Disaster Recovery Guidelines

Overview

A business recovery plan has many descriptive names: disaster management plan, disaster recovery plan, emergency preparedness plan, contingency plan, business resumption plan or disaster contingency plan. For simplicity -- and because it's the term that regulations use -- the term "contingency plan" is used throughout this material.

Developing a contingency plan for an institution is one thing: developing a contingency plan that is effective and that examiners will support and approve is another. **A contingency plan should not be a secret or a mystery. It's just a routine part of business planning and operations.**

An effective contingency plan simply covers all the facets of the institution's business operations. This means personnel, customers, facilities, functions, assets and records. In brief, everything. This means a straightforward, uncomplicated approach to resuming business operations in case of a disaster.

An effective contingency plan is developed as if all the key players will be absent. This means developing written procedures that support policies; using a clean, standardized format that is easy to understand and implement; acquiring appropriate business tools with which to work; and most important of all, guaranteeing the absolute support of and guidance from the institution's board of directors and administrators -- from start to finish.

This worksheet contains a sample examination checklist for the entire institution, not Information Systems only. **Additional guidelines are available in the FFIEC Information Systems Examination Handbook, and in publications available in the private sector.**

These are basic questions to be answered during an examination. If the institution has not adequately addressed these issues, it may be unable to restore even basic services after a disaster. This worksheet contains both questions and the rationale or explanation for an examiner's inquiry. ***Disaster Recovery & Business Resumption Plan Components***
Has the institution:
1. Received a commitment from its Board of Directors and senior management to develop a contingency plan, on an institution-wide basis?

- This should be in the form of a written directive from the institution's Board of Directors or the President/CEO. This directive should clearly state the institution's intention to implement a plan according to the guidelines issued by the appropriate regulatory agency, and it should also contain an acceptable timeline for completion. The plan should be:
    - Simple and effective;
    - Logical and progressive; and
    - Appropriate for the institution.

2. Established a management group responsible for the development and implementation of a contingency plan?

- This management group should contain executives and senior department managers -- and Board members if it's appropriate. If a service bureau is involved, a senior member of the service bureau should also considered as a member of this group. Other vendors and service providers should be represented, as they're participation is appropriate. The written directive should contain this information.
- Those persons responsible for the succession of management and recovery efforts should be designated -- by name, not title -- in the contingency plan:

    - Line of succession (2): One for the Board of Directors and one for the institution's executives;
    - Line of succession for the institution's management;
    - President/CEO: Responsible for leadership and media/public relations at the corporate level, and the notification to the regulatory agency of a disaster;
    - Chairpersons (2): responsible for leadership, media/public relations and executive decisions at the institutional level;
    - Coordinators (2): responsible for implementation, assisting with media/public relations and managing people and processes at all levels;
    - Branch/department/functional leaders (2): Responsible for leadership, implementation and managing people and processes at assigned branch, department or functional level; and
    - Service providers, vendors, insurance representatives and legal counsels: Responsible for providing guidance and advice regarding their particular areas of expertise

3. Defined the components of, and structural framework and appropriate methods for creating and updating the institution's contingency plan?

- No two institutions are structurally alike and a contingency plan should be developed in consideration of the institution's actual needs;
- A sensible contingency plan contains at least three (3) core elements:
    - Management business resumption plans;
    - Emergency operating procedures; and
    - Information systems' data processing recovery procedures.
- Considering the massive amount of information and data requiring input, updating and storage, the institution should assemble its contingency plan using two (2) technologies:
    - **Text:** All information requiring only original input and printout, minimal updating and distribution, approval, and no sorting should be created using a word processor; and
    - **Database:** All information requiring continual changes of data affecting the entire plan, frequent updating and distribution, no approval, and all lists requiring sorting should be created using a database program.
- The contingency plan should contain a table of contents and an appendix. Copies of the approved contingency plan should be distributed to each branch, department and facility designated as an alternate operations site; and
- A mechanism should be developed to update and replace contingency plan information at least annually.

