G-Cloud Service – Pan Government Security Accreditation Scope

This form is intended for Suppliers of services on the G-Cloud to complete.
Upon receipt, the G-Cloud Programme will check Section A, Reference information.
The CESG Pan Government Accreditor (PGA) looking at this has two goals in mind when reviewing this document:

- *To understand the scope of the service proposed and ensure all relevant aspects have been included in the boundaries;*
- *To identify and provide early feedback on issues that will make it difficult to accredit services at a later stage.*

Top tips

- *Be concise. This is not the place for marketing speak, the accreditor is not purchasing the service;*
- *Answer the question;*
- *You can provide supporting material to the scoping statement as long as the documentation has suitable identification (e.g. title, reference number and date), version number and the relevant paragraphs are referred to;*
- *Don't send documents that are not needed at this stage.*
- *Example answers to questions are shown in blue. Information to aide answering the question shown in italics.*

A. Reference information	
A0. G-Cloud Programme unique ID number for the service and version number of this scoping template *This should be a single Service ID unless it is the same service on different frameworks i.e. 3.G3…. & 4.G3….* *Other services based on a single service need to be submitted separately but can be linked in A0.1 below*	
A0.1 List technically related services that have been separately submitted but should be considered together. *Such as Gold Silver & Bronze versions of a service that have different Service IDs on the CloudStore. Note separate submission scope documents are required for each service being accredited but you can link them here.*	
A1. Supplier name	
A2. Service name and Type (Saas, Paas or Iaas)	
A3. Point of contact *Name, email address and phone number of the specialist that can carry out a dialogue and agree scoping statement with the programme and the Pan Government Accreditors*	
A3.1. Management Responsibility Name and contact details of a Chief Officer or board member responsible for security. *Name, email address and phone number*	
A4. Is this service PSNA Accredited or going through PSNA Accreditation? *Include PSN Unique service ID number*	
A5. Government Security Classification What is the Government Security Classification of the service? *State the Government Security Classification that you are seeking accreditation of.* *Example answer: OFFICIAL.*	
A6. ISO 27001 certification organisation	

Which organisation(s) will be used to conduct the audit and certification against ISO/IEC 27001 certification? As the certifying body must be accredited by UKAS, please also state the UKAS Reg No from http://www.ukas.com/about-accreditation/accredited-bodies/certification-body-schedules-ISMS.asp *Example answer: Certification Supplier name, UKAS Reg no 0999*	
A6.1. Status of ISO/IEC 27001 certification Please give the status of the above. If this is not yet achieved, please estimate the approximate month and year you think you will have achieved it.	
A7. Personal data Will the service be used to process or store personal data? *If this is the customers' option, answer Yes.* *If **Yes** you must complete & return **Appendix F: DPA Checklist For G-Cloud Suppliers**.*	
A8. Offshoring; sites, operations and data flows outside the UK Does the service use sites outside the UK to store, backup, process, transmit, manage or support? Include any third parties you use to provide the service in your answer.	
A9. Functional description of the service Provide a short description of the service in business language. *We are looking for a functional description of the service; including what business requirements the service meets. A logical diagram may be helpful. This is not the place for marketing speak.*	
A9.1. Maturity of the service. Clarify if this service is already in existence, currently in development or built to order.	
A9.2. Attached documentation List the documents and versions submitted.	

B. Scoping Information	
B1. ISO/IEC 27001 information What scope will be submitted for ISO/IEC 27001 certification? *Please supply the high level scope statement stated on your ISO 27001 certificate (if you have one) or that you propose to use.*	
B2. Technical description Provide information that describes the technical solution, including a simple diagram explaining the information assets and networks involved. A diagram will be helpful. If virtualisation is used, please ensure the hosting and	

underlying layers are explained. *We are looking for a technical description of the service. This is not the place for marketing speak.*	
B3. Physical sites and location of operations Where will the service be hosted? Please identify all the locations the service uses (including support locations and third parties) and describe the nature of the operation, service provided or data flow. *Please identify any overseas locations down to at least a country level and UK locations to town or city level.*	
B4. Network boundaries Describe the physical and logical network boundaries of the service. Diagrams may be helpful. Include any connectivity to PSN, noting that services will be connected to PSN DNSPs.	
B5. Support and service management including other organisations and third parties Provide a simple description of how the service will be managed and identify each high level process / group / service that supports your service. Include details of any service management including follow the sun / moon operations. For each process / group / service, identify the company performing the activity. *Identify all parties involved, recognising that organisations' structures, scale and degree of outsourcing is varied across G-Cloud suppliers. Example answer: My company name provides all the management and support. Another company name operate, host and manage the backup services.*	
B6. External interfaces and data flows Describe any extranet, internet or third party connections and associated data flows to/from the service. Include details of what types of data might traverse what network and the protection or encryption mechanism in use (for example PSN bearer, SSL). A logical diagram and / or data flow may be helpful.	
B7. Out of scope Are there any connections / processes / groups / services / third parties in any way associated with the service that you are identifying as out of scope of the ISMS? If it is not immediately obvious why this is the case please explain. A diagram may be helpful.	

