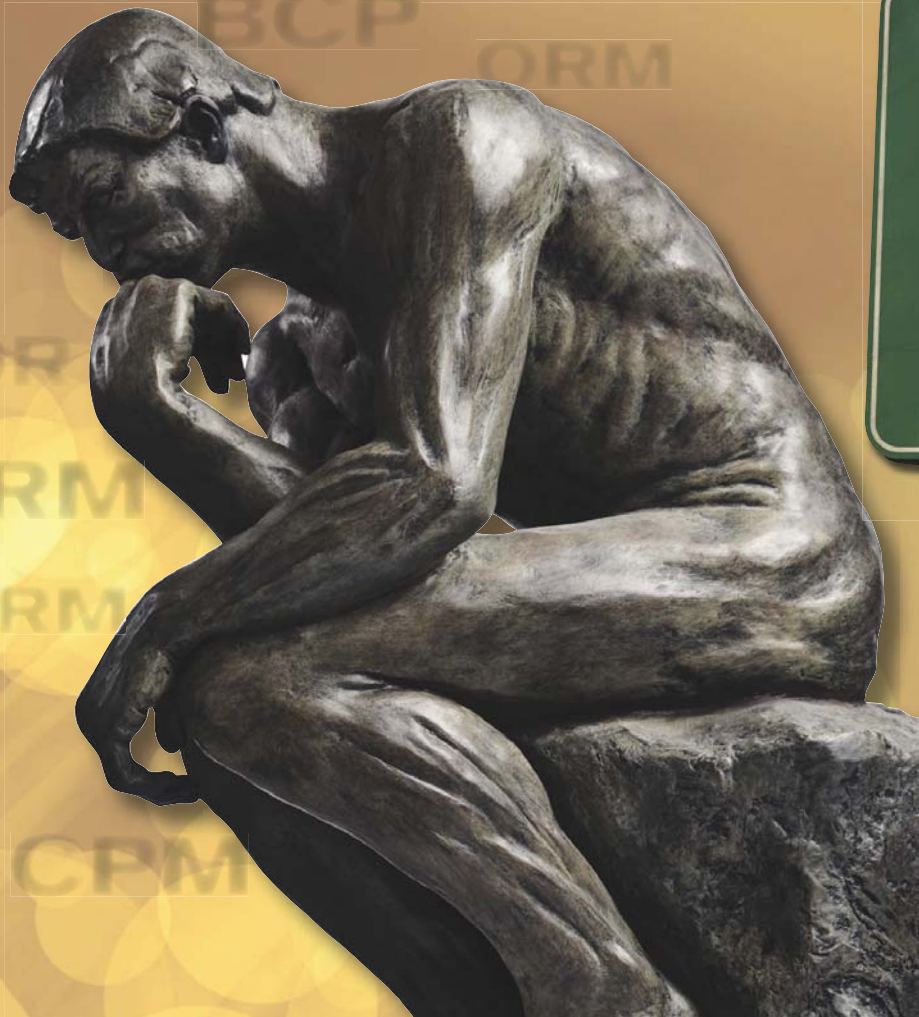


Continuity Insights



David Nolan explains the new approaches required to embrace continuity risk management, and how it can lead to a more resilient and agile enterprise.

ALSO INSIDE:

- PS-Prep Certification
- Critical Issues Survey
- CI Podcast 001: ISO 22301
- Audio: ERM
- Editor's Note: Hurricane Hype
- Emergency Response Tools

Continuity Risk Management: The New “Big Dog”

By David Nolan, CEO, Fusion Risk Management, Inc.

Every indication suggests that we have passed a major inflection point in the continuity industry.

Continuity risk management (CRM) has been the tail on the disaster recovery (DR)/business continuity planning (BCP) dog for the last three decades, having been narrowly defined to mean “business impact assessment” or “risk assessment,” and only engaged periodically for the purpose of making a business case to spend more money. But there are compelling signals that clearly indicate CRM is now front and center, and traditional continuity programs are falling in line as part of a bigger risk management agenda. This represents a profound shift and one that companies and practitioners can ill afford to deny or ignore.

Risk management is fundamental to the effectiveness, relevance and management of every continuity program. It is not to be confused with continuity program management (CPM). Risk management capitalizes on fundamental risk-based decision-making processes that already operate in most organizations.



