Executive Guide to Business Continuity Management

What every C-level executive should know to effectively manage business continuity risk.

Business Continuity ("BC") programs are becoming increasingly important as every organization seeks to manage risk that could result from natural, man-made, geo-political, and public health catastrophes. Business continuity strikes at the heart of the fiscal and fiduciary responsibilities of the executive team. Strong arguments can be made that a solid BC management program can more than pay for itself in fiscal benefits while simultaneously minimizing the probability, impact and duration of a disruption. This white paper provides the guidance that every C-Level executive should have to ensure that their BC Programs are aligned with their business needs and objectives.

Executive Guide to Business Continuity Management

What every C-level executive should know to effectively manage business continuity risk.

Business Continuity Defined

Business Continuity ("BC") can be concisely defined as the business process that prepares us to keep our products and services, and therefore our revenue flowing under extreme adverse circumstances.

A typical business continuity program should consider, at a minimum, four primary disruption scenarios including:

1) **Disruption of IT Services** – any disruption affecting access to IT Services. Too often referred to as "IT Disaster Recovery".
2) **Workplace Disruption** – any disruption of a business entity (offices, call centers, trading rooms, manufacturing plants, labs, warehouses etc.).
3) **Workforce Disruption** – any disruption involving personnel such that sufficient, trained and skilled personnel are not available. Possible causes may include labor actions, pandemic, and regional disasters where the community or public infrastructure is severely impacted causing severe absenteeism.
4) **Supply Disruption** – any external supplier, service provider, utility or logistics disruption that stops or slows the movement of critical products and/or services.

"Business is the art and science of managing risk for profit!"

BCM Focus

Business Continuity Programs should focus on four primary types of disruptions:

- Workplace Disruption
- Workforce Disruption
- Supply Disruption
- IT Disruption

Risks and potential impacts should be identified and quantified in terms of:

- Operational Impact
- Reputational Impact
- Financial Impact
- Compliance Impact

Why every C-level Executive Should Care About Business Continuity

Business is the art and science of managing risk for profit! Risk management is a core competency of every C-level executive manifested in the tactical and strategic decisions we make every day. There are many forms of risk management that all contribute to executive accountability on both fiscal and fiduciary matters. Simply looking at risk management, and business continuity in particular as a discretionary expense can hurt your business in more ways than you might think. Too many executives think of risk management as purely a defensive concept when very often it is a fundamental component of nearly every strategic decision. Business relationships are built on trust. An organization must manage risk effectively to be trustworthy.

As a fiduciary of your firm, shouldn't you be aware of any risk that could produce a catastrophic impact to the firm? Shouldn't you be concerned that such risks are managed to the "reasonable and prudent" standard? Are you concerned that an external entity such as a critical service provider or supplier could derail your business plan? Should you be surprised that your clients may look at your company as a risk and may take some or all of their business somewhere else to mitigate that risk? If not, you should be!

In the wake of a seemingly endless stream of natural disasters including hurricanes, tsunamis, tornadoes, earthquakes, and wildfires, not to mention acts of terror, there is little argument that continuity risks are real and the results can be catastrophic. It would be hard for an executive team to use the defense that they had no way of knowing that something could happen when literally hundreds of events occur annually around the globe. From a defensive fiduciary perspective, every company has to at least understand and monitor continuity risks, even if they ultimately decide not to take actions to mitigate and manage them.

The fiscal drivers also provide a compelling Return on Investment story. Generally accepted industry practices call for scrutiny of operational risk management practices. Companies are increasingly reluctant to place their business with a few or just one supplier, especially if that supplier doesn't have a solid contingency plan to ensure the flow of products and services. As a result, a comprehensive and tested business continuity program may now be the difference between gaining and losing business AND access to the Capital Markets as customers and lenders consider business continuity plans as indicators of your firm's viability.

ROI from continuity risk management programs is derived more from retaining and obtaining clients than it is from loss avoidance.

