White Paper

Building and Maintaining a Business Continuity Program

Successful strategies for financial institutions for effective preparation and recovery

intel Security

This white paper was written by:
John Reeder
Principal Consultant
Foundstone® Services

Table of Contents

Introduction

With the increasing number of natural disasters, terrorism events, and unrest around the globe, the importance of business continuity planning and disaster recovery planning is becoming more apparent. The recent onslaught of these events has highlighted the importance of system availability and forced senior management of many organizations to think seriously about contingency planning. Senior management understands if systems are not available, financial losses occur by the hour and their business reputation drops rapidly. While business continuity issues don't always occur on a daily basis, it is important to prepare for the day a disaster does occur.

Contingency planning is a critical function that involves many different departments over multiple phases. As with many business continuity programs, an iterative process is most effective in developing a refined set of procedures. This strategy allows an institution to take advantage of knowledge gained and lessons learned through the development, testing, and maintenance of a business continuity program. The best practices of a business continuity program reviewed in this paper are categorized into four sections:

- **Management oversight**—Strategic and decision-making responsibilities with a top-down management approach for overseeing the overall business continuity program.
- **Risk management**—Procedures and steps taken to identify, prepare, and respond to threats and vulnerabilities.
- **Recovery strategies**—Business continuity strategies to increase likelihood of recovery in the event of a disaster.
- **Program management**—Governance of business continuity program through people, policy, and process.

Business Continuity Defined

Most employees incorrectly believe that business continuity is solely an IT process. The terms business continuity and disaster recovery are commonly used synonymously. While they are related, they are different functions within an organization. For this paper, the terms are defined as:

- **Business continuity**—The processes involved in managing exposure to internal and external threats that can disrupt the availability of an organization's business operations. This involves the management oversight, risk management functions and the documentation of plans and processes to maintain business in the event of a disruption of business.
- **Disaster recovery**—It's part of the business continuity program but is focused on the assets, people, processes, and technologies involved in critical aspects of business operations. Disaster recovery is often considered the IT portion of the business continuity program but it also includes key non-technology assets, people, and processes in recovering from a disruptive event.

A common debate within a financial institution is identifying who is responsible for the business continuity and disaster recovery functions for the organization. According to the *Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook for Business Continuity*, "It is the responsibility of an institution's board and senior management to ensure that the institution identifies, assesses, prioritizes, manages and controls risks as part of the business continuity planning process."

This means the financial organization's board and management are the ultimate owners of the business continuity program and have the responsibility of establishing policies and oversight. While senior management is responsible for oversight, day-to-day managers and staff are responsible for the implementation and maintenance of the plan. This includes business and technology managers and staff, so business continuity and disaster recovery should not be considered an IT-only function. Without business leader involvement in the business continuity program, the effectiveness of plans can be weakened and the recovery time during an event can be greatly extended or halted altogether.

While this paper is focused on financial institutions, the business continuity best practices outlined can be used by any organization in their contingency planning. Financial institutions are organizations that are significantly engaged in the exchange and transfer of monies and these institutions are members of the FFIEC. As such, they are required to adhere to the recommendations outlined in the *FFIEC IT Examination Handbook on Business Continuity Planning*. This Handbook is a great resource for the basis of formulating an organization's business continuity program. Four best-practice areas are outlined below for building and maintaining a business continuity program that includes disaster recovery best practices.

Business Continuity Best Practices

Management Oversight

As noted earlier, senior management approval and oversight is the first critical function in making a business continuity plan successful. Management has overall responsibility for the creation, funding, review, and maintenance of a business continuity program. Key management best practices include:

- Adopt a formal business continuity framework that will be the basis for the organization's business continuity policies and plans.
  - This framework will define the mission statement and business continuity planning objectives for the institution and delineate the organizational structure of the business continuity committees, teams, and specific business and technology recovery plans.
- Conduct regular risk assessments to identify the likelihood of threats and exposed vulnerabilities and their impact to the organization's environment.
  - Potential losses from downtime and recovery points and times are analyzed and established.
- Require periodic reviews, tests, and updates of each department's business continuity and disaster recovery plan.
  - Regular training for personnel should be included with testing to optimize response.

