Business Continuity Planning

Expanded Practices Guidelines

April 2011

SIFMA Business Continuity Planning Tactical Committee

Best Practices Sub-Committee

Preface

This document presents guidelines that can assist in the establishment of a comprehensive business continuity program. It is not intended to be an outline of a business continuity plan or as a single best approach, but rather it should be viewed as a summary of significant components that an organization may wish to consider when developing a full business continuity program. The plan itself is but one component of the program. Organizations may also consider executive support, policies, measurements, maintenance, and reviews of the plan that constitute the program.

SIFMA does not guarantee the accuracy of any portion of this document, and does not assume any liability for any inaccuracy or omission in this document. This document should not be construed as legal advice. Readers are advised to consult with counsel regarding the relevant requirements for business continuity plans, prior to adopting any such plan.

TABLE of CONTENTS

1 Business Continuity Program

1.1 Overall Program Elements

Each firm should have in place a Business Continuity (BC) program that ensures:

a) The development, implementation, testing and maintenance of business continuity and emergency response plans that enable the business to protect its assets and meet its business recovery objectives.
b) Prevention and/or mitigation activities that reduce the likelihood and impact of a disruption that could significantly affect its personnel, customers and stakeholders**.**
c) An ongoing employee awareness program.

1.1.1 Relevancy of Stated Guideline

A Business Continuity Program is a top down approach focused on mitigating the affects of disruptions to the business achieved through the establishment of documented "Policies", "Guidelines for Implementation", and "Procedures to Follow" when a disruption to the business does occur. The program is important to sustain the viability of the institution by protecting physically and financially personnel, customers, and stakeholders. It is also now required by industry regulators for the same reasons.

Key Concerns/Issues (To work through)

- Regulations
- Risk Management including exposures of vendors
- Executive ownership, commitment, and support of the program.
- Program as part of the company culture recognizing it is part of "doing business".
- Adequate funding and staffing.
- Incentives and penalties in place to make it happen.

Key questions (To ask)

- What business are you in?
- Do you know your exposures?
- Who are your customers and what are their expectations?
- What is your reliance on critical vendors, including major utilities?
- What is your reliance on critical infrastructure, clearing firms, industry utilities?
- What functions/operations/products are critical?
- What are the minimal resources required to maintain the business for a selected time period?
- What immediately non-critical functions become critical after a given time period?
- What is the "proximity" risk to your firm (internal and external)?

1.1.2 Possible Strategies

After executive-level commitment could be:

- Technology Driven: Application resiliency drives strategy
- Business Driven: Business impact analyses drives strategy

1.1.3 Possible Solutions

- Who: Do you hire outside consultants to build and document your plans, do you do it in-house, or do you use a combination of both?
- How: Do you use an automated database tool to document the plan, simple Word documents, or a combination?

1.2 BC Policy Document

Each firm should have a Business Continuity policy document which provides the framework for its business continuity program and the development of business continuity and emergency response plans.

1.2.1 Relevancy of Stated Guideline

The Policy Document should be at a high level that demonstrates the accountability and intentions of executive management as to how they understand and support the overall Business Continuity Program. It should provide conceptual frameworks for implementations such that changes in details or procedures do not require changes of policy. The Policy document should also recognize the existence as a separate document, guidelines to be used to develop and implement plans and procedures. Finally, the plans with procedures should spell out the details to be followed when a disruptive incident occurs. This separation of policy, guideline, and procedure provides the flexibility to respond rapidly to changes of business process and the implementation of new products. Some characteristics include:

- A framework should be consistent and have an enterprise wide approach;
- Implementation of said practices could be local/regional focused to account for cultural and regulatory requirements.

Key Concerns/Issues (To work through)

- Establishment of key operating principles which BCP program is founded upon
- Consideration and incorporation of regulatory requirements including rules, guidelines and market practices
- Establishment of ownership of both the program and emergency response plans
- Establishment of a risk assessment framework for identifying priority and emergency response plans needed for that specific location.
- Commitment at the Executive level with constant communication with BCP for understanding of the Program implementation and Executive accountability.
- Policies that outline the use of metrics and audit of the achievements against metric service levels.

Key questions (To ask)

- Who is the target audience for the policy document – BCP, senior management, regulatory bodies and auditors?
- What level of detail do I include and how can I make document have an enterprise wide focus?
- What type of information should I include using the distinctions of Policy, Guideline, and Procedure?
- How often should I review and update?
- Is this document a regulatory requirement?
- Who will be responsible for creation and updating?
- Who should sign-off on it and to who should it be distributed?
- Does the firm have the critical infrastructure to support the policy and ensuing program?
- Does the firm have the personnel resources to support the policy and ensuing program?

1.2.2 Possible Strategies

- Approval and sponsorship is at the highest levels. It is top down.
- Incorporate a globally consistent, enterprise wide BC policy which is governed by board level and monitored by firms internal control units
- Incorporate business unit level BC policy managed and controlled by individual business areas

1.2.3 Possible Solutions

- For the structure of the Program, follow the FFIEC Guidelines or similar program outline documents.
- Any strategy to ensure firm-wide adherence to BC policy must be tied to corporate governance and/or audit standards to be effective.
- Identification of framework components such as people who have a role, processes that support the execution of the principles and tools that are needed to ensure an efficient roll-out should be maintained in the "Procedure" level document, while the need for these components is spelled out in the "Policy".
- Policies should outline the use of and audit of metrics.
- Approval and sponsorship must be at the highest levels and cannot be delegated.
- (removed because – redundant)Incorporate a solution that uses incentives to supplement adherence to BC policy.
- Creation of a global (or national) document which is based upon the BCP operating principles and which describes the BCP policies, high level practices, roles and responsibilities, and frequency of updates. The document should cover the key areas of the BCP program such as
    - Organization, governance and compliance
    - Business impact analysis and business contingency planning
    - Risk and threat assessments
    - Emergency/crisis response
    - Alternate communication
    - Testing and exercising
    - Recovery strategy and resources
- Establish a compliance and metric reporting process to ensure compliance to the practices and frequencies described in the document
- Document should be endorsed by governing body, such as a Steering Committee, and signed off by senior management (board level)
- Document should be high level supported by local, detailed procedures describing how the practices have been implemented.

1.3 BC Documentation

Business continuity plans should be documented and readily accessible to those who need access.

1.3.1 Relevancy of Stated Guideline

If it is not written, it is not said, must remain the mantra of the Business Continuity Program. In line with this philosophy, the following characteristics of the documentation program have been most effective:

- Business unit level BC plans and corporate level practice documents need to be documented and maintained in a central, easily accessible place
- Documentation of plans is required to ensure they are communicated and to provide evidence to internal and external audit and regulatory bodies
- Documentation should be such that someone who is not normally in the course of business continuity can use the document to successfully resume / recover business operations.
- Documentation should have actionable points which can be used to enable recovery within designated timeframes.
- Format of the documentation should be in line with company standards or culture.