Would you bet your business on a company that had reckless disregard for continuity risk? Not likely. Your procurement team is undoubtedly already vetting suppliers, especially sole and substantial sources. Putting pressure on the supply chain to eliminate single points of failure can reduce risk significantly with minimal relative cost and effort. Virtually every large organization vets suppliers based on security, business continuity and financial risks before entrusting significant business to them. Many companies are re-evaluating long term suppliers and shifting business to other firms, eroding the value of business relationships that have developed over many years. It should not surprise anyone that the supply chain is rife with risk given decades of programs aimed at driving efficiency through consolidation. At the same time, lenders are becoming increasingly aware of

continuity risk and its potential effects on an organization's ability to service its debt. In this regard, business continuity becomes more relevant as a firm's readiness may determine in part its ability to compete day to day.

Many executives remain apathetic about business continuity often only casually considering the tactical and strategic importance. "Not me!" and "Why me?" These reflexive behaviors suggest that we won't care until we have to and then, somehow, it won't be our fault! However when the need for business continuity moves into the critical path of efficient and effective day to day operations, loss of a key account can provide a compelling wake up call. Addressing business continuity on your own terms, before someone puts a gun to your head provides cost savings and strategic value. On the other hand, knee jerk reactions to business continuity can be expensive. It is better not to put all of your eggs in one basket in the first place because it can be disruptive to diversify suppliers and financially and operationally devastating to replicate an internal business operation like a plant, warehouse, call center or datacenter purely for risk management purposes. This is especially troublesome when you consider that addressing internal risks may require you to give back most, if not all of the savings accrued when you "consolidated" and "streamlined" operations to drive efficiency. Unfortunately, the dark side of many efficiency improvements is risk, which regrettably, is often not factored into the equation until it's too late. None of this absolves executives of their fiduciary responsibility to protect the business, its asset value and its brand.

Strategic advantage can and should be derived from your business continuity program investment. Who can you trust? Can you be trusted?

Could it be that in the pursuit of efficiency gains to make us more competitive, we have created unacceptable operating risks that may cause us to lose the very customers and opportunities we sought to win? Absolutely! You're demanding more resilience in your supply chain, and your clients expect (or soon will expect) the same. Addressing business continuity after strategic decisions are made subjects the firm to unnecessary cost and risk.

Our suppliers should expect to answer to our standards. And we should expect to answer to our customer's standards. We are at once, the hunter and the hunted! The business continuity discussion (and security, privacy etc.) becomes a much higher priority when it sits in the critical path of retaining and obtaining clients. What representations does your company make in the sales and contracting process? Can you live up to them? Few executives know what representations are being made on their behalf and fewer still can actually live up to them. The resulting liability is a serious exposure to many firms.

The truth is that virtually every organization is placing increasing emphasis on managing continuity risks in their supply chain. There is no place to hide. Your brand, your reputation, and now winning and losing deals relies on having a firm grip on your own operational risks and a program to actively manage them. If you are not demanding that your suppliers carry the right levels of insurance coverage, deploy state of the art security measures, and have rational continuity plans in place, you are in a shrinking minority.

No longer is the ROI for business continuity dependent on surviving a crisis. Now the ROI is more immediate and predictable, embodied in the retention of existing accounts and revenue and securing new business, and possibly access to and cost of capital and insurance.

Continuity Risk Management

Continuity risk management extends basic risk management principles to include not only loss prevention and compensation, but also protection of the very essence of every firm, its business operations. The impact of operational disruption grows geometrically over time and can reach extraordinary levels. There are practical limits to the amount of insurance coverage that can be justified or even purchased at any price. Therefore, businesses need to plan for alternative methods for operating the business to manage potential losses within reasonable limits. Businesses are complex highly engineered ecosystems. Replacing critical pieces in short periods of time is unrealistic without careful consideration and planning. In the absence of pre-planning or inherent redundancies, business outages affecting clients and revenue could last months, if not a year or more. Few brands can be "off shelf" for months without dramatically impacting equity value and damaging long term relationships. And no insurance coverage can adequately compensate for the catastrophic impact to a major brand and the associated asset value caused by a protracted business interruption.

The thrust of BC programs and plans therefore is to prepare such that the response is faster, more effective and efficient and less error prone resulting in shorter operational disruptions, less customer impact, and acceptable levels of financial impact. In this regard, BC Program Managers think more about restoring operations than about filing claims to cover losses. Laser focus on restoring operations or avoiding disruptions altogether is the domain of the BC professional. The operational nature of business continuity complicates matters beyond simply buying insurance and filing a claim to cover losses. But the same principles apply when deciding where to invest and how much.

