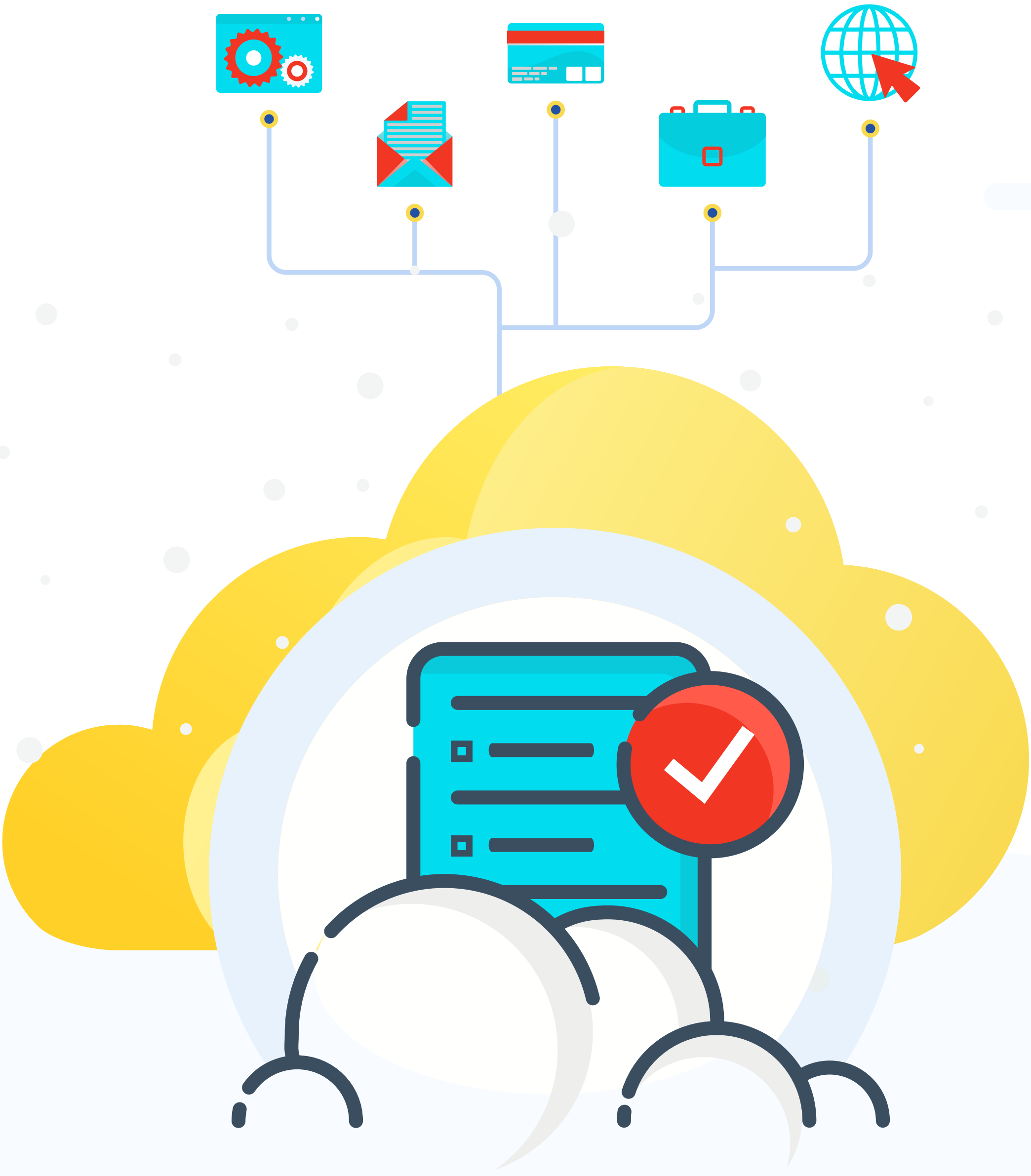
net solutions

21-Point Cloud Services Provider Due Diligence Checklist



What You’ll Learn:

This tool will help you select a cloud services provider best suited for your requirements by providing a framework that covers all important aspects you need to evaluate to choose between different options.

If you are starting off, you can use it to compare different providers to make a decision. On the other hand, if you are already leaning towards a specific cloud services provider or have chosen one, you can use it to ensure your preference is the right match for you.