Key Concerns/Issues (To work through)

- The document for BC Plans should follow the guidelines established at the Policy level.
- Establishment of generic template to document the BC plans in a consistent manner across the organization.
- Consideration of utilizing a database to collect business unit requirements, do business impact analysis and generate BC summary plans
- Establishment of a process to post or file plans in an easily accessible means and also to ensure that most current version of the document is stored and available
- All documented plans should be signed off by appropriate level and person/s
- Establishment of an update frequency consistent with risk and priority of the location
- Consideration for dividing information to supply access to employees without divulging private or confidential information.
- Plans must be continually updated to reflect current information.
- Plans should be of sufficient detail that surviving firm members can recover tasks/ functional work areas.
- Plans must be reviewed on a periodic basis, at least annually, and signed off by a designated officer.

Key questions (To ask)

- If cost-risk profile of my organization warrants it, how do I go about selecting a database to house the business unit requirements and plans? Build or buy?
- Do I have a secure website in which to house the plans so they are easily accessible?
- How do I establish ownership and get the business unit owners to agree to owning and maintaining their plans?
- What should be in the BC templates – are there any samples available for me to use?
- What will my process be for ensuring that the plans are current and the latest version maintained for those who need access?
- How detailed should the BC plans be; should I include a one page summary that is action/task oriented and easily accessible to all who need it?

- Have the documents been verified through testing to ensure that information is adequate to recover business at a time of disruption?
- Do employees understand how to access the information they need.
- Do employees understand their role in the plan(s)?
- Does management understand its role in the plan(s)?
- Who owns the documentation and update process?

1.3.2 Possible Strategies

- BCP should establish the process, tool and templates to be used in document, maintain and make the plans easily accessible.
- The plan can be a single integrated document or multiple documents.

1.3.3 Possible Solutions

- Deploy an in-house web-based database to house and maintain BC plans which is administered at the enterprise level but maintained and updated by the business areas.
- Deploy a third-party database to house and maintain BC plans which is administered at the enterprise level but maintained and updated by the business areas.
- Each business area is responsible for designing, documenting and recording their BC plans; quality control and oversight at the corporate level.
- Deploy a paper based BC plan template designed at an enterprise wide level and rolled out and maintained by the business areas. Store on the website or other easily accessible place.
- If cost effective, a central database, preferably web-based, should be used to collect the business requirements, do the impact analysis and produce (or use the data to produce) the BP unit level plans.
- Corporate BCP principles/practices should be maintained in a secure web-page or other easily accessible place and regular process for updating and maintaining current process should be established.
- Annual sign-offs and reviews should be established for major sites; for smaller, low risk site an 18 month or two year process may be more appropriate.
- Consider Flowcharts, timelines, and checklists to help facilitate the recovery process.

1.4 BC Oversight Group

Each firm should have an Executive and corporate group responsible for overseeing the business continuity program.

1.4.1 Relevancy of Stated Guideline

According to the regulators, accountability and responsibility can not be delegated to subordinates and or vendors. Only the responsibility for doing the work can be delegated or transferred. Additionally, with Executive sponsorship, funding and resources will be more easily obtainable and the development and implementation of the business continuity plan will be a success. With Executive accountability, BC will be better assured of the necessary direct communication of requirements, solutions, and remaining risks.

Line managers are charged by Executive Management to work through the process Consequently, executive support needs to be ongoing; with a governing body established to approve the BC program and strategies.

Key Concerns/Issues (To work through)

- Executive support is the best way to ensure appropriate resources are provided to enable he project to be completed within budget and on time.
- Communication between the BC Planning team and Executives/Audit Committee needs to be continuous and consistent.

Key questions (to ask)

- Does Executive policy include the vision/mission statements for enabling authority?
- Does Executive policy it include program goals and objectives?
- Does the business continuity program plan include procedures, budget, schedule and milestones?
- What is the regular status reporting structure based on the corporate culture?
- Is the Executive sponsor involved in key response decisions and/or planning?
- Is this a topic for performance reviews of line managers?
- Does the business continuity program follow the Change Management process?

1.4.2 Possible Strategies

- Establish program at the executive level with broad level of approval and oversight for the program.
- BCP function reports into a high level governance function

1.4.3 Possible Solutions

- Assemble an advisory committee of senior managers, which is representative of the various facets of the company to set the direction of the plan.
- Establish a BCM steering committee at the local, regional or global level responsible for overall governance of the program

1.5 Business Unit Ownership

Business managers should be responsible for the review, implementation, funding and sign-off of business continuity plans and associated exercise results.

1.5.1 Relevancy of Stated Guideline

Business managers should be responsible for the review, implementation, funding and sign-off of business continuity plans and associated exercise results. Ownership of the plan and funding of resource requirements to meet the stated objectives should be at the Business area level. With ownership comes the responsibility to attest the plan meets stated objectives and is verified through exercise of the procedures. The Business Continuity Organization is the knowledge experts providing organization, coordination, and guidance to the planning process.

Key Concerns/Issues (To work through)

- Only the business manager can set the appropriate priorities.
- Knowledge of the business continuity plan and process
- Availability of SMEs to assist business managers.
- Appropriately designed metrics.
- Funding and budget concerns addressed.

Key questions (to ask)

- Is it possible to integrate business continuity planning activities with normal business procedures?
- Will there be centralized budgeting, or will each business unit fund their own business continuity effort?
- Is part of the business manager's review tied to goals and objectives of the business continuity program?
- If plans are decentralized, is written governance available and are all plans reviewed and signed off on according to company policy?

1.5.2 Possible Strategies

- Incorporate the business continuity function into the business area manager's normal responsibilities making them accountable for reviewing, funding and signing off
- Establish ownership of the BC plans at the business area level; corporate oversight and requirement to provide tools and expertise to assist business areas

1.5.3 Possible Solutions

- Business managers are provided the tools and authority to perform their role.
- Appropriate documentation should be available to indicate types of exercises performed and the results.

1.6 Recovery Exercises

Recovery exercises for critical business functions should be conducted no less than annually and as is warranted by changes in the business and/or information system(s) environment.

1.6.1 Relevancy of Stated Guideline

Validate that the plan functions effectively. Provide an opportunity to validate that what is written in the plan receives the desired result. Verify that connectivity to customers, vendors, and industry utilities has not been negatively affected by on-going industry and business changes.

Key Concerns/Issues (To work through)

- Ensure that the plan relies on the documentation and not on specific knowledgeable individuals to be successful.
- Ensure testing is robust enough to find deficiencies, if any.
- Verify that the Firm is onboard with the testing efforts.
- Ensure that the Production environment is not affected during testing.

Key questions (To ask)

- Is testing funded?
- Is management supportive of the testing efforts?
- Will management review the results?
- Is there a process in place to act on the results, and follow up through closure?
- Test the overall testing program address multiple test scenario types?