Continuity risk management and traditional risk management both require a balance between fiduciary responsibilities and fiscal realities. An effective business continuity program can not only reduce losses, but also may pay dividends through reduced insurance premiums. Conversely, a flawed business continuity program can produce outsized losses that overwhelm even the most substantial insurance programs, and certainly any that would make fiscal sense.

The synergies and differences between traditional risk managers and continuity managers can be seen in the context of their roles, focus and point of reference when something happens. The table below shows the focus of the Risk Manager, Location Manager and Continuity Manager at time of a crisis. All roles are complementary and necessary. All serve to reduce risk and impact though with decidedly different focus and execution.

Situation	Risk Manager Focus	Location Manager	Continuity Manager Focus
A serious fire occurs at a company location requiring evacuation.	Property Loss	Evacuation	Process disruption
	Injuries	First Responders	Surviving operations
	Business Interruption Losses	Triage	Operational alternatives
	Liability	Loss control	Mobilization of resources
	Claims	Salvage	Logistics adjustments
	Financial impact	Restoration	Operational Impact

On a day to day basis, there is a similar alignment. The risk manager is focused on things like property protection, safety and loss avoidance while the continuity manager is focused on preparing for an inevitable

disruption of unknown origin with the express purpose of reducing the resulting disruption to operations and resulting financial, compliance and reputational impacts.

In the wake of a catastrophic event, some operational impact is to be expected. This can be viewed as the operational disruption "deductible" wherein some amount of impact is rationalized. Though there may be some near term collateral damage, a crisp, effective and efficient recovery will bring customers back if adversity has been handled responsibly. History has shown however, that outages that last weeks or months destroy brand and shareholder value, cause catastrophic fiscal losses and threaten the viability of the firm. By definition, losses on this scale are uninsurable using traditional insurance products. They must be dealt with through careful preparation, planning and execution of the business continuity program.

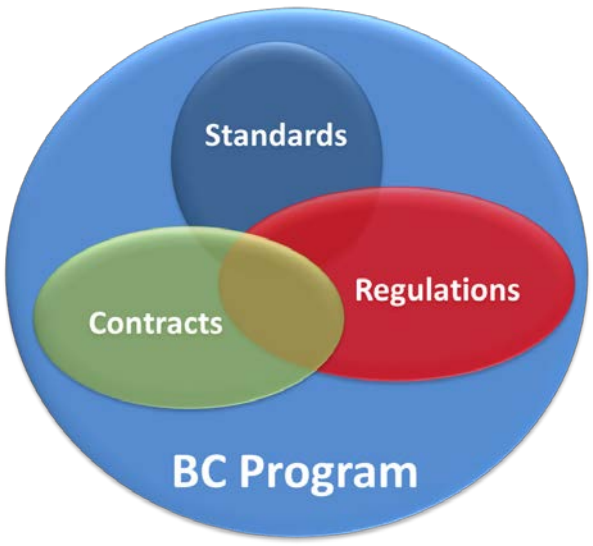
Business continuity derives much of its DNA from traditional risk management. But it is dangerous to assume they are one and the same. Firms that make this mistake view the BC program as a project that results in a plan that sits on a shelf. The viability of that plan decays every day as the business evolves away from the basis used in creating the plan in the first place. Continuity risk management is a business process designed to enable the business to continue to function effectively regardless of circumstance, thereby limiting losses. To be successful, the continuity risk management program needs to have executive attention and support and needs to be closely aligned with business operations.

Regulatory, Standards, and Contract Compliance

As a general rule, it is always best to drive the business continuity program as a component of your commitment to consistently delivering high quality products and services to your valued customers. In reality, business continuity programs are often influenced by, if not completely driven by the need to comply with a Regulation, Standard, or Contractual commitment.

It is important to completely understand the commitments that an organization may have and the standards by which it will be measured. In this regard, your program should absolutely take them into account. However it is extremely important that executives not slip into a false sense of security simply because they see audit checkmarks next to a series of third party requirements. In most cases, compliance defines what others say you have to do, but rarely defines what you should do or what you really need to do to protect your company. In fact, a "compliant" company can be a long way from resilient.

When building a continuity program, requirements should not only reflect what is needed to comply with regulations, standards and contracts, but also what is needed to actually manage the likelihood and impacts within reasonable thresholds. The BC Program Venn diagram depicts the overlapping relationship of various business drivers as components of a much bigger program agenda designed to ensure continuity of operations under adverse circumstances.



