How to Evaluate Your Bank's Disaster Recovery Needs
and What You Didn't Know to Ask

Integris.

Disaster recovery and maintaining the continuity of your bank: yet another technology-driven issue that has the potential to distract you from what you do best – serving the financial needs of your customers.

We at Integris have written this white paper with you in mind. Please use it as a starting point for evaluating and planning the best solution for your bank's disaster recovery and business continuity planning needs.

It is not our intention to answer all of your questions or develop a full disaster recovery/business continuity plan (DR/BCP) with this white paper. We recognize that each bank has a unique set of needs.

For this reason, we encourage you to find an expert to help guide you through the process of understanding your bank's own DR/BCP needs. Of course, we at Integris are always available to assist you in such a manner.

What's Covered in This Paper:

Understanding your bank's basic technology needs in the event of a disaster

Setting priorities and knowing what questions to ask as you evaluate DR solutions specific to your bank

Understanding the difference between a public versus a private data center

Part 1: What Drives a Good Disaster Recovery Solution

Two overriding factors should drive your bank's technology DR/BCP choice: your bank's

1 Business strategy ***and*** 2 Risk tolerance.

Obviously, money is another key factor for any business. But it's your business strategy and risk tolerance levels that should drive how you will remain productive and service your customers in the event of a disaster. We have found that a good Business Impact Analysis will help determine the level of need and what is appropriate to spend.

Generally speaking, an effective business impact analysis contains two central elements:

1. A list of all relevant technology-dependent systems within an organization.
2. A realistic ranking in terms of importance to your business goals/strategy, and in terms of disruption to your customers' experience.

With these two central elements listed and prioritized, your bank can make an educated decision regarding two important DR/BCP factors:

Recovery Time Objective (RTO) – the amount of time your institution and its customers are willing to wait until your technology and data infrastructure (system) is back up and running at a normal level of functionality. [Hint: Your bank's business strategy should be helpful here.]

Recovery Point Objective (RPO) – the amount of data loss your institution is willing to sustain (i.e., how time-dispersed your data backups are). [Hint: Your bank's risk tolerance levels are key.]

RTOs and RPOs are usually measured in terms of business hours, and generally, the cost of your DR/BCP solution increases as your RTO and RPO decreases. Additionally, a bank might have different RTOs and RPOs for various systems within the bank.

In evaluating these two factors, it is vital to consider how much money your bank stands to lose in employee productivity and customer attrition. With customers, how well your bank recovers after a disaster affects its reputation. For instance, if your branches are dispersed, how much tolerance does a customer banking at a branch under clear skies have when the central branch is down due to bad weather?

> These are the types of questions that a good Business Impact Analysis will help you evaluate to arrive at your bank's priorities when choosing an effective and sensible disaster recovery and/or business continuity solution.

Part 2: Setting Priorities and Asking the Right Questions

Choosing a DR/BCP solution should not be driven by price alone. After a Business Impact Analysis, consider these questions:

Q: *Am I considering solutions that fit my true needs?*

A: Are you looking at only DR? Does your bank need more than a DR site? Do you need a solution that ensures no downtime or only some?

Q: *Am I comparing apples to apples?*

A: The level of security, regulatory provisions and needs for a bank's IT disaster recovery plan are different than those of most organizations. As you evaluate the solutions available, make sure they are certified to meet (or exceed) current bank regulations.

Q: *Should I build an internal DR solution or look externally?*

A: When it comes to an internal versus an external DR solution, sometimes we forget longer-term costs associated with maintaining such an infrastructure – things like regular and unexpected hardware and software upgrades. Know the long-term trade-offs of taking on IT infrastructure continuity inside your firm versus leaving it to an outside expert.

Part 3: Understanding Private vs. Public Data Centers

Think of Private Data Centers as a direct link between your bank branch and core provider. Unlike cloud providers, Private Data Centers adhere to stringent standards based on market focus (e.g. Finance & Banking, Health Care, or Government). In contrast, cloud providers service many different markets simultaneously, which dilutes their ability to deliver against industry-specific security and regulatory requirements. Private Data Centers also benefit clients with the knowledge of knowing exactly where data is stored, while cloud providers often disseminate stored data all over the United States or the world.

Q: ***Is a private data center (PDC) safe?***

A: The answer depends on your provider. PDCs can be as safe as (and even more secure than) keeping servers at your headquarters.

Q: ***Who has the ability to view my data?***

A: This varies with providers, but ideally, only your organization and the provider itself would be able to view that information. And even at that, only those with credentials into your systems/software would have access.

