Remember The Wizard of Oz? When the tornado struck, Dorothy was whisked away to a far-off land. Dorothy, the Tin Man and the others followed the yellow brick road for miles, running into problems on their way to Oz. Finally, after enduring obstacle after obstacle, Dorothy clicked her heals together and she was back home in Kansas.

Business continuity planning is much like a movie, but hopefully with different results than that seen on The Wizard of Oz. In the movie, there was no plan to get the characters back to where they belonged in the event of a tornado or other disaster. A lot of time, energy and resources were used before they were able to return to "business as usual".

Not only does planning keep you from having to endure the proverbial yellow brick road, but the best process is as follows:

1. "Cast" your main characters
2. Finalize the script
3. Find the "extras" that will be needed
4. Set the stage
5. Have a proper dress rehearsal!

Advanced Production!

First and foremost, you need to have complete support of the Board of Directors and senior management when planning, developing, testing and implementing your Business Continuity Plan. Once you obtain that, you are ready to begin!

Choosing the Cast:

When developing your Business Continuity Plan, you should start with a Business Impact Analysis (BIA). The BIA is developed to identify critical business assets or functions to determine what is critical for operations. What information resources, systems, processes, supplies, suppliers, etc. can the organization not function without? Think outside the box and include all information resources, not just the obvious like servers and workstations. Consider interviewing key personnel within the organization to get an accurate picture of what is needed. Also, make sure to include all business functions in the process. Then, prioritize those findings based on criticality, financial impact, and maximum allowable downtime. Also consider the acceptable levels of data and operations that will be required for the organization to be operational.

The following classifications of systems (as provided by ISACA) can be used in determining criticality:

- Critical: These functions cannot be performed unless they are replaced by identical capabilities. Critical applications cannot be replaced my manual methods. Tolerance to interruption is very low; therefore, cost of interruption is very high.
- Vital: These functions can be performed manually, but only for a brief period of time. There is a higher tolerance to interruption than with critical systems and, therefore, somewhat lower costs of interruption, provided that functions are restored within a certain time frame (usually five days or less).
- Sensitive: These functions can be performed manually, at a tolerable cost and for an extended period of time. While they can be performed manually, it usually is a difficult process and required additional staff to perform.
- Nonsenstive: These functions may be interrupted for an extended period of time, at little or no cost to the company, and require little or no catching up when restored.

Finalizing the Script: The Risk Assessment

If a movie director doesn't prune out unnecessary scenes in the script, the movie goes on forever, and the important scenes get lost in all the noise. The purpose of performing a risk assessment is to identify the most likely events that could cause an interruption to business processes and / or services. Some threats to consider include:

- Technical / System Failures
- Information Security Incidents
- Loss of Services / Utilities
- Natural / Environmental Disasters
- Malicious Acts

You should also take into consideration worst-case scenarios. This would include total destruction of facilities and loss of life.

Identifying just the nature of the threat isn't enough. You also need to consider the probability that a certain threat will "materialize". *Figure 1: Probability* can be used as a starting point.

Figure 1: Probability

Ranking	Likelihood of Occurrence	Starting Point (not to be used literally)
1	Highly Unlikely	Is just not going to occur no matter what.
2	Negligible	Unlikely to occur.
3	Very low	Likely to occur two/three times every five years.
4	Low	Likely to occur one every year or less.
5	Medium	Likely to occur once every six months or less.
6	High	Likely to occur once per month or less.
7	Very high	Likely to occur multiple times per month.
8	Extreme	Likely to occur multiple times per day.

Take into consideration the impact the realization of the threat will have on operations. What impact will that threat have on the information resources, systems, processes, supplies, suppliers, etc. identified during the BIA phase? *Figure 2: Impact Severity* illustrates potential impacts that a threat can have on a vulnerability.

For each item identified, calculate the total risk by taking the rank of each (total Probability plus total Impact Severity) to determine the overall risk ranking. Then, when developing your overall Business Continuity Plan, prioritize based on the most critical Likelihood of Occurrence and Impact Severity items. *See Figure 3: Overall Risk.*

Figure 2: Impact Severity

Ranking	Impact Severity	Starting Point (not to be used literally)
1	Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
2	Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
3	Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
4	Serious	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair. May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise of large amount of information or services.
5	Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

Figure 3: Overall Risk

Risk Ranking	Interpretation
13	**Critical**
12	**Critical**
11	**High**
10	**High**
9	**Moderate**
8	**Moderate**
7	**Moderate**
6	**Low**
5	**Low**
4	**Low**
3	**Low**
2	**Low**