The key point here is that contractual commitments, Standards and Regulations all provide input to the BC Program but fall well short of fully defining its scope and purpose.

Building the Business Continuity Program

Building an effective, efficient, and economical business continuity program is not rocket science, especially when C-level executives drive the program using sound business and risk management decision-making skills. The key is to embrace business continuity as a business process, not unlike quality management, training or safety and to understand, appreciate, and communicate the tactical and strategic value across the organization. In the sections that follow these proven business concepts are applied to business continuity management to help executives drive and support a successful BC program.

Step One: Define Program Charter and Policy

The program charter can and should be succinct and aligned with the business needs. As an example:

"*The business continuity program at ATAP, Inc. is focused on managing the risks and related business impacts that could accrue from a disruption to:*

- *IT Services,*
- *ATAP workplaces,*
- *ATAP workforce,*
- *ATAP supply chain,*

…such that ATAP can continue to meet its obligations.

The Charter and Policy set the tone with direction from the top. The result is always a more effective and efficient program.

Mitigation measures will be applied where needed to reduce ATAP's projected financial, operational and compliance impacts to within accepted tolerance levels. All risks and projected impacts will be monitored and managed on an ongoing basis and mitigation measures will be applied where a projected impact exceeds ATAP's tolerance thresholds. Mitigation measures will be reviewed, tested and updated periodically but no less than annually."

This charter sets the tone that while every risk will be monitored, not every risk will be mitigated. Implicit in this charter is the notion that some risks will be accepted and therefore some impacts are to be expected under extreme circumstances. There will simply not be enough money to protect against every risk nor would that be considered prudent…which sets up the next logical step.

Step Two: Risk and Impact Management

Risk and Impact Management is a refined top-down approach as compared to more traditional and cumbersome "bottom's up" Business Impact Assessment (BIA) approaches. The Risk and Impact Management process is critically important when setting priorities for allocation of limited resources and funds. It should be an ongoing business process, albeit one that is performed with a minimum of effort and impact on core operational priorities. To be effective this process must be…

- Data driven so that objective analysis can follow and feed the decision-making process,
- Validated and debated to arrive at a single truth reflective of the values of the firm,
- Supported by automation that reminds stakeholders to review and update risks, and exercise plans,
- Simple and efficient so that business users can contribute and get back to their primary jobs with a minimum effort and little to no special training.

Many organizations report that the risk and impact management is the most challenging and time consuming aspect of the program. This is the result of flawed approaches and bottoms-up thinking. In fact, this process can and should require a minimum of resources if properly conceived and executed. Remember that there will be limited budgets and therefore some risks will have to be accepted so that funds and resources can be applied where they will yield the greatest benefit. That being the case, it only makes sense to drive the process from the top down, zeroing in on the most compelling risks, and not wasting precious time and resource on risks that will ultimately have to be accepted.

The trick to streamlining this process is to focus on "risk intersections" in and around the organization. This may be easier to do than one might think. High potential risk intersection targets can be found where all or most of a critical process is subject to the same potential event. They are amplified when they occur where significant vulnerabilities may be present. Risk intersections are present within the organization or in the supply chain. For example, at a datacenter, call center or factory, or sole source supplier. Any of these located in a hurricane zone or on a fault line would certainly warrant more attention. A critical business process with a single point of failure or the majority of its function dependent on one risk intersection is easily identified and should take priority over obviously less critical ones. In other words, where do you have all or too many of your eggs in one basket?

With a little effort, executives can substantially streamline the Risk and Impact Management process. Senior leadership support and direction makes a project more focused and relevant. This paves the way for an efficient first pass which can followed by deeper inspection and action into those risk intersections that are most concerning. By commissioning the effort top down, the executive team can:

1. Define risk tolerance so only substantial targets are evaluated and time and resource is not wasted on risks that don't meet certain business thresholds.
2. Define parameters for assessing risks in terms of operational, financial, compliance, customer service and reputational impacts.
3. Define terms as they will be used in the decision making process. For example the choice of the word "catastrophic" can mean different things to different people. A firm needs to agree on a definition that can be defended and debated. Impact levels might be defined as follows:
    a. Minimal: an impact contained at the department or location level.
    b. Material: an impact that would be visible at corporate levels but can be managed locally.
    c. Significant: an impact that would require corporate management intervention and resources.
    d. Catastrophic: an impact, visible in the public domain, managed at corporate, and possibly affecting the stability of the firm tactically and strategically.

