Microsoft

Cloud Services Due Diligence Checklist

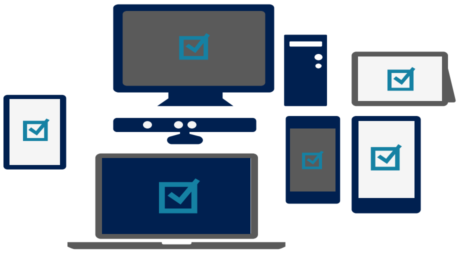
The multitude of cloud service options and service providers can cause challenges for organizations that want to move to the cloud and consume cloud services. The pressure caused by regulations and standards covering a wide range of topics—security, privacy, trust, personal information, and business-specific needs—further complicates these challenges.

Why use this Checklist?

This Checklist is based on international standard ISO/IEC 19086-1, the Cloud Computing Service Level Agreement Framework. This Checklist can guide and help drive discussions about moving to the cloud. It will support your move to the cloud holistically and empower you to conduct a meaningful due diligence evaluation of cloud services.

Audience

- Risk Management
- Procurement
- Legal
- CIO



How to use the Checklist?

This Checklist raises key considerations as you move to the cloud. Different organizations and cloud projects should place different requirements for each element. In order to deploy the Checklist for cloud due diligence evaluations, organizations need to define the organizational cloud requirements for applicable Checklist elements, define the project specific requirements, and assess project options accordingly. Detailed guidance is available from the instructional guide and video for the use of this Checklist.

Performance

Availability	□ The percentage of time that the service is available and usable.
Capacity	□ The number of simultaneous connections. □ The maximum capacity of resources. □ The number of inputs that will be processed over a period of time. □ The amount of data that will be transferred over a period of time.
Elasticity	□ How fast and how precise the service can adjust to the amount of resources that are allocated.

Service	
Service monitoring	□ The parameters and mechanisms to monitor the service.
Response time	□ The maximum, average, and variance in response time.
Service resilience/ fault tolerance	□ The methods used to facilitate resilience and fault tolerance (include mean times, maximum times, and units of measurement).
Disaster recovery	□ The maximum time required to restart the service in outage. □ The maximum time prior to a failure during which changes may be lost. □ The recovery procedures to restore the service and data.
Backup and restore data	□ The number of data backups made in a period of time. □ The methods of backup and backup verification. □ The backup retention period. □ The number of backups retained. □ The location of backup storage. □ The number of restoration tests and the availability of test reports. □ The alternative methods for restoring data.
Cloud service support	□ The available support plans, associated costs, and associated hours of operation. □ The specific contacts for service support. □ The service support methods (phone, web, tickets). □ For incident support: the incident support hours, levels of support, response time (average and maximum), reporting methods, and notification terms.

Data Management

Cloud service provider data	❑ Define cloud service provider data.
Cloud service customer data	❑ Define cloud service customer data and usage terms.
Intellectual property rights	❑ Describe any intellectual property rights the cloud service provider claims on cloud customer data and vice versa.
Account data	❑ List the required account data fields (names, addresses, etc.).
Derived data	❑ Define the types of derived data and policies for use/access.
Data portability	❑ Data portability capabilities including methods, formats and protocols.
Data deletion	❑ Define the minimum and maximum times to completely delete cloud service customer data. ❑ Describe the data deletion process. ❑ Describe the data deletion notification policy.
Data location	❑ List the geographic locations that data may be processed and stored, and if the cloud service customer can specify location requests.
Data examination	❑ Describe how the cloud service provider examines cloud service customer data.

Governance

Accessibility	□ List accessibility standards, policies, and regulations met by the service.
Roles and responsibilities	□ The roles and responsibilities for the parties.
Personally identifiable information (PII)	□ The PII protection standards met by the cloud service provider.
Information security	□ The information security standards met by the cloud service provider.
Termination of service	□ The process of notification of service termination, including the length of time that data and logs are retained after termination, the process for notification, and the return of assets.
Changes to features and functionality	□ The minimum time between service change notification and implementation, and service change notification method. □ The minimum time period between the availability of a feature/function and the deprecation of that feature/function.
Law enforcement access	□ The policy for responding to law enforcement requests of cloud service customer data.
Attestation, certification, and audits	□ List/define the standards, policies, regulations, and applicable certifications that the cloud service provider attests to. Include audit schedule and location policies.

ISO/IEC 19086-1 Clause Mapping

Accessibility	Clause 10.2	**Roles and responsibilities**	Clause 9.5
Availability	Clause 10.3	**PII**	Clause 10.5
Capacity, Elasticity, Response time	Clause 10.4	**Information security**	Clause 10.6
Service monitoring	Clause 9.4	**Termination of service**	Clause 10.7
Service resilience/fault tolerance, Disaster recovery, Backup and restore data	Clause 10.11	**Changes to features and functionality**	Clause 10.10
Cloud service support	Clause 10.8	**Law enforcement access**	Clause 10.12
Data Privacy and sub-sections	Clause 10.12	**Attestations, certifications, and audits**	Clause 10.13 and 10.9

Please note that this Checklist is not intended to be and should not be considered a substitute for ISO/IEC 19086-1. To obtain access to the full text of this standard, please see the ISO/IEC 19086-1 webpage.