ARCHER

WHITE PAPER

The Path from GRC to Integrated Risk Management

Managing Risk in Times of Change

Risk management has been on a constant evolution path for decades. The early concepts of Governance, Risk and Compliance (GRC) laid the foundation but organizations today seek a more agile, fluid approach. Integrated Risk Management has emerged as the term to describe the modern approach to identifying, assessing and treating risks. As business operations grow in scope and complexity, the need to manage risk in a more nimble, responsive manner becomes increasingly pressing.

GRC in its initial incarnation—a set of tools for managing compliance risk—remains valuable for that specific challenge, but it aligns less precisely with today's evolving definitions of risk and risk management. The answer is not to abandon GRC, though; rather, it's to allow it to evolve into an approach that is better suited to today's multifaceted challenges: integrated risk management.

This transition does not happen overnight. It takes vision and planning to map out your path from a compliance-driven risk-management strategy to an adaptable, integrated approach that can keep pace with the fast-changing digital world. While the path to integrated risk management may vary between organizations, the benefits are tremendous. The resulting capability to respond to business change and manage the uncertainty of today's landscape enables an organization to take full advantage of the opportunities at hand.

Starting Point: Recognize New Risks at a New Pace

GRC emerged as a way of improving corporate governance and internal controls to address regulatory compliance requirements. Today, however, the need has shifted from managing compliance risk to better managing overall risk. As the definition and scope of risk itself has evolved, the pace of risk has increased as well. With expansion of digital products and services, increased reliance on third party ecosystems supporting business operations and constantly evolving compliance and industry pressures, organizations face a litany of risk moving to the forefront. Strategies that drive business success today, such as technology adoption or market expansion, are creating new opportunities—but at the same time, they are introducing more risk.

Digital Transformation

Digital transformation is clearly a strategic priority today. 2020 has proven the need for technology services and has accelerated the push towards digital transformation. Digital transformation creates new opportunities to thrive and compete—but it also creates digital risk. Digital business typically involves fast-moving projects supported by processes that require a multitude of different applications, expanding the points of risk and the stakes for the organization. The key to seizing the opportunities is managing the risk in critical areas as the business pushes the technology envelope.

Vendor and Other Third-party Relationships

Looking to move more quickly and nimbly to exploit business opportunities, organizations are increasingly relying on external parties, such as service providers. However, they can struggle to efficiently manage and govern these third parties because traditional methods aren't scalable. Third-party relationships introduce unpredictable, inherited risks that can lead to surprises and potential losses. In addition, regulators are establishing increasingly higher standards of accountability for the oversight of third-party relationships.

Data Governance and Privacy

Organizations are creating more data on a daily basis than ever before. The ambitious initiatives of digital transformations create a tremendous challenge not only in the scale and scope of data but also in understanding the value of different types of data and the protection requirements necessary to manage risk to the data. The fundamental challenge regarding risk during this the data explosion is determining:

- What the value of the data is.
- Where the data is flowing.
- What needs to be done to properly protect the data.

A core tenet of risk management is you can't protect what you don't know about. The complex data flows within a modern enterprise strains any processes designed to understand data protection requirements. Any inefficiency in the strategy to identify, assess and treat risks to data will be quickly overwhelmed under the avalanche of data.

These examples represent major categories of risk for organizations today, but they are by no means the only risks organizations face. Every organization is a complex ecosystem of people, processes and technology, and risk can be hidden away in many areas.

Next Logical Step: An Integrated View of Risk

A Vertical View of Risk

In the early days of GRC, independent functions were focused more on operational risks with less emphasis on connecting to the strategic business impact. Business and IT were essentially separate functional parts of an organization and there was little connection between these two worlds. That changed as enterprise GRC became a requirement of risk management.

Today, when business and technology are intimately connected (or at the very least, mutually influential), risk management must link operational risks to business strategies and vice versa. Security events are one example. Security-related incidents must be prioritized based on the business context of the systems, data and processes involved to understand the business impact of a security event. Another example is building audit plans based on strategic business objectives – not just a historical 'we always audit these business processes' approach.