Definitions like these drive crisp responses and meaningful metrics. The supporting commentary provides invaluable insight into the true nature of a particular risk and impact.

The key point here is that the process should begin with direction from the executive team inclusive of a clear understanding of the data and information that is needed to support the decision making process. This needn't take more than a couple hours of executive committee time but can save hundreds and even thousands of hours later on!

Lastly, once the first pass of data has been collected and consensus has been reached, there is no reason to execute the entire process over again every year. On the contrary, risk profiles should be reviewed periodically and updated as business conditions warrant. This can and should be simple and straightforward. If no material change has occurred, then the profile remains stable. If major changes have occurred, a revision or review is warranted. In all cases, the existing data serves as a relevant base from which to work and avoids the pitfall of re-hashing issues that have previously been debated and resolved.

Step Three: Risk Disposition and Strategy Development

Vulnerabilities and threats are endless but the funds to address them are not. This practical reality will govern what risks will have to be accepted, which will be addressed, and to what extent they will be mitigated. As a result, Risk Disposition and Strategy Development are inexorably linked.

Vulnerabilities and threats are endless. The funds to address them are not! Programs that lack executive sponsorship invariably waste resources, time and funds.

The decision framework for risk disposition for Business Continuity risks is similar to that for other risks. High impact, high probability risks will jump to the front of the line over those with lesser inherent risk, notwithstanding obvious cost considerations.

Grass roots business continuity programs typically operate tactically and with a narrow focus, taking steps to address each risk as it becomes known. A serial “Identify >>>Mitigate>>>Identify>>>Mitigate” process is common when business continuity is driven from the bottom of an organization. The result are programs that spend too much on risks that are identified early, leaving potentially larger risks lurking in the shadows and no money, time or resources to address them. Examples include perfecting IT recovery, at great expense and not focusing at all on business operations like manufacturing, logistics, call centers and your supply chain.

By definition, strategy is significantly influenced by facts and assumptions. The more complete the picture the more likely the strategy will work as planned. Grass roots programs are serial and limited in scope. They deny the organization the opportunity to align its business continuity strategy with its business strategy which sets the BC Program up to underperform. Having visibility into the big picture, even if information is limited, can help the organization chart a course that will minimize waste and rework, and ensure that serious gaps are not left unprotected.

BC Strategies must be aligned with an organization’s business Charter and Policy and set direction for the scale and scope of investment that the organization is willing to commit in exchange for mitigation of risk related to losses that may be incurred from a catastrophic event or a loss of a customer or opportunity.

It is important that the BC Strategy factor into other business strategies. For example, there is no sense in embarking on a program to consolidate operations to drive efficiency if it will result in an unacceptable risk when complete. Similarly, it makes no sense to market to a certain target customer base if your strategies and the program that results will not pass their vendor assessment scrutiny. Lastly, product and service pricing needs to factor continuity cost and risk to ensure that you don’t end up with contracts that will never be profitable.

Step Four: Implementation and Planning

Implementation and planning involves establishment of controls and other measures to reduce the likelihood, impact, and/or duration of outage, the planning to ensure that precious time is not wasted, and that costly mistakes are avoided.

Implementation of controls and corrective actions can take time and often involves significant capital and operating investments. These might include implementing property protection solutions, qualifying an alternate supplier, splitting production between two sites, implementing a backup call center or datacenter, or subscribing to alternate workplaces. One of the most effective and economical control strategies is building business continuity plans.

Business continuity plans provide executive and line management with the benefit of forethought and access to information that is critical to making the right decisions quickly at time of disaster. They ensure an organization's response is driven by timely and accurate information so that costly surprises and delays are minimized. Importantly, effective business continuity planning nearly always results in process improvement and efficiencies in every day operations offering yet another tactical benefit.

