G-Cloud or PSN Service Description and Commitment for Security Accreditation

This form is intended for Suppliers of PSN or G-Cloud services to complete.
Upon receipt, the G-Cloud or PSN 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 help answering the question is shown in italics.*

A. Reference information	
A0. G-Cloud or PSN Programme unique ID number for the service and version number of this scoping template	
A1. Supplier name	
A2. Service name *A short simple name for the service.* *Example answer: Email and collaboration service*	
A3. Is this a PSN service for accreditation? *If already accredited please state the unique PSN service ID number*	Yes / No / Already PSN accredited
A3.1 If **Yes** what type of PSN service are you asking to be accredited as?	GCN / PSNSP/ DNSP / Other
A3.2 If **Yes** is this a service for the PSN, but not to the PSN's encrypted domain; or the PSN and to the PSN's encrypted domain	To the PSN but not to the PSN's encrypted domain / To the PSN and to the PSN's encrypted domain / Unsure
A4. Is this a G-Cloud service for accreditation? *If already accredited please state the unique PSN service ID number*	Yes / No / Already G-Cloud accredited
A4.1 If **Yes** what type of Cloud service are you providing?	IAAS / PAAS / SAAS / Multiple / SCS / Other
A4.2 What is the BIL for confidentiality, integrity and availability of the service? *We are currently asking for BIL's only as the existing G-cloud frameworks have been let and are sold on that basis. We recognise that the ongoing use of BIL's is not ideal and is intended to be phased out as the new Classification scheme is recognised on future G-cloud frameworks. Please just state the BIL that you are seeking accreditation of. In most cases no further explanation is needed.* *Example answer: BIL 2-2-4 or BIL3-3-3.*	
A4.3 Service ownership Is this your service or are you reselling another accredited service?	Own / Reselling / Unsure
A5. Contact details **A5.1. Accreditation leader**	

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	
A5.2. Responsible Executive *Name, email address and phone number of a Chief Officer or board member responsible for security. This could be the same as A3.1. for small organisations, state if same as above rather than repeat.*	
A6. Readiness to accredit Briefly describe the readiness of your service for accreditation as at the time of this submission. *The programmes may consider your readiness when deciding which services to prioritise to pass to the PGA. Example answers: At the planning stage, not built yet; Built but not tested; Built but not in live use; Fully operational and tested; In use and already accredited for use by department X.*	
A7. Status of external certifications State the current status of the certifications below that cover the scope of your planned service. *These questions (A7 to A7.6.) ask about a range of certifications that you MAY or MAY NOT have. The PSN/ G-Cloud programme guidance will drive which certifications (if any) you need to have.*	
A7.1 ISO27001 certification *If a certification is not yet achieved and planned, please estimate the approximate month and year you think you will have achieved it.*	Certification Achieved / Not started / In progress / Expired
A7.2. If **achieved** or is **in progress** which organisation(s) is being 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*	
A7.3 Cloud Security Alliance CSTAR *If a certification is not yet achieved and planned, please estimate the approximate month and year you think you will have achieved it.*	Self certified / Independent Certification Achieved / Not started / In progress / Expired / Not planned
A7.4. If Independent Certification has been achieved or is in progress, which organisation(s) is being used to conduct the audit and certification *Example answer: Certification Supplier name, UKAS Reg no 0999*	
A7.5 CESG Assured Service (Telecoms) CAS (T) *If a certification is not yet achieved and planned, please estimate the approximate month and year you think you will have achieved it.*	Certification Achieved / Not started / In progress / Expired / Not planned
A7.6. If Independent Certification has been achieved or is in progress, which organisation(s) is being used to conduct the audit and certification *Example answer: Certification Supplier name, UKAS Reg no 0999*	
A8. Personal data Will the service be used to process or store personal data?	Yes / No If **Yes** have you included a completed **Appendix**

*If this is the customers' option, answer **Yes**.* *If **Yes** you must complete & return Appendix 1 :DPA Checklist* ***Appendix 1 is identical to the G-Cloud Appendix F: DPA Checklist For G-Cloud Suppliers ,and can be interchanged, but now applies to PSN & G-Cloud suppliers.***	**1: DPA Checklist** or Appendix F: DPA Checklist For G-Cloud Yes / No
A9. 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.	Yes / No / Unsure
A10. 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, showing key datastores and key dataflows may be helpful.*	
A11. Attached documentation List the documents and versions submitted.	

