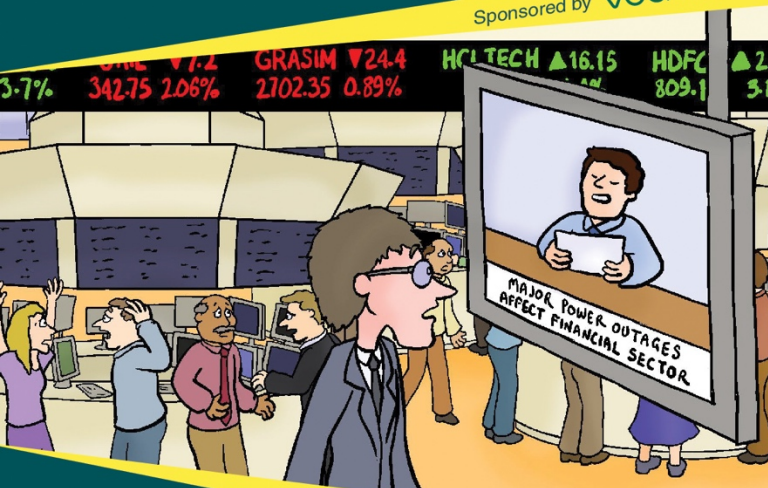
Conversational

Business Continuity and Disaster Recovery for Finance

A ConversationalGeek® Book

Sponsored by VEEAM



Learn about:

- Finance-specific BCDR concerns, regulations and focus points
- The value of business continuity and how to properly execute a BCDR plan

MINI Edition

By Wayne Dipchan
(Senior Technical Infrastructure Architect, Technical Author/Speaker)

Sponsored by Veeam

Veeam® recognizes the new challenges companies across the globe face in enabling the Always-On Enterprise™, a business that must operate 24.7.365. Veeam has pioneered a new market of Availability for the Always-On Enterprise™ by helping organizations meet recovery time and point objectives (RTPO™) of less than 15 minutes for all applications and data, through a new solution that delivers high-speed recovery, data loss avoidance, verified recoverability, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs, while always supporting the current and future business goals of Veeam customers.

Founded in 2006, Veeam currently has 49,000 ProPartners and more than 255,000 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland, and the company has offices throughout the world.

VEEAM

To learn more, visit
www.veeam.com .

Conversational Business Continuity and Disaster Recovery for Financial Services (Mini Edition)

by Wayne Dipchan

ConversationalGeek

Conversational Business Continuity and Disaster Recovery for Financial Services (Mini Edition)

Published by Conversational Geek Inc.
www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this book:

Author:	Wayne Dipchan
Project Editor:	J Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer(s):	Karla Reina

The “Conversational” Method

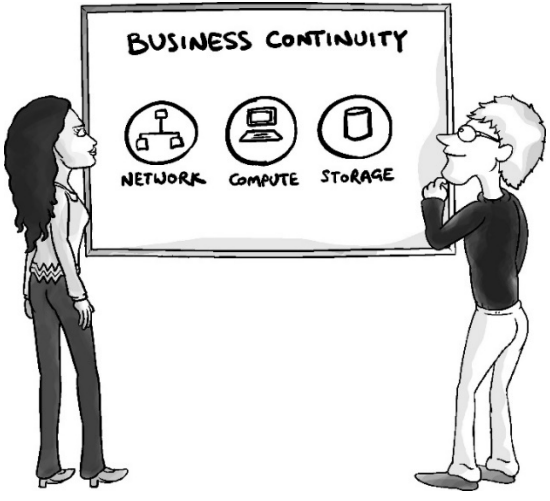
We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

“Geek in the Mirror” Boxes

We infuse humor and insight into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote; it might be a personal experience.

Within these boxes I can share just about anything on the subject at hand. Read ’em!

Business Continuity and Disaster Recovery for Financial Services



Financial service organizations face the challenge of a 24/7/365 operational requirement. Beyond constant availability, they face a bevy of challenges revolving around data security, protection and integrity.

To accomplish this requires a solid Business Continuity and Disaster Recovery (BCDR) plan.

Failure to implement one, playing the “hope” vs. “plan” game, can lead to lost or compromised data, which would ultimately lead to reputation damage for the organization and other detrimental consequences.

The Pressure to Succeed

Financial services are made up of many moving parts. On the one hand, you have banking institutions, credit unions, investment firms and even insurance companies. These are handling stored data that is growing year-over-year at an exponential rate.

