

# BUSINESS CONTINUITY PLANNING AND THE NEW FFIEC GUIDANCE

## Executive Summary

In May, the Federal Financial Institutions Examination Council (FFIEC) issued revised guidance for examiners and financial institutions on business continuity planning (BCP).

According to the FFIEC, the booklet, "provides guidance and examination procedures to assist examiners in evaluating financial institution and service provider risk management processes to ensure the availability of critical financial services."

A comprehensive business continuity plan does more than meet FFIEC regulations; it proves to customers, employees, and others that the business will withstand any disaster. In today's fast-paced, volatile business climate, financial institutions cannot risk having outdated, incomplete, or inefficient plans and need to automate the plan building and maintenance processes. For this reason, many community financial institutions are searching for a planning tool developed to meet specific needs and regulatory requirements.

This paper outlines the new FFIEC guidance and discusses how PLANet®, an online business continuity planning tool from Strohl Systems, can help financial institutions meet them.

A business continuity plan is a collection of procedures and information that is developed, compiled, and maintained in

readiness for use to help an organization respond, recover, and resume in the event of a disaster.

The objectives of business continuity planning are to minimize disruptions to the financial institution and its customers, to minimize financial loss, and to ensure that operations resume quickly if a disaster occurs.

The FFIEC has published a Business Continuity

Planning booklet, which provides guidance and examination procedures. This booklet helps financial institutions develop detailed processes, thereby ensuring critical financial service availability.

The booklet is an update to work published in 1996. The comprehensive guidance reflects the fact that BCP has changed immensely in the last seven years. Changes include an increased emphasis on senior management and boards of directors involvement, enterprise-wide planning, interdependencies, and plan testing and updating.

The FFIEC advises that comprehensive planning should be conducted using the following, sequential structure:

- Business Impact Analysis,
- Risk Assessment,
- Risk Management, and
- Risk Monitoring.

## Business Impact Analysis

The first step in the BCP process is to conduct a business impact analysis (BIA). A BIA is the foundation of any viable recovery planning effort. It is a management-level assessment of financial and operational impacts that would result from a prolonged disruption of business operations. It is often an eye-opening process that further underscores the need to establish continuity planning in an organization.

In addition to financial and operational impacts, a sound BIA should identify extraordinary expenses that could be incurred from a disaster, the organization's current state of preparedness, any single points of failure, technology requirements for recovery, special recovery resources needed, and the organization's critical information systems. The results of the BIA are used to develop recovery requirements for computer processing, telecommunications, and business units.

A comprehensive BIA can also be used to help garner senior management support by showing the cost of not building a continuity plan should a disaster occur. When senior executives see dollar amounts attached to potential outages, they begin to take BCP a lot more seriously.

The BIA begins by developing and distributing a sur-

## Business Impact Analysis

BIA Professional® from Strohl Systems is the world's premier business impact analysis tool and, when used in conjunction with PLANet<sup>2</sup>, can ensure that your organization has effective, thorough information on which to build your plan.

In addition, PLANet's experienced, certified business continuity consultants have conducted hundreds of business impact analyses for financial institutions. Strohl Consulting Services can help customize an effective survey for your organization, or can manage the entire process.

# BUSINESS CONTINUITY PLANNING AND THE NEW FFIEC GUIDANCE

( C O N T I N U E D )

vey. The survey contains questions such as:

- Does your business unit have reporting requirements to any regulatory body such as a government agency, office or commission?
- Under the “worst-case scenario,” how long could your business unit be completely idled before it would have a significant impact on the overall organization?
- Do your business processes use any special, or one-of-a-kind items to conduct normal operations?

Knowing what questions to ask and what information will be needed is the key to the survey. Without much experience in BCP, this can be a very difficult process.

An effective solution to this problem is to purchase a BIA software package. The software comes with pre-written and formatted questions that users can pick through or customize for their own BIA. You can even find software packages that feature electronic assistants designed to guide the whole BIA process step-by-step from building the survey to analyzing the data to presenting the information.

