe all the information that is logged for further analysis both at the CSP and at the o For creating the INES annual report, all the applicable security measures related to the minimum elements of the ENS to be audited (see above) are registered for analysis, Guide CCN-STIC-824 provides templates for evaluation according to maturity levels (supported by the SW tool PILAR[2]). The guide also Defines the XML format to report the data that resulted of the assessment (for easiness of further statistical processing).
Which tools are used for logging evidences/monitoring?	N/A	SARA´s Centralized incident correlation system. CCN-CERT has been developing since 2008 an Early Alert System for fast detection of incidents and anomalies within the Government in order to carry out preventive, corrective and retaining actions.
Is the monitoring scheme continuous or discrete?	N/A	Continuous
Are both operational and administrative levels covered in monitoring?	N/A	N/A
Are log/monitor reports periodically generated? With which frequency?	N/A	N/A

[2] http://www.pilar-tools.com/es/tools/pilar/v54/470F1_2014-04-11_e.pdf

	CHECK Phase	
With which frequency are log reports send to the customer? What information do they contain?	N/A	N/A
Are incidents recorded and documented following a standard format? (e.g., VERIS)	Information on security incident are reported.	N/A
Are incident reports public or shared with 3rd parties?	NO	N/A
	Audit	
Assessment Question	**UK**	**Spain**
Which audits are required to provide evidences that the agreed upon provisions in the SLA/local policy are actually fulfilled?	The G-Cloud framework foresees a security audit on a sample of the assertions. The Cloud Customer can perform additional audit. It should be noted that the right to audit is included in the G-Cloud framework agreement.	Ordinary regular audits at least every two years, to verify compliance with the ENS. On an extraordinary basis, the audit will be performed whenever substantial changes are made to the information system that could affect the required security measures. (Details of the audit process are given in guides CCN-STIC 802 and CCN-STIC 808)
Do the required audits need to be stated in the SLA/local policy?	As mentioned above the "right to audit" is included in the G-Cloud framework agreement	The Collaboration Agreement refers to the fulfillment of the ENS, which in turn requires regular audits.
Which are there different audit levels? (e.g., BASIC, INTERMEDIATE and HIGH)	N/A	Documented in ENS, CCN-STIC 802 and CCN-STIC 808.

	CHECK Phase	
		Guide 808 provides a template for conducting the audit, indicating requirements to check for each system category and security dimensions affected. For information systems categorized as BASIC, it is enough with a self-audit performed by the same personnel that administers the system (or delegated people).
Are the audits related to security certifications? (e.g., SGSI - ISO/IEC 27001, SGSI - ISO/IEC 27001)	Not necessarily.	Concept of “conformance” Entities publish in their electronic websites the security certifications they are conformant with (e.g., ISO 27k). CCN is elaborating guides to map standard certifications to the fulfillment of ENS requirements. So far, guide CCN-STIC-825 provides the mapping between ISO27001-27002 and ENS.
Which is the audit frequency?	Annual	See Above.
Who performs auditing?	Accredited auditor (e.g. those included in the CLAS Consultants).	An audit team must be created with external and/or internal personnel, supervised by an audit leader. The audit team members have to prove accreditation and/or experience in regard to information systems and security, and a confidentiality agreement must be signed before the audit. More information on the requirements to be satisfied by the audit team, is specified in CCN-STIC-802, Annex 1.

A.4 ACT Phase

	ACT Phase	
	Changes Management	
Assessment Question	**UK**	**Spain**
How do you handle feedback from the CHECK phase? Which feedback triggers changes in the security programme and or Gov Cloud approach?	The results of the CHECK phase are used to review the G-Cloud framework. The changes and improvements are reflected in the new G-Cloud call. For instance the G-6 call will reflect the lesson learnt in the first 5 iterations to the G-Cloud process.	Documented in the audit guides 802 and 808. A template for the elaboration of the audit report is provided in guide CCN-STIC-808. For each security measure in the ENS, a set of requirements is listed that can be marked as fulfilled or unfulfilled. Then the percentage of requirements coverage for each measure is calculated and assigned to a qualitative category that represents the degree of fulfillment (Complete 100%, High 50-99%, Low 1-49%, Inexistent 0). Based on this, the final audit report is elaborated with recommendations for improvement and changes of measures when necessary. Reports are sent to the Security Responsible for revision, and then given to the System Responsible, who applies the appropriate corrective measures.
Which feedback trigger re-negotiation of the contract? How is the re-negotiation of the contract performed?	Not contemplated.	Not contemplated.
Which changes trigger re-accreditation?	N/A	n/a