Please note that all sections may not apply to you and some sections may be of higher importance to you than others based on business goals and other requirements.

Identify Your Requirements

1.

List your technology requirements.

- □ Identify whether you need infrastructure (IaaS), platform (PaaS), or managed (SaaS) services.
- □ Create a list of all technologies (languages, databases, etc.) & services (DNS, CDN, etc.) that you need the cloud services provider to support.
- □ Identify the data storage capacities you currently need as well as future projections.

2.

List business & regulatory requirements.

- □ Identify the regulatory compliance requirements you need to fulfil.
- □ List your business requirements like uptime minimums, performance requirements, etc.

Service & Performance

3.

List & match all the services offered by the provider.

□ Ensure all the necessary services are offered by the provider with the appropriate tools and monitoring mechanisms.

□ Identify any future requirements and confirm whether they feature on the future services roadmap of the provider.

4.

Identify the capability of services.

□ The various services should be able to handle current and projected service requests like connection requests, bandwidth, etc.

□ The services should have elasticity to quickly scale to handle any spikes in processing requirements.

□ The services should have frequently-synced geographical presence near core user centres to ensure ideal performance metrics.

5.

Identify any caps to services (bandwidth, storage limits, any service counters, etc.).

□ Ensure what happens when hitting the cap within a subscription cycle.

□ If choice is provided, choose between suspension of services and additional charges when caps are hit.

6.

Ensure uptime guarantee is listed in their Service Level Agreement.

□ Identify how service monitoring is done and reported.

□ Ensure service quality metrics, including “scheduled down time”, are clearly defined and listed including acceptable variances.

7.

Identify the support mechanisms.

□ Identify support methods available (tickets, phone, chat, etc.).

□ Document support availability timings and any resolution assurances.

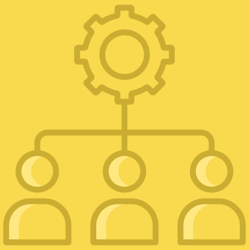
□ Identify the escalation mechanism for both requested and automated escalation for various support types.

□ Ensure general support and incident support are identified specifically and have corresponding systems and policies for tracking and resolution.

Data Management/ Security

8.

Ensure any data is identified & protected at all times.

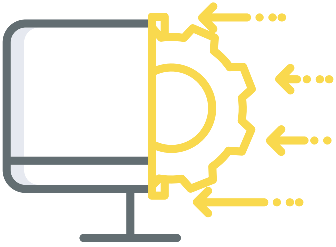


□ The provider should clearly identify and differentiate between your data and service provider data, including any derived data.

□ The provider should clearly list data usage terms & access restrictions, including how these are implemented and ensured.

□ There should be clearly enunciated data security guidelines (physical protections, encryption, incident detection, etc.), procedures (audits, vulnerability scans, alerting mechanisms, etc.), and policies (frequency of audits, security mechanisms implemented, notifications, etc.).

□ Only authorised users should get access to data through two-factor authentication, IP filtering, role based access, etc.



9.

Identify the physical locations of data centres offered by the provider and choices offered to configure usage.

□ There should be an easy-to-use configuration mechanism that can be used to prohibit data pass-through/storage/processing in specific geographies.

□ The choice should not come at the cost of performance penalties.

10.

Identify the mechanism for retrieving all your data from all services you have signed up for.

□ There should be an easy-to-setup & use data backup mechanism, whether cloud-to-cloud or cloud-to-local.

□ Any backups should not be encrypted or in proprietary formats.

11.

Document data retention, back-up, & disaster recovery mechanisms.

□ Identify how long data is retained by the provider and how it is deleted.

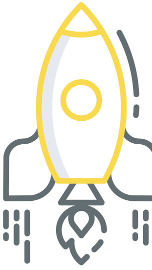
□ Document the mechanism, number, and frequency of data backups by the provider including any data replication mechanisms.

□ The restore systems should be a combination of automated and manual triggers, procedures, and systems to restore data and services with clearly defined metrics and tracking mechanisms.