Then you have employees of those various institutions. The loan officers, the insurance agents, stock and bond traders and brokers, the bankers and so forth. These folks need their services ready and available or they can’t do their jobs. Their duties include validating credit applications, obtaining credit information, getting quotes on premiums, finding buy/sell trade prices and more.

And finally, you have customers who wish to avail themselves of the solutions provided by those

services. For example, most banks have mobile apps that allow individuals to make deposits, transfer funds, pay bills and check their account balances. And people have grown accustomed to using these services at any time from anywhere thanks to mobile apps and the ever-present Internet.

All sides require and have come to expect ever-ready, always-available services. Success in providing those services falls to IT administrators and decision makers who hold sway over the solutions your company will ultimately deliver. They aren't just going up against hardware or software failures that occur accidentally or due to user error, they must also be vigilant and on guard against cyber criminals seeking to either disrupt their business flow (for profit or other nefarious purposes) or access and steal sensitive data.

The pressure to succeed goes beyond the needs of your financial services firm and their customers. There are specific regulatory compliance requirements that need to be met when dealing with consumer information. As a professional in the financial IT field, you are likely familiar with the following regulatory standards:

- Gramm-Leach-Bliley Act (GLBA) – per the FTC.gov site this act requires financial institutions (companies that provide loans, financial or investment advice, insurance and such) to explain their information sharing practices and requires them to safeguard sensitive data.

- Dodd-Frank Act – Launched after the financial crisis of 2007, this was designed to encourage the financial stability of the United States by improving accountability and transparency within the financial system. Note: Dodd-Frank is currently under revision as the Financial CHOICE Act which might roll back many of the Dodd-Frank provisions.

- Sarbanes-Oxley Act (SOX) – Sarbanes-Oxley requires the protecting, securing and retaining of financial information. Banking, investment and insurance companies all must adhere to these stipulations.

- Payment Card Industry Data Security Standard (PCIDSS) – A security standard for those organizations that handle credit cards (Visa, MasterCard, etc.)

- General Data Protection Regulation (GDPR) – an EU regulation that will have global impact when it goes live in 2018. GDPR is a data protection initiative that allows individuals to request their personal data be given to them or destroyed (aka right-to-be-forgotten). Failure to comply will result in heavy fines.

These are just a handful (literally… just 5) of the many regulatory compliance laws that exist. It's essential for you to know which ones apply to your specific financial services organization.

Business Continuity Basics – Building Blocks for a Successful BCDR Plan

The term “Business Continuity” refers to a continuation of your critical business applications during a disaster (man-made or natural), outage, changes to the business, and/or cyber-attack.

The basic steps to achieve business continuity are the same for companies of varying sizes and verticals. It’s crucial that BCDR infrastructure be implemented at the point an application is deployed.

If BCDR is baked into the project lifecycle and created proactively, going forward, all application deployments will adhere to your plan. Therefore, having a team dedicated to scalable, process-driven BCDR planning, testing, and improving is key to your success.

Two key terms you’ll hear often when discussing business continuity are RPO and RTO (or collectively RPTOs): Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

RTO – The amount of time it takes to recover an application, starting from the time a disaster is declared to when users can log on again. Simply put, RTO is the amount of time you can be down. Depending on the application, the RTO might be 0.

RPO – The point in time that an application's data is restored counting backwards from the time of the disaster. This can be quantified by thinking about the amount of data in time that you are willing to lose. For example, a 15-minute RPO means that post recovery you will lose up to 15 minutes of data. Depending on the financial solution we're talking about here, 15 minutes might not be acceptable. Again, the RPO might be 0--a zero downtime tolerance policy.

The fact is you're not going to achieve an RTO/RPO of <15 minutes without a great deal of planning, a reasonable budget, and the right third-party solution(s).

Some of you may have legacy hardware and software you're working with and you might think we're just talking about updating and modernizing your existing environment. But you need to dig deeper here. A financial institution is going to have to create a BCDR plan that goes above and beyond the average company.

Ideally, you'll put a team together (a governance committee) to define SLA's for each level of your applications based on their criticality and then define the SLA's in tiers.

Once the tiers are defined, the governance committee should discuss each application in your environment and decide which tier it should be assigned to. Any new applications being introduced to the environments should be assigned a tier before being deployed.