C. Reliances

C1. PSN / G-Cloud reliances Does your service rely on any G-Cloud or PSN accredited infrastructure (IaaS), common elements or services? If Yes, please explain, and include PGA Accreditation Expiry dates. *Include any services that are planning to be or are known to be in the process of being accredited.* *Example answer: Yes - we use Company name, G-Cloud accredited IaaS service, PGA Expiry date: xx/xx/xx; We use the PSN DNSP supplier name, service name to provide our connectivity.*	
C2. Support for other services Are you aware of any G-cloud or PSN services that will have a reliance on your accredited service? If Yes, please explain. *Include any services that are planning to be or are known to be in the process of being accredited* *Example Answers: Yes - Supplier name, G-cloud Service name are planning on using our storage service as part of their accredited solution; The ID management solution is the same across all our services; the collaborative working zone is application the same for our service name1 and service name2.*	

D. Additional Information	
D1. Personnel security checking procedures Identify which of the Personnel checking levels below are in use for groups of staff or organisations that support your service: A. Equivalency with BS 7858:2006; B. Less than equivalent with BS 7858:2006; C. Baseline Personnel Security Standard (BPSS); D. SC clearance; E. DV clearance; F. Other – please explain. *Example answer: Our infrastructure administration team and Database Administrator (DBA) have SC clearance, the remainder of our staff are BPSS checked. All Third party supplier company name staff that support the service are also BPSS checked.*	
D2. User authentication requirements Identify the authentication methods in use for each group of staff or organisation that use the service, remotely connect, manage, support or administer the service: A. Anonymous, or no authentication; B. Username and password; C. Username, pin and multi-factor authentication code; D. Authentication based on end device characteristic (e.g. IP, device type, certificate, device connection method, etc.) – Please explain which. E. Other – please state. *Example answer: Our support team who access the service data, infrastructure administration team and DBA use C. username, pin and multifactor authentication and D. corporate machines with particular individual IP addresses. Users access the service using a B. username and password. Third parties remotely connect using C. username, pin and multifactor authentication to connect to our network from D. corporate machines with particular individual IP addresses and then use a different C. username, pin and multifactor authentication to connect to the customers' service to access the backups of customer data.*	

D3. Security Incident management Please confirm that you will report all service-related incidents (in line with the Govcert guidance) that potentially impact the G-Cloud consumer to the relevant point of contact within the public sector consuming organisation.	
D4. Business continuity, disaster recovery and backup arrangements Provide a description of business continuity, disaster recovery and backups arrangements for the service. *Include details of the level of service that will be provided for availability, e.g. is resilience built in to the service through the use of multiple data centres? Will there be a loss of service during switchover etc?*	
D5. Aggregation At what scale of customers, users, assets or data would you consider applying additional controls to protect your service from breaches of the confidentiality, integrity or availability of your service? How will you scale the security aspects of your solution as the number of consumers (and volume of data) grows beyond the scale identified? *Example answer: We would need to apply more sophisticated or automated identification of security events if we had more than 20 customers on our service.*	
D6. Forensic readiness Do you have a forensic readiness plan? If No or unsure, then summarise the functionality your service will provide in assisting consuming organisations with maintaining forensic readiness. *The aim is to enable consumers of G-Cloud services to establish if they need to use additional services in order to meet their requirements for forensics readiness. Example answer; We will provide customers details of our Forensics readiness plan so they can compare approaches and identify any shortfalls. We will retain and protect at the customers request any virtual / physical server initially for 30 days to support security incident investigation and further if requested.*	
D7. Data end of life management Provide a statement to cover BOTH: • How data is adequately removed from the service and access to any stored, or previously stored, data is rendered impossible when a consuming organisation ends their use of a service; • How data will be put beyond use when physical media is destroyed.	
D8. Protective monitoring Provide a statement on the functionality your service will provide in assisting consuming organisations with protective monitoring and accounting and audit. *For your service explain your logging arrangements (which may vary by level e.g. application, platform, database, operating system, hardware, etc), logging protection and storage duration or limits.* *Explain any Security event management (SIEM) solutions in use, and any SOC / NOC monitoring you will be doing and summarise the service*	