## **Risk Assessment**

The next step recommended by the FFIEC is to conduct a risk assessment, which involves identifying specific risks an organization may face.

When conducting a risk assessment, it is important to remember that you should focus on the impact of possible threats more so than the nature of the threat. For example, a severe winter storm may not necessarily cause physical damage to your facilities, but it could disrupt the power, making it impossible to conduct most business processes.

Usually, it produces a risk matrix that plots the likelihood or probability that an event will occur versus the severity of a possible disaster. Using the results of a risk assessment, organizations can try to mitigate as many risks as possible, avoiding certain business disruptions

altogether. For the risks that either cannot be mitigated, or cannot be mitigated in a cost-effective manner, the organization will need to build continuity plans.

Historical data and educated judgments should be used to determine the probability and severity of particular disasters. For example, the likelihood of a hurricane hitting an organization located on the eastern coast of Florida can be determined by studying weather data. The severity of the event would depend on many factors, many of which would ultimately be determined by a best professional judgment.

A multitude of potential threats should be considered. Threats include natural disasters (earthquake, flood, hurricane, etc.), intentional manmade disasters (war, acts of terrorism, hacking, etc.), and accidental disasters (power outage, equipment failures, software errors, etc).

## **Risk Management**

The FFIEC defines the risk management phase as “the development of a written, enterprise-wide BCP.” A solid plan should be written to deal with specific impacts. A plan should be written to recover and resume business operations based on the fact that the facility is no longer available. It may not particularly matter that a fire, flood, or other disaster has rendered the facility unusable.

The contents of a plan vary widely from one organization to another. But, at a minimum, a plan should contain the following:

- Documented procedures and resources necessary to recover critical business functions;
- A prioritization of recovery for processes and operations;
- Information about who can declare a disaster and under what circumstances;
- Contact lists of critical personnel (including employees and vendors);

## **Risk Assessment**

PLANet’s comprehensive risk assessment feature can help determine where the institution is most vulnerable. The risk assessment includes the probability, forewarning, onset, and potential duration of a particular risk, and it can be edited to completely tailor it to a particular institution. It generates a risk report that highlights the areas where you’re most exposed. The risk report provides a risk matrix and a gap analysis, highlighting organizational vulnerabilities.

# What PLANet Can Do For You



The FFIEC has issued new guidance for business continuity planning (BCP). The new guidance means that planners at community financial institutions will be facing tougher questions from auditors. PLANet from Strohl Systems is an Internet-based BCP tool designed specifically for community financial institutions. PLANet automates plan building, facilitates plan maintenance, and provides built-in BCP experience. It is a comprehensive planning tool that meets and exceeds FFIEC policy. PLANet is also easy to use, flexible, and affordable. The features of PLANet are outlined below. For more information visit [www.planetstrohl.com](http://www.planetstrohl.com) or call 1-800-634-2016.

## **Manage My Resources**

From the moment you log on to PLANet, you'll be given access to any part of your plan from your Manage My Resources screen, enabling you to manage your entire plan from a single home page.

## **Creating Your Plan**

Using PLANet to build your plan is simple. Log on and follow the step-by-step instructions. PLANet's intuitive instructions are so easy to use no lengthy training is needed. When a crisis or a loss of service strikes use PLANet to access critical, accurate information fast. It is available anytime; from anywhere there is an Internet connection.

## **Risk Assessment**

PLANet's built-in risk assessment is essential to determine where your institution is most vulnerable. Simply click to enter the probability, forewarning, onset, and potential duration of a particular risk. PLANet generates a risk report that highlights the areas where you're most exposed.

## **Predefined Recovery Teams/Roles**

Simply click on one of the predefined recovery teams and PLANet generates responsibilities, possible company positions to fill that role, and the employee personality traits that best support the role. With a simple click, PLANet lets you select which employees are best suited for that role. It's that easy to assign employees to recovery teams and roles.