Business continuity plans need to have three essential elements:

- **Information** – bad decisions get made with bad data. A business continuity plan has to provide access to crisp data in context to enable executives to make good decisions, fast. In our experience with over 1,000 events, it is the quality of information that defines the outcome more than anything else. Things never play out exactly as planned and the ability to call an audible on the line is critical to success. A plan can dramatically reduce outage duration by streamlining response, even if ideal contingency resources and assets may not be available or justifiable.
- **Strategy & Approach** – the approach embodies not only how an organization views a situation, but also how it will react, respond, mobilize and communicate. The approach should include clear definition of Teams, Rosters and Resources along with a strategy for engaging and communicating with stakeholders in support of the chosen strategy.
- **Procedures** – procedures provide prescriptive guidance focused on what and how things should be done inclusive of consideration of priority and sequence. Actions that need to be done right, and quickly, need to be documented, communicated and rehearsed. Evacuation is a great example but there are others. In addition to alternative means of operating, plans should include procedures for evaluating a situation, plan activation, mobilization and communications. Procedural sections of the plans don't need to be protracted tomes. They can be concise and simple like forms and checklists. But they need to be crisp. And they need to be exercised, refined and evaluated.

Overall, the plan must provide the information and guidance to enable an organization to execute effectively under adverse, unpredictable circumstances.

Step Five: Exercise and Evaluation

Business continuity plans move from theory to reality in the exercise and evaluation process. Exercises can serve multiple purposes including training participants to work effectively in unusual situations and identifying flaws and areas for improvement before your business depends on them. A third function is to identify areas for process improvement that often surface when discussing continuity plans.

Exercises take plans which are built based on an impact to Entities and/or Processes and subjects them to scenarios that challenge the plans and the teams that execute them to respond effectively and efficiently. Some scenarios provide little to no warning like a terrorist attack, tornado or earthquake. Other scenarios provide advance warning of hours and sometimes days like storms and wildfires. The key is to challenge your plan with multiple scenarios being sure to include at least one where the breadth of impact is substantial, yet there is some time to shore things up based on the potential impact of an impending event. This model is commonplace in the southern United States where Hurricane Season provides an annual reminder of the havoc that Mother Nature can impart on business operations.

Advance warning can make a big difference if you use the time wisely. This is the equivalent of "bracing" the organization to take the hit so it can continue to function effectively, possibly avoiding some or all of the impact. A healthy practice is to use a hypothetical exercise scenario with several days advance warning at least annually as a call to action to draw attention to the importance of legitimate recovery capability. Companies that prepared well fared much better in the aftermath of Super-Storm Sandy than those who had never drilled under a complex and comprehensive scenario.

Realistically, few potential catastrophic impact scenarios provide any meaningful notice. This can leave companies that don't conduct business continuity exercises with stale plans in the hands of untrained teams.

Planning can vastly improve the situation but the viability of the plan and the readiness of the teams to execute it cannot be known without exercising and evaluating it. Exercises are invaluable opportunities for executives to see how well their employees understand the business and how well they operate under pressure. It serves the additional purpose of identifying weaknesses in the contingency plan and providing team building and leadership opportunities that will pay dividends for the day to day business and at time of crisis.

Executives should not only support these exercises, but also make a point to participate. Adverse events put the executive team to the test more than anyone. Employees, Customers, Suppliers, Investors and often the general public look critically at how executives handle difficult situations. Exercises provide executives with the context, training and feedback to ensure that they lead effectively and stay on point when communicating with constituents. Leadership performance at time of crisis can make or break careers and companies.

Step Six: Governance, Management, and Continuous Improvement

Your business changes daily. Your plans need to evolve with your business. Ongoing program management not only keeps the program current while addressing areas for improvement, but also provides a thoughtful look at every day business processes and practices.

Governance models define the cadence for updating critical program information like Process, Site, Vendor, Team, Contact and Plan Procedure content. The program should be aligned with the shelf life of various forms of information. For example, Site data can usually be effectively maintained on a semi-annual or annual basis, while Contact and Team data should be updated monthly, if not more often.

The ongoing plan review and test sequence should be tightly coupled with post-mortems and plan updates so that key learning can find its way into the strategies and plans.

The half-life of traditional business continuity plan is about 90 days which stands in stark contrast to annual or even less frequent reviews, updates and exercises. More precise governance models improve quality, currency and efficiency.