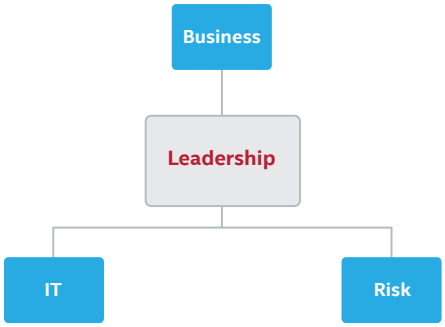

Figure 1. Oversight organizational structure example.

The business continuity framework established by management should include the creation of a crisis management team that is made up of executives and senior management who have the knowledge and authority to make the critical decisions during a disaster event. This crisis management team should have a documented plan that outlines the committee chair, coordinators, and potential alternates, as well as how the notification, communication, and purchasing process should be handled during and after a disaster event.

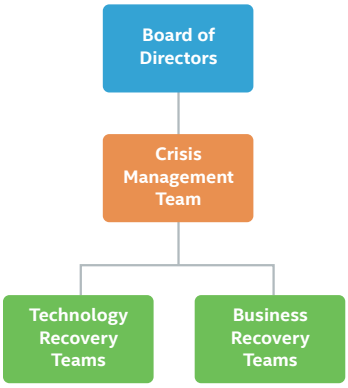

Figure 2. Business continuity management organizational structure.

This team should also oversee and coordinate with the technology and business recovery teams and designate who can communicate with external parties before, during, and after an event. Some additional roles and responsibilities include ensuring oversight of the emergency response and incident management functions, such as:

- Safety and health of the institution's employees and surrounding community.
- Timely and accurate assessment of an incident and any secondary impacts.
- Available personnel and resources to support a timely and affordable recovery.
- Property and financial losses are minimized.

Risk Management

A critical function in any business continuity program is to incorporate risk management into the planning process. Identification, classification, and management of the availability risks to an organization's location, people, processes, and technologies are the basis for the creation of business and technology recovery plans. A good risk management program includes identification of key legislation and regulations affecting the institution, insurance policies that can mitigate financial losses during downtime, and any financial industry codes of practice that may be affected or required during a disaster event.

Accounting Critical Business Process	Dependencies	Recovery Time Objectives	Customer Impact	Regulatory Impact	Financial Impact
Credit Card Processing	Network	Immediate	Medium	Low	>1 million
Point of Sale	Network, SFTP	1 Day	Low	None	>1 million
Payroll	App1, Fileserver	Immediate	High	High	>1 million
Accounts Payable	Network	1 Day	Medium	Medium	>1 million
Check Printing	Network, Email	1 Day	Medium	High	>1 million
Financial Analysis	Network, Fileserver	1 Week	None	None	>10k but <100k

Table 1. An example of a traditional business impact analysis matrix identifying critical business processes and the recovery time objectives and impacts.

The risk management program should include regular assessments of the threats to an organization, the likelihood they will occur, and what impact they could have given the present vulnerabilities an institution may have. These assessments are typically performed in what is called a business impact analysis. The primary objectives are to identify critical assets, business functions, availability requirements, and the operational and financial impact of downtime to the organization. The business impact analysis is crucial to aid in the development of an effective continuity strategy and the prioritization of business and technology recovery efforts.

