BCP AND DR PLANS

WHAT EVERY FINANCIAL INSTITUTION SHOULD KNOW

Safe Systems®

Contents

Safe Systems®

Introduction

Financial institutions are well aware of the importance of disaster preparation and the need to be ready for the unexpected. If your financial institution were affected by a disaster and your systems went down, how long would it take to get your institution up and running again? Would your organization have the resources in place to restore critical systems quickly and efficiently?

While hurricanes, tornados, earthquakes, severe thunderstorms, and wildfires are top of mind when preparing for disruptions, pandemics, man-made, cyber, and other disasters can also have a negative impact on your banking operations.

To ensure all community banks and credit unions are prepared for a disaster – of any kind – the FFIEC guidelines require them to have **Business Continuity Plans (BCP)** and **Disaster Recovery (DR) plans** in place.

BCP and DR are subsets of the overall Business Continuity Management (BCM) process which also encompasses resilience, emergency response, crisis management, and third-party integration. The FFIEC wants community banks and credit unions to **take an enterprise-wide, process-oriented approach to business continuity**, meaning institutions should go beyond planning to recover and focus on the overall resilience of operations. Resilience is the ability to prepare for—and adapt to—changing conditions and both withstand and recover rapidly from disruptions, whether that includes deliberate attacks, accidents, or naturally occurring threats or incidents. The terms **"withstand"** and **"recover"** are the two keys for understanding resiliency, with an emphasis on withstanding adverse events.

The goal is for financial institutions to be more proactive and in doing so, avoid or minimize having to implement traditional recovery measures down the road.

This eBook will outline the **key differences between BCP and DR** as well as provide specific steps and recommendations an institution can follow to be prepared and efficiently recover from disasters or business interruptions.

BCP vs. DR - What are the Key Differences?

You might think, "I have a good BCP in place already, so why do I need a DR plan too?" **A business continuity plan refers to strategies and protocols that enable a financial institution to operate during and immediately after a disaster.** The BCP is the crucial blueprint for guiding a financial institution through the process of recovering from a business interruption. This plan outlines what needs to happen to ensure that key products and services continue to be delivered in case of a disaster.

On the other hand, **DR refers to having the ability to restore critical data and applications that enable the financial institution to operate normally**. The DR plan is designed to outline what needs to be done immediately after a disaster to begin to recover from the event.

So practically speaking, a BCP informs your business with the steps to be taken to ensure key products and services remain available to customers and members, while a DR outlines the specific steps to be taken to recover the institution's required technology needs after a disaster. Both are vital to have for any financial institution and are designed to work in tandem. Essentially, the DR plan is a part of the bigger BCP.

There are some differences in how each is structured as well. The BCP consists of a business **impact analysis, risk assessment, and an overall business continuity strategy**.

It is important to note that the FFIEC released BCM guidance in November 2019 emphasizing the importance of **pandemic planning**. The FFIEC no longer requires financial institutions to have a separate pandemic plan, but instead, they expect community banks and credit unions to assess pandemic risk alongside all other possible disasters. In other words, an institution's BCP plan is also its pandemic plan.

The DR plan, on the other hand, includes **evaluating all backups and ensuring any redundant equipment critical to recovery is up-to-date** and working.

While the plans work together, they are two separate concepts.

- **BCP:** A plan to continue business operations
- **DR:** A plan for accessing the required technology and infrastructure after a disaster

Business continuity and disaster recovery planning represent a continuous cycle. And both processes require adequate time for preparation and maintenance. Once the plans are complete, organizations must test to verify the effectiveness, train staff on what to do in a real-life scenario, and identify areas where the plans need to be improved. These plans are different enough that they are often **tested separately**.

A **BCP test** is often a "table-top test" where a potential disaster and outcome are used to ensure all employees know where to go and what to do. A **DR test** is usually a more hands-on process, where all servers and communications are made unavailable, and the backup technologies are implemented to confirm the institution will be able to function as needed and expected in the correct amount of time or Recovery Time Objective (RTO).