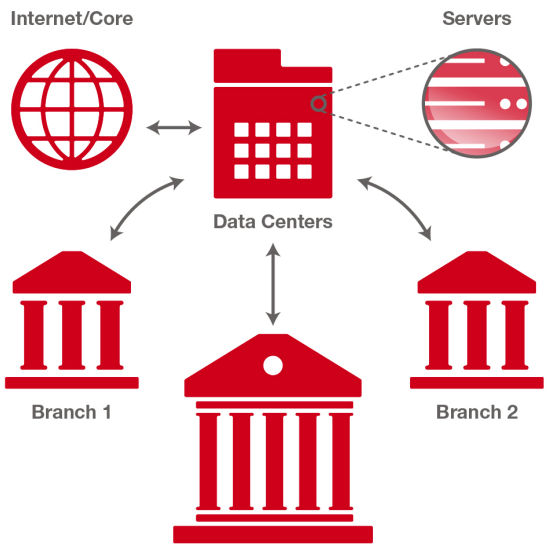
Q: ***What happens in the event the data center is down?***

A: Before working with any PDC providers, understand their Service Level Agreements for availability. It is very rare that the PDC will be down. In most cases, providers guarantee well over 99% uptime.

Q: ***Are there regulatory standardized guidelines for the PDCs?***

A: In February of 2015, the FFIEC added Appendix J to the BCP handbook. It outlines the increased measures a financial institution should consider when making a move to a public data center.

When it comes to the continuity of your bank's IT infrastructure, a DR/BCP solution can ensure virtually no system-wide downtime and certainly no single point of failure.



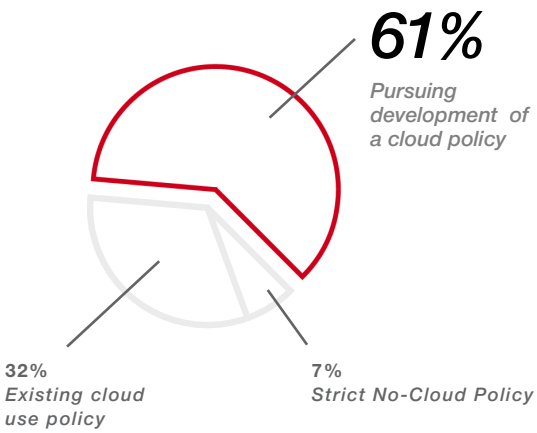
Conclusion

Because of the increasing layers of bank regulation and the number of factors to consider, we recommend taking a measured and realistic approach to a DR/BCP solution for your community bank. Consider both your bank's business strategy and level of risk tolerance. Then, perform a simple Business Impact Analysis.

Once you've determined the appropriate course of action for your bank, review the spectrum of solutions available. There are custom-made solutions out there for community and regional banks. Smaller banks no longer have to opt for a 'go-it-alone' approach, or worse, do nothing at all. In today's technology-driven world, it's too costly a decision not to make.

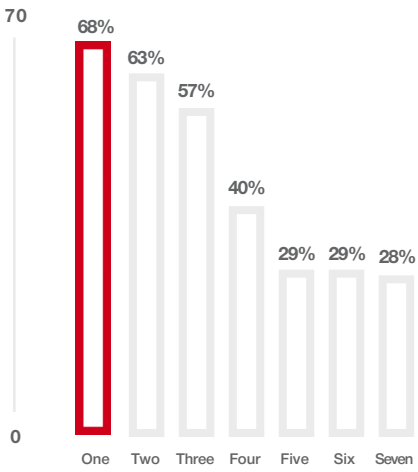
Download our free Business Impact Analysis template, or call us directly at (325) 223-6115 to discuss your options.

CLOUD-BASED INFRASTRUCTURE POLICY ACROSS FINANCIAL INSTITUTIONS



Source: "Banks Ramp Up Cloud Adoption; Holdouts Cite Hands-on Control" American Banker 5/6/2015

PRIMARY REASON FOR BANKS' ADOPTION OF CLOUD INFRASTRUCTURE



One - Flexible infrastructure capacity
Two - Reduced time for availability of applications
Three - Reduction in total cost of ownership
Four - Reduced time to market/value
Five - Limited in-house tech resource
Six - Service value
Seven - Flexible payment model (pay as you go)

Source: Cloud Adoption in the Financial Services Sector; March, 2015 study by Cloud Security Alliance