Technical

Cloud Assurance Questions
(adapted from ICO)

Updated on 06/01/2023

Introduction

Cloud computing is a means for services to be developed and hosted by a third party supplier, and remotely accessed by LSE as users of the service. Using Cloud services means LSE information gets stored outside LSE, and so we rely on the supplier to ensure our data are stored in the right way. There are different forms of cloud computing, the most common of which are:

- SaaS (Software as a Service) – applications built and hosted by a provider, on their own systems and infrastructure, which are then accessed over the Internet
- PaaS (Platform as a Service) – a platform through which we can develop web-based applications that are hosted on third-party infrastructure
- IaaS (Infrastructure as a Service) – compute resources, storage and networking that are configured and operated by us, but owned and hosted by a third party are offered for use on demand. Most typically, projects will be dealing with SaaS solutions. It is the responsibility of the project to establish whether the risk of storing the data in a cloud application, building a web application on cloud infrastructure, or using cloud compute is acceptable. In order to assess this the below questions need to be answered by the business and the chosen cloud provider, following which the responses need to be collated and provided to the LSE DTS Cyber Security and Risk Management team for review.

GDPR

LSE is required to comply with the General Data Protection Regulation, which mandates how Personally Identifiable Information must be controlled, processed and secured. In particular, it is important to note that Personally Identifiable Data can only be stored outside the EEA if:

- The EU has judged that the country has equivalent data protection laws (e.g. Canada)
- The supplier is in another international country and has signed standard contractual clauses with the School or is willing to offer to sign such clauses.

Data Owner

Data Ownership Principles

- Each data set has only one data owner or data domain owner
- Data is understood and treated as an asset
- Data is managed and used holistically. Silos or functional barriers should not hinder the holistic approach to data value, outside legitimate agreed confidentiality issues.
- Data is fit for purpose
- Changes in a data set must be advised to consumers of that data

Data Owner Role Summary

Data Owners are senior individuals accountable for the quality of one or more data sets. Data Owners are responsible for:

- Approving data definitions
- Approving data criticality classifications
- Directing/overseeing data quality activities
- Attending the Data Governance Strategic Group
- A Data Owner will usually be a Head of Department but, by exception, can be a different level. The criticality and sensitivity of each data set will be assessed to determine who is the appropriate Data Owner.

A Data Owner may appoint one or more subject matter experts in their data domain as Data Stewards to undertake day-to-day Data Governance responsibilities.

Data Protection Impact Assessment (DPIA)

Filling in the form

Questions within Section A are to be answered by the project team that's commissioning the solution, and questions in Section B are to be sent to the chosen provider requesting a response to every question.

Section A – Questions to be answered by the LSE Project team

1.1	Make a list of the data you hold that will be stored and / or processed in the cloud. If unsure, please inquire the cloud provider.
Response	
1.2	If any of the personal data listed here meets one of the below criteria: • Special categories personal data as defined by the GDPR

	• A new method of processing personal data. New can mean new to the School • Large aggregates of personal data from separate sources • Or any other of the triggers listed on the form mentioned below You are required to fill in a Data Privacy Impact Assessment (DPIA). You can download the DPIA here. Please discuss your DPIA with the School's Data Protection Officer (DPO) Rachael Maguire. Please indicate below when you have completed a DPIA below.
Respons e	DPIA completed (Y/N)

To be completed by Information Security			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

2.	For each item on the list can you state whether it should be classified as Confidential, Restricted, Internal Use or Public. See LSE's 'information classification standard' for help: https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecStaIT.pdf

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

3.	For listed items marked 'Confidential' or 'Restricted', identify the owner of that data. This will normally be the head of the division or department from where the data originates. Have the data owners given their consent?

Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

4.	What are the data deletion and retention timescales? Please refer to the School's Retention Schedule (retSch.pdf (lse.ac.uk)) for guidance. If still unsure, please speak to the School's DPO (Rachael Maguire)
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

5.	If there was a major outage at the cloud provider how would this impact on your business? (*i.e. think about the criticality of your system and impacts on your business continuity in case of disruption or loss of the system. Note that the cloud provider shall store the data in multiple datacentres if the system is considered mission critical to your department or LSE.*)
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

6.	If you were to go with your chosen cloud provider, will you have a written contract in place?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

7.	Do you require a test environment? YES / NO / NOT SURE **Important Note:** Under GDPR, Personally Identifiable Information cannot be held in test environments.
Respons e	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

Section B – Questions to be answered by the proposed Cloud Provider

1.	Please provide details of appropriate third-party security assessment. For example, regular vulnerability or penetration tests of your data centre and systems. Also please detail if you perform internal and external penetration tests, and what scope the tests cover. Can you also please confirm if critical, high and medium risks findings from your most recent penetration test have been remediated.
Respons e	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Follow up Required			

2.	Provide details of any industry code of practice or other quality standard for your security assessment, e.g. ISO27001, ISO9001, SOC2; if you are working towards certification; or if you do not hold any certification.

Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

3.	How quickly will you react if security vulnerability is identified in your product?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

4.	How will you notify us once security vulnerability has been identified?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

5.	What are the timescales for you suspending and deleting accounts?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

6.	Do you integrate with LSE's Active Directory (AD) or Azure Active Directory (AAD)? If you do not integrate with AAD, what is your password policy, and can MFA be enabled on accounts?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

7.	Does your solution involve an email service? If so, is there a requirement of sending emails to LSE users from your infrastructure? Is there a need for the emails to look like they come from an @lse.ac.uk address?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

8.	Is all communication in transit encrypted? Please provide protocols used.
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

9.	Does the hosting agreement include end-of-life data destruction?

Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

10.	Will you delete all our data securely, to a non-recoverable extent, if we decide to withdraw from your service? Please provide technical details of the method you use and timescale of the data deletion.
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

11.	Will our data or data about our cloud users be shared with third parties or shared across other services you may offer?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

12.	Describe any audit trails that are in place so you can monitor who is accessing which data? How long the logs are stored?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	

Further comments	
Follow up Required	

13.	Will you allow us to get a copy of our data, at our request, in a usable format? If so, please specify the formats available.
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

14.	How quickly could you restore our data (without alteration) from a back-up if you suffered a major data loss? What is your RTO and RPO please?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

15.	Do you have sufficient capacity to cope with a high demand from a small number of other cloud customers?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

16.	How could the actions of other cloud customers or their cloud users impact on the quality of the service you provide to us?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

17.	Please provide details of any guarantees you have on service availability.
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

18.	Please provide details of any exclusions to the service availability guarantee e.g. maintenance windows
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

19.	How will you communicate to us changes to the cloud service which may impact on our agreement?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	

Further comments	
Follow up Required	

20.	If a test environment is needed, what security controls are in place to protect the test environment?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

21.	If you provide a test environment, is any Personally Identifiable Information anonymised? If so, how?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

22.	List the countries where you will process our data and describe the data safeguards that are in place for each location.
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

23.	Is the data kept in a single datacentre or multiple datacentres? If multiple, where are they? Do you own the datacentres, or are you renting space and or services from a datacentre provider?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

24.	Describe any circumstances under which our data may be transferred to other countries?
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			

25.	Can you provide encryption for data at rest? If so, please provide details of ciphers used.
Response	

To be completed by LSE DTS Cyber Security & Risk Management			
Risk Level (RAG)		**Risk Owner**	
Further comments			
Follow up Required			