Contrary to what some might think, executives are keenly aware of risks – they make risk management decisions every day. The emergence of enterprise risk management (ERM) has paved the way for continuity managers to participate in a more productive discussion related to risks that might impact business or IT operations. While ERM is more concept than reality in most large organizations, it sets in motion a vision state where a broad array of risks can be measured and prioritized, providing executives with the data needed to make difficult decisions about where to invest, and what level of risk to accept.

By contrast, CPM is focused on doing, coordinating and managing myriad activities related to building and testing plan capabilities. Program management tasks are more tactical, whereas risk management activities tend to be more strategic. Risk managers decide what to do. Program managers do what needs



David Nolan

to be done. This subtle but important distinction provides insight into the challenges practitioners and program managers have experienced in the past, and also the opportunities for the future.

Traditional DR/BCP programs are built “bottom up,” and are very often driven by and owned by IT. While it is true that the epicenter of operational risk is IT in most organizations, rarely can a continuity program be optimized when IT is tasked to run it. This is not a criticism of IT. On the contrary, IT has done a remarkable job in many cases, in spite of a lack of ownership from the business units.

Recurring themes at industry conferences have focused on topics such as “how to get management buy-in,” “getting your business units engaged in the testing process” and “making the case for advanced recovery solutions.” These are all symptoms of an industry trying to find its way rather than one driven by a unifying call to action.

Leading programs have embraced a risk-based approach for years, though even those programs are experiencing a paradigm shift. The concept of risk management implies a set of business processes

in which risk profiles are actively managed. While most organizations perform business impact and risk assessments, the objectives of those projects and the uses of the data are to support a business case and/or a budget cycle.

Successful risk-based programs are driven by risk tolerances that are understood and agreed upon at the highest levels of the organization. Risk tolerance thresholds serve to establish a standard for determining what risks are truly concerning versus those that might be very real but just not as important as others. It is critical that an organization correlate risk tolerances to key performance indicators (KPIs) so that impacts require no translation or extrapolation to make business sense.

The most common risk tolerance threshold metrics relate to financial losses or compliance. However, the most compelling metrics often relate to operational impacts. It's hard for a manufacturer to dismiss the business impact caused by the loss of a sole-source supplier or the loss of a factory that takes an entire product line off the market for months or more. Similarly, an insurance company can't survive if it can't process claims or underwrite new business. While direct financial impacts are concerning, such losses can usually be mitigated in whole or in part with insurance.

Operational impacts directly affect customers, and therefore relationships that may have taken decades to develop, and a brand that the organization has fought to build and defend. An organization that has lost its ability to function has lost its identity and everything of value that goes with it.

Risks that could cause catastrophic harm are admittedly rarer, but they do happen. Operational impacts tend to escalate geometrically – and quickly.

An outage that disables your ability to manufacture a product, support a client, or deliver a service can be merely inconvenient in the first few hours, though over a longer timeframe, that outage can strike at the core of client relationships: trust.

How much of a disruption will your customers

Mike McFarland, Manager, Enterprise Risk & Insurance at Great River Energy, has lived through the convergence of the operational and continuity risk management disciplines. For Great River Energy, it's all about making sure they are in compliance and in control of their operations.

“There are always risks in a distributed, complex business. The key is to tap the vast resources of an organization to identify, organize and measure those risks. To remain competitive, we always have to balance our fiscal and fiduciary responsibility and find new ways to make our limited funds go further.”

The risk management function at Great River Energy encompasses all aspects of operational risk management including BCP. With a comprehensive risk management program, the organization is well positioned to make investment decisions. “We’re careful to make sure we have a complete picture so that we can be certain that we invest prudently. We don’t like surprises,” says McFarland.

tolerate before they want compensation? How much time will they give you before they consider competitive alternatives? Departing customers amplify negativity in the market, often giving passionate justification for their departure, and encouraging others to avoid the same fate. Once customers begin to leave, the business unravels and the situation becomes increasingly unmanageable. Like a run on a bank, or customers departing a bankrupt company, operational failure can escalate into catastrophic failure more quickly than one might expect.

So what is your risk tolerance threshold? How much of a financial loss is acceptable? What level of compliance findings are simply noise? Exactly what length of an outage are you willing to sustain?

