COMPLIANCE WEEK

Connected Management of Operational Risk Prevents Disruption

Many things can disrupt the business. The measure of this disruption is operational risk. Understanding the true scope, nature and impact of risk to operations is more possible than ever before. While the individual needs of different functions are often best supported by use of separate technologies, connecting them and the data they manage provides the holistic view of operational risk needed to support informed business decisions. In this illustration, we outline what connected management of operational risk looks like and how having it benefits the organization.

Compliance Week and OCEG have teamed up to provide readers with this regular illustrated series on governance, risk, and compliance programs. For information on this series, please go to www.complianceweek.com.

DEVELOPED BY OCEG®

WITH CONTRIBUTIONS FROM

The Financial and Risk business of Thomson Reuters is now Refinitiv.

REFINITIV™

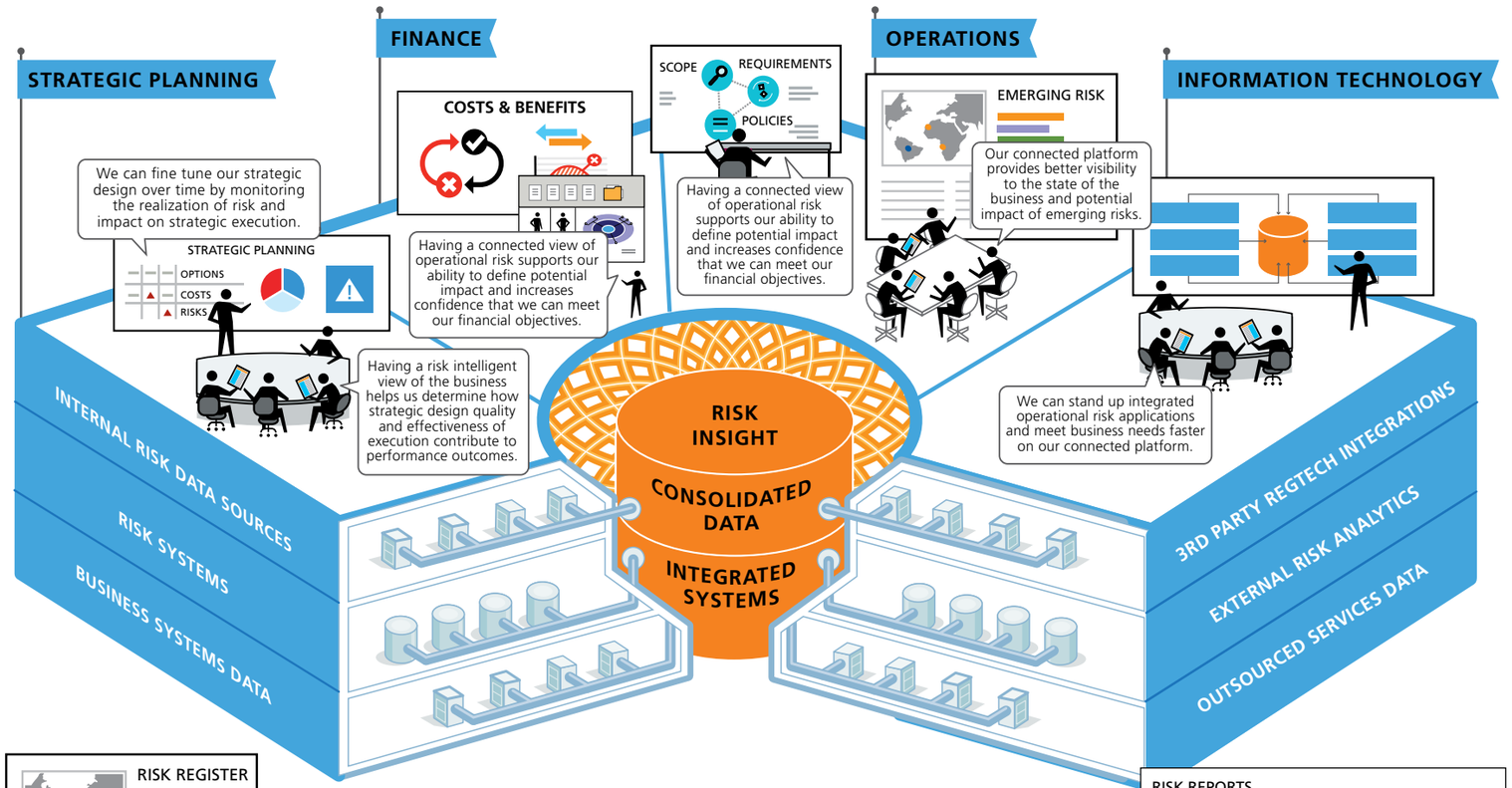
DEFINING OPERATIONAL RISK

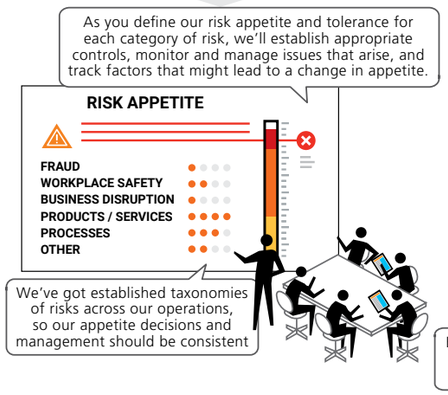
Any event that can disrupt business processes presents an operational risk and potential for loss. Failed procedures or systems, employee errors or improper actions, unidentified regulatory change, model use failures, unexpected business actions, fraud and other criminal activity – all present operational risks.

THE OPERATIONAL RISK TEAM

The team should include business risk managers in each unit, together with a number of risk specialists, including:

- legal
- security
- fraud management
- disaster recovery
- business continuity
- compliance
- insurance
- data privacy
- cyber risk
- third party management
- environmental, health and safety



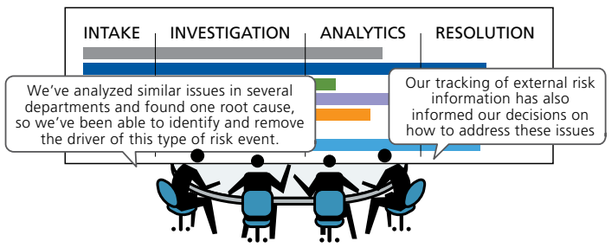


OPERATIONAL RISK APPETITE AND TOLERANCE

- Establish risk policy with clear decision-making guidance
- Align appetite and tolerances to specific objectives
- Communicate broadly throughout the organization

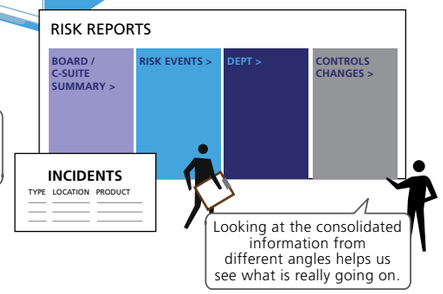
SELF-ASSESSMENT AND CONTROL PLANNING

- Deliver information to support well-reasoned risk decision making
- Streamline assessment processes and controls aligned to risk appetite
- Enable effective review and challenge by risk leadership team



INCIDENT IDENTIFICATION AND EVENT MANAGEMENT

- Manage with consideration to multiple effects and contributing factors