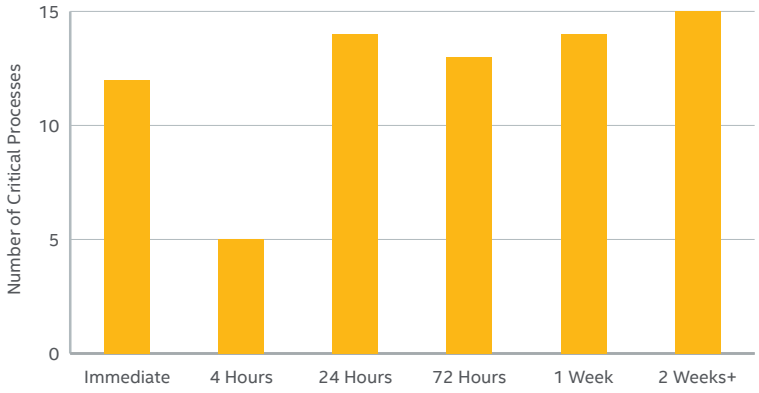

Figure 3. Business impact summary.

For successful achievement of an institution's availability risk management goals, the business impact analysis process should include the following:

- Identify critical assets, key business processes, vital dependencies, and the impact of potential business interruptions.
- Document recovery time objectives for critical systems and processes.
- Establish minimum requirements and recovery point objectives to restore business operations to an acceptable level.
- Prioritize recovery procedures from the identified recovery time objectives.
- Analyze service level agreements with vendors and suppliers.
- Identify and document critical assets:
  - People (employees, contractors, vendors).
  - Facilities (headquarters, branches, data centers).
  - Infrastructure (servers, workstations, laptops, phones, faxes, printers, work space).
  - Applications (automated clearing house, accounts receivable, check processing, deposits, bank cards, general ledger).
  - Equipment (technology hardware, calculators, check encoders, scanners, sorters, typewriters).
  - Vital records (logical databases and storage, bonds, check stock, cashier checks, cash drawers, check kits, GL tickets, money orders).

Recovery Strategies

With any business continuity planning, organizations will want to strategize and implement the best options for efficient recovery from an event. This will include business and technology strategies. From the results of the business impact analysis, institutions should base device recovery strategies on the identified threat impact and recovery objectives. From the business perspective, analyses should be performed to determine what costs will be associated. The following are critical areas where attention should be focused for development of a successful recovery strategy.

- Secure and stable information-processing facilities and office locations with adequate physical and environmental safeguards.
- Redundancy in communications and critical systems.
- Maintain data-protection procedures and conduct regular backups of critical applications, platforms, configurations, and data with off-site rotation.
- Use different vendors in contracting for critical services in order to limit a single point of failure in the event of a disaster and review vendor risks regularly.
- Identify and document information and procedures for contact with local, state, and federal authorities.
- Formulate and document emergency procedures that include maintaining adequate reserves of food, water, medical supplies, and batteries.
- Identify and establish regional diversity for alternate recovery sites for all critical business processes, including service providers, telecommuting, and alternative workforce.
- Conduct a cost-benefit analysis to determine the costs associated with recovery site alternatives and the distance from the primary site.

Figure 4. Example recovery strategy phases.

Program Management

The fourth and most difficult area is the management of the business continuity program itself and the underlying plans. This section involves the majority of the time expended in business continuity planning.

Business Continuity Policy

Program management involves implementing and maintaining the framework outlined by senior management. Implementation includes the creation and approval of a business continuity policy. The overarching business continuity policy outlines the high-level statements and goals of an organization's senior management. The contents of a business continuity policy are detailed in the table below.

Policy Element	Description
Purpose	Outlines the reason for the policy and objectives to be prepared to respond to the event in order to efficiently regain operation of the systems that are made inoperable from the event.
Scope	Details what locations, systems and processes are required to be able to respond to, recover, and restore business operations.
Ownership	Identifies the person(s) designated to enforce, maintain, and update policy.
Roles and Responsibilities	Documents responsibilities related to the continuity of business services. The persons and units listed have specific responsibilities with regard to the reporting and handling of disruptive incidents. Management, business, and technology teams' responsibilities are detailed.
Risk Management	Specifies the steps taken to identify, assess, and manage threats, vulnerabilities, and risks to an organization.
Plan Management	Defines the types of recovery plans for an institution and how plans are documented, tested, and updated.

