FUSION
RISK MANAGEMENT

Tying It Together

Why You Should Take an Operational Approach to Risk Management

ROBERT SIBIK

Combining business continuity and risk management into a single operational process is the most effective way to prepare for the worst.

Many companies treat risk management and business continuity as different entities under the same workflows, and that is a mistake; to be optimally effective, the two must be combined and aligned.

Evolving Approaches

Business continuity traditionally starts with a business impact assessment, but many companies don't go beyond that, making no tactical plan or strategic decisions on how to reduce impact once they have identified what could go wrong. The risk management process has been more mature, identifying various ways to treat problems, assigning it to someone, and trying to reduce the likelihood of the event occurring, but not doing much to reduce the impact of the event.

Organizations must move beyond simplistic goals of creating a business continuity plan using legacy business continuity/disaster recovery tools, or demonstrating compliance to a standard or policy using legacy governance, risk management and compliance software tools. Those approaches incorrectly move the focus to, "do we have our plans done?" or create a checklist mentality of, "did we pass the audit?"

In addition to legacy approaches, benchmarking must be avoided, because it can provide misleading conclusions about acceptable risk and appropriate investment, and create a false sense of having a competitive advantage over others in the industry. Even companies in the same industry should have their own ideas about what constitutes risk, because risks are driven by business strategy, process, how they support customers, what they do, and how they do it.

Take the retail industry. Two organizations may sell the same basic product – clothing – but one sells luxury brands and the other sells value brands. The latter store's business processes and strategies will focus on discounts and sales as well as efficiencies in stocking and logistics. The former will focus on personalized service and in-store amenities for shoppers. These two stores may exist in the same industry and sell the same thing, but they have vastly different types of merchandise, prices and clientele, which means their shareholder value and business risks will look very different from each other.

Businesses need to understand levels of acceptable risk in their individual organization and map those risks to their business processes, measuring them based on how much the business is impacted if a process is disrupted. By determining what risks are acceptable, and what processes create a risk by being aligned too closely to an important strategy or resource, leadership can make rational decisions at the executive level on what extent they invest in resilience – based not on theory, but on reality.

Creating an Integrated Approach with the Bowtie Model

Using the bowtie model, organizations can appropriately marry business continuity and risk management practices.

The bowtie model – based on the preferred neckwear of high school science teachers and Winston Churchill – uses one half of the bow to represent the likelihood of risk events and the other half to represent mitigation measures. The middle – the knot – represents a disaster event, which may comprise disruptions like IT services going down, a warehouse fire, a workforce shortage or a supplier going out of business.

To use this model, first, determine every possible disruption to your organization through painstaking analysis of your businesses processes. Then determine the likelihood of each disruption (the left part of the bow), as well as mitigating measures one can take to reduce the impact of the disruption should it occur (the right part of the bowtie).

Consider as an example the disruptive event of a building fire – the "knot" in this case. How likely is it? Was the building built in the 1800s and made of flammable materials like wood, or is it newer steel construction? Are there other businesses in the same building that would create a higher risk of fire, such as a restaurant? Do employees who smoke appropriately dispose of cigarettes in the right receptacle?

On the other half of the bowtie are the measures that could reduce the impact of a building fire, such as ensuring water sources and fire extinguishers throughout the building, testing sprinkler systems, having an alternate workspace to move to if part or all of the office is damaged during a fire, and so on.

The mitigating measures are especially key here, as they aren't always captured in traditional insurance- and compliance-minded risk assessments. Understanding mitigation measures as well as the likelihood of risk events can change perspectives on how much risk an organization can take, because the organization then will understand what its business continuity and response capabilities are. Mitigation methods like being ready to move to an alternate workspace are more realistic than trying to prevent events entirely; at some point, you can accept the risk because you know how to address the impact.

A Winning Combination

Where risk management struggles is where business continuity can shine: understanding what creates shareholder value, what makes an organization unique in its industry among its competitors, and how it distinguishes itself. Alternately, risk management brings a new perspective to the idea of business continuity by focuses on types of disruptions, their likelihoods, and how to prevent them.

To create a panoramic view of where an organization can be harmed if something bad happens, businesses must merge the concepts of business resilience (dependencies, impacts, incident management, and recovery) and risk management (assessment, controls, and effectiveness) and optimize them.

Bringing the two views together and performing holistic dependency mapping of entire ecosystem allows an organization to treat both as a single operational process, bringing data together to create actionable info (based on the "information foundation" the company has created about impacts to business operations that can result from a wide variety of disruptions and risks) to empower decisive actions and positive results.

Using the bowtie method to create this holistic view, companies get the best of both worlds and ensure they understand the possibilities of various disruptions, are taking steps to mitigate the possibilities of disasters, and have prepared their responses to disasters should they strike. This approach to risk management will help keep a business up and running and ensure greater value for shareholders – this year and in years to come

To learn more about tying your business continuity and risk programs together, contact Fusion today.

Robert Sibik is Senior Vice President
at Fusion Risk Management
Robert can be reached at rsibik@fusionrm.com