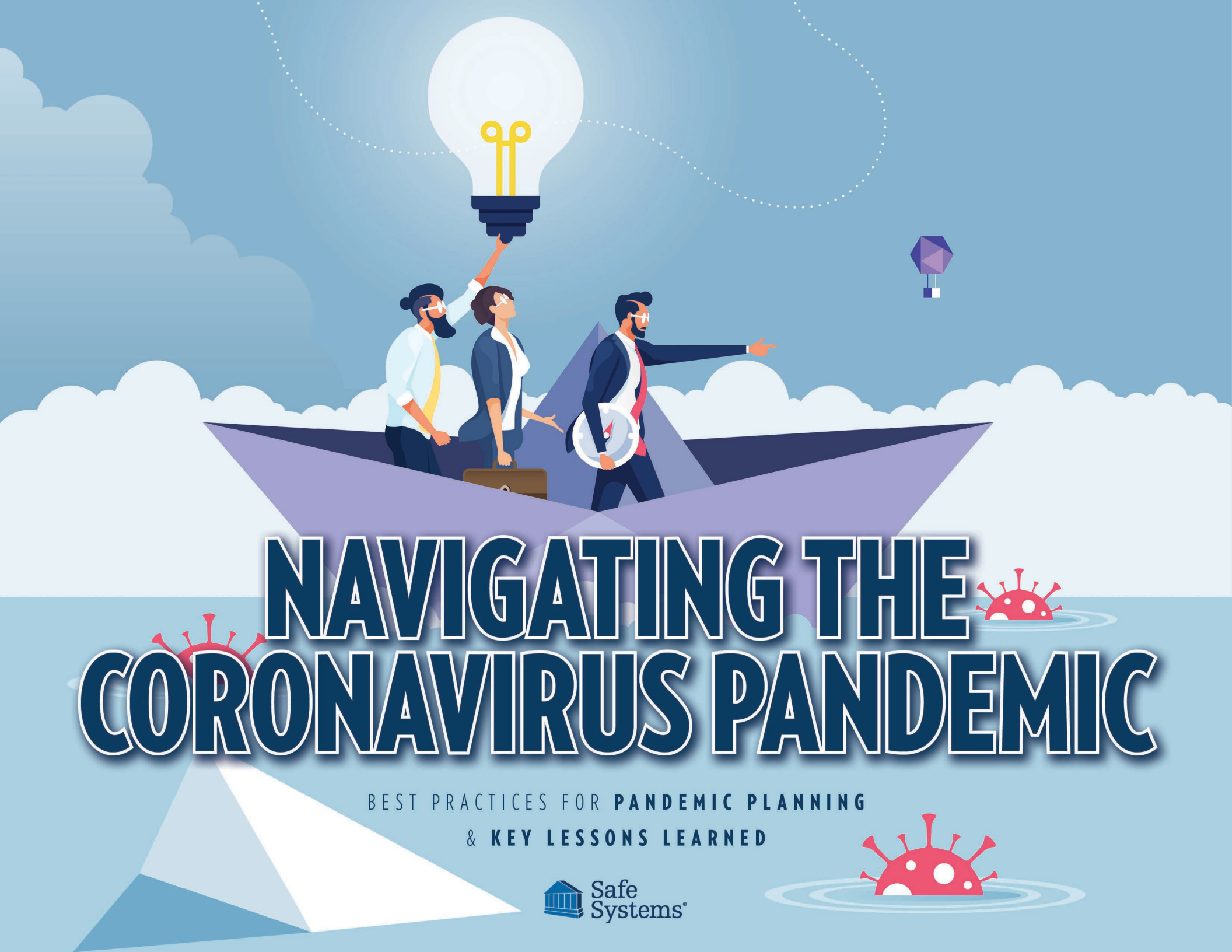


NAVIGATING THE CORONAVIRUS PANDEMIC

BEST PRACTICES FOR **PANDEMIC PLANNING**
& **KEY LESSONS LEARNED**

Safe Systems®

NAVIGATING THE CORONAVIRUS PANDEMIC

BEST PRACTICES FOR **PANDEMIC PLANNING** & **KEY LESSONS LEARNED**

The persistent coronavirus (COVID-19) pandemic is having a significant—and evolving—impact on the nation's banks and credit unions. Financial institutions are being forced to **react in real-time while trying to maintain a high level of best practices and resourcefulness** to ensure they continue to operate effectively for their employees, customers, members, and other stakeholders. Key areas of priority for institutions include pandemic planning, response, and testing; security for remote or mobile employees and customers; business continuity management (BCM) and succession planning; and preparing documentation for auditors and examiners. As the unprecedented pandemic persists, **banks and credit unions are learning important lessons**—and more insights will follow—as they grapple with how to address the present situation and successfully plan for an uncertain future.

Evolution of Pandemic Planning

Pandemic Planning Pre-COVID-19

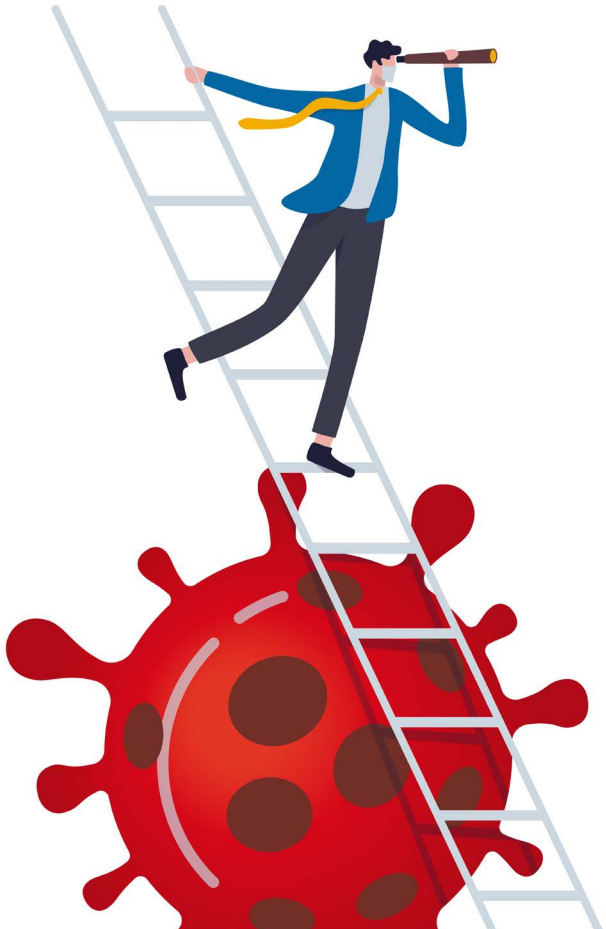
Prior to the COVID-19 outbreak, few banks and credit unions anticipated any healthcare threat lasting for an extended length of time. Consequently, their pandemic plan—if they had a comprehensive one available—was short-term in length. **The plan typically centered around addressing seasonal influenza (flu)** and made provisions for an outbreak to last anywhere from a few weeks to a month or two. Additional disaster planning focused on recovering from a hurricane, fire, flood, or some other sudden crisis.

Short-range planning for threats such as seasonal flu and hurricanes makes sense given their historically predictable and fleeting nature. Flu cases typically begin to increase in October, with activity peaking between December and February, according to the Centers for Disease Control and Prevention (CDC). Hurricane season officially begins on June 1 and ends November 30, according to the National Oceanic and Atmospheric Administration (NOAA). An average season is expected to produce perhaps a dozen storms.

Over the years, regulatory expectations for pandemic planning have evolved. Since 2007, financial institutions were required to have a separate pandemic plan, and regulators only looked for documentation that institutions were testing their plans periodically. In 2019, the Federal Financial Institution Examination Council (FFIEC) implemented a BCM update to deemphasize a pandemic by categorizing it the same as any other disruptive event. In effect, an institution's BCM should take a non-threat specific approach to process recovery. **As a result, the FFIEC no longer requires entities to have a separate pandemic plan**, any more than having a separate hurricane or snowstorm plan. Instead, they are expected to evaluate and manage pandemic risk similar to all other possible disasters, based on their probability and impact.

