Technical

Cloud Assurance Questions for Commissioning Teams in LSE

(adapted from ICO)

Updated on 12/11/2024

Introduction

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.

It is the responsibility of the commissioning team at LSE 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 for us to assess your requirements and advise on the suitability of any solutions, you need to answer the below questions.

There is another form, Cloud Assurance Questions for Suppliers, that the provider of any solution will need to fill in.

Both your response and the supplier's need to be provided to the LSE DTS Cyber Security and Risk Management team for review.

Legal note – UK GDPR

LSE is required to comply with the UK's 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 UK / EEA if:

- The EU has judged that the country has equivalent data protection laws (e.g. Canada, Japan)
- 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
- 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
- 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.

Questions on this form are to be answered by the team that's commissioning the solution.

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

Name of requestor:
Department/division of requestor:
Name of software:
Please share a link to the provider's website:

Please write a short description (2-5 sentences) explaining the scope of the project and how this product will meet your requirements.

Are there any existing LSE provided tools/software that meet your project's requirements?

How many LSE users will use this product? – individual only, small project team, department/division, LSE-wide

- Small project team, please provide the names of other LSE users?
- For departments/divisions, please provide HoD:
- LSE-wide tender, please contact Tony Payne, Director of Strategy and Architecture.

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.
Response	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
Response	

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.
Response	

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