	ACT Phase	
Are the changes notified to the customer? How?	The changes are included in the G-Cloud call for service	Not ´a priori´
[optional] What is the degree of automation of the triggered actions when a change occurs?	None	If changes are significant, a new audit must be conducted to check ENS fulfillment. This process is not automated.
Are there any procedures to detect and notify SLA violations? And is generation of "alerts" contemplated when the SLA is at risk of being violated?	There's no such a procedure. The G-Cloud approach foresees the removal from the CloudStore of the services provided by organizations caught to misrepresent reality in their security assertions.	Yes/No. If "Yes", describe the procedures and tools used for detecting SLA violation. Explicitly state if there are also mechanisms to predict a future SLA violation before it happens ("alert" mechanisms) and describe them.
Which mechanisms are put in place to guarantee continuity of operation in case of severe incidents?	N/A	Defined in the ENS. For systems categorized as HIGH, a continuity plan must be defined to deal with service interruption. The plan must contemplate: a) Functions, responsibilities and activities to be carried out. b) Consideration of alternative means to continue providing the service. c) Alternative means need to be planned and materialized in agreements or contracts with the corresponding providers. d) People affected by the plan will receive specific training for their role in such plan. e) The continuity plan will be part of organizational continuity plans in other areas different to security.
	Exit Management	

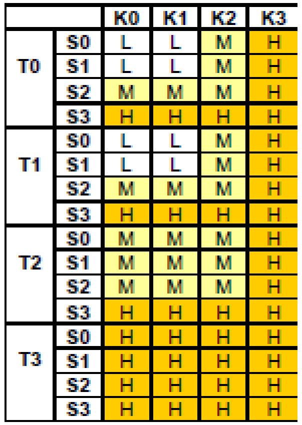
	ACT Phase	
Assessment Question	**UK**	**Spain**
Do you have a procedure to deal with contract termination? E.g. are customer data securely deleted when the service is terminated? (e.g., a destruction certificate is issued by a 3rd party)		There is a clause in the Collaboration Agreement related to finalization. Both parties can ask for finalization with one month in advance.
[optional] Are data given back to the customer in a portable standard format? Which format is used?		See above.

Annex B. Case Studies Estonia and Greece: Interviews

This annex presents the results of the interviews we carried out to gather information about the state of implementation of governmental clouds for the selected use cases: Estonia and Greece. The results are presented according to the proposed security framework's PDCA structure.

A.1 PLAN Phase

	PLAN Phase	
	Risk Profiling	
Assessment Question	**Estonia**	**Greece**
Do you have a National Information Asset classification scheme? How do you classify government assets? How do you classify government assets and define the global risk profile?	Yes. For instance to classify information security in Estonia we use the security model, based on three pillars: availability, confidentiality and integrity of data. The owner of data determines the information security level needed. Risk is assessed based on table (table with explanation is listed in the end of questionnaire).	No national information asset classification scheme In GRnet there is a scheme to classify assets based on the ADAE directive. GRnet classifies the data based on the level of sensitivity, which is based on the Hellenic Authority for Communication Security and Privacy (ADAE) regulation. There are 4 types of data: public, internal, confidential, and special data. The security parameters are different per type of data, the security domains remain the same, the level of security becomes stricter when the information is classified. Some parameters: physical security, risk assessment, impact assessment, business continuity, tests, audits, safe usage, back up, performance levels, logic access, network management and monitoring, change management etc. (these can be found in the ADAE document cited above).