## **Predefined Recovery Tasks/Resources**

PLANet provides 59 recovery procedures for your organization's various functions and the resources needed to support all your recovery efforts. Simply review and customize PLANet's built-in scripts to your liking.

## **Enhanced Importing**

PLANet's import wizard is capable of transferring employee records, vendor, software, and equipment data with easy to follow step-by-step instructions that make importing information simple.

## **Plan Printing**

PLANet gives you the choice of either printing your entire plan or just your individual recovery scripts. You can print to paper, or keep it in electronic format (PDF). You also have the ability to incorporate any of the over 50 standard reports into the plan.

## **Testing Schedule**

PLANet's test scheduling feature shows all business units and departments along with information on when their plan was last tested and when additional tests are scheduled.

## **Call Chain**

PLANet lets you build a comprehensive call chain quickly and easily. With just a few clicks, you can build a call tree that accounts for every employee.

## **Plan Progress**

The Plan Progress feature is essential, as it helps you stay on top of your planning efforts. PLANet's Plan Progress feature lets you keep track of the last time any area of your plan was modified and whether or not your plan has been approved for use.

## **Vital Records**

How useful are documents and vital records stored in a fireproof cabinet in a building you can't enter? Use PLANet to protect or store any document. Simply scan or copy them into electronic form and easily import them into PLANet.

# BUSINESS CONTINUITY PLANNING AND THE NEW FFIEC GUIDANCE

( C O N T I N U E D )

- An inventory of critical equipment, office supplies, computer equipment, software, and documents;
- Specifications for an alternate site (if necessary); and
- Descriptions of the responsibilities and procedures to be followed by each continuity team.

The plan should also identify methods and procedures for maintaining and testing the plan. The new guidance states, "a BCP is a 'living' document; changing in concert with changes in the business activities it supports." It further states that plans should be reviewed and updated at least annually to ensure that changes in business processes, technology, and personnel are adequately reflected in the document.

The final plan may be a complex document. In order to manage it, organizations may want to consider using automated software.

## Risk Monitoring

The final sequential step outlined in the FFIEC guidance is risk monitoring. "Risk monitoring ensures a BCP is viable through testing, independent review, and periodic updating," according to the guidance. Testing helps financial institutions adjust recovery time objectives by giving realistic, tested time estimates needed to complete tasks. A thorough testing program also makes sure that the plan does not overlook resources needed for recovery or are not used elsewhere in the recovery process.

The FFIEC guidance outlines four types of tests a financial institution may perform. They are:

- Walk-through - Consists of key planning participants discussing how to handle a crisis. Its primary goal is to ensure that personnel are familiar with the financial institution's continuity plan and takes place in an informal setting.
- Tabletop Drill - Consists of a scenario with a specific event for which recovery personnel have to run the continuity plan. It usually involves more role-playing and its goal is to practice and evaluate specific recovery tasks.
- Functional Test - Involves actually completing some of the recovery tasks and may include sending personnel to alternate sites. One of its goal is to set realistic recovery time objectives by measuring the time to complete certain tasks.
- Full-scale Test - Involves testing all aspects of a continuity plan. Data and transactions are processed at an alternate site. It usually takes place over an extended period of time and its goal is to test all aspects of a BCP plan.

Choosing which test works for a financial institution depends on the objective of the planners.

Additionally, a formal audit of the entire business continuity plan should be conducted at least annually and the entire plan should be presented to management and the Board of Directors for approval.

The guidance suggests that an "independent party should review the adequacy of the business continuity process to ensure the board's expectations are met." It further suggests that the independent auditor should directly observe the financial institution's BCP tests.

## Additional Considerations

In addition to the four phases of business continuity planning, the new FFIEC guidance also provides other suggestions.