B. **Reliances & linked services**	
B1. PSN / G-Cloud reliances Does your service rely on any G-Cloud or PSN accredited services? If Yes, please explain. *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 infrastructure hosting service; We use the PSN service name, Service number to provide our connectivity.*	Yes / No
B2. 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.*	Yes / No
B3. Related Services 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.*	

C. Scoping Information	
C1. 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.*	
C2. 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.*	
C3. 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.*	
C4. Network boundaries Describe the physical and logical network boundaries of the service. Diagrams may be helpful. Include any connectivity to PSN, noting that BIL 3-3-x services will be connected to PSN DNSPs.	
C5. 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 the supplier community. Example answer: My company name provides all the management and support. Another company name operate, host and manage the backup services.*	
C6. 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.	
C7. 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.	

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 or PSN consumer to the relevant point of contact within the public sector consuming organisation.	Yes / No / Unsure
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 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.*	Yes / No / Unsure
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 audit.*, *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.*	Yes / No

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.*	Yes / No
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.*	Yes / No / Unsure

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 have read and understood the PSN RMARD (c.) 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. (d.) You understand IT Security Health Check reports are required annually, or as directed by the PGA, to maintain accreditation	Yes / No ←*G-Cloud ONLY* Yes / No ←*PSN ONLY* Yes / No Yes / No
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.	*Signature and role of the authorised representative of the supplier.*

Appendix 1: DPA Checklist for PSN and G-Cloud Suppliers

The following is the Checklist for Suppliers of PSN and G-Cloud Services and is based on the Information Commissioner’s PIA Handbook and Personal Information Online (code of Practice).

Suppliers of PSN / G-Cloud services will generally be ’Data Processors’ under the Data Protection Act (DPA). The organisations using their services will generally be ‘Data Controllers’. Data controllers have the legal duty to comply with the DPA. However, service providers can help them to do this by ensuring that their IA documentation for PSN/G-Cloud provides clear evidence of how their service will allow the consuming organisation to complete its Privacy Impact Assessment and in turn to comply with the DPA. Please note that reference to “Personal Data” in this checklist also includes Sensitive Personal Data (as defined under the DPA). Therefore, the PSN & G-Cloud programmes are expecting suppliers to demonstrate that their services are appropriate for Sensitive Personal Data.

Please note that the advice of the ICO to consuming organisations is that if the service supplier cannot provide satisfactory answers to any of the questions below, then this should raise concerns about the supplier’s ability to look after the information you have entrusted to it. If this is the case, potential consumers should not use the provider concerned and should seek alternatives. Remember that the ultimate responsibility for information remains with the ‘data controller’.

ID.	**Service supplier checklist**	**Evidence, including paragraph-level reference to corresponding IA documentation**
1.	Can you provide written guarantees about your security arrangements?	
2.	How will you guarantee that you will only process personal data in accordance with your clients’ instructions, e.g. How will you maintain an appropriate level of security? Ensure that personal data will not be retained for longer than instructed?	
3.	How will you guarantee that your staff are trained and vetted to suitable standards, wherever they are based?	
4.	What are your complaints and redress procedure, e.g. do you offer compensation for loss or corruption of clients’ data?	
5.	Can you ensure that any information identified as ‘personal data’ within the information provided to you will be protected adequately, e.g. prevent any unauthorised or unlawful processing of personal data within the service? Does your service allow the Data Controller to create and maintain a comprehensive and up to date record of personal data usage? What facilities do you have that would help your client to locate all personal data items falling within a ‘subject access request’ as defined by the DPA?	
6.	What facilities do you have to comply with your client’s instructions on (a.) rectification, (b.) blocking, (c.) erasure, or (d.) destruction of personal data? Note that the instructions to carry out these measures may be placed on the Data Controller by Court Order.	
7.	If information is not erased or destroyed as a result of positive instruction from the consumer (see question (6.)), how long will data is likely to be retained and in which forms)?	

