CLOUD VENDOR ASSESSMENT CHECKLIST

A cheat-sheet to assess your cloud vendor.

S. No.	Question	Response	Mitigation Required?	Comments (Action/Impact)
Regulations & Certifications				
1.	Is the cloud vendor compliant with international standards and quality frameworks like **ISO 27001, ISO 27017, ISO 9001, SOC1, SOC2, SOC3,** etc.?	☐	☐	
2.	Is the data collected out of the system stored, processed and managed based on the applicable regulations (such as GDPR applicable to the specific region)?	☐	☐	
Privacy & Security				
3.	Is the data protected and encrypted in the cloud?	☐	☐	
4.	Is the cloud service provider transparent about their data center locations?	☐	☐	
5.	Are adequate controls in place to protect the physical security of your facility, servers, etc. to prevent the data loss and breach?	☐	☐	
6.	Are network security controls like firewalls placed to prevent unauthorized access, protect data and information, etc.?	☐	☐	
7.	How do you prevent the introduction of viruses into work products, tools, network servers, etc.? Are virus scans performed on the product before being released?	☐	☐	
8.	Do all your employees sign a Confidentiality Agreement that also includes procedures for handling breach of confidentiality?	☐	☐	

ZIFO
RnD SOLUTIONS

CLOUD VENDOR ASSESSMENT CHECKLIST

S. No.	Question	Response	Mitigation Required?	Comments (Action/Impact)
Back-up & archival				
9.	Are adequate back-up and archival procedures put in place that demonstrate compliance to applicable regulations like 21 CFR, EU Annex, etc.?	☐	☐	
10.	Do you have a procedure for backup and restoration processes? How often do you perform restoration tests?	☐	☐	
Data security on the cloud				
11.	Has the cloud service provider shared established, documented and proven processes for dealing with planned and unplanned down-time?	☐	☐	
12.	Are risk evaluation and mitigation strategies clearly defined by the vendor?	☐	☐	
13.	Has the cloud service provider shared details regarding data hosting?	☐	☐	
14.	Does the vendor provide Single tenant and or multi-tenant cloud? If they are providing multi-tenant cloud, are data security and confidentiality aspects in place to ensure the data that is stored in the cloud is secure?	☐	☐	
15.	Are sub-contractors/third-party vendors involved in the provision of the cloud services? For example, SaaS providers often build their services on existing IaaS platforms, so it must be clear how and where the service is being delivered. Do they have an SLA established for the same? (Note: Refer to the ISO standards ISO/IEC 19086-1:2016 for SLAs)	☐	☐	
16.	Does the cloud service provider offer comprehensive Data transfer and migration services?	☐	☐	
17.	Do you have a procedure on the Disaster Recovery process with a specific maximum tolerable downtime in the event of a disaster?	☐	☐	

CLOUD VENDOR ASSESSMENT CHECKLIST

S. No.	Question	Response	Mitigation Required?	Comments (Action/Impact)
Personnel and Training				
18.	Are personnel trained on Security Policies?	☐	☐	
19.	Are qualification records and training logs of your employees maintained?	☐	☐	
20.	Are employees trained on applicable regulatory requirements? Are these documented?	☐	☐	
Cloud Infrastructure				
21.	Has the vendor shared an overview of cloud infrastructure?	☐	☐	
22.	Is a preventive maintenance for the cloud infrastructure planned?	☐	☐	
23.	Has the vendor validated / qualified the cloud infrastructure?	☐	☐	
24.	In case of a change to the cloud infrastructure / upgrade or migration activities, would you be informed by the vendor?	☐	☐	
25.	Has the vendor defined criteria where a revalidation / re-qualification of the infrastructure is required?	☐	☐	
Necessary Documentation				
1.	Development Process	☐	☐	
2.	Validation Process	☐	☐	
3.	Infrastructure qualification Process	☐	☐	
4.	Automated deployment Process	☐	☐	
5.	Configuration logs	☐	☐	
6.	Source code	☐	☐	

ZIFO
RnD SOLUTIONS