

The Inflection Point in Enterprise Risk Management is Underway

FUSION
RISK MANAGEMENT

Are you **leading**, **following**, or **struggling to get organized?**

If you're like most risk management and business resilience practitioners, the answer is some combination of all three.





Can You Get There From Here?

Initial approaches to governance, risk, and compliance have brought forth an ability for enterprise organizations to manage risk more proactively, yet much work remains to make this a truly productive and value-added set of initiatives. Risk registers, compliance checkmarks, and control effectiveness ratings have served to drive awareness of risk throughout the enterprise, resulting in more consistent risk management practices, and the recognition that over-controlling for some risks can be as much of a problem as under-controlling for others. Nonetheless, many organizations struggle to ensure that risks are addressed to appropriate levels both within the enterprise and among critical business partners. As enterprise organizations strive for higher levels of maturity in their risk management programs, more risk agendas are being established, more assessments are being conducted, more data is being generated, and more analysis is needed to make sense of it all.

In some respects, it seems the more you try to solve the problem, the harder it becomes.

Regulatory requirements, assessment methodologies, and industry best practices continue to expand and evolve. Tools and technologies continue to be acquired, configured, and reconfigured all in an effort to keep pace with the growing array of risks to be managed. Enterprise organizations continue to make significant investments, yet integrating disparate risk agendas into meaningful perspectives remains challenging. More generally, the concept of "risk tolerance" remains elusive for boards and executive management to embrace and leverage as a decision-making tool.

Many times, what gets lost is the idea that more risk management doesn't necessarily bring greater business resilience. Business resilience is concerned with maintaining business operations within acceptable tolerances, irrespective of which risks may be the source of disruption. Business resilience, by definition, focuses on business processes, their dependencies on assets and resources inside and outside of the enterprise, and the impacts from any type of disruption that may occur. Equally important is the idea that business resilience should strive to strike a balance between the investments required to withstand disruptive events vs. those needed to recover quickly within levels of impact deemed acceptable to the business.

The Point of Inflection

Intel founder Andy Grove originally defined a strategic inflection point as "an event that changes the way we think and act." While rapid inflections can occur, many times strategic inflections build more slowly over months or years, and reflect a collection of experiences, awareness, and new considerations that drive new solutions. Today, the inflection in enterprise risk management can be described as the need to operationalize risk management by making business resilience fundamental to the process of managing risk. Many organizations are now redefining their approach in order to bring these concepts of risk and resilience together under a single lens.

As one example, last summer the Bank of England in conjunction with the Financial Conduct Authority issued a discussion paper on operational resilience to the UK financial services industry highlighting this need. While the discussion paper is written from the perspective of financial services providers and financial market infrastructure, the considerations are applicable to every enterprise organization.

Key points include:

"The supervisory authorities envisage that boards and senior management should assume that individual systems and processes that support business services will be disrupted…"

"…it is not possible to prevent every risk materialising, and dependencies are often only identified once something has gone wrong."

"Setting impact tolerances which quantify the amount of disruption that could be tolerated in the event of an incident may be an efficient way for boards and senior management to set their own standards for operational resilience, prioritise and take investment decisions."

At Fusion, we share their view that risk management and business resilience must be brought together for a common perspective. Yet for most enterprise organizations, this can be daunting to consider. Looking across myriad departments, budgets, and agendas dedicated to managing risk, compliance, safety, crisis response, continuity, and recovery, on a potentially global scale, the key question becomes, "What is the right approach to accomplish this objective?" The underlying challenge is the need to establish a common "information foundation" organized to engage and support all of the constituencies concerned with these issues throughout the enterprise.

[1]Building the UK financial sector's operational resilience https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

How Does an **Information Foundation** Operationalize Risk Management?



An information foundation represents an integration of multiple sources of data used for understanding and assessing business processes, their dependencies on assets and resources inside and outside of the enterprise, the business impacts resulting from disruption, and the myriad risks and controls associated with each. As noted above, this can create an overwhelming amount of information without an organizing model to bring it all together, or the tools and technologies to enable, automate, and streamline an integrated risk and resilience program.

With the right approach and commitment, a continuously maintained information foundation provides a current and clear picture of your organization's risk profile, control effectiveness, tolerances for disruption, current levels of resilience, and capabilities to recover critical operations within defined timeframes. Executives and program leaders utilize the information foundation to prioritize risk in the context of business impact, define and allocate investment, maintain continuous compliance, develop contingencies, and ensure their people are ready to respond when disruption occurs.

As the Bank of England notes, "***senior management should assume… business services will be disrupted.***" This is a powerful statement that puts executives and boards of directors on notice.

Where We Go From Here

Beyond assessing and quantifying risks, control effectiveness, and compliance, risk management programs are becoming "operationalized" through a common information foundation that enables executive decisions about tolerances for disruption, and the capabilities needed for resilience, continuity, and recovery.

Doing so requires understanding business process dependencies in order to link risk with business impact, maintaining controls and resilience capabilities through effective program governance, and ensuring continuous alignment to changing business conditions so that any disruption to normal operations can be managed within acceptable tolerances and taken in stride. The goal is to ensure the enterprise can maintain its flow of products and services, protect its stakeholders, and retain the trust it has established in its marketplace.

Learn more at *fusionrm.com/integrated-risk-managment*

FUSION RISK MANAGEMENT

Andy Mercker

Vice President of Market Development

Over the past decade, Andy Mercker has helped drive change in the risk management industry through executive leadership roles at Fusion Risk Management.