How Pandemic Planning and Response Have Changed

The impact of an event is calculated based on several factors: the suddenness of onset of the event, the duration of the event, and whether or not the event generally provides any forewarning. In the past, a pandemic event came on slowly, lasted maybe a few weeks, and provided plenty of forewarning. **Now financial institutions are planning for a long-term pandemic event, perhaps many months in duration, which was not considered to be reasonable in the past.** In addition, planning employs a different approach to ensuring that the proper personnel, security, incident response, and other measures are in place long after recovery from the event. The current coronavirus response underscores how pandemic planning has impacted the entire enterprise, and the measures taken and lessons learned will persist long past this specific event.



Regulatory Guidance on Pandemics

Agencies of the FFIEC have jointly issued guidance to remind financial institutions that **BCM plans should address the threat of a pandemic outbreak** and its potential impact on the delivery of critical financial services. The FFIEC Interagency Statement on Pandemic Planning identifies actions that financial institutions should take to minimize the potentially adverse effects of pandemics, which is officially defined as epidemics or outbreaks in humans of infectious diseases that can spread rapidly over large areas, possibly worldwide.

> *"Specifically, the institution's business continuity plan (BCP) should address pandemics and provide for a preventive program, a documented strategy scaled to the stages of a pandemic outbreak, a comprehensive framework to ensure the continuance of critical operations, a testing program and an oversight program to ensure that the plan is reviewed and updated. The pandemic segment of the BCP must be sufficiently flexible to address a wide range of possible effects that could result from a pandemic and also be reflective of the institution's size, complexity, and business activities."*
>
> **- FFIEC Interagency Statement on Pandemic Planning**

To adequately address a protracted health crisis, such as the COVID-19 pandemic, community banks, and credit unions **will need to tailor the guidance** outlined in the FFIEC Interagency Statement on Pandemic Planning to their specific organization.

Pandemic Intervals Framework

Financial institutions may also use the CDC's Pandemic Intervals Framework to help guide their pandemic planning efforts. The framework describes the progression of an influenza pandemic using six intervals or phases and includes recommendations for risk assessment, decision-making, and action in the United States. The six intervals, which also summarize a common method for entities to describe pandemic activity, are:

1. **Investigation** of cases of novel influenza virus infection in humans and animals
2. **Recognition** of increased potential for ongoing transmission
3. **Initiation** of a pandemic wave, with the ability to spread in a sustained manner
4. **Acceleration** of a pandemic wave, with a consistent rise in the number of cases
5. **Deceleration** of a pandemic wave, marked by a consistently declining number of cases
6. **Preparation** for future pandemic waves, once pandemic flu activity has diminished

In addition, large companies can refer to the Business Pandemic Influenza Planning Checklist developed by the CDC and the Department of Health and Human Services (HHS). The checklist includes specific strategies businesses can incorporate to effectively prepare for a pandemic or other emergency.

Impact of Face-less Banking

Know Your Customer

Financial institutions have traditionally operated on a know-your-customer (or member) rule before opening an account, completing a transaction, and sharing anyone's private information. Often, the most effective solution for satisfying this requirement (particularly for community banks and credit unions) is to verify customers face to face during their in-branch visits. Most customers like to be recognized and want to be trusted, but now institutions are having to increase their security posture to accommodate more remote, less personal, "face-less" transactions. Banking in a pandemic means **institutions must adopt a zero-trust stance** where every individual or transaction is presumed suspicious until proven otherwise.

Technology Updates

The know-your-customer principle is significantly affected by the use of online, telephone, and ATM banking as well as the drive-through and other channels that allow people to access their account without setting foot inside a brick-and-mortar location. **The remote delivery of banking services requires a whole new set of security protocols for customer verification.** This requirement can be more impactful to smaller, community institutions that rely more heavily on in-branch services, and it can be particularly challenging for all institutions during a pandemic when some branch locations have closed or offer limited hours and services.