To answer these questions, an organization

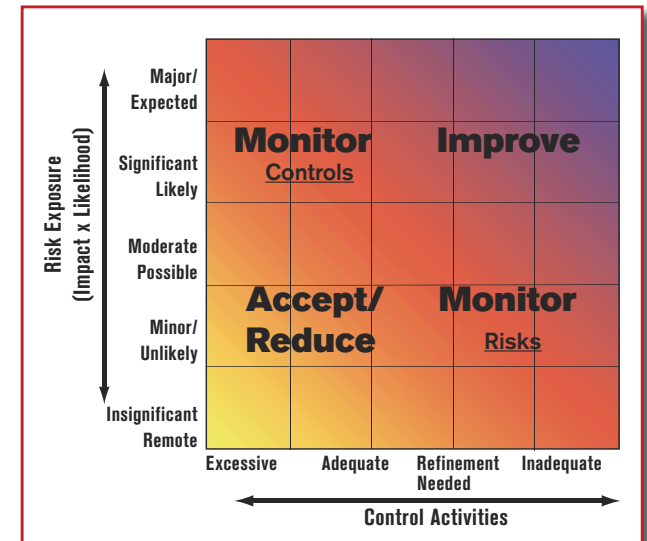


Figure 1: The risk/control matrix provides guidance for priorities based on impact, likelihood and control effectiveness.

ultimately has to factor in likelihood. Very high likelihood events that are merely annoying may be unacceptable. You can't run a business with natty issues recurring every week. On the other end of the spectrum, it's hard to turn a blind eye to risks that could literally destroy the firm – even though the likelihood is low. Instead of the traditional impact/likelihood matrix, consider a risk/control matrix, which provides context and guidance as it relates to answering the question of what risks to accept, what risks to address, and the extent to which they are accepted.

For recurring “nuisance” risks, an operational control should be applied so that it simply stops occurring with the same frequency. Virus detection is a good example of such a control. For mid-impact, mid-likelihood risks such as a power outage, generators provide a prudent solution to carry the operations through a failure.

High impact, lower likelihood incidents are more difficult to address and typically are aligned with large operational components that represent single points of failure. For example, how can you justify building a backup plant or a backup call center to address a risk that might be considered remote?

Risk management implies a structured, disciplined business process that seeks to identify, measure and organize all risks as a means of making sound business decisions. With a complete picture, executive management is in a position to make tough decisions to assign, avoid, mitigate or accept risks.

The case for ERM is built on the notion that risk management silos almost guarantee that an organization will spend more than they should on some risks, and not enough on others. Worse yet, an undisciplined process can leave an organization blind to

the mere existence of a risk that could cause serious harm.

Operational risk management (ORM) is a strategic business issue and the answers often lie in fundamental changes in the way an organization thinks about its business and the risks it takes. Prevailing incentives in most organizations reward “margin improvement.” Unfortunately, most margin improvement results in increased risk. If that risk exceeds a risk tolerance threshold, the margin improvement is often offset entirely by risk mitigation costs.

For example, consider the decision to consolidate a business function from four locations down to one. The impact of an operational failure quadrupled, and the challenges to rebuild have escalated as well. A more rational “risk adjusted” compromise would be to move from four to two. In addition to limiting downside to half of the original plan, the surviving site

provides a foundation for serving your most important customers, and for rebuilding lost capacity. The marginal cost on a risk adjusted basis may well make business sense when the potential for catastrophic impact is factored in.

“Instead of the traditional impact/likelihood matrix, consider a risk/control matrix ...”

We often hear complaints that executives don't care; that they don't understand the risks; that they have more important things to worry about; that they simply don't believe it could happen to them. While this may be true in some cases, another view suggests they don't understand risks as well as we'd like because we don't present and manage risks in a manner that is consistent with other and more well accepted risk management programs and practices currently in place.