<table>
<tr><th></th><th colspan="2">PLAN Phase</th></tr>
<tr><td>Which are the considered security dimensions? (e.g., Confidentiality, Integrity, …).</td><td>Availability, confidentiality and integrity.</td><td>- Availability,
- Integrity,
- Confidentiality,
- Privacy,
Identity management.</td></tr>
<tr><td>Do you have impact levels for each dimension?
How many categories or levels are considered for each dimension?</td><td>Each dimension has four levels (0, 1, 2 or 3).
L – low security risk
M – medium security risk
H - high security risk
T – integrity of data
S – confidentiality of data
K – availability of data
<table>
<tr><th></th><th></th><th>K0</th><th>K1</th><th>K2</th><th>K3</th></tr>
<tr><td>T0</td><td>S0</td><td>L</td><td>L</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S1</td><td>L</td><td>L</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S2</td><td>M</td><td>M</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S3</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td>T1</td><td>S0</td><td>L</td><td>L</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S1</td><td>L</td><td>L</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S2</td><td>M</td><td>M</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S3</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td>T2</td><td>S0</td><td>M</td><td>M</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S1</td><td>M</td><td>M</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S2</td><td>M</td><td>M</td><td>M</td><td>H</td></tr>
<tr><td></td><td>S3</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td>T3</td><td>S0</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td></td><td>S1</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td></td><td>S2</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
<tr><td></td><td>S3</td><td>H</td><td>H</td><td>H</td><td>H</td></tr>
</table>
Availablity:
K0 – availability is less than 80% per year and the lenght of service interruption can exceed 24 hours.
K1 – availability is more than 80% and less than 99% per year and the lenght of service interruption must be between 4 and 24 hours
K2 – availability is more than 99% and less than 99,9% per year and the lenght of service interruption must be between 1 and 4 hours
K3 – availability is more than 99,9% per year and the lenght of service interruption must be between 0 secund and 1 hour
Integrity:</td><td>No impact levels per dimension.
There are 4 security levels: Low, medium, high, very high but for Cloud services it only goes up to ‘high’. The security levels are applied according to the nature of the data (public, internal, confidential, etc.) – MATRIX in the supporting document (GR net classification doc)</td></tr>
</table>

	PLAN Phase	
	T0 –identification of changing and deleting data in information source is not important, controlling the data integrity, accuracy and timeliness are not needed T1 – changing and deleting data in information source must be identified T2 – facts of changing and deleting data in information source must be identified. Required are periodical controls of data integrity, accuracy and timeliness T3 – changing and deleting of data in informations source must have proof of the value. Data integrity, accuracy and timeliness in real-time is requied. Confidentality: S0 – public information: no restriction to the access of data S1 – confidential information: access to information is restricted S2 – secret information: using this information is possible only for determined group of peole S3 – topsecret information: using this information is possible only for determined group of people	
[Optional] Are security dimensions aggregated into a final risk category?	Yes. Depending on security dimensions and its level final risk is estimated (see the table below).	No security risks profiles per se but based on the different information levels, the security objectives are different and thus the customers are categorized based on the information they store, transfer, etc.
[Optional] Do selection and evaluation of security dimensions comply with a security standard?	Yes. ISO 27001, ISO 27002 and BSI IT.	They consider ISO 27001 and NIST.

	PLAN Phase	
	Architectural Model	
Assessment Question	**Estonia**	**Greece**
What are the security criteria and functional criteria for selecting IaaS, PaaS or SaaS?	So far no specific criteria isn't assigned. RIA (Information System Authority) is running analysis to set up security and functional criteria for IaaS, PaaS or SaaS. Analyses will be ready in beginning of 2015.	N/A (only IaaS offering)
What are the security criteria for selecting a Private, Public, Hybrid or Community Cloud?	At the moment there are no criteria for selecting cloud type. However RIA is running analyses which determine guidelines and principles for selecting cloud type for housing of data. Analyses will be ready in beginning of 2015. Definitely ISKE (IT baseline security system) doesn't allow to house the governmental data in Public clouds if the service is critical for the state (such as Population Register, Land Register, etc).	N/A (public and hybrid solutions)
Are the above criteria standard-based?	Yes. ISKE is providing the guidelines for secure information systems in Estonia https://www.ria.ee/iske-en	N/A
Under which conditions is subcontracting permitted?	In compliance with Public Procurement Act https://www.riigiteataja.ee/en/eli/509072014009/consolide	N/A
	Security and Privacy Requirements	
Assessment Question	**Estonia**	**Greece**

