Contingency Planning for Senior Management

What you need to know about your business recovery
Agenda

- Current Regulatory Environment
- Risk Management
- What is Contingency Planning
- Components of a solid recovery program
- Lessons from Sept 11
- Questions to ask your team before the disaster happens
- Eleven Steps to a Business Contingency Plan
- Where to get help
Current Regulatory Environment

- Interagency White Paper
- Privacy regulations
- Sarbanes Oxley
- Corporate Governance
- Prudent Man Rule

More to follow - The rules will not get any easier to comply with – start now
Governance

Governance: regulators, corporate governance requirements – Turnbull, Sarbanes-Oxley

• Typically: CEO or Board must certify that risks are understood and under control

• Requirements:
  • aggregate reporting from all areas
  • good lines of communication
  • efficient reporting processes
Governance

- A concise summary of your key risks
- A common vocabulary to discuss risk
- A means to have productive discussions with your team
- A roadmap to help you in your business planning
- A set of actions to help improve your risk management process
Risk Management Program

- Three components of Risk
  - Threats
  - Assets
  - Mitigating Factors
Elements of Risk

Threats -

- Events or situations which would cause financial or operational impact to the organization.
- Threats are measured in probabilities, such as “may occur 1 time in 10 years”.
- Each threat has a duration of time that the business or operation would not be able to function in its normal manner, if at all
Elements of Risk

Assets -

- Assets are composed of many elements
- Physical assets that are owned by the organization
- Information assets
- Financial assets
  - Revenues lost for the duration of the incident
  - Additional costs to recover
  - Fines and penalties incurred
  - Lost good will or competitive advantages
Elements of Risk

**Mitigating Factors** -

- Mitigating factors are the protection devices, safeguards, and procedures which are in place that reduce the effects of the threats.

- *They do not reduce the threat; they only reduce the effect of the threat.*

Examples of mitigating factors in use are UPS (Uninterruptable Power Supply) and Generator backups for replacement power, sprinkler systems to control the spread of fire, Assess Card Readers to control physical access to Fidelity space, etc....
Risk Mitigation Strategies

Protecting People and Workspaces

Protecting Information

Protecting Reputation
Protecting People and Workspaces

- Access Control
- Alarm Monitoring
- Floor Warden
- Evacuation Drills
- Background Investigations
- Landscape Design
- Lighting
- Cameras
- Visitor procedures
- Backup Power systems
- Facility design
- Facility sighting
Protecting Information

- Information Security policy and procedures
- Privacy Policy
- Firewalls
- Intrusion Detection
- Strong Passwords
- Controlling access to information
- Vendor Management
- Secure offsite storage
- Proprietary Waste Disposal
- Virus Protection and Response
Protecting Reputation

- Strong Governance
- Media trained
- Communication Plans
- Internal and external audits
- Operational Management
- Recoverability
- Code of Ethics
Risks that are an inherent part of the business environment and have an effect on business objectives and performance

Risks associated with the use of systems and technology, including availability, capacity integrity, operational support, functionality systems integration and change management

Risks relating to enforceability of contracts, interpretation of laws, compliance with law and impact of regulation

Inability to raise debt or equity capital as needed for short-term liquidity or long-term growth, as well as uncertainty in pricing or sales of assets or liabilities

Exposure to loss relating to a change in the credit-worthiness of a counter-party, collateral, customer or partner that may impact the counter-party’s ability to fulfill its obligations under a contractual agreement

The uncertainty in the future market value of a portfolio of assets and / or liabilities

The risk of loss resulting from people

The risk of loss resulting from inadequate or failed processes

The risk of loss resulting from unique, unusual or extraordinary events
Contingency Plans are what we exercise when all other mitigating factors fail

Contingencies start with Event Management

If you do not properly manage Events, all the other Risks may occur

Event Management is about Communication and Response

Event Management needs to be practiced
Event Management Requirements

- Strategy must be consistent regardless of event
- Need to establish an assessment process
- Event Ownership needs to be defined
- Management teams identified
- Response Teams identified
- Process for gathering of key decision makers
- Methods of communication need to be defined
Event Management example
Facility event

- Built by Building
- Three teams:
  - Assessment Team
  - First Escalation Team
  - General Team
- Permanent standing conference bridge that always has the same phone number
- Event owners defined
- Escalation process defined
Contingency Planning

If you are reading your plan for the first time and you are in the middle of a disaster...........

You are in trouble
How ready is your business?

