Acronis

IT DISASTER RECOVERY

SERVICE PROVIDER CHECKLIST

Ask your Cloud Service Provider these key questions when preparing to move ahead into implementing your IT Disaster Recovery Solution (DR)

- [ ] **Do you help your clients to define and plan to meet key system availability objectives?**

  Identify the scope of your Disaster Recovery implementation – servers, applications and user services. Clearly define RTO and RPO and make sure that the Service Provider will meet the scale of your current and future scope, and your current and future RTO and RPO objectives.

- [ ] **Do you provide Service Level Agreement (SLA) and guarantees?**

  Ensure that the Service Provider offers clearly defined guarantees meeting capacity availability, acceptable RTO and RPO and has proven track record of assuring the SLA.

- [ ] **Is the solution secure?**

  Ensure that your solution includes a level of encryption in-transit and at-rest, to meet requirements of your organization for internal policies, IT guidelines or regulatory compliance requirements. Also, double-check that the solution has all the necessary mechanisms of authorization and authentication in place.

- [ ] **What options are there to balance RTO and cost?**

  Check that the solution offers a range of cost options for the tiers of your workloads and servers based on their criticality and target RTO.

- [ ] **Is it a recognized solution?**

  Select a Service Provider with the solution trusted by customers and industry experts. Look for rankings and ratings in addition to positive reviews and word of mouth from existing customers and recognized analyst firms.

- [ ] **Will the solution be able to protect your entire environment?**

  Recheck that the entire scope of your servers are protected – whether physical or virtual, runs Windows or Linux, different hypervisors. Look for the absence of hidden dependencies, solution that is storage and network-agnostic and integrates easily into existing environment.

- [ ] **Is the solution hybrid?**

  Procure the solution that offers both on-premise and cloud failover. You would not want to failover your data center or a group of servers to cloud for a single server failure when you can quickly activate the single server locally.

- [ ] **Does the solution include automation and orchestration?**

  After a disaster, your most skilled personnel may not be available. Your DR solution should be able to automate the failover and reduce the reliance on dedicated engineers and specialists.

- [ ] **Does the solution include Disaster Recovery runbooks?**

  Successful DR is all about good planning and documentation. Check if your DR vendor can help you with planning, and the DR solution supports documented executable runbooks to follow during the disaster.

- [ ] **Does the solution support testing and DR exercises?**

  Disaster Recovery success is not guaranteed until you test. Make sure that the DR solution provides an easy path for testing the failover and running DR exercises on a regular basis.

- [ ] **Are both self-service and service provider support included?**

  When disaster strikes, your team should to be able to initiate failover whenever they want – from any location, from any device. Yet you should also be able to ask your Service Provider to perform the failover over the phone, if your team members are not available. Only with both options, you can control the best flow of the process during the disaster.

- [ ] **Is the solution easy-to-use?**

  The last thing you want to do during a disaster is to read documentation and call support with solution usage questions. Make sure that the solution is easy to use – ask to see the product videos or live demos.

Acronis

For additional information, please visit http://www.acronis.com

To purchase Acronis products, visit www.acronis.eu or search online for an authorised reseller.
Acronis office details can be found at http://www.acronis.com/company/worldwide.html