Governance

12.
Ensure there are clear and accessible policy documents available.

- □ The Terms of Service should cover all aspects of the business that will affect the services you wish to sign up for.
- □ The Privacy Policy should provide a clear framework on how your information and your data will be used.
- □ Ensure you are explicitly recognized as the owner of any data and software you upload to your account.
- □ Identify how Termination of Services is handled and how long your data is retained, backups provided, notice period when initiated by the service provider, etc.
- □ Document notice periods involved and mitigation solutions offered when new services are offered or any services or specific capabilities are deprecated or removed.
- □ The service provider should have clear ownership of all responsibility especially when any subcontractors or third-parties are involved.
- □ Ensure the legal jurisdiction in the event of any problems is comfortably approachable.



13.

Identify the policy for legal notices received by the provider for your software/data.

- □ There should be a clear policy of notification when receiving any notices from law enforcement or governmental agencies regarding any software/data stored by you.
- □ Identify the duration of advance notice provided before any action is taken on the basis for any requests received especially involving access to your data by third parties or removal of any part of your data.

14.

Ensure the provider has the necessary structure conforming to various regulatory requirements.

- □ There should be properly identified individuals manning specific positions with clear roles and responsibilities.
- □ The contact information and response SLAs should be clearly listed.

15.

Ensure the systems are conformant to applicable data management requirements.

□ Personally Identifiable Information (PII) protection standards should be set-up and met.

□ PCI-DSS requirements should be met.

□ Data residency requirements should be met.

□ Applicable information security standards must be met.

□ There should be specific accreditations granted by competent audit and certifying organisations confirming policy compliance, legal compliance, services and capabilities claimed, etc. backed by a clearly documented regular, recurring audit schedule. Perform a hygiene check for the listed certifications.

Pricing & Billing

16.
Be clear on initial charges.

□ Document any set-up fees.

□ Confirm whether any initial training to use their tools and services is paid.

17.
Charges of services should be clearly listed.

□ Identify how charges for various services are calculated.

□ Frequency of invoicing should be clearly stated with the number of days when it becomes due.

□ Identify what (if any) additional charges are applicable for delay in payment of due invoices.

18. Identify any additional charges during service use.

- □ Identify how often and with what prior notice the provider can change pricing structure of the services hired.
- □ Confirm if there are any charges for overages (bandwidth, number of queries, file write/read counters, etc.).
- □ Confirm support charges and if any additional tiers of support exist and cost extra.

19. Identify any charges for termination of services.

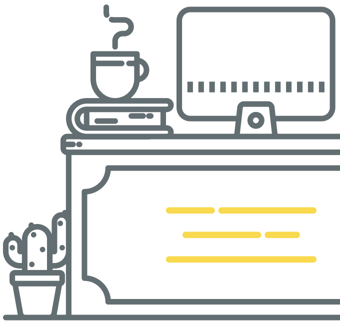
- □ There should not be any charge for terminating services.
- □ Any charges to retrieve your data before closure should be acceptable.

Additional Considerations

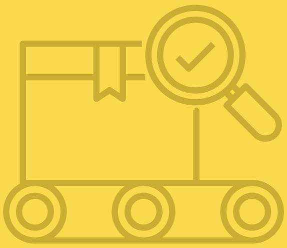
20.
Research any publicly available information on the service quality, incident responses, customer handling, etc. of the service provider to identify corporate culture and approach.

□ They should treat all customers with respect and humility.

□ They should take ownership of any incidents and lead the way to acceptable resolutions.



21.
Evaluate service provider stability.



□ They should not phase out technologies/services without ample notice to their customers.

□ Confirm they are not in the market seeking to be bought, and are financially stable to continue long-term.

Contact Us

Net Solutions is a strategic design & build consultancy that unites creative design thinking with agile software development under one expert roof. Founded in 2000, we create award-winning transformative digital products & platforms for startups and enterprises worldwide.

To discuss our services, call us on any of these numbers, or email us on info@netsolutions.com

LOS ANGELES

11601 Wilshire Blvd, West
Los Angeles, CA 90025,
USA

NEW YORK

101 6th Ave, 8th floor,
New York, NY 10013,
USA

TORONTO

111 Queen St E #450,
Toronto, ON M5C 1S2,
Canada

LONDON

Aldgate Tower,
2 Leman Street,
London E1 8FA,
UK

HQ

CHANDIGARH

Site No. 15, Phase 1,
Chandigarh Technology Park,
Chandigarh, U.T. 160101,
India

PUNE

Pride Purple Square,
B 315-316, Wakad, Pune,
Maharashtra 411057,
India