4. Conducted and documented a risk assessment analysis by the management group?

- It's impractical to create a contingency plan to address unlikely potential risks. The risk assessment analysis should concentrate on real, likely or historical risks, and should include:
    - A definition of a disaster as any event that will significantly - and negatively - affect the institution's operations; and
    - Potential threats by natural, technological and human causes;
- Prioritized disasters likely to occur, based upon a historical review of the region's or the institution's:
    - Weather and geographical conditions (e.g., fire, flood, storm, earthquake, adjacent hazardous businesses);
    - Facilities' issues (e.g., age, condition, repairs);
    - Equipment issues (e.g., age, condition, repairs, hardware/software failure, compatibility);
    - Utilities' services (e.g., interruption of communications, water, electricity, gas, sewer); and
    - Human issues (e.g., robberies, strikes, riots, sabotage, bomb threats);
    - An assessment of the potential impact resulting from loss of information and services to:
        - Financial condition;
        - Competitive position;

        - Customer confidence; and
        - Legal/regulatory requirements;
    - An analysis of the anticipated short-term and long-term costs to minimize exposure, including appropriate insurance coverage for:
        - Directors and officers;
        - Casualty claims, both from employees and customers;
        - Property damage, both institution and vendor-owned; and
        - Business interruption costs;
    - Special data processing procedures should address:
        - LAN and WAN systems;
        - Personal hard drives on networked computers;
        - Standalone PCs -- particularly those used to make the institution's website available;
        - Personal off-site PCs if they're used to process organizational work;
        - Employee email addresses -- both at work and at home;
        - Data backup programs and recovery plans;
        - Backing up customer account data as an ASCII stream;
        - Off-site storage and transportation issues;
        - Virus programs and updates; and
        - Use of unauthorized programs.

5. Evaluated, prioritized and developed written **critical and secondary functions** for the continuing operation of all departments, branches, facilities, functions, and personnel?

- Every function contains critical tasks that must be performed -- and secondary tasks that may be performed after critical tasks have been completed;
- An appropriate response to disaster recovery dedicates all available resources to stabilizing critical functions first, and then restoring secondary functions;
- Prioritize cash-handling facilities, departments and other functions in the order that they should be restored, concentrating upon restoring basic services first:
    - Cash-handling functions (e.g., delivery, storage and transfer);
    - Payment of negotiable instruments (e.g., checks, money orders and travelers checks); and
    - Acceptance of deposits and payments (e.g., payment coupons, DDA transfers and checking account deposits);
- Develop operations manuals for all critical functions, including:
    - Accounting (e.g., payroll and vendors);
    - Administration (e.g., board of directors and media relations);
    - Audit (e.g., documentation);
    - Branch network (e.g., cash handling and ATM servicing);
    - Facility management (e.g., heating, air conditioning and alarms)
    - Information systems (e.g., FedWire and account balances);
    - Lending (e.g., emergency credit limits and cash flow financing);
    - Purchasing (e.g., equipment and services);
    - Security (e.g., protection of employees and facilities);
    - Telecommunications (e.g., landline telephones and Internet account); and
    - Transportation (e.g., employees and supplies).

6. Developed, maintained and updated comprehensive written policies and procedures governing the routine duties and responsibilities of all departments, branches, functions and personnel?

- Written in the form of an operations manual, or "desktop procedures", these guides provide immediate help to persons involved in both day-to-day and exceptional disaster recovery tasks. Cross-training employees to perform tasks in more than one role increases the likelihood of a successful recovery from the disaster;

- Lack of a comprehensive policy manual may indicate ineffective leadership and direction from management. This may also promote "arbitrary and capricious decisions" by personnel at all levels within the institution, based upon an individual's interpretation of a policy that is "understood" but is not committed to writing;
- Lack of comprehensive policy and operations manuals may indicate ineffective planning and preparation for the accomplishment of tasks. This may also promote "arbitrary and capricious decisions" by personnel at all levels within the institution, based upon an individual's interpretation of a procedure that is commonly accepted, but not committed to writing;
- Functional responsibilities for both departments and branches that are informal and unwritten, poorly defined or nonexistent may cause confusion, an ineffective prioritization of tasks and a misinterpretation of directions. This also makes assessing the responsibility for results difficult, if not impossible;
- Position (job) descriptions that are informal and unwritten, poorly defined or nonexistent make assessing the responsibility for results difficult, if not impossible; and
- Policy and procedure manuals, position descriptions and the institution's description of functional duties and responsibilities may be introduced into court proceedings if there is a legal action. This may be done to demonstrate that the institution failed to exercise reasonable and prudent care in developing and implementing its plan -- and it may open the institution to costly civil actions.

