Completion of this tab is not required if you are not processing using an electronic system

Suppliers of systems to the CCG that utilise cloud based computing resources are requested to provide their approach to the following areas of information / cyber security.

This section is to be completed by the supplier

No	Question	Response	IT Security Notes
1	All of the usual information security concerns still exist; simply in a cloud context instead[1]. What security standards are you certified against? What policies do you employ?		
2	Using cloud brings the norm of a shared responsibility model, dependent on the service model[2]. For SaaS, the cloud provider (CP) is responsible for all aspects of security, except application user entitlements. With PaaS, the CP is responsible for the platform component security, the cloud consumer (CC) for everything they implement on those platforms. For IaaS, the CP has foundational security responsibility; CC everything else. How do you reflect this approach?		
3	Information system development lifecycle stages apply: solution / cloud requirements; selection of a cloud provider (ref. C-Star registry); definition of cloud architecture; assessment of security controls3; design of controls for security gaps; management of changes. How to do you employ these management processes?		
4	All major cloud technology providers will have certifications and attestations for the security of their operation (e.g. ISO27001). Although compliance inheritance applies, the cloud is only one component and the security of the solution as a whole will still need to be assessed. What practices do you implement separate to the cloud provider's processes?		
5	Governance and enterprise risk management considerations: What is your governance structure? What is the outline of your organisation's framework? How are information security risks managed? What compliance objectives do you need to meet?		
6	Information 'life-cycle' aspects (creation, storage, classification, location, use, sharing, archiving, destruction) along with the volatility of compute resources must be defined, with consideration given to the deployment model. How are these incorporated into the solution architecture?		
7	Cloud technology specifics need to be assessed for IaaS and PaaS, such as management plane access controls, software based infrastructure code management, network segregation. What is your approach to theses technology deployment concerns?		
8	Business continuity, resilience aspects and incident response processes (including cyber incidents). How are these addressed?		
9	Application security (designed and built-in defences and vulnerabilities) – how are these managed? What practices do you use?		
10	User access controls technologies – what is your approach to managing user accounts, both in the solution and in your business?		
11	How data encryption technology deployed for both data in transit and at rest? What encryption is built into the solution? Broadly, how are encryption keys managed?		
12	Cloud technology advantages should be leveraged in applications. Lift-and-shift deployments avoided. How does your application reflect this principle?		
		Yes/No	**Further info**

Do you have Business insurances? e.g. professional indemnity, employer's liability, public/product liability.		
ISO 27001 / ISO 27002		
Cyber Essentials		
Do you have any of these:	**Yes/No**	**Further info**
ISO 9001 (Quality Management System)		
ISO 29100 (Privacy Framework Standard)		
ISO 27017 (Cloud Specific Controls)		
ISO 27018 (Personal Data Protection)		
ISO 27701 (Privacy Information Management System)		
PCI DSS		
G-Cloud Framework		
IASME Governance Standard		
Cloud Computing Standards		
SOC Report		
Transaction Monitoring		
Any other compliance programme you have that is not listed here, please list them in the next column		
Have you had a Data protection or cyber security breach within the last 3 years requiring external reporting i.e. to ICO, European Supervisory Authority, NCSC		
International data transfers scheme Do you have approriate safeguards to make a restricted transfer of personal data outside of the UK/EEA, i.e. Privacy shields, BCR, standard contractual clause		