Your tiers could be defined as follows:

- Tier 0 with RTO 0 minutes and RPO of 0 minutes
- Tier 1 with both RTO and RPO up to 15 minutes
- Tier 2 with RTO up to 4 hours and RPO up to 24 Hours
- Tier 3 with RTO up to 1 week and RPO up to 1 week
- Tier 4 Best Effort

Infrastructure services such as network connectivity, Active Directory, DNS, DHCP, etc. all need to be accounted for and assigned a tier. One factor to consider is having these services already existing on the recovery side. This will allow failover to be quicker and more efficient as there will be fewer services that will need to be failed over and started when a disaster occurs.

Having a solid BCDR plan in place not only mitigates risks and reduces cost of disruption, but also opens doors to financial institutions much more easily, helps to build customer confidence if communicated, prevents significant harm to your employees, your image and your key stakeholders, as well as provides compliance benefits.

Business Continuity in Reality – Practical Guidelines for IT Professionals

All the planning and theory in the world won't help you if you don't have the tools you need to execute your plan. Modern BCDR includes a virtualization solution that allows for immediate fail-over of your VMs. It includes a backup/recovery solution that can help you get back up and running no matter what has hit your environment (from a hurricane to a ransomware attack). It includes a secondary site location which may be in the cloud. That's the reality. There is no way to provide enterprise-grade BDCR without the help of third-party tools to make it happen.

Backup Strategy

Before you worry about availability of services, you need to make sure you have a way to recover from a disaster outside the scope of your wildest imagination. And there is only one way to do that: old school backup of your data. This is needed for recoverability but may also be necessary due to laws that require long-term data retention.

The 3-2-1 plan is touted by most IT administrators as the best approach for a backup strategy: 3 copies of your data, 2 stored on different types of storage media and 1 copy off-site.

To create these backups, you'll need an enterprise-grade solution--not just "Joe's Backup Solution" if you want to do more than just take the backup. Taking the backup is just half the battle. The key is restoring it. Don't forget: that data must be encrypted to ensure data privacy.

Let's consider that off-site copy portion of the 3-2-1 rule. Assume you have at least two data centers. These may be buildings owned by the company or rented rack space in a co-location data center. The cloud is also becoming more and more prevalent as a data center choice for companies. Even if you are using on-premises datacenters, you should look at tools that are cloud-ready. This will give you the option to leverage the benefits of the cloud in the future. A hybrid-cloud model might be your first step towards taking advantage of the cloud while remaining on-premises.

Before choosing a continuity solution make sure it isn't just vapor ware (going to be developed) or magic ware (too good to be true and not possible to be developed). Talk to others; see what they are using. Do your homework.

Logically, you hope never to have to use a backup; you want your redundancy and resiliency to be solid. Perhaps you have worked with something in the past you trust. Or you are looking into emerging technologies and new solutions. Again, choices have to be made on which solution to use.

Recovery Strategy

At the same time, you plan your backups, you need to consider how you will be recovering them. In some cases, recovery options available based on the solution used – like an ability to recover application items, or direct recovery into public cloud providers such as Microsoft Azure – and will impact your backup strategy.

For example, if you plan to leverage restores to Azure, you obviously will look at the technical requirements that will define what the backups need to look like for recovery to be successful.

So, as you plan your backup strategy, include the recovery strategy as well, as they are not mutually exclusive.

Virtualization Failover

Let's talk about how you can achieve an RTO and RPO of 0 minutes. To accomplish this, you will have to employ an active/active VM failover configuration. Workloads providing a tier 0 service will need to be online and servicing requests in all data centers. For the most part, infrastructure services will fall into this tier and they usually have built-in mechanisms to assure this active/active configuration.

Web applications can also be load balanced between data centers by using appliances such as F5 or NetScaler. A thick client application could be virtualized, then the publication of the application between all data centers could be load balanced

using technologies such as Citrix and App-V. The data that supports these applications will need to be kept in synch behind the scenes possibly in SQL or Oracle DB and flat image files.

Your mission-critical financial applications will also fall into this tier as they will need to provide real time data to both employees and consumers of the financial institution.

RTO and RPO of 15 minutes.

Less critical financial applications will fall into this category. These are the applications where up to 15 minutes loss-of-data is acceptable.