1.6.2 Possible Strategies

- Establish firm-wide testing strategy including specific requirements for what types of tests, frequency of performance and what documentation/evidence is required
- Individual business area responsible for testing and documenting test results

1.6.3 Possible Solutions

- Perform desktop and/or tabletop tests.
- Perform connectivity tests.
- Perform people relocation tests.
- Perform Call Tree/Emergency Notification Lists tests.
- Partner with local Emergency Management personnel (municipality, county, state, OEMs, industry-wide organizations, and industry tests).
- Test with vendors, counterparts, and industry utilities.
- Conduct, at minimum, annual call notification tests; where possible combine with crisis simulation or physical test so that you are simulating reality.

1.7 Annual Review

Plans should be reviewed and updated no less than annually and as warranted by changes in the business and/or information system(s) environment.

1.7.1 Relevancy of Stated Guideline

This is a regulatory requirement, and it is important to ensure that the most current information is updated in the plan in case there is a business continuity event.

Plans should be updated outside of the annual cycle when there are significant organizational or business changes that would render the existing BC plans ineffective

Key Concerns/Issues (To work through)

- Ensure the ability to integrate plan updates into the change management process of the Firm is present.
- Business unit and technology organizational changes affecting the plan need to be captured and communicated on an ongoing basis.
- Ensure an individual with an appropriate level of knowledge and authority is assigned to complete, or, at a minimum, review the plan updates.
- Incorrect data in the plan could lead to extensive chaos/confusion for business continuity events participants.

Key questions (To ask)

- Is this a task assigned to the business units?
- Is the assignee accountable?
- How do you ensure plans accurately reflect the most current technology and business unit environments?
- Are the plan elements consistent with current regulatory requirements?

1.7.2 Possible Strategies

- Establish a corporate policy, backed by the executive committee and/or Board of directors that requires updating the plan no less than annually and whenever significant changes occur. Include a clarification of significant.
- Integrate Plan Updating with project and change management.

1.7.3 Possible Solutions

- Implement a periodic review process of the plan, at least every six months and, possibly, on a quarterly basis.
- Require an annual presentation by the BC to the audit committee which includes a scorecard review of who has not updated their plan in the preceding 12 months and/or who has not updated their plan after a significant change in operations due to changes in such items as location, personnel, systems, and/or procedures. In conjunction with this review, hold the business manager responsible for failure to meet the annual review requirement and provide for essential BC resources to audit plans.
- Ensure plan updates are applied based on business continuity exercise results.
- Institute a plan peer review process for updates.

1.8 Employee Awareness

Each firm should have in place a Business Continuity (BC) program that ensures an ongoing employee awareness program.

1.8.1 Relevancy of Stated Guideline

BCP Program practices and principles need to be communicated to staff in order to be effective. This includes such items as:

- Regular staff updates and communication that can be achieved via presentations, website, BCM/Crisis response procedures, newsletters, promotional items, and participation in training and awareness exercises
- Awareness/induction program for new employees and new senior/crisis team members

Key Concerns/Issues (To work through)

- Resource considerations for providing a full education and awareness program
- Decision on what levels to target – educate staff who have a key role in BCP or Crisis Management and then communicate key points to all staff via cost effective methods like corporate emails or website
- Establishing process to maintain and refresh program to account for regular staff turn-over
- Decision on what information to provide, the frequency of update and responsibility for creation and distribution

Key questions (To ask)

- How can you deliver the key messages in a cost effective manner?
- How to verify the effectiveness of the education and awareness program?
- How can you ensure staff participates and reads communication – make it part of performance criteria if they have a key role?
- What is your target audience for exercising and practicing the staff – senior execs, crisis management and recovery team members, or all staff?
- Do you have the budget to launch a full program or can you leverage off other corporate initiatives?

1.8.2 Possible Strategies

- Partner with HR department to include BCP awareness as part of the new employee induction program.
- Utilize existing means of communication like Intranet postings, websites to rollout education and awareness.
- Integrate awareness into the culture.

1.8.3 **Possible Solutions**

- Establish with your HR department including BCP awareness as part of the new employee induction program; include any promotional or response guides as part of that package.
- Include business continuity awareness and participation in continuity exercises in everyone's job description/responsibilities and employee evaluations with expectations established that it is part of running the business not an exception or add on function.
- Conduct periodic surveys of staff's awareness and then target training and awareness exercises at audiences that need educating

- Establish a regular process with corporate communication to issue quarterly or semi-annual reminders to all staff on key BCP principles and practices
- Create and distribute one-page (z-cards) to all staff on standard response/recovery procedures – should be standard, static information, that changes infrequently.
- Conduct periodic exercises, desk top simulations, or other means by which employees are reminded that it is part of running the business.

2 Recovery Strategies

2.1 Strategy Elements

Each firm should develop recovery strategies that would enable them to continue their most critical operating, service and technology functions in order to:

a) Meet defined recovery objectives
b) Meet the service level commitment to customers
c) Meet fiduciary requirements
d) Minimize financial, legal and / or regulatory exposure

2.1.1 Relevancy of Stated Guideline

Each firm should determine the time required to recover and still meet regulatory and customer requirements. This recovery time should be the stated "Recovery Time Objective" or RTO. Meeting it is based on the location of its recovery center, the time for resources to get there if they are not already at that location, and the time to bring the critical systems up and running.

Once the recovery environment is established, the team must recovery from the point of interruption either prior to or simultaneously with the processing of new incoming work. That point again should take into consideration the ability to meet regulatory and customer commitments. This is referred to as the "Recovery Point Objective".

Both these objectives will vary by the criticality of the application. Less critical applications can be postponed longer than the critical, the determination of which is based on a business impact analysis.

Key Concerns/Issues (To work through)

- Adequacy of recovery time frames must be in line with the actual business needs.
- Clearly define business unit expectations in order for effective technology recovery.
- Business unit time frames must drive the requirements.
- Each business unit must obtain sign-off for time frames and strategies defined.
- Develop strategies specific to business unit requirements and viable scenarios.
- Ensure periodic revisit of recovery strategy to verify it still meets business needs, and that "lessons learned" from prior internal/external situations are included.
- For service provider firms, ensure your Firm knows and understands the Service Level Agreements the Firm has committed to.
- Realization that some functions, although not immediately critical, may become critical over the extended time of a disruption.

Key questions (To ask)

- Has the Firm identified fiduciary requirements?
- Has the Firm determined what the service levels for customers should be?
- Has the Firm ensured recovery time frames are in line with actual business needs?
- Do the business unit time frames drive the requirements?
- What is the minimum system availability time?
- If the firm is a service provider, does it know what its clients are looking for?
- Does the firm know all of its exposures, and are they clearly understood?

