5 Steps to Implementing Business Continuity Services

By David Davis, vExpert

Symantec™

**Brought to you by Symantec –
Keeping Your Applications Running**

Your company's customers and end users (and even executives) have come to expect their applications to always be available. In their eyes, critical company applications are like the electricity, TV or telephone—utilities that are "always on."

Certainly, you do your best to ensure that applications are always available: Servers, storage, and network devices have redundancies and the datacenter might have redundant power and cooling. Assuming you're using server virtualization, you may even be employing a high availability (HA) solution (such as VMware vSphere HA) or replication (such as vSphere Replication).

However, don't get a false sense of security. vSphere HA will monitor the virtual machine (VM) and the physical server, but it only does basic application monitoring. If it discovers a problem, there may be downtime if the VM requires a reboot. There are also numerous scenarios where your application may be unavailable and vSphere HA doesn't even recognize it.

Unless your applications are protected by an HA solution, those critical company applications still have the potential to go down at some point (likely when you least expect it) and your customers, end users and executives are going to be disappointed.

You never want to be in the uncomfortable position of being called into a meeting of executives to attempt to explain why an important application went down. You'll always be asked the question, "What else can we do to prevent this from happening in the future?"

Now is the time to learn how business continuity solutions can help your company and how you can go about implementing one.

5 Steps to Implementing Business Continuity

#1 Analyze your applications, recovery time objectives and recovery point objectives with app owners and executives. Prioritize your findings based on the financial impact to the company if those apps were unavailable.

#2 Architect a business continuity solution that will meet the recovery time objectives and recovery point objectives for your critical applications.

#3 Evaluate technical solutions that will meet your objectives, ensuring those solutions will be easy to use and comprehensive.

#4 Deploy your business continuity solution, testing various failure scenarios.

#5 Test your business continuity solution on a regular basis or whenever changes to the environment occur.

The best thing you can do to protect your company, your career and your reputation is to propose a business continuity solution (if your company executives turn down a proposal to implement such a solution, at least you've covered yourself by proposing one).

Here's a step-by-step guide that shows how easy it is to implement a business continuity plan.

#1 Analyze

When it comes to Business Continuity planning, considering all components and the associated cost (be it dollars, server resourced management overhead) is complex. To break down the complexity, the first step is to develop a business impact analysis (or BIA). The goals of a BIA are:

1) **Identify your company's applications (all of them)**: It's important to identify all applications as there may be applications or dependencies about which you don't know.
2) **Identify application dependencies** - your well-known critical applications may be dependent on little-known applications or network services.
3) **Prioritize applications:** Working with application and business owners, determine the recovery time objective (RTO) and recovery point objective (RPO) for each of your company's applications, taking dependencies into account. Once the applications and recovery objectives are known, prioritize the applications to determine what is most critical to your business. In most cases, this prioritization is done by asking the question, "What is the financial cost to the company if this application is down?" (in other words, loss of cash flow).

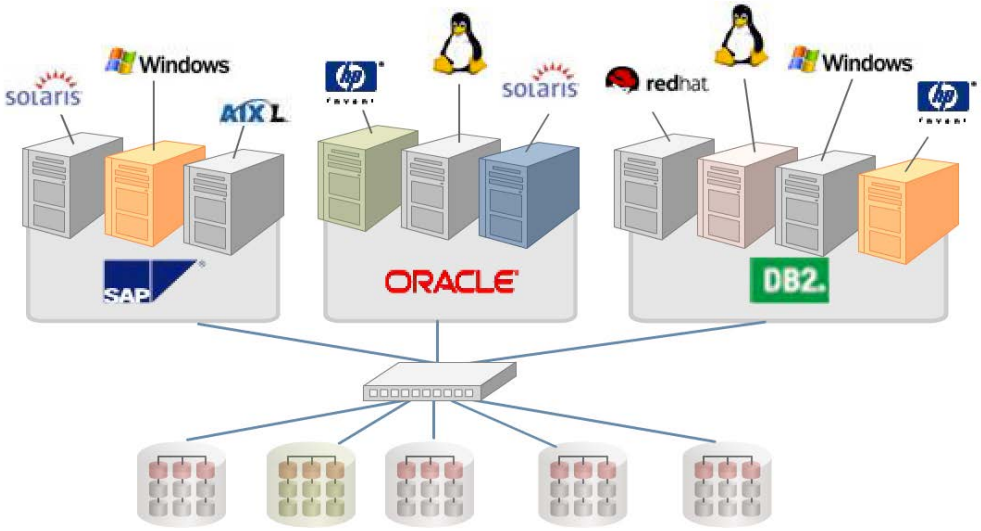
Note that the BIA must be done periodically because new applications will be brought up and old applications will be decommissioned on a periodic basis.