- Evaluate and address deviation from tolerances and impact on strategy
- Leverage occurrences to better inform future risk decision-making



INDICATORS AND REPORTS

- Establish data driven alerts and actions based on indicators and established thresholds
- Enable 360° reporting throughout the management process for all affected stakeholders
- Customize real-time lenses providing relevant analytics and metrics for each audience

Connected Risk Management Enhances Better Business Decisions

When risks are well understood, they can be used to the advantage of the business. By combining multiple risk data streams in one system with advanced data mapping capabilities, everyone with responsibility for identifying and responding to operational risk can contribute to meaningful decisions about business plans and risk management. Systems offering connected management of operational risk provide the ability to:

- **Enable integrated ecosystem of internal and external content and technology to inform decision-making**
- **Establish a dynamic view of risk appetite that changes as inputs change**
- **Develop and maintain an aggregated picture of risk across the business**
- **Monitor trending risk data to inform a predictive view of emerging risk**
- **Track and manage status and impact of risk projects across the business**
- **Support unified self-assessments and analyses for a standardized approach to risk decision-making**
- **Manage and monitor action plans to maintain risk within tolerances**
- **Coordinate responses to risk incidents to minimize direct and cumulative impacts**

{AN OCEG ROUNDTABLE}

Operational Risk Challenges

Switzer: Managing operational risk has always been a challenge. What can be done today to better manage the entire process that wasn't possible even a few short years ago?

Rasmussen: A key change is the architecture. Up until recently organizations were focused on a platform view that tried to do everything for operational risk management and broader GRC. The reality is that no platform truly did everything, and many functions it only did somewhat well. While there is still the need for a core platform to connect and manage risk, this platform has evolved to be a point of integration with other expert systems and business applications to bring in diverse risk data and monitor and enforce controls to those risks.