- Is the recovery strategy flexible and is it utilized sufficiently to appropriately recovery?
- Does your firm understand your risk exposure profile during a crisis? Can it adapt?

2.1.2 Possible Strategies

- In the event of a significant business disruption or disaster, strategy is to recover and resume critical business functions in a priority order which looks to ensure client, legal and regulatory obligations are satisfied
- In the event of a significant business disruption or disaster, strategy is to ensure minimal disruption and high availability of all critical business processes and applications
- Base prioritization and immediacy of recovery on business impact analysis.

2.1.3 Possible Solutions

- Ensure strategies contain flexibility to adapt to all scenario types.
- If key primary employees are not available, the strategy must be able to be implemented by those who are second in command.

2.2 Geographic Impact Strategy Assumptions

A firm's strategy should be based upon an event impacting an extended geographic zone and having a significant impact on the firm and its resources.

2.2.1 Relevancy of Stated Guideline

Firms must account for a regional interruption, and have pre-established methods to provide client access to funds and securities. Of course the extent to which one addresses the issues vary with such factors as cost, probability of occurrence, firm size, etc. and key business decisions on the firms propensity for risk. Also included in the planning process are dependencies on vendors, their ability to support the extended geographic zone, and the accessibility of vital records at the alternate location.

Key Concerns/Issues (To work through)

- Cost
- Probability
- Firm Size
- Distance / Time to relocate personnel
- Natural disasters
- Utilities
- Access
- Ability to replicate data
- Capacity
- Supervisory procedures exist for employees working remotely
- Vendor cannot be a single point of failure for the Firm

Key questions (To ask)

- Have costs associated with this type of event been gathered and analyzed?
- Has the Firm determined the probability of this type of event occurring?
- Are vendors susceptible to same risk profile as the Firm? If so, how is this addressed?
- Has the Firm planned for natural disasters?
- Will utilities be available during a disaster?
- What is the maximum acceptable time to relocate personnel?
- Is the Firm able to replicate data within an acceptable time frame?
- What other firms are located in proximity to the Firm's recovery location?
- Are there any natural hazards and/or manmade risk exposures to the recovery location?
- How far enough is "far enough", so that primary and secondary sites are not too close?
- If primary and secondary sites are "too close", is an additional strategy needed?
- Are business continuity requirements specified in RFPs, contracts, and SLAs?

2.2.2 Possible Strategies

- Geographically diversify recovery locations
- If internal resources are not sufficient, consider outsourcing recovery components to geographically dispersed service providers, either as primary or secondary contingency.

2.2.3 **Possible Solutions**

- For smaller firms, a possible alternative to an expensive, geographically separated hot-site is a warm people and data recovery site with a reciprocal agreement with another firm.
- Ensure associates working remotely can complete their jobs with technology provided.
- For mid-sized firms, if using a third-party recovery vendor, ensure they are not susceptible to a single event affecting both sites.

3 Recovery Resources

3.1 Communication Alternatives

The firm should have the capability to communicate with employees using multiple methods of communication (i.e. phone, pager, cellular phone, e-mail, internet, etc).

3.1.1 Relevancy of Stated Guideline

In any emergency situation firms need to be able to contact/notify employees at work, home or while in transit and provide information updates as necessary. However, as seen in past events, communications may be disabled. Therefore it is critical to have active (send communication to employees), passive (employees retrieve information) communication methods pre-determined and multiple means of achieving each

Key Concerns/Issues (To work through)

- Ability to account for employees
- Accuracy of information
- How to keep contact information updated
- Periodic testing
- If technical solutions are used, will they be affected by the incident?
  - Loss of power (company, employee and region)
  - Loss of communication infrastructure
  - Reliability of systems

Key questions (To ask)

- Do employees know (away from the office) how to reach us?
- Do employees have multiple methods?
- Do your employees know what to do if they don't get contacted?
- Do we have multiple contact methods for employees and are they current?
- How do you maintain accuracy?
- Outsource providers – Backup, redundancy, Critical Infrastructure Survey
- Internet Search term: Emergency Notification Systems

3.1.2 Possible Strategies

- Employ an alternate communication policy requiring diverse set of communication means and a diverse service providers to ensure resiliency

3.1.3 Possible Solutions

- Use of Web sites or corporate intranets
- 800 hotline
- Updated manual phone tree
- Specific notification call-out systems (in house or commercial)
- Use of call-in solutions (in house or commercial)
- Utilize Call Trees, contact lists, and/or wallet cards.

3.2 Roles and Responsibilities

The firm should have pre-defined business continuity teams, detailing management structure and roles and responsibilities.

3.2.1 Relevancy of Stated Guideline

Waiting until a disaster strikes is too late to determine who should do what. Teams should be established with clear lines of authority and communication and the roles and responsibilities of each team member documented without actual assignments of individuals. Secondarily, assignments of the individuals should be made with contingency or lines of succession in case a particular individual is not available to perform the stated responsibilities.

Key Concerns/Issues (To work through)

- Flexibility and fungability of staff.
- Training content for each target audience.
- Clearly defined roles and responsibilities
- Overlapping of responsibilities
- Structure must be commensurate with firm's culture

Key questions (To ask)

- Can a recovery process function without Coordinator?
- Are there any single points of failure?
- Should a firm use a Centralized structure or a decentralized structure?

3.2.2 Possible Strategies

- Include in Programs each type of team by roles, such as incidence response, recovery, and restoration and define the means by which these teams are staffed and lead.

3.2.3 Possible Solutions

- Refer to management structures in the public sector
- Exercises
- Training
- Business Responsibility/Ownership
- Governance

3.3 Training

Essential business staff should be trained and fully capable of performing business functions at the recovery location.

3.3.1 Relevancy of Stated Guideline

Staff members performing critical business functions need to be identified, trained and accessible to perform their functions at an alternate location in the event of a major business disruption. Also taken into consideration in the training are the unique circumstances relevant to the recovery planning. This would include reduced staff, different surroundings, and differences in work flow and document handling.

Key Concerns/Issues (To work through)

- Turn-over – people change often but critical functions do not. There should be a method of assessing and identifying critical business functions and who performs them.
- Staff demographics – critical business functions should have back-ups; back-ups should not live in the same geographical location as critical business functions personnel.

Key questions (To ask)

- What is your methodology for determining "essential business staff" that performs critical functions?
- How do I keep this information up-to-date in light of staff turn-over?
- How do you ensure that "essential business staff" can get to the alternate location and that they are trained to perform these functions?
- What is your plan of action there is a major disruption and essential staff cannot get to the alternate location?
- Have you identified all options for performing critical business functions including transferring work to other location and cross-training of mission critical functions?

3.3.2 Possible Strategies

- Include cross training and job rotation as part of the corporate culture.