Organizations actively manage a wide array of risks including, for example, commodity price fluctuation, labor unrest, sovereign risks, and physical and information security to name a few. There are many others. These programs include a clear communication of the risk on an ongoing basis. There is a cadence to updating risk profiles; in some cases in real-time or at least daily. There is clear accountability, full transparency and high levels of understanding. The actions to hedge these risks are clearly defined and purposeful. And the residual risk is measured and monitored as a matter of course. Insurance is a familiar risk management concept that reminds us of the linkage between the premiums we pay and the amount of coverage we receive, adjusted for the risk

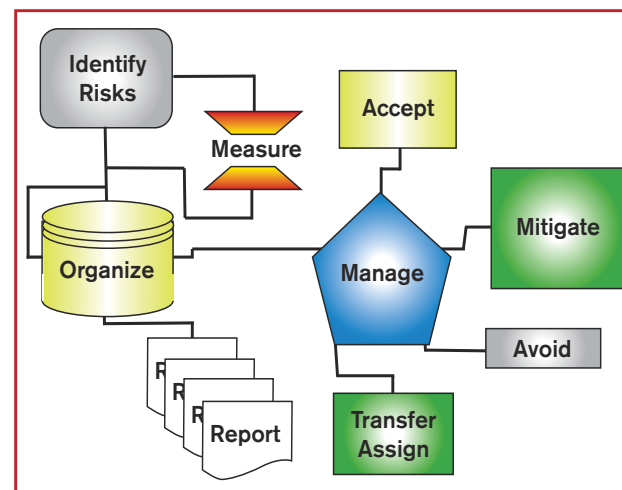


Figure 2: Risk management process flow aligns continuity risk management with proven and accepted risk management processes.

we accept, also known as the “deductible.” We need to be mindful of inherent risk, residual risk and the business value we are delivering for the premiums we seek. What is the “deductible” on your BCP program or on your IT DR program?

The truth is most people don't know. We think in terms of “recovery time objectives” and “recovery point objectives” and the capabilities we build and support. We present risks with claims of apocalyptic devastation if our initiatives don't get funded. We passionately defend our ability to recover when in reality our capability to do so may not be as good as we want it to be. The disconnect comes from the fact that very few organizations understand exactly how much pain the organization can handle. Risk is pain. Risk management, therefore, is pain management; neither a magic bullet, nor a cure.

Based on experience, we find that most organizations stand to absorb a considerable impact from the loss of a data center. But very few C-suite executives understand just how the business will be affected and how such an impact will propagate through the organization, into the supply chain and out to customers, even if their BC/DR plans work as desired.

Even worse, most organizations take a very narrow view of the operational risks that could result from a disruption of any one of many entities on which the organization is dependent. Could your company continue to ship product if a key sole source supplier were to fail? How long would it take you to recover from the loss of use of an important piece of public infrastructure like a port, border or rail line? Exactly how would you manage through the loss of headquarters, or a major call-center, plant or warehouse?

While each of these individually may seem like

Claudia Temple and Leslie Borders at Kraft Foods have spent the last several years driving the convergence of risk management and business continuity. Their program is evolving quickly as a result of the clear definition of risk tolerance.

“Kraft executive management set clear guidelines for risk tolerance. We are as concerned about controlling financial losses as we are about making sure that we continue to keep our product on store shelves,” says Temple.

Borders adds, “In an enterprise as vast as Kraft it is critical for us to identify the most significant risks and apply our resources to implement strategies and plans to manage those risks to within acceptable levels.”

The alignment with risk management has elevated visibility of the BCP agenda to the Board of Directors and has helped drive accountability throughout the enterprise.

remote possibilities, collectively they are not. In fact, the larger your organization, the more likely your operations are experiencing a disruption somewhere throughout the enterprise. And some of these scenarios could cause catastrophic harm to the business in terms of financial, operational, brand and regulatory/compliance impact, even though the likelihood is relatively small.

The time has come for continuity risk to align with

the broader risk management process and culture of the enterprise. In doing so, business realities will challenge our traditional notions of business continuity and disaster recovery.

Starting with the concept that “vulnerabilities and threats are endless, but the funds to address them are not,” it is not only possible, but probable, that an organization will have to accept more risk than the executive team is comfortable with because there simply isn't enough money to fully address every risk. With risk acceptance comes risk management, and risk-adjusted decision making that leads to a more resilient and agile enterprise.

David Nolan is CEO and founder of Fusion Risk Management, Inc., a provider of Advisory Consulting Services, and the Fusion Framework® Risk Management and Contingency Planning System. Mr. Nolan is a frequent contributor and innovator in the Continuity Services industry. He can be reached at dnolan@fusionrm.com. CI