7. Developed, maintained and documented written strategic recovery procedures for all departments, branches, facilities, functions, and personnel?

- Strategic recovery procedures are designed to dedicate the institution's resources appropriately to:
  - Minimize disruptions of services to the institution and its customers;
  - Minimize financial loss; and
  - Ensure a timely resumption of operations in case of a disaster;
- Create a strategic and tactical response based upon these priorities:
  - People: Employees, customers and service providers;
  - Places: Branches, departments and facilities; and
  - Things: Assets and records.

8. Developed, maintained and distributed listings of individuals and companies who will help the institution recover from the disaster?

- The institution should take advantage of all available resources for its disaster recovery efforts. Contacting these resources in a timely manner is critical. This component should include at least listings of appropriate:
  - Personnel (from Human Resources);
  - Emergency services and local governmental agencies (from a telephone book);
  - Vendors (from Form 1099 and approved vendor lists);
  - Equipment (from fixed asset lists);
  - Transportation, both public and private (from a telephone book);
  - Media representatives (from telephone book and personal contact, include FAX numbers); and
  - Insurance policies and representatives (from original policies or related correspondence);
- Additional information should be available for all facilities, to include diagrams showing the location of:
  - Emergency staging areas;
  - Evacuation routes;
  - Public telephones and numbers; and
  - Utility shut-off devices.

9. Developed, maintained and periodically reviewed written position descriptions, levels of authority and reporting routines for all personnel, for both routine and exceptional operations?

- This should provide estimates for the minimum and maximum number of hours acceptable to restore basic functions;
- These functions are essential to the institution's overall operations and, if a disaster occurs, they should be operational within **8 - 24 hours**:
  - Administration (including Board of Directors);
  - Security;
  - Human Resources;
  - Telecommunications;
  - Public relations; and
  - Audit.
- The itemized critical tasks performed by these functions are essential to the institution's operations and, if a disaster occurs, they should be operational within **24 - 48 hours**:
  - Legal counsel;
  - Marketing;
  - Accounting or finance;
  - Courier or transportation services;
  - Facilities management;
  - Office support; and
  - Office and platform operations.
- The itemized critical tasks performed by these functions are essential to the institution's continuing operations and, if a disaster occurs, they should be operational within **48 - 72 hours**:
  - Insurance;
  - Information systems;
  - ATM network;
  - Wire transfers;
  - Loan services; and
  - Purchasing, delivery and receiving; and
- The itemized critical tasks performed by all other functions that are essential to the institution's continuing operations should be reinstalled as time and resources permit.

10. Evaluated the adequacy of its service bureau's contingency plan, if one is used, and ensured that the institution's contingency plan is compatible with its service bureau's plan?

- This should include a written recovery plan created by the service bureau, similar in format to the branch, department and function recovery plans created by the institution, and furnish:
  - Names and telephone numbers of the persons responsible for recovery;
  - Physical addresses, telephone and FAX numbers -- and maps and directions to the facilities to be used for recovery efforts;
  - Appropriate access and security information;
  - Recovery steps and time-lines for each function to be restored; and
  - costs for services.

11. Developed, acquired or contracted to use at least one alternate location to house critical functions on a temporary basis?