	PLAN Phase	
Which are the security requirements for the Cloud services? Is there a baseline or minimum?	Cloud services can be used currently only for public information. If there is need for higher confidentiality then encryption is definitely needed.	The minimum requirements that are based in the security policy document provided by Hellenic Authority for Communication Security and Privacy (ADAE) (based on ISO 27001 and NIST).
Are there specific security requirements for IaaS, PaaS or SaaS?	Estonia has ISKE requirements which apply to the state information systems. If IaaS, PaaS or SaaS fulfills ISKE requirements then IaaS, PaaS or SaaS models are permitted.	No
Are there specific security requirements for a Private, Public, Hybrid or Community Cloud?	Provided solution has to fulfill ISKE requirements for information system.	No
Are additional requirements contemplated?	No.	No
Are the requirements standard-based?	Yes (ISKE is standard based)	ISO 27001, NIST
Are requirements formalized in a policy document? Which format is used?	Yes. Concept of Estonian Government Cloud and Data Embassies.	Internal GRnet policy
What are the privacy regulations/laws you took into account?	The Public Information Act, Personal Data Protection Act, Regulation of Information Systems Security System, Information Society Services Act.	Hellenic Authority for Communication Security and Privacy (ADAE) law

	PLAN Phase	
Are there limitations for international transfer of data? Which ones?”	There are some limitations. The Public Information Act and ISKE regulation require regular audits of server rooms and audits of availability of services. In case of transferring data abroad this kind of audits are difficult to execute. Additionally Personal Data Protection Act requires permission of Estonian Data Protection Inspectorate for international transfer of data.	There is no international transfer of data.

A.2 DO Phase

	DO Phase	
	Security Controls	
Assessment Question	**Estonia**	**Greece**
Do you have a security control framework / checklist to assess the fulfillment of your requirements? How are security requirements mapped to security controls?	Yes. We have ISKE which is three level security framework for information systems.	Three security profiles, low, medium, high; different security controls (maturity levels) per security profile. Based on the 1st version of the CCM, but no categories per se, more high level security domains and controls.
Are security controls formalized in a policy document? Which format is used?	Yes. Regulation of Information systems Security System regulates implementation of ISKE.	N/A
Are security controls defined for the different security levels/risk profiles?	Yes	There is no categorization of controls. Their job is to protect simply the infrastructure, while the user himself handles his data's security (incident handling document). GR net is informing their customers according to the data they are handling which are the security controls they should take into account but they are not categorizing the ones they are performing (GRnet).

	DO Phase	
Could please describe the structure of your security control framework? (e.g. are security controls categorized? Which are the considered categories?)	Presentation about ISKE: https://www.ria.ee/public/ISKE/ISKE_english_2012.pdf (see also the table in the end). ISKE is based on a German information security standard - IT Baseline Protection Manual (IT-Grundschutz in German).	Categorization exists and is based on the ISO27K and the CCM (version 1). But the categorization is informal and comprises only of the parts/domains that fall into the IaaS protection.
Which are the specific security controls for each service model (IaaS, PaaS, SaaS)?	Currently we do not specify security controls of information systems based on service models. Security controls depend on specific database.	N/a
Which are the specific security controls for each deployment model (private, public, hybrid, community)?	Currently we do not specify security controls of information systems based on deployment models. Security controls depend on specific database.	N/a
Are the security controls compliant with any standard (e.g. NIST 800-53, CCM, ISO 27k)?	Yes. ISO 27001, ISO 27002, BSI (Bundesamt für Sicherheit in der Informationstechnik) 100-1, 100-2, 100-3 and 100-4.	They make use of the minimum requirements that are based in the security policy document provided by the Hellenic Authority for Communication Security and Privacy (ADAE) (based on ISO 27001 and NIST).
Are security controls formalized in a policy document? Which format is used?	Yes. It is officially regulated by following regulation: https://www.riigiteataja.ee/akt/13125331 (in Estonian).	Most of them are included in the incident handling policy of the GRnet. In the incident reporting policy there are security profiles and controls per profile and a check list in the end. – this cannot be shared with the public