Digital Adoption

As the pandemic accelerates the banking transformation, more consumers are demanding—and institutions are adopting—solutions that allow them to complete transactions remotely. Although financial institutions have invested extensively in brick-and-mortar locations, they are keen to **convert more customers to electronic banking during the pandemic.** (In fact, some banks and credit unions are gaining a renewed sense of appreciation for antiquated telephone banking!) As the pandemic persists, institutions are working diligently to expand and encourage customers' use of remote banking services even more, but increasing remote banking activity requires a careful balancing act. Every measure that is implemented to enable mobile customers increases the overall risk to the institution.

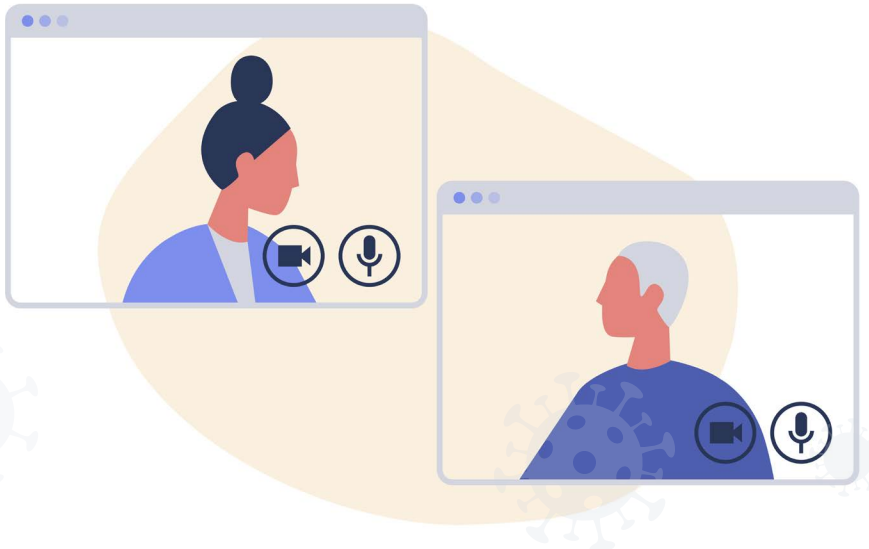
Security for a Remote Workforce

Security enhancements are also essential to facilitate the increased telecommuting workforce that many financial institutions have found themselves managing due to the pandemic. However, accommodating teleworking employees can be daunting. Personnel who have job duties that can be performed off-site must also have the capability to log into the corporate network remotely, and those **remote connections must be kept secure.** Teleworking staff must also have the appropriate office equipment, software, and other resources to support their ability to work from home productively.

A VPN is a common way to provide employees with a remote connection to the financial institution's network through an encrypted isolated tunnel. The VPN connection uses public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. But because VPN connections provide access to sensitive internal networks, the connections require additional authentication from remote users. This is particularly true for employees of financial institutions, which handle a variety of confidential information. In addition, telecommuters may also be able to leverage other methods of remote access, such as remote-control software and third-party services, file transfer software, conferencing/ session sharing tools, and other remote desktop software. Moreover, a VPN connection cannot normally block virus transmission, so remote endpoints must be kept up to date with anti-virus and antimalware.

Regardless of the technical solutions that are adopted, management should develop policies to ensure that remote access by employees, whether gained through their own devices or those of the institution, is supplied safely and soundly.

> *"Such policies and procedures should define how the institution provides remote access and the controls necessary to offer remote access securely."*
>
> **- FFIEC IT Handbook's Information Security booklet**



The booklet recommends the following remote access policy measures:

- Disable remote communications if no business need exists
- Tightly control remote access through management approvals and subsequent audits
- Implement robust controls over configurations at both ends of the remote connection to prevent potential malicious use
- Log and monitor all remote access communications
- Secure remote access devices
- Restrict remote access during specific times
- Limit the applications available for remote access
- Use robust authentication methods for access and encryption to secure communications

Most financial institutions have adopted a "bring-your-own-device" (BYOD) approach, but those that allow workers to use authorized remote access methods with institution-owned devices should take steps to enhance security. They should **consider implementing mitigating controls** such as restricting users from installing software or having administrative privileges on the devices. Institutions should also use firewalls, host-based IDS, and packet content filtering to identify, monitor, and limit remote access activities, according to the FFIEC IT Handbook's Information Security booklet.