Governance, Management and Continuous Improvement applies not only to maintaining plans but also to managing risk. Earlier in Step 2, we discussed the concepts of Risk and Impact Management, a process designed to replace the cumbersome and error prone Business Impact Analysis (BIA) process. The concept is simple: create risk and impact profiles in the first pass, and continually improve them over time as part of periodic business review process. This subtle adjustment saves substantial amounts of time, provides more timely and accurate information and ensures that you have the best possible information available when you need it most, at time of crisis. To be clear, we are advocating a business process to manage the currency of important information on a cadence reflective of that data's life expectancy by the people who are closest to that information. Trying to make everyone a Business Continuity expert is expensive and never works. But enabling business users to contribute what they know, and holding them accountable to do so can drive efficiency and improve effectiveness.

Effective use of current technology can substantially reduce the need for large teams focused on business continuity making it easier for business users to contribute their pieces of the puzzle. Having people wade through a 50 page document does not inspire excellence. Giving them a link to review a specific section of a plan where they can make a quick change and get back to doing their jobs keeps people in touch with the BC Management process while providing a more realistic user experience. The result is a program that is more current and less costly to build and manage. Engaging them in a process that enables them to easily contribute what they know is more effective and efficient.

Governance, Management and Continuous Improvement can be effective and efficient if implemented thoughtfully.

Conclusion

Continuity Risk Management and Business Continuity Planning are functions that fill important gaps in the risk management models of most companies. Organizations survive by being competitive. They improve their ability to compete by becoming more efficient. Efficiency generally involves consolidation at the physical level or the process level. The dark side of efficiency improvements is often increased risk.

Business Continuity is about being able to continue to deliver products and services, drive revenue and protect your brand. At its core it is all about Trust.

While consolidating your business with a single supplier may yield savings, it is often at the expense of substantially increased risk. The same is true for consolidating business processes into a single location. Not only does consolidation put all (or at least more of) your eggs in one basket, it also raises the potential business impact while limiting recovery options and flexibility in the event something goes wrong.

Continuity risks are characterized by relatively low likelihoods coupled with potentially devastating consequences. Clear and thoughtful consideration should be given to anything that could cause a thriving organization to fail. More immediately, and almost certainly, every organization will need to improve its BC capabilities in order to remain competitive as every organization seeks to reduce its risk through aggressive supplier management practices.

Are you prepared? Are your suppliers prepared? Do your customers expect you to be ready? Could casual management of continuity risk cost you a customer even if disaster doesn't strike your business directly? Could a weak or flawed business continuity program impact your creditworthiness or insurability?

Business Continuity is about being able to continue to deliver products and services, drive revenue and protect your brand. At its core it is all about Trust. Just as having adequate insurance coverage is a requirement for all B2B businesses, you can expect to see increasing scrutiny of your security and business continuity programs, if you have not already. At the same time, some of your greatest risks lie in your supply chain. You should be taking action to make sure that a key supplier doesn't cause you to fail. And make sure that you are not the reason that others fail. Nothing good can come from either scenario.

Finally, embrace the notion that business continuity is not only your job but also that of everyone who counts on your company for their paycheck. Your company, your career, your reputation and your market success may depend on your having a viable business continuity program in place, even if you never take a direct hit!

Do unto others as you would have them do unto you. Be prepared!

About Fusion Risk Management, Inc.

Fusion is a growth stage Software as a Service (SaaS) and Advisory Consulting firm headquartered in the Chicago area. Fusion was founded by recognized industry leaders and is committed to bringing game changing solutions to the Continuity Risk Management industry. Fusion is proud to have won the Business Continuity Institute Award for Innovation in both 2012 and 2013, and the Initiative of the Year award in 2012 for a Global Risk Assessment at a Fortune 100 Enterprise. For more information on Fusion, check us out on LinkedIn or on our website www.fusionrm.com.

About the Author

David Nolan is CEO and Founder of Fusion Risk Management, Inc. David has more than 25 years of experience helping organizations manage continuity risk and delivering operational continuity under the most adverse circumstances. David's career includes executive positions in both public and private companies ranging in size from the mid-market to the Fortune 500 including IBM, Comdisco, and Forsythe Solutions. He is a frequent speaker and contributor in industry forums and conferences.

David Nolan, Founder & CEO

Fusion Risk Management, Inc.

dnolan@fusionrm.com

847-632-1002 x501

@FRMDave