- If you were evacuated from your building and you were standing in the evacuation area and they announce that you could not work at that site for at least the next 2 weeks,

*Do you know what to do next?*

*Does your staff?*
What is a Contingency Plan

- The documented process for continuation/recovery of business functions in the event of an unexpected disruption of service.
- The plan describes the pre-planned sequence of events that allows for the continuation/recovery of business functions, computer resources, networks, and facilities.
# Components of a Solid Business Continuity Program

<table>
<thead>
<tr>
<th>Deliverables</th>
<th>Due date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency Notification List</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Business Functions/ Resource Requirements</td>
<td>Semi-Annually</td>
</tr>
<tr>
<td>Business Resumption Plans with sign-off</td>
<td>Annually</td>
</tr>
<tr>
<td>Training &amp; Awareness</td>
<td>Quarterly</td>
</tr>
<tr>
<td>Vital Records Program</td>
<td>On-going</td>
</tr>
<tr>
<td>Technology Reviews</td>
<td>Annually</td>
</tr>
<tr>
<td>Strategy for loss of site/systems</td>
<td>Annually</td>
</tr>
<tr>
<td>Procedures for loss of site/systems</td>
<td>Annually</td>
</tr>
<tr>
<td>Call Exercise</td>
<td>Semi-Annually</td>
</tr>
<tr>
<td>Walk-Through Exercise</td>
<td>Annually</td>
</tr>
<tr>
<td>Simulated Or Actual Exercise</td>
<td>Semi-Annually</td>
</tr>
<tr>
<td>Compact Exercise</td>
<td>Annually</td>
</tr>
<tr>
<td>Systems Loss Test</td>
<td>Annually</td>
</tr>
</tbody>
</table>
Contingency Planning Program Status

Program Compliance (%)

<table>
<thead>
<tr>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Rating* =</td>
</tr>
</tbody>
</table>

% of A-AAA with a recovery solution for loss of building** % of A-AAA with a loss of application recovery solution***

<table>
<thead>
<tr>
<th>% of Business Functions Completing Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>A - AAA</td>
</tr>
</tbody>
</table>

** % of A-AAA business functions that have completed ALL four of the following:
1) Vital Records Program in place
2) Resource Requirements Defined
3) Alternate Sites in Place
4) Alternate Site Test

*** % of A-AAA business functions that have completed ALL three of the following:
1) Technology Review
2) Procedures for Loss of Systems
3) Systems Loss Test

Comments

* Risk Rating -- The impact to Fidelity Investments if this business unit is out of business.

*(DRPS)*
Business Impact Analysis

- The process used to identify what would happen if a risk occurred
- The end result is to determine the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) of all processes within your organization
- Includes technology and non-technology functions
- Results should be signed off by Senior Management as evidence of review
- RTO and RPO drive the recovery strategies available for each business process to be recovered
Lessons from September 11

The events of September 11th and the resulting business disruptions have highlighted the need for companies to revisit the assumptions underlying their disaster recovery and business continuity plans. Such plans have primarily focused on the loss of systems and information or the inability to access a main processing facility. After September 11th, planning considerations have expanded to include:

- loss of key employees or emotionally-impacted staff,
- loss of access to major business districts,
- long-term operation at back-up sites,
- need for alternative back-up sites,
- availability of contact information for key employees,
- loss of paper documentation, and
- loss of critical vendors/business partners.
How Close Were We?
Ariel View After the Attack
Another View
What We Learned from 9/11

- Testing was the key to the success of the recovery
- Critical operations in a single site are bad business
- We don’t have problem by business, we have problems by building
- Transportation was a major issue in the first few days
- Incomplete/inaccurate inventories make the insurance claim difficult
- People do not want to travel away from their families
- Very few business operations stand alone
- Voice is harder than data to recover
- Some of our vendors were in trouble too
- The devil is in the details
The Good News

- We experienced no loss of life in New York and injuries were not serious. All the required personnel were available.
- The Full Market remained closed, allowing initial recovery efforts to be augmented and the business to prepare to conduct business for a long period of time in the alternate sites.
- Two-way pagers. They worked consistently when other forms of communication were either busy or completely unavailable.
- Buildout of all of the alternate sites occurred very quickly to allow critical business functions to resume.
- Bench Strength - All of the people involved exhibited teamwork, flexibility, availability and an excellent attitude. Many volunteered to work longer hours and additional shifts to get the job done.
- The ability to use alternate network resources to get the New York Operations back online quickly and to provide redundancy for network lines running in backup mode.
Planning Assumptions to re-think

- Assume only one disaster strikes at the same time
  - We lost access to WFC and simultaneously lost access to key buildings in Boston that were evacuated as a precaution
  - This led to multiple disaster declarations in diverse locations that had to staffed at the same time by multiple support groups

- Assume infrastructure required for recovery is in place
  - Telecommunications, power and transportation were all impacted. No one had ever imagined a scenario where all the planes in the country would be unavailable.
Planning Assumptions to re-think