3.3.3 Possible Solutions

- Identification of essential staff should be based upon identification of critical business functions. A risk assessment model should be used to identify and prioritize these functions.
- Essential staff that performs critical business functions should have a backup.
- Demographic mapping could be used to ensure there is geographical diversity between primary and backup
- Identify multiple ways of providing coverage including transferring work to other locations, and working from home or remotely as in some circumstances essential staff may not be able to get to an alternative location.
- Focus crisis and BCP training exercises on senior staff who have a key decision making roll; involve other tiers of staff in exercises such as practicing bridge lines and call notification exercises which can target a large number of staff at a low cost
- Budget and resource permitting, establish an on-line course targeting all staff

3.4 Facilities and Geographic Considerations

Recovery facilities should not be located in the same geographical zone as the primary business facility and should be supported by separate telecommunication and utility (water, power, etc.) infrastructure.

3.4.1 Relevancy of Stated Guideline

Facilities that house backup data centres and work area recovery space should be far enough away from the primary facilities that house the production data centre and working area so that both facilities will not be severely impacted in the event of a significant business disruption or catastrophic event.

Key Concerns/Issues (To work through)

- Current technology for running synchronous data centers is very expensive; workable solutions have distance limitations of 60 miles.
- Work area recovery facilities that are too far away may present issues concerning staff's ability to get there and work there for a prolonged period of time.

Key questions (To ask)

- What is the correct formula for determining where recovery facilities should be located?
- What strategies can we employ to ensure critical business functions are fully backed up without spending an exorbitant amount of money on technology?
- What other strategies/resources can be deployed to keep costs reasonable but assurances high that critical business functions can be performed?

3.4.2 **Possible Strategies**

- If internal resources do not provide sufficient diversity, consider outsourcing of facility for recovery.

3.4.3 **Possible Solutions**

- Data centre strategies that provide synchronous capabilities for critical business functions within the distance limitation supplemented with a tertiary site for less critical functions and as a backup in a further distance location.
- Work Area recovery solutions should encompass a variety of alternatives like: contracting with a third party provider who has the capability of providing multiple sites; transferring work or people to other locations; employing reciprocal agreements and remote access capabilities.

3.5 Facilities and Accessibility, Availability, and Capability

The accessibility, availability and capability of recovery facilities should support the firm's requirements and recovery objectives.

3.5.1 Relevancy of Stated Guideline

Recovery facilities should be accessible and available to you when required not based on a first come first serve basis. Also of importance is:

- The location of the recovery facility considering the time and convenience to reach the facility during a disruptive incident and the cost to staff the facility
- The appropriate infrastructure at the recovery facility to support your business functions and applications that you are recovering
- The "state of readiness" at the recovery facilities compatible with the recovery time objectives and recovery point objectives of those functions and applications.

Key Concerns/Issues (To work through)

- Recovery facilities that are third party vendor operated usually have conditions associated with them that make it difficult to guarantee that they will be available and accessible when you need them. Service Level Agreements with vendors and contracted commitment of resource availability should include network access.
- Recovery facilities need to be kept in synch with production facilities – how can I ensure this happens?
- Recovery facilities are expensive and may never be used – need to ensure a risk-cost based approach so that business functions that would have the greatest impact if they could not be recovered are supported
- Distance of recovery facility to original location
- Means of transportation to reach the recovery facility
- Cost of room and board for personnel, non-local to facility, needed to staff the facility
- Cost of redundant or cross-trained staff to substitute for staff needed for operations during a recovery.
- Resources maintained at recovery facility including hardware, software, and personnel.
- Additional or substitute software licenses to be used during a recovery on hardware different from that contracted for with original software license.
- State of readiness of equipment to meet recovery point and recovery time objectives
- Ability to redirect network through recovery facility
- Ability to redirect internet connectivity through recovery facility
- Any necessary reprogramming of routers and firewalls to adjust to different IP Addresses that may exist at recovery facility
- Maintenance of Information Security / Customer Privacy Practices at recovery facility

Key questions (To ask)

- What are your Recovery Time and Recovery Point Objectives and the respective Business Impact Analysis justification?
- Trade-offs of cost vs. active-active load balanced facilities?
- Trade-offs of distance from original site
- Cost Benefits of outsourcing to a vendor and at what level of "hot-site" vs. "shared resources"

- Cost Benefits of having work-space located differently from recovery infrastructure
- Impact of regional outage
- How do I determine what recovery facilities and what services I need for my business?
- What alternatives do I have – third party, alternate work locations, reciprocal agreements?
- How much money do I need to spend to ensure my critical functions are covered?
- What provisions are in the contract or do I have for validating the recovery facility capability?
- What conditions exist around the use of these facilities – may I use them when I need them?
- Do I need a recovery facility for every branch and/or location?
- Should the personnel work site be co-located with the infrastructure of servers / mainframes, etc.?

3.5.2 Possible Strategies

- Program includes an assessment of the accessibility during disasters and ability to withstand such events as floods, blackouts, and access due to problems from surrounding businesses.

3.5.3 Possible Solutions

- Risk assessment and impact analysis model should be used to determine critical functions, impacts of non-recovery of those functions in order to determine how much you need to cover/spend on these facilities
- All alternatives should be considered in line with your business model. Firms should utilize alternate locations, transferring of work and systems to other locations and other low cost solutions as appropriate
- Contract terms, available vendors and options should be thoroughly researched and understood before contracting.
- Implementation of processes to keep work area recovery hardware/software in line with production should be maintained and tested regularly
- Separate facility built at alternative existing corporate location already on existing network running in a load balanced active-active arrangement.
- Separate facility built at alternative existing corporate location already on existing network set up in a "warm-site" facility that would require some recovery time to bring to recovery point.
- Use of a vendor provided location with company owned dedicated equipment integrated into the corporate network, i.e., vendor provided "hot site".
- Use of a vendor provided facility utilizing shared resources either available on a first come first serve or proportional access
- Separating work-site from infrastructure
- Combinations of the solutions mentioned above

3.6 Critical Business Applications - Availability

Businesses should ensure that the functionality and availability of critical business applications/end-user computing meet business recovery objectives.

3.6.1 Relevancy of Stated Guideline

Not every function performed in an organization is critical on an immediate basis. Additionally, priorities may change during a disaster. Perhaps the new advertisements may give way to a communication program of the firm's continuance of operations during a disaster. This may include a slight variation of hours of operations or services. Whatever the issues, a firm must first identify its most immediate critical functions in order to prioritize the application of resources. It must also address the time lines when other services, not deemed immediately critical, will become critical. This planning process includes:

- The identification and prioritization of the critical business applications/end-user computing capabilities and the subsequent rehearsing (testing/exercising) of the recovery process including end user participation, to demonstrate that the business recovery objectives, with all required functionality to meet client and legal obligations, are being met.