	DO Phase	
	Implementation, Deployment and Accreditation	
Assessment Question	**Estonia**	**Greece**
How are security responsibilities defined and divided between the different parties (Gov Cloud, provider, customer, etc)? What are their roles and responsibilities? Does a contractual agreement designate the responsibilities of the parties (e.g. CSP, Cloud customer - local administration, etc) for the security of service provided via G-Cloud?	The owner of information system is responsible for fulfilling security requirements which are assigned to information system. The owner can also make contractual agreement, e.g. SLAs. G-cloud is designated with the highest security ranking which operating information systems in G-cloud have. For instance if G-cloud consists information systems with medium level and high level security class then G-cloud is always ranked with high level security class.	There is no contractual agreement, no contract no SLA, the customer has to agree with the terms of use and this is the proof of all the security requirements that need to be met. The GR net team explains to the customers in the terms of use the security controls that are being conducted and in some cases advises the IT dpt of the customer on the additional measures they need to take depending on the data/systems usage. GRnet (for OKEANOS and not only) provides physical security (servers, racks etc), server and VM security (operational systems and hypervisor security), isolation, traffic control and monitoring, incident handling and reporting. Okeanos, is responsible for the security of the service they provide. That is the servers' security and data storage in virtual machines. For example, if the user's website is hacked it is Okeanos responsibility to see that there won't be an attack to another virtual machine, through the first one. Their responsibility is to cut the "bad" traffic that generated from that particular IP since it belongs to the organization. On the other side, Okeanos informs the user of the attack but it is the user's responsibility to "clean" his website.
[if reply above is contract]How is the contract established?	SLAs	There is a high level contract (an agreement is the most correct term to use) that is done between the organisation (and the

	DO Phase	
		university in the case of Okeanos), which doesn't include in detail each of responsibilities user-Okeanos share.
Do you define a set of standard SLA, and in particular Security SLAs? Could you give us an example of SLAs or SLOs in use? Is it possible to negotiate the security contents of the SLA?	SLA requirements depend on assigned ISKE security risk class.	There is no specific SLA or SLO, all the terms and procedures are described in the terms of use, there is no possibility for negotiation (until not this wasn't requested by any customer). If a customer would need (after the services provision) additional security services, this can be considered as an update of the terms of usage and has to get the confirmation of the management board before implementation.
How do you assess / verify ex ante the suitability of a Cloud service to provide a sufficient level of assurance? Do you have in place a formal authorization and accreditation system? How does it work? It is directly managed by a National Agency (e.g. similar to US FedRamp)? It relies on commercially available certifications (which ones)? It is based on self-attestation /assessment?	Service has to pass ISKE accreditation process, which verifies if it is applicable. Or service has to have certificate from other similar standards (e.g. ISO, BSI) which corresponds to ISKE security classes. Accreditation is made by Information System Authority.	n/a – the procedure followed could be described as self-attestation/ assessment, that takes place in the end of every year (checking stats etc.) to see the level of security offered, but this is based on the internal policy of the provider, a report is produced that is not shared with the customer.
Is there any procedure for verifying that the initial	At the moment there isn't. However service accordance to ISKE can be pre-verified with ISKE implementation guide.	N/a

	DO Phase	
deployment (when the service is just launched and starts running) is SLA-conformant?		
[Optional] Are the deployment and verification procedures automatic or manual?	Manual	If we could say that the annual check is part of the verification process, then it is manual.

A.3 CHECK Phase

	CHECK Phase	
	Log/Monitoring	
Assessment Question	**Estonia**	**Greece**
Do you periodically check that the security requirements are met? How? Do you monitor the execution of the agreements (e.g. monitoring SLAs, audit the 3rd party, etc)? Which are the objects of monitoring?	The owner of information system is responsible for fulfilling the security requirements. There is no specific regulation.	Yes, twice per year. The objects that are monitored: network monitoring (traffic etc), web applications (vulnerabilities etc), systems monitoring + third party equipment (side of service). Traffic monitoring is followed by an analysis (server monitoring). Not monitoring execution of SLAs per se but the monitoring objects are also there in a check-list (process is established with all items described).
Which evidences are registered for analysis and documentation?	Security and availability incidents of the state information systems must be reported to CERT Estonia (CERT-EE). Security incident is a situation where the confidentiality, integrity and ability of the information system and/or the information of an organisation, institution or a person are being violated. Security incidents are also situations where somebody else's information system is used without an authorisation or its functionality is being deliberately interfered with.	They analyze the traffic monitoring on server level, e.g. if it has terminated unexpectedly.
Which tools are used for logging evidences/monitoring?	Availability of important services is logged by the owner of information systems, Information System Authority, etc.	Commercial tools: Linux scripts, Nagios expecting new equipment (install honey pots, IDS, IPS to enhance the incident/events management and to monitor the flow).