- Assume your disaster recovery team and the rest of the corporation survive the attack
  - We was unaffected by this, but other New York based corporations lost entire recovery teams and the documentation required to recover
  - Other corporations are struggling to do required day to day business functions because those responsible died in the event and the training materials for the position were stored in the building

- Assume the ability to get required equipment from your vendors very quickly
  - This did not impact We, but the drop in the economy has left many vendors with little or no inventory. The ability to obtain required equipment quickly was hampered.
Planning Assumptions to re-think

- The disaster recovery plan should be built for a short interruption in business and only for the data center, not a long term disaster.
  - This type of planning assumption led many business units to assume that plans only needed to be done for very small numbers of employees or only for their technology infrastructure. This led to scrambling during a disaster and not necessarily the best recovery plan for the employees involved. Recovery is for the whole business.
Questions to Ask Your Team BEFORE the Disaster

- Are we recoverable or just “green”? 
- What is our Recovery Time Objective? 
- What is our Recovery Point Objective? 
- Are we prepared for “loss of people”, not just loss of site? 
- Are we prepared for losing a critical application? 
- Where is the alternate site? 
- How will you communicate during the event? 
- When did you last test? 
- Have we identified our critical vendors and do we know what their recovery plans are?
“Well, thank God we all made it out in time.
...’Course, now we’re equally screwed.”
Eleven Steps to having a Contingency Plan for your business

- Follow these steps to a solid recovery program for your business
Step 1
Identify Business Recovery team

- Identify your team and make certain they know how to reach you in an emergency
Step 2
Identify business vital records

- Identify vital records
  - Procedure manuals
  - forms
  - vendor lists
  - contact lists
  - customer lists
  - contracts
  - source documents
Step 3
Identify Business Functions

- Identify the business functions for functional areas
- Perform risk and business impact analysis for each function
- Establish the recovery time for your business functions
- Identify minimum staff requirements
- Identify Interdependencies
Step 4
Identify desktop requirements

- Minimum desktop configuration
- Application connectivity
- Voice Requirements
  - phones
  - Fax
  - Modems
- Print Requirements
- Proprietary software running on desktop
Step 5
Define Recovery Strategy

- Develop recovery strategy for business functions based on the recovery priority
Selecting the Right Recovery Strategy for your business

Recovery strategies will be driven by the recovery timeframe of the function. Recovery options might include the following:

- **Self-service** - A business unit can transfer work to another of its own locations which have available facilities.
- **Internal Arrangement** - Training rooms, cafeterias, conference rooms, etc. may be equipped to support business functions.
- **Reciprocal Agreements** - Other business units may be able to accommodate those affected. This could involve the temporary suspension of non-critical functions at the business units not affected by the outage.
- **Dedicated alternate sites** - Built by your company to accommodate critical function recovery.
- **External Suppliers** - A number of external companies offer facilities covering a wide range of business recovery needs.
- **No arrangement** - For low priority business functions it may not be cost justified to plan to a detailed level. The minimum requirement would be to record a description of the functions, the maximum allowable lapse time for recover, and a list of the resources required.
Step 6
Internal Site Survey

- Survey existing sites
- Identify equipment/phone services
- Identify desktops to be used for contingency
- Identify staff to be displaced or moved to off shift
Step 7
External Site Recovery

- Prepare RFP which includes all requirements
- Identify essential vs. “nice to have”
- Receive proposals from vendors
- Compare for requirements and costs
- Visit sites identified as potential vendors
- Select vendors
Step 8
Internal Systems

- Identify all platforms and applications supported by internal systems group
- Identify recovery priority for each application
- Identify recovery strategy which meets the business requirements
- Develop recovery procedures for critical applications
Step 9
Document Plan

- Pull the information together into a plan document and distribute
Step 10
Train staff

Everyone should know the answer to the question:

*If you couldn’t get back in your building today, what would you do next?*
Step 11
TEST, TEST, TEST

- Event Management tests
- Alternate site tests
It could happen anywhere...

Don’t be the one taken by storm!!
Websites

- **Industry Group Websites**
  
  **DRI International**
  [www.drii.org](http://www.drii.org)

  **Continuity Insights**
  [www.continuityinsights.com/conf.cfm](http://www.continuityinsights.com/conf.cfm)

  **Contingency planning and Management**
  [www.contingencyplanning.com](http://www.contingencyplanning.com)

  **Disaster Recovery Journal**
  [www.drj.com](http://www.drj.com/)

  **Global Association of Risk Professionals (GARP)**
  [www.garp.com](http://www.garp.com)

  **Professional Risk Managers International Association (PRMIA)**
  [www.prmia.org](http://www.prmia.org)

  **Institute of Internal Auditors**
  [www.theiia.org](http://www.theiia.org)