These workloads will need to be replicated from the primary data center to any secondary data centers (or the cloud) at intervals of 15 minutes. You are essentially making an exact copy of the workload in the secondary data center and updating that copy with any changes every 15 minutes. The connection between data centers has limited bandwidth (bandwidth size will depend on your type of connection). This connection may also be used for production traffic. Therefore, there is a need to

consider the amount of traffic being replicated and how often that replication occurs. When deciding what tool to use, you should look at the Wide Area Network (WAN) replication optimization features (you may also consider throttling bandwidth used for replication on the network) and the ability to replicate only changed blocks.

Something to keep in mind: when you first set up VM replication, there is a real potential to saturate the bandwidth on the link between your data centers as you will be replicating the whole VM. Depending on the amount and size of the VMs, the bandwidth utilization may affect your production traffic on the link. It's recommended that you seed secondary datacenters with your VMs before turning on replication.

This will accomplish your RPO of 15 minutes or less, but what about the RTO of 15 minutes or less?

To achieve this, a well-orchestrated workflow to implement the BCDR strategy is needed. Most software tools built to perform replication include or offer an orchestration toolset that will allow you to manage, monitor, and troubleshoot replication. The

toolset will allow you to easily failover and failback workloads from the primary datacenter to the secondary datacenters within the 15-minute RTO tolerance. Workloads can also be grouped by dependency, thus making sure you bring up services in the correct order.

If there are two physical data centers, the underlying hypervisor infrastructure will need to be present and running at both. There is also the option to replicate workloads into the cloud and use a disaster recovery as a service (DRaaS) offering. The cloud option alleviates the need to have the hypervisor layer sitting and waiting for a disaster, so it may be a more efficient solution. Having availability extended to the cloud will help avoid the cost and complexity of having a secondary off-site data center. But that doesn't mean there isn't a cost involved. Weigh your cloud-based options carefully, looking to see if your backup solution supports seamless integration into cloud environments like AWS and Azure to enhance recovery ability.

Application Workload Failover

So far we have focused on a complete data center outage and the need to bring up all the applications in a secondary data center. A more likely scenario may be just one application failing for some reason and the need to bring just that one system or service up in the secondary data center. Orchestration tools make this possible. You can select the workloads you want to failover and group workloads to failover as one unit. Of course, you would need to keep in mind your IP strategy and make sure the service is able to communicate with other upstream or downstream services.

Testing Your BDCR Solution

Testing your solution is a must. An annual (or more frequent) disaster recovery test will help ensure you're ready for anything that may come your way. But it's not an easy thing to do.

The amount of planning and staff involved in the BCDR testing depends on the size of the infrastructure. Some companies can turn the connectivity off to the primary data center and have

all infrastructure and application teams sign off on their part of the recovery. This will highlight any inefficiencies with the plan or any unexpected results that can be remediated before the next test. Of course, this will need to take place outside of regular business hours.

But what if you have applications that need to be available 24 hours a day, 7 days a week or the application team is only available for testing during business hours? For those, look to your orchestration toolset. Many of these tools provide features that enable a full BCDR test of a workload or multiple workloads while keeping the production workload running. This is accomplished by bringing up the replicated workloads in the secondary data center within an isolated network. The isolated network will prevent duplicate name and IP address conflicts on the network. This feature allows the application team to connect to the application from within the isolated network, test the application and eventually sign off on the success of the testing. Some orchestration tools allow you to test the infrastructure piece of a failover with the push of one button. Reports can be generated and sent to

management for confirmation of error-free testing. Here again, of course, any issues encountered need to be documented and remediated and then tested again in the next BCDR testing cycle.

Key Takeaways

Proactive BCDR planning, implementation, testing, and training should be a cornerstone of your business continuity strategy. With the right governance in place, coupled with the technology available, you can have confidence that you can meet your agreed upon RPTO's should disaster strike.

NOTES

NOTES


VEEAM
IT'S HERE
NEW Veeam
Availability Suite 9.5
AVAILABILITY for the Always-On Enterprise
go.veeam.com/v9-5

Continuity of services is a key requirement for employees and customers alike of the financial sector (banks, brokerages, insurance and loan office, etc.). Therefore, it's essential that a well thought-out BCDR plan be push-button ready to go into action to ensure downtime is avoided should a disaster strike.

About Wayne Dipchan

Wayne Dipchan (MCSE/MCDBA) has nearly 15 years of enterprise IT experience, ranging from educational organizations, to private investment banking, to health care. He is a published author and technical speaker.