Key Concerns/Issues (To work through)

- Business Impact Analysis to determine critical applications
- Recovery exercises at recovery facility and with operations personnel to ensure preparedness
- Recovery resources (see recovery facility practices)
- There is no scientific method of determining recovery and resumption time objectives – so how realistic are they?
- Applications and technical processes in place for recovery cannot actually support the business requirements
- Interdependencies – internal and external – how many applications depend on external vendors or other systems to operate.

Key questions (To ask)

- How does one assure the critical applications have been identified (with end user involvement)?
- What type of exercise should be performed and what are its objectives?
- How often should the plan be exercised?
- How often should plans be updated to assure currency of procedures and new applications?
- Are all tasks and functions (like core infrastructure setup) considered when determining recovery time objectives for systems/applications?
- How many businesses/locations depend on these business applications and how do I prioritize?
- How do I validate the functionality and availability of business applications meet business recovery objectives as current testing strategies are not focused on proving this under multiple scenarios?

3.6.2 Possible Strategies

- Program includes risk ranking applications and prioritizing recover according to the risk ranking.

3.6.3 Possible Solutions

- Frequent recovery exercises with end users, vendors, and service providers.
- Include customers when not disruptive.
- Use of desk-top simulation and/or plan walk-through exercises with end users
- Use of independent audit of effectiveness of exercises both in functionality and timeliness
- Integration of plan updates with Change Management
- Application recovery time objectives should factor in core infrastructure setup times.
- Gaps between application recovery time objectives and business recovery time objections should be documented. Processes or system upgrades to fill the gap should be developed.
- Database which houses details of business functions, impacts, recovery time objectives, and applications should be centrally maintained and used to identify and prioritize.
- Technical/user tests should be designed to validate recovery time objectives; all tasks required for recovery, including getting to the alternate site, should be factored in

3.7 Staff – Geographic Considerations

Firms should consider geographic diversity of critical staff and critical production applications, data, or data centers supporting them.

3.7.1 **Relevancy of Stated Guideline**

Regional disruptions not only complicate accessibility of recovery site, they also disrupt the ability of individuals to travel. Real or potential injuries to staff or their families may also interfere with an individuals travel. Additional resources located in remote locations where recovery can take place provide additional assurances for continuation of business. This requires that these resources are trained well enough to follow existing documentation and that the documentation is detailed enough for resources that may not perform the functions on a daily basis.

Key Concerns/Issues (To work through)

- Fully active redundancy in both business and systems operations is a high cost solution that maybe prohibitive to many firms due to size or corporate culture
- Current business locations and data centers are in close proximity sharing common infrastructure and transportation providers
- Corporate commitment to “rethink” concentration of business processes and the staff that supports key functions for the firm.
- Geographic concentration of work force and key staff members to support critical business and systems functions
- Geographically diverse business locations that perform dissimilar business functions or use different applications to perform similar functions
- High costs associated with data center redundancy

Key questions (To ask)

- Do business opportunities exist in expanding business operations to client service office?
- Can staff that is geographically dispersed performing different functions be cross-trained to support each other in the event of an interruption?
- Do technical opportunities exist to consolidate market data sources and applications that support critical functions?
- Can critical applications be leveraged through load balancing and hot server recovery strategies between existing data centers?
- Can certain applications be managed in asynchronous mode (which allows distance of over 1100 miles with latency measured in less than 6 minutes)?
    - Identify location and back up for all critical and client service applications
    - Can back-up or test servers supporting applications be moved?
    - Identify gaps in network recovery (data and voice)
- Do real estate opportunities exist that can help support migrating to less costly location(s) that offers geographic diversity and adequate "talent" pool for staffing
- Are there regulatory and compliance concerns/issues with operating in different states/countries and having staff properly licensed that may impact using this model?

3.7.2 Possible Strategies

- If the organization is large enough to sustain redundant skill sets in multiple locations, one strategy would be to leverage that redundancy.
- Another possible strategy is to outsource the redundancy requirements to a service provider.

Note: in either scenario, detailed recovery documentation is important.

3.7.3 Possible Solutions

- Leveraging existing business locations
    - Migrating towards using the same applications and market data providers across business functions and locations will can significantly reduce cross training, test and recovery of key operations
    - Review centralized critical business functions with owner of function to explore market opportunities to expand to another location
    - Leverage call centers, operations and client support groups across diverse locations to support different business functions, client base and business lines to support each other
        - Identify data security and client privacy issues that can impede the process
        - Identify training and testing opportunities to maintain function/application knowledge
- Leveraging existing data center(s) and back-up locations to migrate to an Active/Active model
    - Review existing critical applications and change management process for
        - migrating to systems that by design or through use of shared equipment be active in both locations
        - identifying where "clustered servers supporting applications reside in the same data center for relocation
        - understanding when a new application is being developed or acquired to ensure that redundancy costs are part of the initial costs
    - Review existing recovery strategies for cost reduction opportunities and improved availability whether systems is recovered internally or through use of a third party recovery provider

Internal and External Business Partners

BC plans should include internal and external business partners (operations, tech support, clients, vendors, regulators, exchanges, etc.), ensuring that acceptable levels of operational connectivity can be resumed within recovery objectives.

Firms should be familiar with business partner BC plans (both internal and external) and understand any associated risk

3.7.4 Relevancy of Stated Guideline

One's firm is accountable to clients, stakeholders, and regulators to fulfil their obligations. It becomes necessary to assess a chosen vendor's ability to help the firm achieve this. Part of the planning process includes this assessment which covers the vendor's contribution to critical functions, ease of finding an alternative during a disaster, and the vendor's own resiliency planning. Consequently, a data feed provider selection conveys more risk than the choice of vendors for paper clips and pencils.

Key Concerns/Issues (To work through)

- Non-recovery of a internal/external partner can be a single point of failure
- Reliance on business partners assessment of their ability to recovery their business
- Testing with external parties is not always possible making it difficult to validate that level of operational connectivity is sufficient
- It could be difficult to get an accurate assessment of external business partners capability and risks of non-recovery – not all business partners are willing or able to share their plans

Key questions (To ask)

- What process is in place to identify key business partners and dependencies – how can I assure that I have captured them all?
- Do I include these partners in my risk assessment and factor in their time to recover in my recovery time objectives?
- What level of confidence do you have in your business partner's recovery capability and how can I confirm their level of readiness?
- What alternative procedures or processes do you have in place for external business partners who could lead to a single point of failure?
- How may I decrease my reliance on a single point of failure?

3.7.5 Possible Strategies

- Treat your external partners as extensions of your internal departments.
- Apply peer pressure from user groups to get vendors to meet new levels of service and regulatory concerns

3.7.6 Possible Solutions

- Business partners/dependencies should be identified during the risk assessment/BIA process and their risk and readiness evaluated
- External party surveys to identify their capability and/or review of their business continuity plans to confirm capabilities

- As part of vendor management process, new critical business partners, need to evidence their business recovery capability and readiness – this should be part of the due diligence process
- Testing with internal/external providers to validate their capabilities and synergy during a disaster.
- Identification of key risks including single point of failures; establish alternative partners or process to minimize this risk
- Maintain alternate contact information that is readily accessible

3.8 Redundant Copies of Vital Records

Business units should ensure that redundant copies of vital records are stored in a secured and geographically diverse location and are available for use during an emergency within stated recovery objectives.