Key Pandemic Response Tips (Reminders)

Cross Training and Succession Planning

Experts predict that perhaps the most significant challenge likely from a severe pandemic event will be staffing shortages due to absenteeism. In the short-term, assuming adequate cross-training has been provided, **employees could be rotated in and out of different positions**, such as repositioning a customer service representative to a teller line. In areas with a high degree of specialization such as funds management, HR, and shareholder accounting, cross-training is essential to ensure the process will continue uninterrupted.

It is also important for institutions to know how many staffing layers are available in their succession plan, especially during a pandemic. Having only one alternate identified for each position may not be enough if up to 40% of the workforce is unavailable. The succession plan can become compromised if there are not enough healthy employees to work in these areas. **Having a primary and a secondary alternate for key positions and processes is essential** because it can alleviate a potential staffing shortage.

Pandemic Testing

Financial institutions should have both exercise and testing components to ensure their pandemic planning practices and capabilities can help them maintain crucial operations during a crisis. An exercise is a task or activity that involves people and processes, and it is designed to validate one or more aspects of the BCP or related procedures. A test, on the other hand, is a type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment.

According to the FFIEC IT Handbook's Business Continuity Management booklet, management should develop a comprehensive exercise and testing program, including objectives and plans, to validate the entity's ability to restore critical business functions.

> *"Exercises and tests should occur either at appropriate intervals, when new risks are identified, or when significant changes affect the entity's operating environment. Significant changes can render existing test plans obsolete, so BCP(s) should be retested soon after the change … A key objective for management should be to develop a testing process that validates the effectiveness of the entity's business continuity program and identifies any deficiencies that may exist."*
>
> **- FFIEC IT Handbook, Business Continuity Management Booklet**

Since potential test scenarios can vary, pandemic testing requires revisions to be made to the scope of traditional disaster recovery and business continuity testing. This is especially important for institutions to keep in mind when addressing the extraordinary circumstances caused by the COVID-19 pandemic. **Ideally, an institution's pandemic plan should be adaptable enough to incorporate new information and risk mitigation approaches** as health care experts and governmental officials release updated details about the causes and effects of a pandemic.

In addition, management should **devise a realistic exercise and test scenarios that are risk-based.** The scenarios should simulate disruptions in business functions and assist management with ascertaining the institution's ability to fulfill business requirements as well as customer expectations.

> *"The goal should not be to execute perfect exercises without issues; instead, it should be to continuously strengthen the business continuity program and validate the BCP(s) … Management should identify and document assumptions used in developing each scenario. The scenarios should include threats that could affect third-party service providers and others, such as significant business partners."*
>
> **- FFIEC IT Handbook, Business Continuity Management Booklet**

However, the analysis must go a step further. Financial institutions should **record any issues discovered during the exercises and tests** and then create detailed action plans for resolving these issues.

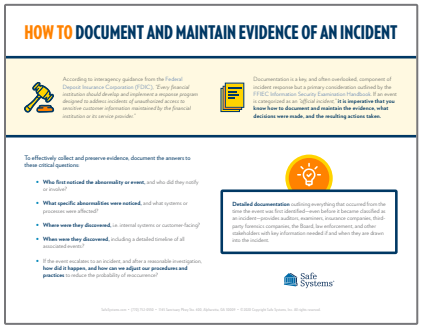
> *"Exercise and test results should be analyzed and compared with the objectives and success criteria in the exercise and test plans and reported to appropriate levels of management … For those items not remediated, management should document decisions to accept risks identified during the exercises."*
>
> **- FFIEC IT Handbook, Business Continuity Management Booklet**

Essential Priorities for Financial Institutions

Documentation

Few financial institutions are documenting their efforts and strategies as they are being implemented during the COVID-19 pandemic, but they should. **Whenever strategic changes have been made, examiners will expect to see the outcome of the institution's analysis**—even if the decision results in no changes being made. So, if an institution has determined it will not adopt any changes, examiners will want to know how it reached that conclusion. With loans, for example, they might want to know if the institution is able to originate new loans, has revised its lending standards, or is planning to modify its lending priorities.