It outlines five specific areas of responsibility for senior management and boards of directors with regards to BCP. Among the things auditors will be reviewing is whether a financial institution's leadership is allocating sufficient resources and personnel to the planning

## Risk Management

Hundreds of financial institutions are using PLANet to build their continuity plan. The tool's advanced plan-building features can save time and money. And, since PLANet is online, it is available anytime; from anywhere there is an Internet connection.

PLANet's predefined recovery teams and roles, 59 customizable recovery scripts (tasks and resources needed for recovery), and easy-to-create call chain enable users to quickly build a plan that can pass any audit – and more importantly – effectively recover a business.

The predefined recovery teams and roles enable users to link people with recovery processes. When selecting one of the recovery teams, PLANet automatically generates responsibilities and creates possible positions to fill the role and the personality traits that best support it. This feature makes it easy to assign employees to recovery teams.

Since PLANet is a relational database, changes are simple to make. Users need only to change information once and it is updated throughout the plan. The global replace and delete makes plan maintenance and review easier, helping ensure that the document is always up-to-date.

Building a plan can be a complex process without the proper tools. It doesn't have to be with PLANet.

# BUSINESS CONTINUITY PLANNING AND THE NEW FFIEC GUIDANCE

( C O N T I N U E D )

## **Risk Monitoring**

Keeping track of test results can be arduous, but PLANet's test scheduling feature helps users stay on top of testing efforts. The testing view shows all business units and departments along with information on when their plan was last tested and when additional tests are scheduled. It helps ensure that plans are always up-to-date through testing. The testing schedule contains all of the results encountered during the testing phase, making audits easy. Additionally, PLANet enables users to document the results of a test for independent auditor review.

PLANet facilitates the process of review and approval by providing a description of the contents of the plan contained within a memo to management and the Board. A printed copy of the completed plan accompanied by this written documentation provides a focused means of gaining approval of the plan, while providing formal documentation of the process for audit purposes.

process and whether the senior management is ensuring that the BCP is kept up-to-date and employees are trained as to their roles and responsibilities.

The new guidance also recognizes one of the most important changes in the BCP industry – planning for data recovery alone, cannot ensure the survival of a financial institution. Plans must be developed on an enterprise-wide basis and take into account people, technology, and facilities. All departments should be included in the development, testing, and execution of a successful plan. In fact, the FFIEC advises, "An automatic red flag should go up in examinations that reveal BCP to be the sole responsibility of a systems administrator."

Finally, the new guidance calls for examiners to determine if financial institutions have appropriate strategies that include, "alternatives for interdependent components and

stakeholders, including utilities, telecommunications, third-party technology providers, key suppliers or business partners, and customers and members."

## **Summary**

The new FFIEC guidance means examiners will now be asking tougher questions about financial institution business continuity plans. The new BCP booklet contains an appendix with recommended questions for examiners. It consists over 60 questions in 13 BCP areas of discussion and is a great starting point for organizations that are beginning the planning process.

Strohl Systems' PLANet can jumpstart or facilitate any institution's business continuity planning process by automating plan building, facilitating plan maintenance, and providing built-in, instant BCP experience and knowledge. Because FFIEC requirements are built into PLANet, users can follow PLANet's step-by-step guidelines and be well on the way to ensuring that all federal specifications are met and that any plan audit will be successful. For more information about PLANet, visit [www.planetstrohl.com](http://www.planetstrohl.com) or call 1-800-634-2016.

## **End Notes**

<sup>1</sup> *The FFIEC's Business Continuity Planning Booklet is available on their Web site at [www.ffiec.gov/ffiecinfobase/booklets/bcp/bus\\_continuity\\_plan.pdf](http://www.ffiec.gov/ffiecinfobase/booklets/bcp/bus_continuity_plan.pdf).*

<sup>2</sup> *More information about PLANet can be found at [www.planetstrohl.com](http://www.planetstrohl.com).*



**PLANet**<sup>®</sup>

For more information visit our website at [www.planetstrohl.com](http://www.planetstrohl.com) or call NetDiligence(610)658-0913