Key questions when considering data resiliency and business continuity

FLEXENTIAL

Key questions

Overall DR readiness

What are you using for disaster recovery today?

Do you test your current DR plan today?

Do you have a written copy of your disaster recovery plan archived outside internal systems?

Are your customers requiring their applications to have a DR plan and testing?

Does your DR plan meet with current compliance requirements?

Do any elements of your disaster recovery plan rely on knowledge of individuals?

Do you have the ability to remotely initiate a disaster recovery plan?

What are your requirements for recovery point objectives?

What are your requirements for recovery time objectives?

Have you ever conducted a business impact analysis?

Who makes the final call to failover and what is the criteria when deciding?

Is there a process or procedure in place to notify your customers in the event of a failover?

Is there a process or procedure in place to notify internal employees, support teams and external vendors in the event of a failover?

Is there a process or procedure to failback?

Is there a process or procedure in place to notify your customers after the primary site is recovered and you're ready to failback?

Is there a process or procedure in place to notify your internal employees, support teams and external vendors after the primary site is recovered and you're ready to failback?

When is the last time you tested your disaster recovery plan?

Were your end-users involved in your DR test and was it validated?

Do you have a plan for voice recovery and switching your telecom lines?

Do you have a crisis communication plan?

- Notification to senior leadership team
- Social media
- Communication internally and externally with updates
- Website communication

Do you have a location selected to serve as an emergency operations center?

Does your team have the training necessary to failover a site?

Where is your DNS hosted?

Key questions
Applications

List your key business functions	List the key applications that run your key business functions

What solutions do you have in place to protect your applications?

Do you have a written and tested disaster recovery plan for each application?

How many VMs are in your environment? How many need to be protected?

How many VMs from each application need to be protected?

What is the DR strategy for the virtualized and non-virtualized part of your application stack?

If you have implemented continuous integration servers for your primary site, are they being redirected to the recovery site?

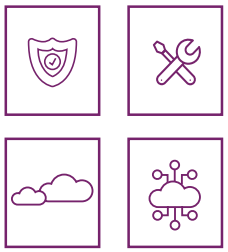
Do you have access to your application license keys?

Do you know how to contact your software vendor on off-hours?

Do you have someone reviewing permissions on the recovery site as well as primary?

Who is responsible for each application on a daily basis and in a recovery scenario?

If you had to apply a critical patch to your application while it is running on the recovery site, are you prepared to do that (with all the processes and procedures)?



List the applications that feed information to this key application

List your key applications

List the applications that are dependent on this key application

Key questions
Security

Does your recovery site require the same security as your primary site?

- Physical
- Firewall
- Intrusion detection prevention system
- Anti-virus
- WAF
- DDoS
- EVS/IVS
- FIM
- SIEM/log management
- Encryption keys
- Dual-factor authentication
- Active directory (or ID management) as a service

Are there security options that cover both sites?

Do you have a backup strategy after you have failed over?