	What are the best and worst cases for when suppliers can give assurance that the information will have been overwritten (include the retention on archive and back up systems).	
8.	How does your service allow the client to change/restrict the use of particular personal data items?	
9.	Does your service offer the ability to flag records for review /deletion? If so how is this achieved?	
10.	How can you help your client to maintain the accuracy of the records at all times (e.g. the Integrity of the information)?	
11.	Can you provide your consumers with copies of their information regularly, in an agreed format and structure, so that they hold useable copies of vital information at all times?	
12.	Can you ensure that your service will continue to maintain high data protection standards, taking in to account the development in security products and the cost of deploying or updating these?	
13.	How do you restrict access to personal data by members of your own staff? What reporting arrangements will you have in place, for example for informing your client of a security breach?	
14.	Can you provide any guarantees as to where personal data will be located geographically? Note that the DPA contains rules about the transfer of personal data outside the EEA. This means that you should be able to tell your clients where any of the personal data they provide to you is located at any particular time. .	
15.	If your service will involve personal data being outside the EEA, what measures are in place to ensure that levels of protection during its transfer, storage and processing are adequate?	
16.	Can you ensure that your service will continue to maintain high data protection standards even if you store data in a country with weak, or no, data protection law, or where governmental data interception powers are strong and lacking safeguards?	
17.	Can you guarantee the reliability and training of your staff, wherever they are based? Do they have any form of professional accreditation?	
18.	What capacity does the service have for recovering from a serious technological or procedural failure? E.g. human error, computer virus, network failure, theft, fire, flood, other disasters	
19.	How will you demonstrate ongoing compliance with the assurances you have given?	
20.	How will you report breaches of security and security incidents to your client?	

For information about overseas transfers, see: *http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx*

Further guidance is available in The Guide to Data Protection at: *http://www.ico.gov.uk/home/for_organisations/data_protection_guide.aspx*

The ICO code of practice on managing personal information online is available at:
http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/online.aspx

Appendix 2: For completion by the PGA Team once the above has been reviewed and agreed

Required	**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)*	
	Full RMADS	*PGA to confirm if full RMADS needed, in line with the PSN or G-Cloud programme guidance documents.*
	Residual Risk Statement	*Required for all services.*
	Risk mitigation plan	*Required for all services with outstanding risks from ITHC or where there have been risk improvements identified as needed.*
	ISO/IEC 27001 Certificate, Report & any improvement notice, Statement of Applicability.	*Required for all services where the assurance relies on ISO27001.*
	Procedures that support secure operation of the service, or Security Operating Procedures (relevant to the consumer and/or supplier)	*Required for all services.*
	Incident management procedures	*Required for all services.*
	Security Related documentation such as IA conditions that service consumers are expected to meet	*Required for all services that impose security requirements on their customers as a condition of taking a service.*
	Completed DPA questionnaire (Appendix 1 or G-cloud Appendix F)	*Required for all services that will be used to process or store personal data.*
	ITHC (scope and results)	*Required for all services.*
	Other evidence of assurance (e.g. CPA certificate)	*PGA to identify items required.*
	CAS (T) Certificate and Report including the SoA against the Security Procedures for Telecoms Systems and Services (SPTSS) controls.	*Required for all services where the assurance relies on Cas(t). Usually required for PSN connectivity services.*
	CSTAR Certificate	*Optional required, dependent on service being assured. Required for all services where the assurance relies on CSTAR.*