

## **Building Business Resiliency**

Business owners and executive team members work diligently every day to increase sales and sales revenues, gaining and maintaining a competitive advantage, and keeping their client's more than satisfied. While the business is expanding and your client base is growing, an elusive operating metric awaits on the sidelines – business risk.

Business risk today is not what it was when our predecessors built and operated their businesses. The business owner of today is bombarded with new and emerging technologies that promise to help promote new sales, produce new income, and streamline operations. These technologies are designed to keep everyone connected anywhere at anytime regardless of location while maintaining a leg up on the competition. Integrating new technologies is important to maintaining a competitive advantage and keeping operational processes in alignment with client expectations. Unknown to the business owner and/or executive is the level and type of risk inherent with keeping operations up to business challenges. To effectively and efficiently manage business risk, an operational and measureable contingency plan must be developed and integrated into the day-to-day operations of the business.

But where do I start and how do I know if my contingency planning work effort is successful?

### **The First Step - Executive Leadership**

An end-to-end business contingency planning program is made up of the following components:

1. Business Impact Analysis & Assessment (“BIA”)
2. Disaster Recovery Plan (“DRP”)
3. Business Continuity Plan (“BCP”)
4. Exercises & Maintenance

To own and operate an effective program the entire enterprise must have executive level leadership. It's expected the company leadership team or person will lead in the overall integration and implementation of key contingency planning deliverables. Examples of executive level deliverables are:

1. Ensures all departments have fundamental contingency planning knowledge with action plans that support the on-going viability of the business.
2. Contingency planning becomes part of the day-to-day operations of the business.
3. Qualifies and quantifies the on-going financial support for all contingency planning work effort.
4. Positions the contingency planning work effort as a strategic competitive advantage.

Once leadership has owned the initial contingency planning strategy, then technologies and business processes are analyzed and assessed to qualify and quantify business vulnerabilities and risks. This second step is known as performing a BIA.

## **Initial Analysis and Assessment**

Business continuity professionals know that a business can't support a disaster recovery or business continuity plan without first knowing the following:

1. Where do the vulnerabilities exist and why?
2. Where does the risk reside and why?
3. What are the financial and/or legal impacts to the business?
4. What are the vital, critical and less important data and processes?

Performing a BIA will answer these questions. The output data from a BIA is leveraged to gain insight into where and why vulnerabilities exist in the business. When the vulnerability is identified – via the BIA process, then a level or magnitude of risk can be assigned to the vulnerability. Usually, risk is measured by the amount of financial loss incurred due to the unavailability of company data and/or business processes. In the BIA work effort, a classification process is used to identify which data and/or business processes are the most vital, critical and less important to the business. One way to perform classification is to identify all the data and business processes that have immediate financial impact or legal liabilities. Then this information is analyzed to determine which data or business process needs to be available, in which order and in what time frame. This time frame is called the Recovery Time Objective (“RTO”). Think of the RTO as the time it takes to get a specific business process back on line, or a critical database working again.

Unknown for many business executives, the “desired” RTO of any given piece of data or business process is dictated by client expectations. Meaning, your client base has the expectation that your business will be able to provide products and/or services on a “business as usual” basis. The timeframe to meet your client’s expectations could be within seconds, minutes, hours, or days. After questions 1 thru 4 above are answered and the desired RTO’s have been identified, it’s time to analyze and assess your business technology’s ability to support the desired RTO’s as dictated by the customer.

## **Disaster Recovery Planning**

Think of a DRP as the technology intensive action plan that is managed and delivered by the Information Technology (“IT”) department. This department might be one or two people, or a larger number of people with varying skill sets. Regarding contingency planning, the intent of the IT department is to be able to re-build the information systems that support business operations within the desired RTO timeframes.

Given the complexity of most systems environments, coupled with the non-existence of an effective DRP, many technology teams focus their attention on the “expected” RTO.

The expected RTO is the time it takes the IT department to get a specific system(s) that supports a vital or critical business process or database working again. The expected RTO is dictated by multiple variables:

1. Knowledge of the technology team to fully implement a bare metal (worst case situation) recovery.
2. Ability of key technology vendors to deliver products within a timely manner.
3. Complexity of systems SW, HW, and firmware due to multi-application environments.
4. Level of business interruption preparedness by all employees.

The difference between the desired and expected RTO's is identified by performing a gap analysis as part of the BIA work effort. Once the gaps are identified, both business and technology teams plan ahead with making changes in the operating environment that ultimately support the client expectations.

## **Business Continuity Planning**

Think of a BCP as an action plan that supports all other aspects of operating and running a business. This particular plan usually resides outside the immediate realm of the technology department. Example components of a BCP are:

1. BCP Plan Policy
2. Media Policy
3. Recovery Organization
4. Insurance Requirements
5. Business Recovery Site
6. Notification and Reporting Procedures
7. "Offsite Box" Inventories

There are multiple business intentions with developing, integrating and maintaining a BCP. These business intentions are:

- Ensure the ongoing safety of all personnel. This includes full-time, part-time and contracted individuals
- Through continuous improvement, mitigate corporate, legal, and personal risks/liabilities
- Ensure the ongoing operational integrity of the company before, during, and after a business interruption event
- Show direct support of clients, key vendors, stakeholders, and employees
- Allows your company to have a continuous improvement roadmap in operations that's in alignment with strategic directives
- Ensure continued focus on core competencies

The nature of BCP work means that your company must fulfill the "interim" expectations of clients while simultaneously ensuring the safety and well-being of all employees.

Every BCP is an integral component of operations. Continuity planning is primarily focused on operational integrity and availability on an interim basis. During a defined time after a business interruption event your company will be operating in a less than optimal mode. This is only acceptable for a short time and all work effort focuses on bringing operations back to 100% capacity as soon as possible.

Your enterprise is unique and the requirements for successful implementation of a BCP differ from other enterprises. The scope of the work effort is determined by the overall size of the enterprise, the quantity of technology assets, the number of departments at your facility, and deliverables required by your clients.

## **Exercises and Maintenance**

Post the BIA, DRP, and BCP work effort, it is imperative that your action plans be exercised to validate operating functions and processes, and identify any shortcomings. The objective of developing and performing an exercise is to identify and then mitigate the business process and technology exposures inherent to the operating environment.

Exercising the DRP and/or BCP is not based on pass/fail scenarios and is not a finger pointing opportunity. The purpose is to identify where vulnerabilities and risks reside, then put a continuous improvement “maintenance” program in place to mitigate them. Performing a desktop and/or business recovery dry run” against the new or revised action plan consists of identifying the exercise strategy across differing environments. Exercise strategies tailored to the needs and environment of your enterprise are selected, and an ongoing exercise program is established. Without validation, all the work effort, time and money spent with building a resilient enterprise is wasted. Also, it’s imperative to plan for future exercises and maintenance through fiscal preparedness. The action plans that constitute contingency planning are considered as “live” documents. As your technology or operating environment changes so does your action plans. Therefore, it’s necessary to develop a maintenance program that includes scheduled and un-scheduled documentation updates.

Contingency planning is successful when the executive team can prove to themselves, their clients, key vendors, and stakeholders that they can reconstitute business operations within the desired RTO prior, during and post a business interruption event. When this is achieved, every business enterprise should market and sell their contingency planning program as a key differentiator against their competition.

James M. Myers is President & CEO of Contingency Now Inc. A professional risk management company with a corporate office in Los Angeles, CA. Mr. Myers can be reached at 818-510-4939 or on the web at [www.contingencynow.com](http://www.contingencynow.com).