The relationship between strategic business goals and business operations is the key to this vertical view of risk. A decision made at the strategic level will cascade down and affect the organization's ability to execute business operations; a seemingly minor operational event can spiral out of control and impact strategic direction. Thus, connecting the top-to-bottom, strategic-to-operational view of risk is essential to truly understanding, and addressing, the obstacles to achieving business objectives.

...and a Horizontally Integrated View

A vertically integrated view is important—but is not the end game. The other part of the picture is a horizontally integrated view that connects domains of risk. Risk is as hyperconnected today as your organization. As areas of risk within organizations continue to grow beyond just compliance risk, the need to view them as an integrated whole becomes increasingly clear. There are two primary reasons for this. One is that it's simply unrealistic and operationally unsustainable to manage them separately, using different risk management approaches. The other reason—far more critical than the first—is that most areas of organizational risk today don't really exist independent of other risks; rather, they cross over into other areas.

For example, engaging with a cloud service provider presents a security risk, a resiliency risk and a third-party risk. In other words, the cloud service provider could be the source of security data breach, an operational disruption, a compliance issue or a reputational risk. If that business relationship isn't considered in each of these dimensions, there is a gap in truly understanding the risk. Therefore, organizations need to be able to leverage business processes to build an integrated picture of risk that crosses operational functions and fosters a multidisciplinary approach to risk management.

The goal: Integrated Risk Management

As views of risk management broaden to include both a vertically integrated view from strategy to operations and a horizontally integrated view across risk areas,

organizations will become better able to adapt their risk management strategies to address the scope and complexity of risk today.

If compliance is the primary driver of risk management, the organization is coming up short in understanding the true risks within the business. An integrated approach to risk management—going beyond the fundamental elements of governance and compliance represented by the original vision of GRC - provides a more expansive definition of integration that addresses a diverse set of risk areas and includes both business and IT risk.

The evidence for integrated approaches to risk management is present in several trends. For example, the Archer Digital Risk Survey 2020 indicated the pandemic of 2020 has created an increased sense of urgency towards collaboration across teams. When asked, "To what extent do you believe security and risk teams will work together over the next two years, due to the impact of the pandemic?" a resounding 92% indicated the expectation that those groups would work in a more coordinated fashion. The survey also found Integrated Risk Management will become increasingly essential in the coming years and must be positioned to address a continuous cycle of emerging risks. Companies indicated a focus on transitioning to continuous monitoring of controls to improve effectiveness and reduce the cost of compliance. In addition, establishing risk-based approaches was indicated as priorities in many domains including compliance, business continuity/disaster recovery, security and third-party risk management efforts.

On the Horizon Now: Operational Resiliency

Following the path to integrated risk management can seem a daunting prospect. It's no longer tenable to keep the risk management discussion narrowly focused on compliance or confined to IT—but it can be hard to know exactly where to begin.

2020 has proven to be an unprecedented year of disruption that highlights the imperative towards integrated approaches to risk management. The acceleration of digital transformation spurred by the pandemic will require security and risk functions to equally pick up speed. Keeping pace with digital initiatives require efforts to modernize security and risk management. Operational resiliency refers to an organization's ability to absorb and adapt to rapid changes, sudden disruptions or other challenges—and continue to achieve its objectives. Operational resiliency isn't only about business or IT recovery after a disruption; it also includes building resilient business practices across the organization to prepare for disruption.

With so many organizations facing industry shifts, market pressures, and increased competitive landscapes, shifting the focus towards operational resiliency makes sense. Business today is all about speed, and risk can't be allowed to hinder organizations as they move forward. Integrated risk management allows you to keep pace with the business. Otherwise, you will find your organization struggling to manage risk and falling further and further behind. Now is the time to follow a new path that sees GRC in the light of integrated risk management—a path that will prepare you well for managing risk in these times of change.

About Archer

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

ARCHER
An RSA Business