Stohr: Simplification and consolidation is the project theme we hear most from our clients. As operational risk functions have become more diverse and specialized to meet regulatory and business driven objectives, the risk functions have become more siloed and disconnected both in process and technology. As a result, firms are focused today on trying to develop a common taxonomy, a "common language" to identify, measure and aggregate risk. This is an important endeavor to improve top-down visibility though reporting tools, however for most firms this data congruence challenge is proving more difficult than anticipated to resolve. This is where the increased data flexibility and integration capability of more contemporary GRC technologies can help. First technologies that provide the ability to precisely model a firm's risk taxonomies can enable both a fully harmonized risk taxonomy for centralize risk aggregation while fully supporting independent functional specific taxonomies to meet the unique, often regulatory-driven, aggregation requirements for each function. Second, newer technologies are becoming much more adept at integration thereby providing the ability for firms to leverage best-of-breed or best-fit technologies where needed while providing the necessary integration fabric to support harmonization of data across technology platforms.

Switzer: How should an organization go about identifying relevant internal and external sources of data, capturing it, and assessing it?

Rawls: Developing an operational risk data model that establishes relationships and associations between relevant data points such as risk events, assessment results, KRIs, control tests, audit findings, and output from other functional groups helps form the foundation that can collectively support risk management insights and decisions. This connected view of operational risk that may span various systems can assist in enhanced understanding of risks, potential root causes, and better monitoring practices. Focusing on identifying key risk and control indicators and metrics for the most critical and vulnerable risks areas (which can be informed by activities such as risk assessments) can help prioritize where to focus data collection and analysis to help predict and prevent future breakdowns and loss events.

Stohr: The good news is that most compliance and risk organizations are already very good a taking a risk-based approach to planning investments and resource focus. The same approach applies to identifying targets for improved data acquisition, integration, and utilization. Firms should focus their efforts on areas of the business that represent both higher levels of inherent risk as well as areas where enhanced data can provide improved value to the first line of defense. Some of the more common focus areas today include emerging regulatory risk, model risk, third-party risk, or cyber-risk but each firm is unique. Once a catalog of "reliable" data is identified the focus becomes integration. It is critically important that the process support technology is architected to perform under the increase data load condition. If not, the additional data will only contribute to slower user performance. Integration must also include a clear view of how the data will be articulated in the user experience—clear visualization and context are critical to informing better risk decision making.

Switzer: Making decisions about the appropriate types and levels of controls for various operational risk concerns depends first on setting a clear risk appetite and tolerances. How should this be done?

Stohr: Linking of risk appetite statements to strategy and objectives not only helps better define the appetite and tolerance but also helps create a critical relationship between risk management functions and the operation of the business. The linking to strategy can provide a critical dimension for senior management reporting supporting not only control decisions and risk mitigation investments, but critically the ability for second-line risk functions to demonstrably help improve business outcomes. Most firms are moving more responsibility for risk identification, assessment, and control to the first line of defense. Risk appetite and strategic context can greatly assist first-line understanding, identification, and assessment of risk. RCSA processes should incorporate clear definitions of appetite and tolerance in the context of strategic objectives for each RCSA. Historical context such as loss history and business performance data, MRAs, industry benchmarking, and open issues can further assist the business in understanding the nature of its risk relevant to the business appetite and performance goals to inform better risk assessment and prioritize focus on areas that may require better mitigation strategies. Moving from static KRI and KPI documentation to live integrated indicator monitoring with well-established thresholds and alerts enables tolerance statements to be monitored proactively. By enabling the business to understand when risks are more likely to be realized, or more impactful, the business has the opportunity to make course adjustments that may improve the likelihood of achieve desired business outcomes.

Rawls: Determining how to best respond to and control operational risk should begin by defining risk appetite statements at the enterprise level that articulates the company's willingness to accept risk in the pursuit of business objectives. Based upon the risk appetite levels, management can establish risk tolerance metrics and thresholds that outline the maximum acceptable amount of risk associated with a risk-taking activity or risk category. The aggregation of individual risk tolerances should collectively fall within the established risk appetite at the enterprise level.

Switzer: How is machine learning contributing today to better management of operational risk, and how do you see that further developing over the next 5 to 10 years?

Rasmussen: Machine learning, and broader artificial intelligence, is a rapidly expanding technology area with more and more use cases coming to clarity for operational risk management. The value of this is in automating risk management by evaluating patterns in data to identify and monitor risks. A key element is to do predictive analytics that identify trends and issues and address or monitor them before they become big issues to the organization, a way to identify and contain them. It also involves the ability to automate risk assessments by providing guidance on suggested categories, treatment, and response by evaluating past patterns of similar events.

