TruStage™

Business continuity

Tabletop training exercises

Working through a simulation of a real disaster allows us to ourselves and learn from our successes and mistakes. On the other hand, if we think the organization is already fully prepared, then it can serve as a forum for proving it to others. A tabletop exercise is a great way to get plans off the written page and talk through a simulated disaster.

Testing can be a full-scale production that involves first responders and professional moderators. Or it can be a simpler affair conducted by an internal disaster planning cross-functional team.

The idea is to have an escalating scenario that unfolds in several segments in which working groups conduct a practical gut-check of how they'd respond and report back findings or gaps.

Testing should be conducted using realistic conditions by simulating circumstances that could impact the credit union during an actual emergency. It is critical to approach testing as more than a "check the box" exercise and instead leverage the activities as an opportunity to improve on plan weaknesses and inconsistencies.

Frequency of testing

Opinions vary for the frequency in which tests should be conducted since credit unions are unique and utilize different platforms and structures. What's important is that the plan remain up to date and allow for efficient recovery of critical systems and business functions.

In general, testing and updating your plan should occur at least annually. Always re-educate when changes are made, including training for newly hired employees.

Building a robust business continuity plan

- Put together your team
- Assess risks including insurance needs
- Identify critical functions, systems, and dependencies – including vendors - needed in continuing member service
- Establish a back-up office alternative
- Develop an emergency management plan
- Create a crisis communications plan
- Build a disaster recovery kit
- Prepare your employees
- Test your plan – incorporate lessons learned

An untested plan Is like having no plan at all.

3 testing exercise types

Document review

During a document review, assigned disaster team members will review recovery plans, procedures and other related business continuity policies to seek out weaknesses or missing components in the documents.

After an initial review, the team should hold a discussion session to discuss any issues that were identified, and answer questions or concerns brought forth by the team. This is also a great time to thoroughly review responsibilities outlined in the plan to ensure all critical roles are clearly defined and appropriate team members are assigned.

A thorough plan review ensures that all documents are complete and consistent, and everyone is familiar with both their role and their teammates' roles should disaster strike.

Tabletop exercise/simulation

A tabletop or simulation test serves as a mock live scenario where team members are required to demonstrate that they know their duties in an emergency. This may involve engaging your continuity resources and recovery sites in various scenarios to determine how your strategy changes based on the specific threats or disasters.

This activity can also help to identify risks that could cause disruptions to IT services, applications and other business functions or processes. For example, a server room that does not have a backup source of power will mean that services are not available during a power outage. Focus on the implications if the event occurs and if a strategy needs to be developed to address the risk.

A well performed tabletop or simulation will help to identify documentation errors, missing information, or other inconsistencies in your disaster recovery plan before you try to enact the plan in a live scenario.

Live test/operational walk-through

Live testing and operational exercises typically include testing end-to-end recovery of multiple systems (both internal and external), the associated network infrastructures that support connectivity of those assets, and the facilities that house any primary and backup systems.

5 sample testing scenarios

Since disasters can occur anytime, anywhere, and can strike in a variety of ways; scenarios could range from natural disasters to technology failures and everything in between. You can decide the amount of impact you want to use within your testing scenarios.

- Do you want this test to be a physical event with assets damaged and destroyed, or do you just want those things inaccessible?
- Are employee losses included, or are you just testing the ability to get up and running somewhere else?

Scenario 1: Disgruntled employee

An angry IT employee with administrator privileges has turned off monitoring and destroyed a key system prior to being terminated. Due to the use of stealth, back-door tactics, current IT team members cannot properly ascertain how the damage was done or where it was accomplished. The receptionist takes a call from someone who indicates that this damage is "only the beginning" because of how the organization has treated them.

Scenario 2: Storm impact

- After a powerful storm, power is out for several days throughout the town including your credit union. Department of Health on Monday states that any building without running water cannot open for business.
- The credit union must decide what to tell employees; however, several key individuals that are part of your crisis communication plan cannot be reached.
- Members are calling looking for financial services and your voicemail is full, yet employees cannot get to work.

Scenario 3: Trucker hits power cable

When the accident happens, the whole building shakes. Many wall decorations and hanging light fixtures fall, causing a few employees to be injured. Lights go out and only one emergency backup light stays on.

Scenario 4: Corporate headquarters destroyed

The entire building that houses your offices is destroyed overnight. Your current business continuity plan names a secondary work location that is not meant to be long-term, and your credit union needs a more long-term solution since your branch offices are more than 30 miles away. While work-from-home policies are in place, they don't support many of the needs such as infrastructure housing, meeting hosting, or equipment storage, that need to be immediately addressed.

Scenario 5: Civil unrest interrupts office access

For several blocks surrounding the office, civil unrest has erupted. Your corporate headquarters are in an area where much of the activity is occurring, This activity has prevented employees from being able to get to work as most of the city's transportation services have been disbanded until everything can return to a safe level.

In addition, there has been some looting and vandalism at your office. Many of your systems are destroyed and some paper records have been set on fire.

- Encourage misinformation within the scenario, as timely decisions are often made with inaccurate or incomplete information.
- Simulate the confusion by giving groups roadblocks or messages with different information.
- Don't allow verbal communication to reinforce the need to be clear and concise.

Effective planning - tips for consideration

Testing the disaster preparedness or business continuity plan is often considered a disruptive, tedious and therefore dreaded activity. However, proper planning can go a long way in helping to ease the burden while also ensuring a positive and valuable exercise.

Like any activity that takes staff away from normal day-to-day duties, a step in gaining their enthusiasm and full commitment is letting participants know how the testing activity serves the greater good of the organization.