Table 2. Example business continuity policy sections.

Just as with any other control policy, the business continuity policy should be reviewed regularly, updated as needed, and approved by senior management or the board of directors. This policy will drive the entire program and the personnel, plans, and procedures that support the operating environment.

Recovery Plans

The documentation of the business and technology response, recovery, and restoration procedures for each department in the organization is absolutely critical. Without accurately documented plans, organizations could be scrambling to identify which personnel, systems, or processes are required to recover. These plans should outline recovery procedures in a team- and role-based manner—with incident checklists—and should be laid out chronologically with assigned plan coordinators who oversee the distribution and storage of their plan. It is a best practice to store both a hard and soft copy of the recovery plans at the primary operating location and an off-site location.

These are examples of recovery plans:

- Crisis management plan.
- Disaster recovery plan.
- Business recovery plan.
  - Accounting.
  - Customer Service.
  - Human Resources.
  - Product Operations.
  - Sales.

The business and technology recovery plans should document the plans for relocating and recovering of critical business processes based on the recovery-time objectives and recovery-point objectives identified during the business impact analysis process. Identified potential emergency response procedures should be included in each plan, for example, pandemic, fire, and hurricane.

Team member names and contact information with work, home, and mobile phone numbers should be listed in each plan. This is critical for the initial part of any emergency response, notifying the business and technology subject-matter experts a disaster event has occurred. Most importantly, response, recovery, and restoration activities should take into account personnel safety, and physical and IT security in each plan.

The crisis management plan is a comprehensive emergency guide and checklist for how to react to an event that disrupts business and/or technology operations. Crisis management plans are designed for the crisis management team to use in reacting to any situation that cannot be effectively handled within the scope of normal business operations and resources. A crisis management plan includes the purpose for the plan, what is considered in scope, plan objectives, the organizational structure of the recovery teams, plan activation requirements, recovery strategies (emergency procedures, incident management, and business resumption), recovery team tasks and checklists, and contact lists and escalation procedures.

Unplanned disruption can result from a loss of a critical service, facilities, or personnel. Business recovery plans are designed to provide quick response to a disruptive event and manage the recovery process and limit the impact of an unplanned availability event. Business recovery plans detail the strategies, resources, and procedures involved in recovering from any short- or long-term business disruption. Departments that need a business recovery plan are accounting, human resources, sales, customer service, administration, and product operations. Some sample components of a business recovery plan are:

- Recovery strategies.
- Team organizational structure and responsibilities.
- Preparedness measures.
- Notification procedures and checklists for internal and external parties.
- Incident response steps and how team members are mobilized to respond.
- Key systems and tools.
- Vital records recovery.
- Recovery steps of each specific business function.
- Interdependence with other systems.
- Plan resource guides (crash books) that contain:
  - Recovery task checklists.
  - Phone contact lists for employees.
  - Contractors and vendors.
  - Reporting forms.
  - Location emergency procedures.

Emergency procedures describe the actions that need to be taken following an incident that jeopardizes business operations and/or human life. This should include procedures for handling public relations and liaison with appropriate public authorities such as police, fire, and local government. Emergency procedures include the step-by-step instructions on how to react when a specific emergency occurs. The types of emergencies can depend on the organization's geolocation and business model. The emergencies identified in the business impact analysis as the most likely to occur should have procedures developed and documented. Examples of emergency procedures include how to respond to a bomb threat or fire and an institution's response to a pandemic outbreak.

Emergency	Example Type
Notification	• How to Use 911
Environmental	• Fire • Tornado • Hurricane • Tsunami • Flood • Pandemic
Terrorism	• Suspicious letter or package • Bomb threat • Suspicious persons

Table 3. Types of emergency procedures.