- If the institution maintains several locations and facilities, shifting strategic operations to a designated alternate site is simplified. If the institution does not maintain another location or facility, it should arrange to use a facility controlled by another institution. This should include access to a(n) off-site facility(s) to:
  - Store copies of the institution's contingency plan;

        - Allow the institution to resume administrative functions;
        - Allow the institution to resume operations functions, at least:
            - Negotiate checks;
            - Accept loan payments and deposits; and
            - Store or transfer cash;
        - Allow the institution to resume non-service bureau data processing functions, including the storage of:
            - libraries and related data processing supplies;
            - Microfilming; and
            - Proof.
    - The information supplied by the provider institution should include:
        - Names and telephone numbers of the persons responsible for recovery;
        - Physical addresses, telephone and FAX numbers -- and maps and directions to the facilities to be used for recovery efforts;
        - Appropriate access and security information;
        - Recovery steps and time-lines for each function to be restored; and
        - Costs for services.

12. Obtained written backup/recovery agreements to service appropriate critical functions?

- These operations often represent critical services to institutions and their customers. The loss or extended disruption of these business operations poses substantial risk of financial loss;
- A written contract commands performance, and assures the institution of appropriate access and service. Written agreements should include:
    - Cash-handling facilities and appropriate personnel, equipment and supplies (customer service functions);
    - Non-cash-handling facilities and appropriate personnel, equipment and supplies (administrative functions); and
    - Information Systems (record maintenance functions):
        - Central computer processing;
        - Distributed processing;
        - End user computing;
        - Local area networking;
        - Nationwide telecommunications;
        - Federal Reserve Bank;
        - Correspondent institution; and
        - Clearing houses.

13. Stored appropriate emergency supplies of food, water, first aid kits, fire extinguishers and basic tools?

- Both employees and customers may be trapped at a work location for hours or days, depending upon the magnitude of the disaster. They may require nourishment, sanitation facilities and light;
- Both employees and customers may be injured during the disaster, and medical care may not be immediately available. They may require first aid supplies and written instructions;
- The work location may suffer structural and utility damage, placing employees and customers at risk. Basic tools and other non-business supplies should be available to help employees deal with these hazards; and
- Suggested items for placement in branches, departments and facilities include:
    - Basic tools (hand axe with a hammerhead at one end, vice-grips, small pry-bar, small shovel, Swiss army-type knife, pipe wrench, channel lock pliers, 1" wide stiff putty knife, wire cutters, both blade and Phillips screwdrivers);

- Two (2) pair of heavy-duty leather work gloves (size large), and one (1) box of 100 count latex surgical gloves;
- One (1) battery-powered AM/FM radio, and extra batteries;
- Two (2) flashlights and twice the number of batteries necessary to power each one, and one (1) package of light sticks; several candles and matches;
- Three (3) 50' rolls of duct tape; one (1) 50' roll of plastic electrical tape; and two (2) 25' rolls of strapping tape;
- One (1) 100' coil of 1/4" nylon rope, and one (1) roll of yellow emergency "CAUTION" or "WARNING" marking ribbon;
- One (1) box each of 100 count "tall kitchen" and 33 gallon plastic heavy-duty garbage bags with ties;
- "Moon" or metallized emergency blankets; and
- Sanitary napkins and other similar absorbent material.

14. Developed, maintained and delivered a **written contingency plan training program** to employees, at all levels within the institution?

- Training all employees regarding their duties and responsibilities before actual disaster recovery efforts is critical to the contingency plan's success. The delivery of standardized training for all employees results in a disaster recovery teamwork effort -- and it identifies reasonable behavioral expectations;
- Employees who are knowledgeable about the institution's procedures, the risks associated with each employee's role within the institution and appropriate disaster recovery techniques, reduce the potential for operational losses;
- Actual hands-on training eliminates developmental errors, improves procedures and reduces the opportunity for mis-communication. Experiential training promotes employee comfort and confidence;
- An effective training program has three (3) components:
  - **Orientation:** All new employees -- regardless of position description -- should be oriented regarding the institution's philosophy, organizational and reporting structure, goals, priorities and other appropriate information;
  - **Transfer/Promotion:** Any employee who has been transferred to a new department -- or who has received a promotion -- should be thoroughly trained regarding his/her new duties and responsibilities, and the policies, procedures and control mechanisms used in this new capacity; and
  - **Updating:** Any change in management, business philosophy, technology, legal requirements, policy or procedure should require re-training of all involved employees. Periodic exposure increases effectiveness;
- The training program should address:
  - Disaster recovery and business resumption procedures, and the institution's policies and procedures for responding to crimes of violence: robbery, kidnapping, extortion, bomb threats, threatening telephone calls and other identified potential threats. This training should include the institution's philosophy, reporting requirements, individual duties and responsibilities, behavioral expectations and performance standards;
  - Demonstration of all electrical, water, gas and other appropriate shut-off devices, including the device's location, access requirements, physical operation and individual duties and responsibilities for shutting these devices off during an emergency;
  - Demonstration of the facility's emergency staging areas, to be located an appropriate distance from the facility in an area that's clearly visible from the facility and the building's perimeter;
  - Evacuation and building plans -- and the demonstration of all procedures to be used during an emergency, including individual duties and responsibilities, reporting requirements, behavioral expectations and performance standards.