levels that are included in the service being provided. *Include whether the functionality provides evidential quality audit information to support disciplinary or legal action.* *Your statement should enable consumers of cloud services to establish if they need to use additional services in order to meet their requirements in these areas.*	
D9. Assurance plan List any assurance items that are relevant for your service that are planned or have already been undertaken or acquired, include: • Assurance activities. *For example, independent evidence of customer separation, Independent Penetration tests, third party design reviews, independent audits, Example answers: Jan 2012 Name of testing company, Fire wall rule set review; Dec 2011 Name of testing company2, Customer access Portal web application penetration test; Supplier name, External vulnerability scanning service reports daily new vulnerabilities found in the external facing IP ranges we use.* • Independently assured products used in the service. *Example answers; Product name, Supplier name, CAPS Assured Encryption product for VPN of remote workers; use of PSN bearer for transmission of data between data centres.; Product name, Supplier, CESG Commercial Product Assurance Scheme (CPA) product for disk encryption used to protect data on laptops used for managing client services.* *There is no need to send the actual assurance reports at this stage, during the accreditation assessment phase, the PGA may request full copies of the assurance reports.*	
D10. Any other information Provide any other information that may be relevant to the Pan Government Accreditor.	

E. Customer related	
E1. Deployment options Provide a summary of any deployment options and plans that highlight how the service must be implemented. *We are not interested in the pricing or commercial aspects, but to understand any variable or optional elements of the service that are being offered to ensure the scope of accreditation is set appropriately. An example answer might explain the different services that are automatically included in a service level Example answer: Our standard service does not include Protective monitoring or hourly backups (our standard service is targeted at development environments), these are only provided to premium service customers (typical operational environments).*	
E2. Security requirements on customers of the service Are there any security requirements that customers of your service must meet to use or to safeguard your service? *These are any security relevant requirements the service consumer is expected to follow including specific operating procedures that relate to security functions. There may be security related items in any Security Operating Procedures, IA conditions or terms of use that you have. Example answers; Customer must be GSI/GCF Code of Connection compliant; Customer must meet PSN IA Conditions; Customer is responsible for ensuring connecting machines have up to date anti*	

virus;	
E3. Residual risk and vulnerabilities Are there any significant or relevant security improvements that are currently planned? If yes, please summarise that improvement planned and the approximate implementation timescale. *Example answer: Intrusion detection system (IDS) expansion into DMZ 3 planned for Sept 2012.* Are there any currently known residual risks or vulnerabilities in the service that a customer needs to be aware of? If yes, please explain. *A residual risk might be outstanding issues from a penetration test or physical, personnel, procedural audits which have yet to be resolved that the service customer must understand and accept as part of usage.* *We recognise that:-* • *the full set of residual risks and vulnerabilities may not be known until the risk assessment process has been completed, but you must disclose any you know about now.* • *it may be necessary for certain information concerning vulnerabilities and residual risks to be documented separately and assigned a higher protective marking.*	
E4. Legal frameworks outside the UK Are there any legal frameworks (outside UK law) applicable the operation of the service (and therefore the information contained within it)? *If the service is a UK-only service using UK law answer as No. Consider all aspects of your service when answering this, including for example your sub-suppliers, sub-contractors and back-up and archiving facilities. Example answer: Yes, the Laws of California will be applicable to customers who choose to store data in that data centre, a UK only option is available.*	

F. Sign off	
F1. Confirmation Please confirm that (a.) You will have compiled the scoping template and will carry out the remaining security accreditation processes in accordance with the relevant IA guidance from the G-cloud programme. (b.) You will provide the agreed scope from this template and a copy of the relevant IA guidance from the G-cloud programme to the audit team carrying out certification against ISO/IEC 27001 and the scope and IA guidance have been taken in to consideration during the certification process. This must be confirmed by the ISO/IEC 27001 team as part of the certification and the report.	
F2. Confirmation of accuracy Confirmation by the Supplier that the statements in the scoping template and the referenced sections of any attached documentation are an accurate representation of the scope to be used for the security assurance and accreditation phases.	

For completion BY PGA Team once the above has been reviewed and agreed

G. Document / Assurance Checklist The following documentation is required as a minimum checklist when submitting the service for accreditation (i.e. after the scope has been agreed with the PGA)	
RMADS	*Lightweight RMADS required for OFFICIAL / Full RMADS required for SECRET/TOP SECRET*
Residual Risk Statement	*Required for all systems/services*
Risk Register	*Required for all systems/services*
ISO/IEC 27001 Certificate, report & improvement notice	*Required for IL22x systems/services*
Security Operating Procedures (relevant to the consumer and/or supplier)	*Required for all systems/services*
Other Security Related documentation such as IA conditions consumers are expected to meet	*Required for all systems/services*
Statement on personal data and a completed DPA questionnaire	*Required for all systems/services*
ITHC (scope and results) and other evidence of assurance (e.g. CPA certificate)	*Required for all systems/services, though the extent will be less for the OFFICIAL systems/services.*