# Annex C. Questionnaire templates

The next templates, which are derived from the Security Framework presented on this report, are intended to be used by governmental Cloud stakeholders for gathering information regarding how their Gov Cloud infrastructure is or could be implemented from a security point of view. It is to note that, even if it is not explicitly stated for each question, all the aspects covered by this questionannaire refer to security (for example, when the template mentions SLA monitoring or SLA contents, it refers strictly to security monitoring and security contents in the SLA).

## D.1 PLAN Phase

| **PLAN Phase** | |
|---|---|
| **Risk Profiling** | |
| **Assessment Question** | **Description** |
| Do you have a National Information Asset classification scheme?<br>How do you classify government assets? How do you classify government assets and define the global risk profile? | |
| Which are the considered security dimensions? (e.g., Confidentiality, Integrity, …). | Name and semantic description |
| Do you have impact levels for each dimension?<br>How many categories or levels are considered for each dimension? | Scale and explanation of the levels. Description of the procedure to combine the security dimensions and to decide the final risk profile for the service. |
| [Optional] Are security dimensions aggregated into a final risk category? | Description of the procedure to combine the security dimensions associated to a service and to decide the final risk profile for this service. |
| [Optional] Do selection and evaluation of security dimensions comply with a security standard? | Yes/No. If "Yes", provide name of standard. If "No", describe the self-defined selection and evaluation criteria. |
| Arquitectural Model | |
| **Assessment Question** | **Description** |

| | |
|---|---|
| What are the security criteria and functional criteria for selecting IaaS, PaaS or SaaS? | Description of those criteria that are specific to select each particular Cloud service model. |
| What are the security criteria for selecting a Private, Public, Hybrid or Community Cloud? | Description of those criteria that are specific to select each particular Cloud deployment model. |
| Are the above criteria standard-based? | Yes/No. If "Yes", provide name of standard. If "No", describe the self-defined criteria. |
| Under which conditions is subcontracting permitted? | Description of conditions under the subcontracting of services by the CSP is permitted. |
| Security Requirements | |
| **Assessment Question** | **Description** |
| Which are the security requirements for the Cloud services? Is there a baseline or minimum? | Describe the categories into which security requirements are grouped and organized. Describe if there are mandatory requirements. |
| Are there specific security requirements for IaaS, PaaS or SaaS? | Describe the mandatory set of security requirements that must be met for each particular Cloud service model. |
| Are there specific security requirements for a Private, Public, Hybrid or Community Cloud? | Describe the mandatory set of security requirements that must be met for each particular Cloud deployment model. |
| Are additional requirements contemplated? | Describe additional requirements that go beyond the minimum set of mandatory requirements. |
| Are the requirements standard-based? | Yes/No. If "Yes", provide name of standard. If "No", describe the self-defined requirements. |
| Are requirements formalized in a policy document? Which format is used? | Yes/No. If "Yes", describe the format. |

| | |
|---|---|
| What are the privacy regulations/laws you took into account? | Name the applicable privacy laws. |
| Are there limitations for international transfer of data? Which ones?" | Describe the requirements that must be met for moving data outside the customer's country. |

## D.2 DO Phase

| DO Phase | |
|---|---|
| **Security Controls** | |
| **Assessment Question** | **Description** |
| Do you have a security control framework / checklist to assess the fulfillment of your requirements?<br>How are security requirements mapped to security controls? | Description of the method to map security requirements to security measures. |
| Are security controls formalized in a policy document? Which format is used? | Yes/No. If "Yes", describe the format. |
| Are security controls defined for the different security levels/risk profiles? | Yes/No. |
| Could please describe the structure of your security control framework? (e.g. are security controls categorized? Which are the considered categories?) | Describe the categories in which the security controls are grouped. |
| Which are the specific security controls for each service model (IaaS, PaaS, SaaS)? | Describe the set of security controls that must be activated for each service model. |
| Which are the specific security controls for each deployment model (private, public, hybrid, community)? | Describe the set of security controls that must be activated for each deployment model. |
| Are the security controls compliant with any standard (e.g. NIST 800-53, CCM, ISO 27k)? | Yes/No. If "Yes", provide name of standard. If "No", describe the self-defined controls, and underlying rationale. |
| Are security controls formalized in a policy document? Which format is used? | Yes/No. If "Yes", describe the format. |
| **Implementation, Deployment and Accreditation** | |