Plan development

- ☐ Written plan should be reviewed and approved annually by the CU Executive team and the Board of Directors; and, distributed to all employees. Gain buy-in and collaboration.
- ☐ Keep both hardcopy and electronic versions of the plan. Ensure disaster team understands where to access the plan if needed.
- ☐ Establish designated evacuation routes and emergency rally points for employees and members.
- ☐ Review plans for system vendors, buildings/ facilities, and consultants at least annually.
- ☐ Maintain an up-to-date and organizational chart of staff and chain-of-command - including contact information, job duties, and their responsibilities during a disaster. Assure that each response function has at least a primary and alternate responder.

Business impact analysis

- ☐ Safety of people should be considered priority.
- ☐ Understand that location is central to recovery. Be sure to anticipate the impact to back-up plans, facilities, and preparedness of key partners/vendors.
- ☐ Identify critical operational hours and allowable downtime to help establish deliberate prioritization.
- ☐ Focus on risk and threats facing critical business processes, functions, and dependencies. Consider all branch locations, geographical areas, region-specific climates, probability and potential impact.
- ☐ Ensure data is backed up to external media, encrypted, and tested to verify data integrity and recoverability.

Communications

- ☐ Build-in crisis communications and messaging. Know what is planned to communicate, through which channel, and by whom. Be brief, pertinent, consistent, and timely. Establish various communication methods.
- ☐ Consider all audiences: employees, volunteers, members, partners/vendors, community, and media.
- ☐ Designate a Staff Security Marshall to guide and lead in the event of an emergency or disaster during the workday. Identify employees that are trained in basic first-aid, CPR and using the Automated External Defibrillator (AED).

Effective planning - tips for consideration

Office preparation

- ☐ Prepare a basic emergency supply kit and medical kit including an Automated External Defibrillator (AED). Check kit contents and replenish at least annually.
- ☐ Obtain agreements for Backup and Hot sites, including secondary backup sites if necessary.
- ☐ Establish policies and procedures for employees to telecommute or work virtually, including remote access and online support resources. Maintain a list of staff capable of working remotely.
- ☐ Determine a succinct and organized process for restoring daily operations in the event of an interruption.
- ☐ Train all staff on the credit union disaster and recovery plan.
- ☐ Maintain an inventory of all computers and equipment at each location.
- ☐ Identify essential alliances, nearby ATMs (owned and non-proprietary), and the proximity of shared branch network locations.

Plan testing

- ☐ Conduct quarterly testing on robbery, bomb threats, extortion, and active assailant incidents.
- ☐ Test how quickly you can pull together key employees and staff to respond to disasters.
- ☐ Involve individuals at all levels from multiple function areas. Make sure each person has a clearly defined role, understands the specific responsibilities of their role, and knows what to do if someone is unavailable.
- ☐ Assure team members and contact information is accurate – including that of key vendor partners; and that everyone knows one another before a real incident.
- ☐ Acknowledge that some employees, especially first-timers, may be nervous during the testing exercise.
- ☐ Start with mission critical functions such as branch access, core processing, funds transfers, card processing, website / online banking, and cash operations. Don't limit testing to those activities, however, consider secondary functions like payroll processing and email as well.
- ☐ Test application recovery, not just data recovery. Understand the applications and their interdependencies.
- ☐ Allocate enough time and resources to ensure that participants can focus on plan testing without interruptions. In some instances, it is more efficient to host testing activities outside of normal business hours. Some test scenarios on the other hand may be more effective if conducted during normal office hours.
- ☐ Be thoughtful of common impacts such as extra expenses following the disaster, disaster length, and demand surge related to necessary resources.
- ☐ "Re-test" critical functions after updates have been made to measure their effectiveness in elimination flaws.
- ☐ Documentation is very important and will aid in tracking testing initiatives, issues identified and recommended plan updates. Always use a test plan document to record the exercise and require the documents to be retained for future review.
- ☐ Take the lessons with you! Have a designated note-taker that tracks what happens during the testing. exercise. Always leave time to share and discuss lessons learned.

Developing your own testing plan

Test scope
Include purpose of test, any predetermined success criteria and functional areas to be included. Document facilities used to conduct data recovery simulation if applicable. Outline all equipment and supplies used for the test including assets stored off-site that will be used during testing and recovery.

Test procedures
Define all exercise steps in a logical sequence. Include items that were provided to the team during the pre-test phase as well as any surprise items included to assess response readiness.

Scenario description
The scenario makes the difference by introducing key events that occur during the disaster. Choosing the right scenario can make an otherwise mediocre exercise a memorable and valuable experience for the participants and the credit unions. The scenario is the centerpiece of the exercise.

Consider including :

- Event type that has caused the disruption
- How and when it was discovered/reported
- Extent of damage to the credit union site and anticipated period of unavailability
- Extent of damage to equipment/contents, including timeframe for replacement or repair
- Effect on other facilities, surrounding geography, voice & data communications, personnel, etc.

Participants & roles
List all employees participating in the test and their primary responsibilities. For example, your test team may include a disaster recovery coordinator to lead the testing activities and document all findings, functional managers for the areas to be tested who will provide operational knowledge and procedural expertise and IT personnel to assist with system interdependencies and application recovery.

Business units & functional areas likely affected
When identifying areas that will be affected by the event it is important to consider system interdependencies. There may be several systems or applications that are impacted by an event that may not be identified in the original test scope.

Observations
Document all observations throughout the testing process. During live or functional testing, it is important to document the various team members and subsequent activities. Make note of the performance and understanding of everyone's responsibilities, carrying out activities relevant to the recovery, and coordinating with personnel and other teams.

Looking for additional insights?

If you'd like to discuss in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at **riskconsultant@trustage.com** or at **800.637.2676**.

TruStage™