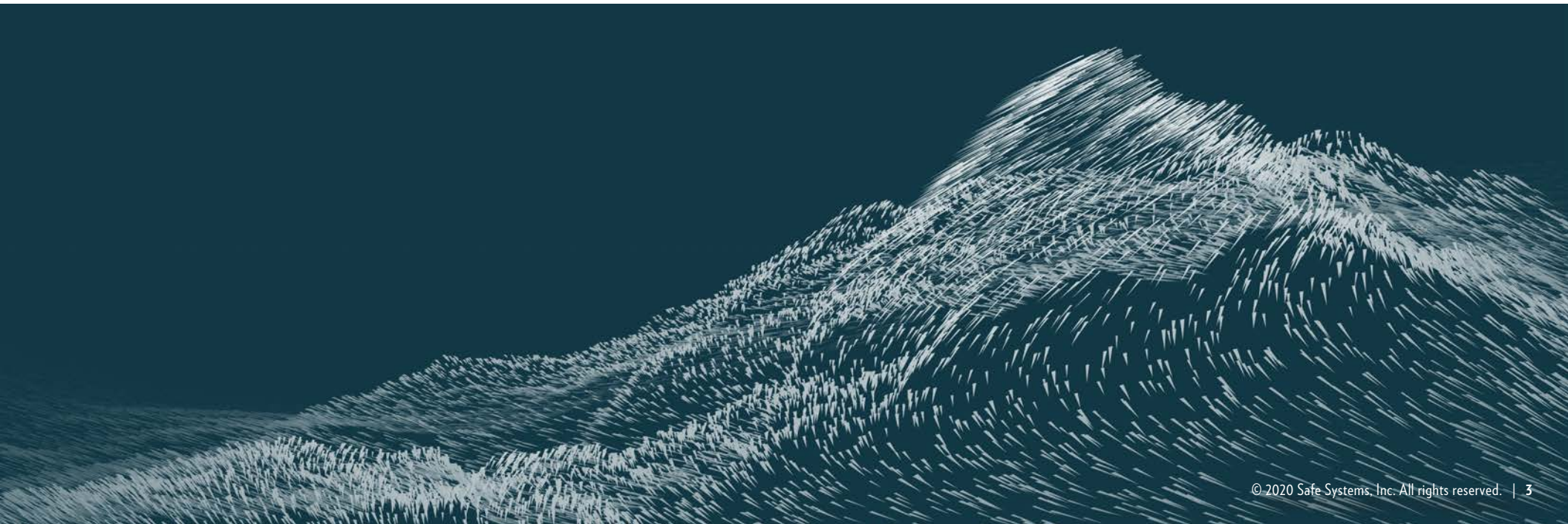
The plans should be **tested at least once a year**; the results of the tests should be thoroughly evaluated, and the plans should be revised based on the results. **These are not static documents** — the disaster recovery plan and BCP should be updated to meet changes in regulatory expectations as they occur to ensure compliance.

Key Steps to Prepare for Disasters or Business Interruptions

As mentioned, **first and foremost**, community banks and credit unions should **have an existing BCP and DR plan in place** as part of their BCM process. While storms and natural disasters cannot be prevented, proactively knowing what critical functions must be restored first provides confidence to executives and staff when responding to a disaster.

Beyond developing, implementing, and regularly testing your BCP and DR plans, **several additional steps can be taken to adequately prepare** for storms, natural disasters, and any other business outages, including:

- Ensure everyone is following the procedures in the BCP and DR plans and is aware of the proper communication protocols and contacts
- Monitor success of backups and/or replication services to DR site
- Utilize Uninterruptable Power Supplies (UPS) for short-term outages
- Preemptively shut down servers and all IT equipment in anticipation of an extended outage - if the equipment is not properly shut down, it can result in failures and malfunctions
- Safeguard the security of the server room making sure it is locked with separate key access and all equipment is secure
- Verify that all equipment and sensitive documentation is secure
- Ensure all ATMs are stocked as customers may require access to cash
- Confirm that key employees have someone to step in should they be unavailable during or after the disaster
- Validate the institution's BCP through appropriate annual testing and
- Confirm technology infrastructure will work in a disaster through an annual DR test



Pitfalls of Managing Technology In-house or with Local Providers

Preparing for or recovering from a disaster or business interruption could be particularly challenging for smaller community financial institutions that often lack the resources of larger institutions. They **may not have the IT staff or in-house expertise** to effectively manage their day-to-day IT Operations, let alone stay on top of their business continuity or disaster recovery responsibilities.

Many of these community banks and credit unions may try to **manage a disaster recovery solution in-house**, where all the hardware and software that is required must be implemented by an IT staff member. This is a very technical and time-consuming process, which can be a burden for institutions that already have limited IT resources.

However, if they choose to **outsource some of the technical responsibilities to a local provider** who may lack expertise in the financial services industry, they may face other difficulties.