The technology recovery plan is referred to as the disaster recovery plan. As noted previously, business continuity and disaster recovery are sometimes used interchangeably, but in reality, disaster recovery refers to the technology recovery planning and procedures. A disaster recovery plan is a documented set of procedures on how to recover and protect an organization's technology infrastructure in the event of a disruption. The plan specifies procedures an organization must follow when a disaster occurs.

As with the other plans, disaster recovery plans should include statements on purpose, scope, and objectives. In addition, it is recommended that technology recovery plans incorporate an iterative process in reacting to a disaster event. This staged process for recovery includes four procedural phases in addressing events that interrupted business operations. These consecutive phases are:

Figure 5. Disaster recovery phases.

The **response phase** involves establishing a plan coordinator or their delegate presence at the incident site. This individual performs an incident assessment to measure the impact and extent of damage and disruption to services and business operations and provides a timely report to the crisis management team and disaster recovery plan coordinators.

The **resumption phase** includes the establishment of a control center to oversee the resumption of operations and mobilization of the support teams involved in the resumption process. In addition, the resumption phase involves the notification to employees, vendors, and other internal and external individuals and organizations that a disaster event has occurred.

The **recovery phase** involves the implementation of the procedures needed to facilitate and support the recovery of critical business operations and the coordination with the crisis management team, disaster recovery plan coordinators, and with employees, vendors, and other internal and external individuals and organizations.

The final phase is the **restoration phase**. This phase contains the procedures necessary to facilitate the relocation and migration of business operations to the new or repaired facility.

Each of the four phases involves exercising documented plans and procedures and the teams involved in executing those plans. The teams associated with the plan represent functions of a department or support functions developed to respond, resume, recover, or restore operations or facilities of an organization and its affected systems.

In order for these phased recovery procedures to be successful, a communicated organizational structure needs to be established. The organizational structure for a disaster recovery plan includes specialized teams that are structured to provide dedicated, focused support in the areas of their particular experience and expertise for specific response, resumption and recovery tasks, responsibilities, and objectives. Each team goal is the recovery and return to normal for business operations. A sample technology recovery team structure is displayed below.

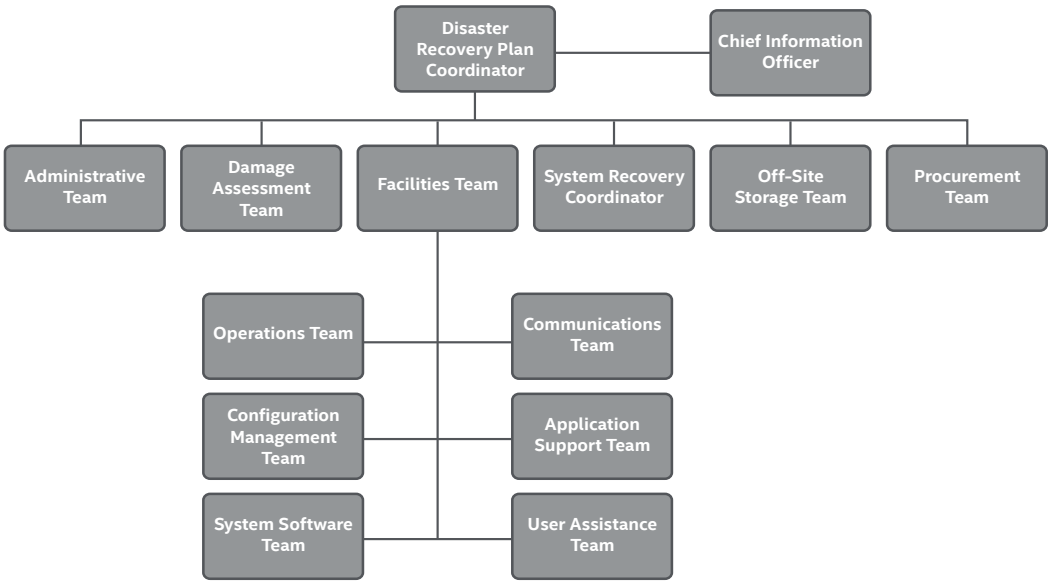

Figure 6. Example disaster recovery team organizational chart.