3.8.1 Relevancy of Stated Guideline

Critical/vital records need to be safeguarded so that they are accessible within the time needed in the event of a significant business disruption that prevents access or destroys the originals. This implies the identification of what is vital, for what applications it pertains, what alternative forms constitute a valid document, and the location and time availability of these documents during a disaster.

Key Concerns/Issues (To work through)

- Ownership and identification of these records – who is accountable to ensure all are identified and stored
- Process for retrieval – is it timely and understood by those who need the records
- Means of copying and storing – in today's world are electronic copies sufficient
- Choosing an appropriate location and vendor//alternate location
- Ensuring records are kept up-to-date for dynamic records
- Recognize that the critical nature of a document may be tied to a timeline such that after a certain date, the document may no longer be critical and should be released from that categorization/classification.

Key questions (To ask)

- Does my business areas own this process or business continuity?
- Who determines what is considered as a "vital record" and who ensures that are kept up-to-date and refreshed if they are dynamic.
- What mediums can I use to store – paper only, paper and electronic or diverse?
- How accessible will these records be and who is responsible for retrieving and disseminating to business owners?

3.8.2 Possible Strategies

- Establish a vital records-retention and recovery program which includes the classification of records and identification of what is vital and what can substitute as a copy.

3.8.3 Possible Solutions

- Establish a process and procedure for storing and retrieval and communicate to appropriate parties?
- Provide guidelines on what constitutes a vital record and what medium of storage are acceptable?
- Agree ownership with business area and include critical information about process in the BC plans
- Include vendor contact information in critical guides and documents used to support the recovery process
- Make duplicate originals.

3.9 Availability of Resources

Each firm should ensure the availability of the resources required to meet its recovery objectives.

3.9.1 Relevancy of Stated Guideline

It is critical to have sufficient qualified individuals, facilities, and equipment to achieve the recovery objectives, which include the recovery time objectives, and to ensure the sufficiency of these resources to achieve the objectives by testing their ability to do so. Having a plan in place with no one to execute it is not effective. Consideration in the planning process must be given to the possibility that specific individuals may not able to reach the recovery site. This can be addressed with documentation that is of a level to reasonably expect a knowledgeable individual to follow.

Key Concerns/Issues (To work through)

- Whether or not one maintains duplicate staff or out-sources part of the recovery to a recovery vendor.
- Currency of documentation in order to guide a knowledgeable contingency resource that may not be familiar with the specific processes.
- Contingency/incident response plans for when an expected individual does not arrive at the recovery site.
- Placing full load on recovery resources including systems and infrastructure.

Key questions (To ask)

- Where should the personnel resources reside?
- How are the personnel resources trained and kept current?
- How will contingency recovery resources participate in testing with base recovery resources?
- How do you test invoking contingency recovery resources? For example, flag specific individuals as "unavailable" during an actual test in an unannounced manner.
- Can one determine sufficiency of resources (people, facilities, technology) through simulation or calculation or must one perform a full production swing?

3.9.2 Possible Strategies

- Deploy a split staff working environment to ensure staff diversity
- Deploy a diverse resource policy which includes identification of critical staff, transfer of functions to other locations, specific operating procedures for critical functions and a robust cross training program.

3.9.3 Possible Solutions

- Run active - active with full capacity.
- Outsource recovery to a recovery vendor that learns your procedures.
- Contract with staffing organizations with appropriate skill sets.

3.10 Pandemic Planning

Each firm should consider planning for Infectious Diseases and especially Pandemics.

3.10.1 Relevancy of Stated Guideline

Infectious diseases, and in particular Pandemics which imply a wide spread illness to which the body has no prior immunity, are known to present unique conditions that could affect the resiliency of an organization. With the implied simultaneous absence of a significant number of people over a broad geography and over an extended period of time, one can not easily expect to solve the dilemma by moving an operation or obtaining additional resources. Additionally, the illness spread is expected to occur in waves or cycles such that preparation requires means that help separate healthy from sick personnel and delays the spread of the disease to allow time for vaccine development

Key Concerns/Issues (To work through)

The Pandemic Program should have and include the following:

- A Formal Plan with guidelines and actions defined for the separation of the sick and to delay spread of the disease. The plan should:
  - Include escalating response stages that corresponding to the spread and severity of an outbreak.
  - Measure impact severity within a local community resulting in corresponding appropriate actions
  - Be flexible enough to adapt to direction and guidance from local health authorities
- A Steering committee to evaluate the quality of the plan and to implement policies during an active pandemic
- A recognition of global, national, and local health authorities as "golden" source for information on spread, severity and required actions concerning disease management
- As a human health issue, planning and implementation involvement from key parties such as Human Resources, Facilities Management and Legal
- Facilities, systems, and/or procedures that provide the organization with the capability to continue critical operations with reduced staffing.
- Within Business Continuity Planning, the business unit must understand critical job functions and the depth of cross training and procedural documentation
- Planning should include post wave strategies that will allow recovery, plan adjustment and preparation for subsequent waves of an outbreak
- A testing program at different levels of absenteeism
- Oversight of the program including, at a minimum, annual review

Key questions (To ask)

- How are the BIA results incorporated into the Pandemic Plan?
- How is your response scaled with respect to the severity of pandemic outbreak?
- How is remote access and work from home incorporated into the planning?
- How is public communication incorporated into the plan?
- Have trigger points been identified and tied to responses and level of plan activation?
- What HR policies need to be modified to accommodate such issues as payroll, sick leave, quarantining individuals after exposure, travel restrictions, temperature screening?

- What mechanisms are in place to measure absenteeism and whether critical job functions are being completed
- What mechanisms are in place to communicate or clarify pandemic media reporting with employees?
- What mechanisms are in place to communicate US CDC or local Health Authorities recommendations to employees for family care?
- What mechanisms are in place to adjust your Formal Plan to US CDC or local Health Authorities recommendations during the implementation of your plan
- At what level do you anticipate the implementation of personal protective equipment (PPE) such as hand sanitizer, masks, respirators, and other equipment?
- What is the availability and how will Pharmaceutical Interventions such as antivirals and vaccines be distributed
- How are you expected to implement preventive Non-Pharmaceutical Interventions measures such as screening, social distancing & quarantining of suspected/identified contagious individuals or site?
- To what extent have you incorporated inventory management (levels, restocking, etc.) into the acquisition and distribution of PPEs & Pharmaceutical Interventions for the initial wave and subsequent waves
- How is building management involved with such issues as cleaning, maintenance, food handling, alcohol based hand sanitizers, screening, etc.?
- Should you bring firm foreign nationals home?
- To what level have your service providers implemented similar pandemic plans?
- How have you communicated to your service providers and vendors about your expectations regarding non-punitive absentee policies for their contagious employees?
- Have you considered procedures and compliance requirements that could potentially require regulatory relief?
- To what extent are you participating in industry discussions?