Setting the Stage: Developing Your Business Continuity Plan

Having selected your cast members and prioritizing the scenes in the script, the next phase is to build and set the stage. The Business Continuity Plan is a crucial part in recovering from a disruption. Based on the information obtained during the BIA and risk assessment, you can now start planning for what should take place in the event of a disruption or disaster. It provides a "script" or guidance in evaluating damage, what should happen during the disruption, and what needs to take place to restore business operations after the disruption is over. In essence, it should include all the steps required to maintain, resume, and recover from a disruption. Also included in the plan should be the "characters" responsible for certain actions.

According to the Federal Financial Institutions Examination Council (FFIEC), your Business Continuity Plan should be:

- Effective in minimizing service disruptions and financial loss
- Specific regarding what conditions should prompt implementation of the plan
- Specific regarding what immediate steps should be taken during a disruption
- Flexible to respond to unanticipated threat scenarios and changing internal conditions
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted rather than on the precise nature of the disruption
- Written and disseminated so that various groups of personnel can implement it in a timely manner

Ready - Set - Action: Plan Testing

Without actually acting out the script, we have no clue whether scenes in the movie really work or not. Once the Business Continuity Plan is written, it should be tested to confirm that objectives of the plan are achievable. There are various methods of testing (or rehearsing) that can be performed. Methods, as taken from the FFIEC guidelines include:

- Orientation / Walk-through: A basic form of testing. Its primary objective is to ensure that critical personnel from all areas are familiar with the Plan. It is characterized by:
  - Discussion about the BCP in a conference room or small group setting
  - Individual and team training
  - Clarification and highlighting of critical plan elements
- Tabletop / Mini-drill: A tabletop/mini-drill is somewhat more involved than an orientation/walk-through because the participants choose a specific event scenario and apply the BCP to it. It includes:
  - Practice and validation of specific functional response capability
  - Focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability
  - Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment
  - Mobilization of all or some of the crisis management/response team to practice proper coordination
  - Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan
- Functional Testing: Functional testing is the first type that involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the BCP. It includes:
  - Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning
  - Actual or simulated response to alternate locations or facilities using actual communications capabilities
  - Mobilization of personnel and resources at varied geographical sites
  - Varying degrees of actual, as opposed to simulated, notification and resource mobilization

- Full-scale Testing: Full-scale testing is the most comprehensive type of test. In a full-scale test, the institution implements all or portions of its BCP by processing data and transactions using back-up media at the recovery site. It involves:
  - Validation of crisis response functions
  - Demonstration of knowledge and skills, as well as management response and decision-making capability
  - On-the-scene execution of coordination and decision-making roles
  - Actual, as opposed to simulated, notifications, mobilization of resources, and communication of decisions
  - Activities conducted at actual response locations or facilities
  - Enterprise-wide participation and interaction of internal and external management response teams with full involvement of external organizations
  - Actual processing of data utilizing back-up media
  - Exercises generally extending over a longer period of time to allow issues to fully evolve as they would in a crisis, and allow realistic role- play of all the involved groups.

The Cutting Room Floor

Just like with the film from a movie, often times pieces of which are found on the cutting room floor, your Business Continuity Plan must be reviewed, updated, and re-tested on a regular basis to take into consideration changes in personnel, technology, possible threats, and recovery scenarios. Make sure your Business Continuity Plan is reviewed and updated on an annual basis. Look at its relevance to the business environment. Update it as it is appropriate and test your Plan again.

Don't take a chance on being stuck on the yellow brick road with Dorothy. Take the time to plan, write the script, and rehearse! It's not as easy as clicking your heals together when it comes to "business as usual" after a disruption. Your business and your customers depend on it!

About the Author:

Bobbette Fagel, CISA, CISM
Vice President
infotex, Inc.

Bobbette is a Certified Information Systems Auditor and Certified Information Security Manager, and has worked with Infotex since its inception. She has been intimately involved in compliance projects for financial organizations and hospitals, and leads our efforts on compliance program development as well as policy and procedure. She handles the reporting aspects of Vulnerability Assessments, Network Architecture Reviews, IT Audits, etc. She has a great understanding of the FFIEC guidelines and stays on top of changes in those guidelines. Bobbette helps clients understand the metrics of risk analysis as well as the business case for information security expenditures (and more importantly, the risk acceptance case for NOT making those expenditures).