Plan Management

A key aspect to business continuity program management includes the handling of documented plans and maintaining the plans on a regular basis. Dedicated personnel should be employed to manage the business continuity program and associated plans. These business continuity planning professionals are tasked with documenting the business continuity policies and plans and updating when necessary. In addition to managing the recovery documentation, business continuity planning personnel should devise and oversee the awareness and skills training for recovery plan team members and general employees. Training should occur on a regular basis so that employees are knowledgeable and prepared to respond appropriately in the time of a disaster.

Plan maintenance should also include following the plan reviews and testing schedules as outlined by senior management. Testing schedules should be established when yearly budgets and schedules are established. This minimizes surprises and unforeseen costs. An organization should test their recovery plans on an annual basis. Incorporating multiple types of testing will increase the effectiveness of an organization's response in an actual disaster. Business continuity plan testing types include:

- **Tabletop**—Conference room review and discussion of mock scenarios of the business and/or technology plan(s).
- **Functional**—Actual enactment of the people, processes, and technologies involved in a business and/or technology plan(s). These can occur parallel or in line with production locations and systems.

It is important to include all roles and responsibilities in the testing process for all critical business units, departments, and functions, not just the IT department. While IT understands the underlying technology that supports the business, they typically do not have the operational business

knowledge to keep an organization operating for its customers. This is why tabletop testing is a vital aspect for management and employees to learn their roles and responsibilities in recovery plans. The final task of plan testing is to document any lessons and obstacles learned from successful or unsuccessful plan testing. This allows institutions to enhance and update their recovery plans before an actual disaster strikes.

Gap reviews should be conducted to ensure adherence to existing business continuity policies and procedures is occurring. These reviews can be performed by internal audit or external vendors. The results of these reviews and tests should be formally documented and provided to senior management for review and approval on a defined schedule.

Conclusion

Business continuity planning is a critical function that involves many different personnel and departments over multiple phases. As with many business continuity programs, an iterative process is most effective in developing a refined set of procedures and plans. This strategy allows an institution to recognize benefits from their investment, placing them to take advantage of knowledge gained and lessons learned through the development, testing, and maintenance of a business continuity program. The business continuity program should include participation from all levels of an organization, including the board of directors, senior management, business and technology managers, and staff. While many incorrectly believe contingency planning is a technology-only responsibility or problem, without business owners involvement in the business continuity program, the effectiveness of plans are weakened and the recovery time during an event can be greatly extended or halted altogether.

References

- Federal Financial Institution Examination Council (FFIEC) **http://ithandbook.ffiec.gov**
- National Institute of Standards and Technology (NIST) **http://www.nist.gov**

About the Author

John Reeder is a principal consultant with Foundstone Services. John is responsible for leading and conducting strategic engagements, enterprise, and IT risk assessments, business continuity and disaster recovery assessments, and penetration testing. His security expertise includes development and implementation of programs for security management and governance, planning, enterprise risk, awareness, incident response, security policies, business continuity, and disaster recovery planning. John is also well versed in FFIEC, NIST, ISO/IEC 27001, SOX, HIPAA, COBIT, ITIL, NACHA, FEMA, and other compliance regulations and standards.

About Foundstone Services

Foundstone, part of the Intel® Security professional services offering, provides expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone consultants identify and implement the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military. **www.foundstone.com**

About Intel Security

Intel Security, with its McAfee® product line, is dedicated to making the digital world safer and more secure for everyone. **www.intelsecurity.com**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

Intel and the Intel and McAfee logos and Foundstone are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 Intel Corporation. 2067_1216
DECEMBER 2016