This may also include a timed mock exercise to test the effectiveness of the evacuation procedures;
- Alert procedures for notifying personnel of an emergency, including the stages of alert and individual duties and responsibilities for all phases of the recovery effort;
- Locations, purpose and use of emergency equipment, such as fire extinguishers, first aid kits and other survival tools and supplies stored at the facility; and
- Basic first aid techniques, if this type of training is considered appropriate.

15. Developed, maintained and implemented an effective storage and recovery plan for the institution's original documents and vital records?

- Recovering business operations after a disaster often requires the use of original documents and vital records not stored as electronic data. The contingency plan should include plans for the consolidation and storage of appropriate original documents and vital records in a central fireproofed location, including:
  - Contracts;
  - Insurance policies;
  - Corporate papers;
  - An inventory list of stored items, stored in two (2) locations; and
  - Annual review for applicability, currency and legality.

16. Developed, maintained and documented an effective **annual reassessment** of the institution's contingency plan?

- A contingency plan should be an **evolutionary program**, designed to adapt to changes as they occur, including:
  - Changes in personnel;
  - Changes in business locations;
  - Alterations to existing facilities; and
  - Other updated data.
  - This should be a synopsis of all changes made to the contingency plan since the last annual reassessment. **This should be presented to the Board of Directors for review and approval. This annual approval must be reflected in the Board of Directors' minutes.**

17. Developed, maintained and documented an effective **annual reassessment of the institution's insurance coverage**?

- This should be a synopsis of all changes made to the contingency plan requiring an accompanying change in insurance coverage, since the last annual reassessment. This insurance coverage reassessment should include all policies addressing:
  - Directors and officers liability;
  - Casualty claims, both from employees and customers;
  - Property damage, both institution and vendor-owned; and
  - Business interruption costs; and
  - This synopsis should be presented to the Board of Directors for review and approval. This annual approval should be reflected in the Board of Directors' minutes.

18. Developed, maintained and documented the **criteria, conditions and frequency for testing** the contingency plan -- and has the institution actually performed, evaluated and documented a test?

- Testing all aspects of the contingency plan -- at least annually -- is critical to the contingency plan's success;
- Actual hands-on testing eliminates developmental errors, improves procedures and tests the interaction of the contingency plan's components;
- It is physically impractical to move a branch, department or function to another location as a test. The use of a hypothetical problem-solving exercise -- in a controlled, documented meeting environment -- will provide the necessary test results; and
- Physically testing the institution's Information Systems' backup capabilities is essential. An appropriate physical test should be conducted at least annually, preferably at each of the institution's designated recovery facilities.

19. **Have copies of the approved plan been distributed appropriately?** Distribution should involve branches, departments, facilities and functions, and all alternate operations sites.

- After the contingency plan has been approved, copies of the plan and appropriate lists should be distributed. Each recipient should receive two (2) copies: one (1) copy to keep at work, and one (1) copy to keep at home or in his/her primary vehicle;
- Full copies of the contingency plan should be delivered to the Chairpersons and Coordinators -- and stored at each alternate site; and
- Limited copies of the contingency plan should be delivered to branch managers, department heads and functional leaders.

First published on BankersOnline, 9/17/01, Updated 3/18/02