| Assessment Question | Description |
|---|---|
| How are security responsibilities defined and divided between the different parties (Gov Cloud, provider, customer, etc)?<br>What are their roles and responsibilities?<br><br>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? | Describe how the SLA contemplates responsible people at the CSP, as well as their responsibilities. |
| [if reply above is contract]How is the contract established? | Describe the mechanisms used to establish the contract between organization and CSP. |
| 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? | Describe whether the security content of the SLA is pre-established unilaterally by the CSP and must be accepted as-is, or if it is possible to negotiate the contents. If negotiation is possible, specify under which conditions. |
| How do you assess / verify ex ante the suitability of a Cloud service to provide a sufficient level of assurance?<br>Do you have in place a formal authorization and accreditation system?<br>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? | Describe the accreditation procedure. |
| Is there any procedure for verifying that the initial deployment (when the service is just launched and starts running) is SLA-conformant? | Yes/No. If "Yes", describe the mechanisms used to verify that the initial deployment is SLA-conformant. |
| [Optional] Are the deployment and verification procedures automatic or manual? | Describe the degree of automation of the service deployment and first SLA-conformance verification. |

## D.3 CHECK Phase

| CHECK Phase | |
|---|---|
| Log/Monitoring | |
| **Assessment Question** | **Description** |
| Do you periodically check that the security requirements are met?<br>How? Do you monitor the execution of the agreements (e.g. monitoring SLAs, audit the 3rd party, etc)?<br><br>Which are the objects of monitoring? | Describe the conceptual basis for monitoring. For example, monitoring can be based on supervising the contents of the SLA, or can be based on checking security controls, etc. |
| Which evidences are registered for analysis and documentation? | Describe all the information that is logged for further analysis both at the CSP and at the organisation. |
| Which tools are used for logging evidences/monitoring? | Describe the tools used for monitoring and data registration. |
| Is the monitoring scheme continuous or discrete? | Continuous/Discrete. If "Discrete", specify when monitoring tasks are performed. |
| Are both operational and administrative levels covered in monitoring? | Yes/No. (Operational refers to the operation of the service, whereas administrative refers to the data access made by CSP or customer administrators) |
| Are log/monitor reports periodically generated? With which frequency? | Yes/No. If "Yes", specify the frequency. |
| With which frequency are log reports send to the customer? What information do they contain? | Specify the frequency and content. |
| Are incidents recorded and documented following a standard format? (e.g., VERIS ) | Yes/No. If "Yes", name the standard. If "No", describe the format. |
| Are incident reports public or shared with 3rd parties? | Yes/No. If "Yes", describe the privacy preserving mechanisms in place. |
| Audit | |
| **Assessment Question** | **Description** |

| | |
|---|---|
| Which audits are required to provide evidences that the agreed upon provisions in the SLA/local policy are actually fulfilled? | Description of the method to map security requirements to security measures. |
| 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) | Name the different audit levels and describe them semantically. |
| Are the audits related to security certifications? (e.g., SGSI- ISO/IEC 27001, SGSI- ISO/IEC 27001) | Name the security certifications related to the audits. |
| Which is the audit frequency? | Specify the audit frequency. |
| Who performs auditing? | Specify if the audits are made by a 3rd party and under which conditions, or if the employed mechanism is self-auditing. |

## D.4 ACT Phase

| ACT Phase | |
|---|---|
| Changes management | |
| **Assessment Question** | **Description** |
| How do you handle feedback from the CHECK phase?<br>Which feedback triggers changes in the security programme and or Gov Cloud approach? | Describe those events that lead to a change in the G-Cloud approach and / or the security framework |
| Which feedback trigger re-negotiation of the contract?<br>How is the re-negotiation of the contract performed? | Describe those events that lead to a re-negotiation of the contract. Describe the re-negotiation procedure. |
| Which changes trigger re-accreditation? | For example architectural changes, or a change in the status of personnel security clearances, or a major security concern. |

| | |
|---|---|
| Are the changes notified to the customer? How? | Describe the mechanisms to notify changes to the customer. |
| [optional] What is the degree of automation of the triggered actions when a change occurs? | Describe the degree of automation of the tasks that are triggered when a change happens, e.g., some tasks may require the intervention of administrators. |
| 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/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? | Describe the mechanisms for business continuity. |
| **Exit management** | |
| **Assessment Question** | **Description** |
| Do you have a procedure to deal with contract termination?<br>E.g. are customer data securely deleted when the service is terminated? (e.g., a destruction certificate is issued by a 3rd party) | Yes/No. If "Yes", describe the mechanism. Specify the time required for data deletion. |
| [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. |