	CHECK Phase	
Is the monitoring scheme continuous or discrete?	Continuous scheme	It's continuous monitoring and can be done specific also
Are both operational and administrative levels covered in monitoring?	At the moment it is not defined. However RIA is monitoring the g-cloud and the state information systems. Additionally the owner of information system has also monitoring capabilities.	Yes both
Are log/monitor reports periodically generated? With which frequency?	Yes. Once a day.	Monitoring reports (statistic) 2 per year and a full security report in the end of the year (this also includes incident classification)
With which frequency are log reports send to the customer? What information do they contain?	Log reports are sent at least once in month. Plus whenever customer wishes.	Nothing is sent to the customer
Are incidents recorded and documented following a standard format? (e.g., VERIS)	Yes. However we are not using international standard. We have internal house format for that.	No
Are incident reports public or shared with 3rd parties?	Yes, if they are accredited and interested party.	No
	Audit	
Which audits are required to provide evidences that the agreed upon provisions in the SLA/local policy are actually fulfilled?	ISKE audit is required.	No audit from 3rd parties. Annually by the security officer, internal audit. By third parties there is a penetration test every six months.

	CHECK Phase	
Do the required audits need to be stated in the SLA/local policy?	Yes	No
Which are there different audit levels? (e.g., BASIC, INTERMEDIATE and HIGH)	There are no different levels. Audits are performed regularly.	There are different levels but always in application level not specific to security only.
Are the audits related to security certifications? (e.g., SGSI - ISO/IEC 27001, SGSI - ISO/IEC 27001)	ISO 27001 certification is required.	No, the usage of the service is different so doesn’t comply with a standard.
Which is the audit frequency?	Depends on security level of database. For high security level database once in 2 years. For medium security level database once in 3 years and for low security level database once in 4 years.	Twice per year
Who performs auditing?	Audits are performed by 3rd party and final audit must be signed by CISA (Certified Information Systems Auditor) certified auditor.	CISO of GRNET

A.4 ACT Phase

	ACT Phase	
	Changes Management	
Assessment Question	**Estonia**	**Greece**
How do you handle feedback from the CHECK phase? Which feedback triggers changes in the security programme and or Gov Cloud approach?	Changes are triggered by incidents or comments done by audit. Additionally development of information system may trigger changes in ISKE classification and ISKE methods.	Extra requirements by the provider have to considered by the CISO, then approved by the management board and then implemented (change in the terms of use, all customers accept etc.)
Which feedback trigger re-negotiation of the contract? How is the re-negotiation of the contract performed?	If requirements for information system (ISKE classification, system availability or security) changes then re-negotiations are performed.	If the organization considers that there is the need to include another feature in the system or change some term in the use of the system, it is included and then notified to the user to accept it (in the terms of usage). So re-negotiation is something that is born during operation from the organization's side, not the customers' side, for the time being. E.g. Someone set up torrent nodes, which created legal issues to the organization. They shut them and inform the user that that is a violation of terms of use.
Which changes trigger re-accreditation?	Re-accreditation is triggered by severe security incidents and by periodical ISKE audit results.	N/A

	ACT Phase	
Are the changes notified to the customer? How?	Yes, but the procedure isn't defined yet.	Example: if a violation happens, the customer will receive an email from the GRnet helpdesk as far as it concerns his own virtual machine. If a change in the terms of use is realized, the customer needs to accept the new terms.
[optional] What is the degree of automation of the triggered actions when a change occurs?		No.
Are there any procedures to detect and notify SLA violations? And is generation of "alerts" contemplated when the SLA is at risk of being violated?	Yes. Fulfilling SLA-s is monitored. Periodical reports are required and penalty measures are applied if agreements are not followed.	No it is ad hoc
Which mechanisms are put in place to guarantee continuity of operation in case of severe incidents?	There are no general mechanisms. However mechanisms are described in recovery plans of every information system.	Nothing specific due to the non-critical information handled until now
	Exit Management	
Assessment Question	**Estonia**	**Greece**
Do you have a procedure to deal with contract termination? E.g. are customer data securely deleted when the service is terminated? (e.g., a destruction certificate is issued by a 3rd party)	No	Usually when the customer himself doesn't want his data to be stored in the GR net Cloud he asks for a deletion. The accounts and data are then removed by the datacenter. The only case when the data are kept (and only for specific time) is when law enforcement is imposed. At any case the CSP doesn't have access to the data, they just continue hosting them until the forensics analysis is over.

	ACT Phase	
		No certification of destruction from a third party.
[optional] Are data given back to the customer in a portable standard format? Which format is used?	Yes/No. If "Yes", describe the format or name the standard.	N/a.