Stohr: The pace of innovation in the areas of machine learning and robotics is increasing every day, and there is little doubt that these technologies will bring a lot of value as well as some new challenges to the management of operational risk. While there are definitely some specific use cases where this emerging technology is showing some utility and practical application today, it is unlikely that any organization can anticipate the many potential applications that may be available in the next 2 years let alone 5 or 10 years. In addition to internal investment and experimentation, the most important thing firms can focus on today is readying their internal risk and compliance solution architecture to be able to plug these new technology solutions in as they become viable and useful to the organization. Firms should think about their future technology environment as a connected ecosystem of technology and data that behaves like a constantly evolving central nervous system. ■

ROUNDTABLE PARTICIPANTS

MODERATOR
Carole Switzer
Co-Founder & President, OCEG

Lisa Rawls
Principal, GRC Technology US and Americas Service Leader, KPMG

Michael Rasmussen
GRC Economist and Pundit, GRC 20/20

Russell Stohr
Director, Market Development, Refinitiv

[GRC ILLUSTRATED]

Operational Resiliency Today

This column accompanies the illustration on the facing page fold-out, which is part of OCEG's GRC Illustrated Series. To download a copy of the illustration and others in the series, visit the OCEG Website at www.oceg.org/resources.

by Michael Rasmussen

I am sitting in a pub in London having a last pint before I fly home in the morning. After an intense week of interactions with organizations my mind is laser focused on the burning issue of the day: operational resiliency.

The FCA, PRA, and Bank of England have recently released a discussion paper focused on the need to build greater operational resilience in organizations. This challenge is much broader than just the United Kingdom and financial services; it is an issue that crosses the globe and industries. How do we build resiliency in our business to risk and disruption?

Today's organization is complex and chaotic—in a constant state of metamorphosis. Keeping complexity and change in sync is a significant challenge for operational risk management functions. Consider that the modern organization is:

- **Distributed.** Traditional brick-and-mortar business is a thing of the past: Physical buildings and conventional employees no longer define organizations. The organization is an interconnected mesh of relationships and interactions that span business boundaries with distributed operations complicated by a web of global relationships.
- **Dynamic.** Organizations are in a constant state of change. Distributed business operations are growing and changing at the same time the organization attempts to remain competitive with shifting business strategy, technology, and processes while keeping current with changes in risk and regulatory environments around the world. The multiplicity of risk environments an organization monitors span regulatory, geopolitical, and operational risks across the globe.
- **Disrupted.** The intersection of distributed and dynamic business brings disruption. Change (dynamic business) combined with complexity (distributed operations and relationships) means the organization is easily disrupted. Organizations are attempting to manage high volumes of structured and unstructured risk information across multiple systems, processes, and relationships to see the big picture of performance, risk, and compliance. The velocity, variety, and volume of risk is overwhelming—disrupting the organization and slowing it down at a time when it needs to be agile and fast.

In defining operational resiliency, I can think of nothing stronger than leveraging the OCEG definition for governance, risk management, and compliance (GRC). This is a capability to reliably achieve objectives, while addressing uncertainty, and act with integrity. To be operationally resilient requires that we understand the operational objectives of the organization and in that context manage the risk and uncertainty in hitting those objectives while operating with the boundaries of values and requirements set on the organization.

Achieving operational resiliency requires a connected view of risk to see the big picture of how risk interconnects and impacts the organization and its processes. A key aspect of this is the close relationship between operational risk management (ORM) and business continuity management (BCM). It baffles me how these two functions operate independently in most organizations when they have so much synergy.

Connecting ORM and BCM is just part of achieving operational resiliency. To be resilient requires that the organization also manage the intersection of compliance, information security, business operations/processes, performance, third-party management, and other risk functions. Operational risk management is an umbrella covering a lot of risk departments that have historically operated in silos. These silos need to collaborate and connect in a broader operational risk strategy focused on the operational resiliency of the organization.

Managing operational risk activities in disconnected silos leads the organization to inevitable failure. Decentralized and disconnected distributed systems of the past catch the organization off guard to risk. The complexity of business and intricacy and interconnectedness of risk requires an integrated approach. Silos of risk fail to actively manage risk and leave the organization blind to intricate relationships of connected risk across the organization. An ad hoc approach to operational risk management results in poor visibility across the organization and its control environment because there is no framework or architecture for managing risk as an integrated part of business.

Distributed, dynamic, and disrupted business demands a strategic approach to operational risk strategy and process enabled with an integrated information and technology architecture. The organization needs complete situational awareness of risk across operations, processes, relationships, systems, and information to see the big picture of risk and its impact on organization performance and strategy. ■

Michael Rasmussen is the GRC Economist and Pundit for the anlyst firm GRC 20/20, and an OCEG Fellow.

FUTURE-PROOF YOUR CAREER

Level up your skills and get the GRC Professional (GRCP) certification by OCEG, the nonprofit think tank that invented GRC

Everything is included in a single fee:

- Online preparation
- Online exam
- Online continuing education

www.oceg.org/grcp

OCEG®