
Checklist For Choosing Digital Disaster Recovery Service Providers

When beginning the search for an information management vendor, it pays off in the long run to keep your needs at the forefront of the conversation. To help with this goal, The Data Vault has put together a handy checklist of some of the most common requirements we see on a regular basis; hopefully it will allow you to easily compare and contrast the various options available on the market.

1) Where are the vendor's physical servers located?

2) How long has the vendor been in business?

3) How long has the vendor been providing cloud based services?

4) Can the vendor provide international diversification, with hubs in geographical locations?

Yes No

5) Can the vendor provide public, private, and hybrid cloud environments?

Public Private Hybrid

6) Can the vendor separate data depending on the data type?

Yes No

7) Does the vendor have a firewall that will adequately address security needs?

Yes No

8) Is data encrypted when using a public cloud environment?

Yes No

9) Does the vendor offer redundant systems?

Yes No



10) Does the vendor have redundant internet connections?

Yes No

12) Is the data center location secure with system to provide authorized access?

Yes No

13) Is the data center located near known or potential hazards?

Yes No

14) Will data be stored so that it is segregated from other organization's data?

Yes No

15) Has the vendor's backup strategy been reviewed?

Yes No

16) Is backup done using disk to disk or magnetic tapes or other methods?

Tape Hard Drive Other

17) Can the vendor demonstrate a business continuity plan?

Yes No

18) Are business critical applications being hosted?

Yes No

19) Is the data center designed around a virtualized environment?

Yes No

20) Are the data on virtualized servers?

Yes No