Institutions should make it a priority to consider all the challenges they encounter during the pandemic and determine if any of them necessitate adjustments being made to their procedures. If so, they should incorporate them into their pandemic plan, so they will have a blueprint to reference if a similar situation arises. This might include cross-training staff or improving technology for an employee to work at home. In essence, institutions should track what they are doing, how they are doing it, and whether their inventive procedures warrant being adapted to their crisis management or response plan.



DOWNLOAD:
How to Document and Maintain Evidence of an Incident

The key is for institutions' steering or strategic planning committee to stop periodically and document—or backfill after the fact. However, they should not wait too long; **documenting should be done at least a month or a quarter later**. If institutions fail to document their processes, they will risk making the mistake of trying to go back to business as usual once the crisis subsides.

Lessons Learned

All banks and credit unions are distinct, so their approach to pandemic planning and response must be tailored to their institution. During this process, they will be learning lessons and applying them to enhance their operations. **Ultimately, all financial institutions will be assessed on their ability to improvise, adapt, and prevail—however they define these attributes.**

Strategic Planning and Technical Changes

Pandemic planning presents unique challenges to the management of banks and credit unions. Unlike natural disasters, technical disasters, malicious acts, or terrorist events, the impact of a pandemic is much more difficult to determine because of the anticipated difference in scale and duration. Therefore, to address the distinctive challenges posed by a pandemic, the financial institution's BCM plan should have a documented strategy. According to the FFIEC, an entity's **strategic planning should be developed to address all foreseeable risks**, and these risks should cover the potential impact on personnel, processes, technology, facilities, and data.

For example, management should also consider access capabilities for voice and data, mapping technology infrastructure to employee needs, and internal and external capacity—including remote capacity—to determine whether telecommuting strategies are sufficient.

> *"Strategies could include cloud architectures, virtualization, and other technologies ... Cloud solutions may provide a cost-effective and high-availability environment. Independent of the strategies selected for architecture and data protection, management should still be responsible for data integrity and overall resilience. Cloud-based disaster recovery services may be considered as part of resilience programs."*
>
> **- FFIEC IT Handbook, Business Continuity Management Booklet**

In Conclusion

Because of their vital economic role, financial institutions must have a plan in place to guide how they will manage through a pandemic event. **Having a sound, well-tested pandemic plan can minimize disruptions to the local and national economy as well as help the institution maintain the trust and confidence of its customers**—and the public. Amid the COVID-19 pandemic, banks and credit unions are having to consider higher risk profiles to accommodate more remote workers and customer-facing services. They are also making a variety of other modifications to cope with the impact of COVID-19.

Financial institutions need to document how they are responding and adapting to the unfolding global health crisis. Then once the pandemic finally abates, they should complete a post-incident assessment of the measures—both temporary and permanent—that were implemented to navigate their way out of the event. Examiners and auditors will be interested in any strategic adjustments that institutions made as well as what lessons they learned from their experience. With the long-term and pervasive nature of the current pandemic, examiners simply will not accept institutions reverting to business as usual.

Thankfully, community banks and credit unions can enlist a third-party expert, such as Safe Systems, to evaluate their current situation, and recommend and implement appropriate IT, compliance, and security solutions. Safe Systems offers a wide range of fully compliant solutions, from IT support and managed services to business continuity and disaster recovery. Our services not only make it easier for financial institutions of any size to weather the coronavirus crisis but can also help them emerge in an even stronger position.

Learn More: Safe Systems® | Pandemic Resources for Community Banks and Credit Unions