Here are some pitfalls to be aware of when managing technology solutions in-house or with local providers:

DIY Disaster Recovery

Most DIY disaster recovery solutions involve multiple technologies along with automation, scripting, and well-documented procedures. These components and processes can be difficult for a static IT environment to manage. A DIY approach requires in-house resources to be available, and in the case of a disaster, communications may be limited, or the employees may be caught in the disaster themselves and unable to respond.

Email Outages

Working with a local provider who hosts the email server locally means the server might also be down due to possible power outages during a disaster. This is also true if the bank or credit union hosts email internally.

Backups

If backups are stored with a local provider, that provider is likely also affected by a disaster, meaning they might also be suffering from damage and loss that they need to recover before being able to help their customers. Furthermore, if using an on-premise backup solution, it brings into question whether backup media will be accessible and/or if it is damaged in the storm.

Evacuation

Some communities may be forced to fully evacuate, which includes bank IT staff, and the staff of the local service provider. The true damage and loss won't be known until they are allowed to return and start attempting to power back up.

Financial institutions, **no matter the size or location of the organization**, shouldn't have to recover on their own. When resources are limited, another alternative is **working with a managed services provider** who can act as an extension of the internal team and provide dedicated support **to ensure the institution recovers quickly and efficiently**.

Choosing an IT Partner to Support Your BCM Process

The hard truth is that several community banks and credit unions **are not adequately prepared or staffed for emergencies** and are unable to quickly recover from a disaster. Partnering with **a managed services provider can provide several benefits**, including streamlined internal processes, improved disaster preparedness, dedicated DR support, and confidence that your institution will be able to resume business operations.

When choosing a trusted IT partner to support your **BCM process**, look for a provider that has an **in-depth understanding of the financial services industry and banking technology solutions**. Here are some key requirements:

Web-based BCP Application and Compliance Expertise

It is increasingly more difficult to get what you need from a paper process. Updates to your BCP must occur when there are changes to regulatory requirements, changes to products and practices at your institution, or when your previous update was at least a year ago. Using a web-based application can help automate, streamline, and simplify the development and maintenance of your business continuity plan. Finding a provider who also offers a team of compliance experts who can provide guidance on testing, GAP analysis, and plan optimization will ensure your institution meets current requirements and is prepared for changing regulations and future trends.

Remote and Secure Back-ups and Data Recovery Practices

Backups should be in redundant remote facilities or the Cloud to ensure your data is always protected. In addition, you should receive proactive alerts when a backup has failed or has issues, allowing time to rectify the situation and ensure all information is stored appropriately. Also, providing annual testing of your disaster recovery plan and the integrity of backups ensures you can recover files and networks as documented in your BCP.

Available Staff and Engineers

With an outsourced solution, there are no evacuated IT personnel! All IT personnel are available to handle situations remotely 24 hours a day / 7 days a week. During a disaster, additional engineers should be made available to help immediately.

Guidance During a Disaster

Different managed services providers have different proprietary technologies to support you in the event of a disaster. For example, Safe Systems has a unique CRM software that enables us to target our customers who might be affected by a storm or other natural disaster. This allows us to contact and guide them through the preparation process as we remain on standby to help if issues arise. It's also important to ensure a provider can verify if you have current backups during a disaster by performing a thorough review of all protected systems.

Offsite Hosted Email

As a vital part of your institution, your email solution needs to function smoothly and consistently to support your business functions, even during a disaster. Hosted email eliminates the burden of running Microsoft Exchange™ internally; meaning email is not disrupted. Look for a solution that is designed exclusively for financial institutions; and includes extra layers of protection, such as SafeSysMail.

Cloud DR options

Cloud-based recovery solutions are not the only options but they can significantly speed up the disaster recovery process. In addition to faster recovery times, they offer the ability to access and restore data from anywhere and eliminate the time-consuming and error-prone manual recovery process. Each institution must evaluate its strategy to determine if cloud-based solutions are the right fit for their BCM process.

Conclusion

Developing, implementing, and regularly testing disaster recovery and business continuity plans is crucial in today's banking environment. Although this is a daunting task, institutions **can use automation or outsourced services to ensure their plans are continuously maintained and updated** as guidance and regulations change.

At Safe Systems, we have been working with banks and credit unions to support their BCM programs for more than 25 years. Our proven experience enables us to provide the services and assistance necessary to ensure our customers have the tools and guidance to restore critical functions and quickly recover from any disaster – natural or manmade.

If you're not sure if your institution is BCM ready, then request a complimentary plan review to ensure that your business continuity plan and DR plan are keeping up with changing regulations.