3.10.2 Possible Strategies

- Health & Sick people separation
    - Educate employees about health and hygiene strategies
    - Empower managers to encourage employees to stay home when sick
    - Communicate situation, expectations and policies
    - Encourage family planning
- Delay the Spread of the disease to provide time for vaccine production
    - Personnel Protection devices
    - Pharmaceutical intervention
    - Non Pharmaceutical intervention
- Post Wave planning
    - After first wave return to normal operations, restoration
    - Begin next wave strategic planning

3.10.3 Possible Solutions

- Deploy a diverse resource policy which includes identification of critical staff, transfer of functions to other locations, specific operating procedures for critical functions and a robust cross training program

- Reduce business functions to “bare” minimum using available staff to perform necessary functions. Be sure to notify your regulator via SIFMA.
- Deploy a split staff working environment to ensure staff diversity
- Jettison application and business functions in a staged manner, based on measures such as e absenteeism
- Contract with staffing organizations or individuals with appropriate skill sets if you currently minimized your preferred vendor list.
- Perform many functions in a work-from-home or less concentrated environments.
- Consider multiple providers of services and/or equipment and supplies.
- Purchase, distribute, encourage usage and replenish inventories for PPEs such as hand sanitizer, masks, respirators, and other equipment
- Arrange purchase or reserve supply, define legal distribution, encourage usage and replenish Pharmaceutical interventions such as antivirals and vaccines
- Develop, document in a formal policy, obtain approval, communicate to management the need to observe and formally implement Non Pharmaceutical interventions such as travel policies, liberal leave, quarantining of sick personnel, temperature screening, social distancing, etc.
- Encourage personal and building hygiene
- Establish effective communication methodologies with employees, vendors, service providers, public entities, health organizations, and industry associations (SIFMA) to track spread/severity, judge peer response and to measure your organizational response .
- At completion of first wave
    - Ensure critical management teams are in place, if not ensure steering committee and department leadership is replaced
    - Encourage, measure and report the return to full functionality
- In preparation for subsequent phases
    - In a timely manner, revise the Formal Plan from lessons learned
    - Replenish PPE and Pharmaceutical inventories
    - Begin employee awareness campaign about possible subsequent waves

Addendum - Reference Material

On Overall Program Elements

Financial Services Industry specific

- FFIEC Audit guidelines
- NASD website

General

- Book “Resiliency of the Enterprise” MIT Press ISBN 0-262-19537-2

On BC Policy

Financial Services Industry specific

- Basel II BCP Operating Principles
- FFEIC guidelines for BCP
- NASD and NYSE Rules
- NYSE 446 Info Memo
- NYSE 401 “Good Conduct” regulations

On BC Documentation

Financial Services Industry specific

- NASD BCP template for small firms
- NASD and NYSE rules to assist with content

On BC Oversight Group

Financial Services Industry specific

- NFPA 1600 Chapter 4, Program Management.
- FIFEC Guidelines, page 3 "Board and Senior Management responsibilities."
- NASD Small firms template
- IDA Canada Template
- Regs 3510 and 446

On Business Unit Ownership

Financial Services Industry specific

- FIFEC Guidelines, page 3 "Board and Senior Management responsibilities."

On Recovery Exercises

Financial Services Industry specific

- NFPA 1600 Chapter 4, Program Management.
- Regs 3510 and 446

General

- OEM Guidelines From Local Municipalities
- 2 books from Mel (“Crisis Management”, and 1 other book) – Mel to provide details

On Annual Review

Financial Services Industry specific

- NFPA 1600 Chapter 4, Program Management.
- Regs 3510 and 446

General

- Most current business continuity plan.

On Communication Alternatives

Financial Services Industry specific

- Rule 3510

General

- Blackout – document on the website from NYC
- Industry lesson learned

On Facilities and Geographic Considerations

Financial Services Industry specific

- Interagency white paper

On Facilities and Accessibility, Availability, & Capability

Financial Services Industry specific

- FFIEC Guidelines

General

- Recovery time objectives are influenced by regulations or contract agreements with customers. Meeting them is dependent on service level agreements with vendors/ service providers.

On Critical Business Applications - Availability

Financial Industry Specific

- FFIEC Guidelines

General

- Methods for conducting business impact analysis.

On Vendor Considerations

Financial Services Industry specific

- FFEIC guidelines for BCP
- NASD and NYSE rules
- NYSE 446 Info Memo

On Vital Records

Financial Services Industry specific

- NASD 3510
- NYSE Info Memo 05-80

4 Addendum - Examples/Lessons Learned from Incidents

On Overall Program Elements

Not all BC events are as catastrophic as 9/11. There are far more recurring events, such as:

- Power blackouts
- Flooding
- Ice Storms
- Hurricanes
- Transit strikes
- Bombings

On Oversight Group

Experience has shown that plans with strong Executive oversight and support have more easily succeeded, and are better able to meet stated project objectives. Executive oversight helps meet the initiative's objectives by maintaining a "big picture" view.

On Recovery Exercises

- SIA 2005 and 2006 Industry Test results
- Lessons from FEMA, DHS, or government-sponsored drills

On Strategy Elements

Hurricane Katrina, New Orleans, USA

On Availability of Resources

After the terrorists attack on September 11, 2000 the importance and changes needed in the planning for resource availability became evident. Some lessons learned are:

- Personnel
  - With bridges closed, companies in the New York City area could no longer assume that employees living on Long Island could get to recovery centers in New Jersey, or visa versa. This awareness permeated through the rest of the country.
  - Concern for family was evident and companies recognized that for employees to concentrate on the business, they must feel confident that loved ones are safe. Plans must take this into consideration.
- Equipment
  - With airlines grounded, companies relying on next day drop shipping of equipment, experienced delays in establishing new agreements during a "disaster".
- Space
  - Alternate sites can quickly get over-crowded in a regional disaster.

On Roles and Responsibilities

- (Insert here?) Sample organization charts – centralized/decentralized
- HEICS (Hospital Emergency Incident Command System? www.heics.com)

On Training

Lessons learned from Hurricane Katrina.

On Facilities and Accessibility, Availability, and Capability

- Access to recovery facility is affected by transportation and/or availability of resources local to recovery facility.
- Vendor facility shared services are affected by the breadth of a localized incident (too many customers needing access to the same resources) 9-ll Highlighted that shared recovery facilities may not be a viable option.

On Critical Business Applications

Fixes made during real incidents should be documented and incorporated into recovery procedures.

On Vendor Considerations

- 9/11/01
- East Coast Blackout 2004
- SARs