Ensure that you spend adequate time on the BIA—your business continuity will only be successful if the right applications are protected.

#2 Evaluate

It's time to determine what specific technology you will use to protect your critical applications (as defined in the BIA).

In the datacenter you have multiple software and hardware layers but, if you just stick to business continuity for applications, you'll find that there aren't too many solutions out there that can offer you what's needed.



Here's a list of features to look for in any business continuity solution you're considering:

- Cross-platform—support for multiple server brands/types and multiple operating systems
- Supports any application—both well-know applications and custom applications

Support for Multiple Applications, Databases, and Operating Systems

- Works for both planned and unplanned downtime
- Helps to reduce the number of idle or standby servers with roaming spares
- Scalable
- Both compatible and integrated with the virtual infrastructure
- Automated testing
- Integration with replication systems/agents
- A complete and integrated disaster recovery solution—not a single application solution or a specific vendor storage array solution
- Single graphical console—Web-based interface that works across all servers and applications

As with the BIA, take your time in evaluating business continuity solutions. If a solution is painful to use it may end up not being use (and your company will go unprotected).

#3 Architect

With your BIA complete, you can use the application priorities identified to architect a business continuity plan (BCP) that is right for your organization.

The plan must take into account the people, software, and hardware that will be required to continue business in the event of a disaster or outage. The recommended approach for business continuity planning is to consider the delivery and availability of the complete business service that IT is providing to customers, employees and partners. Typically, critical applications are delivered across multiple and differing virtual and physical platforms that all provide a function to a given business service. For example, a business service might be a billing system that runs on a three-tier architecture consisting of a Web layer and an application tier that's connected to a back-end database. While the availability of a single component or application is important, IT must consider the availability implications for the entire business service.

When a catastrophic or simple outage occurs, organizations must be prepared to recover based on the criticality of the business service. The main concern is to alleviate or remove as much downtime as possible with the right business continuity solution. The solution requires the elements discussed in the second step, including support for all virtual and physical platforms, integration with the various application components, data replication technologies, and so on.

#4 Deploy

As part of your evaluation, you should have tested the solution you're deploying. However, you may want to perform more thorough testing now, before you deploy the business continuity solution into production.

Once you feel comfortable with the solution, you'll want to deploy the solution for the applications and business services you're protecting. Keep in mind that as you deploy the solution, you'll want to test it for each application. Just because the solution is tested and works for one application doesn't mean that it will work for all applications.

As part of your testing and deployment, continue to ask yourself if the solution will allow you to meet the recovery objectives you identified in the BIA.

Additionally, keep in mind that business continuity solutions aren't deployed "in a bubble." They work with your storage, they need the network, and they communicate with your applications. As such, they need to be deployed carefully.

#5 Test

Depending on the size and scope of the project, creating a BIA, architecting recovery plans, and deploying business continuity technology can take considerable time. You don't want all that effort to go to waste so it's imperative that you test your plan.

Unfortunately, most disaster recovery plans are rarely tested due to the time, effort, cost and the potential for downtime associated with most disaster recovery products.

For this reason, it's crucial that the business continuity solution you select can perform automated testing, that it can simulate a variety of failure scenarios, and that there's a zero chance you'll cause production downtime while testing.

It's likely your company's auditors and compliance groups will require you to provide the results of your business continuity testing. Additionally, over time, your applications, servers, storage and network will change.

For these reasons (and to give you peace of mind), you'll need to test whether recovery will be successful between the primary and secondary site (or even between primary and secondary servers for localized disaster) on a regular basis.

In Summary

Application downtime is not what you want your company's executives to remember you for. Especially when considering your most critical customer facing and internal business services that simply cannot tolerate downtime or data loss.

It is the responsibility of the IT organization to remove as much risk from the operations of these critical business services as possible. That means

implementing the right business continuity plan to meet the service levels required by the organization – one that considers all of the components of the business service stack that typically run across physical and virtual platforms, not just individual applications.

Now is the time to evaluate and recommend business continuity solutions in your data center – before it's too late.

To learn more about how Symantec can help you with the right business continuity solution for your environment, please visit: **go.symantec.com/business-continuity.**

About the Author

David Davis is the author of best-selling VMware vSphere and Microsoft Hyper-V video training libraries from TrainSignal.com. He has written hundreds of virtualization articles on the Web, is a vExpert,VCP, VCAP-DCA, and CCIE #9369 with more than 18 years of enterprise IT experience. His personal Web site is VMwareVideos.com.