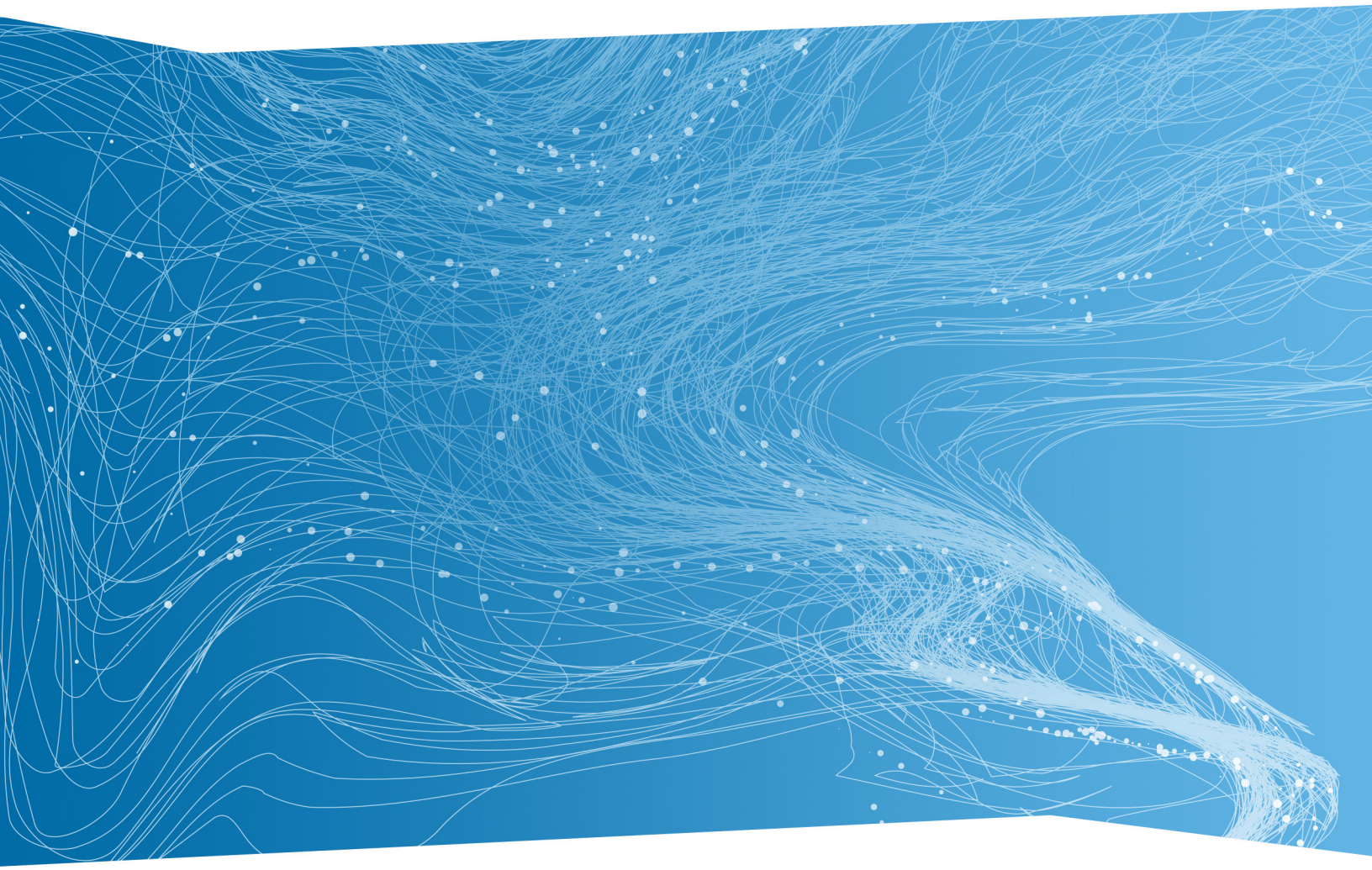
RSA



WHITE PAPER

THE PATH FROM GRC TO INTEGRATED RISK MANAGEMENT

MANAGING RISK IN A DIGITAL WORLD

RSA

Successful risk management today may start with governance, risk and compliance (GRC)—but it shouldn't end there. As more and more organizations embrace digital transformation,[1] business risk grows in scope and complexity, and the need to manage it in a more agile, 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 paper maps out the path from a pre-digital, compliance-driven risk-management strategy to an adaptable, integrated approach that can keep pace with the fast-changing digital world.

STARTING POINT: RECOGNIZING NEW RISKS

GRC emerged early in this century as a way of improving corporate governance and internal controls to address regulatory compliance requirements. Today, however, the need has evolved from better managing compliance risk to better managing overall risk. And the definition and scope of risk itself has evolved as well, with areas such as digital third-party risk coming into play and 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. Consider these examples:

DIGITAL TRANSFORMATION

Digital transformation is clearly a strategic priority today; IDC recently forecast spending in this area to reach $1.3 trillion in 2018.[2] 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:

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 (especially cloud service providers), vendors, contractors and consultants. This increases risk, since organizations don't have direct control over the risk a third party creates—but they are nevertheless responsible for managing the risk in third-party relationships.[3]

COMPLIANCE AND OVERSIGHT

That brings us to the area that originally led to the emergence of GRC: compliance risk. That risk has not gone away; it's only been joined by other risks, such as those described above. Given the increasing complexity of

RSA

business and IT today, compliance has grown more complex, increasing the risk associated with it.

The examples described above 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 HORIZONTALLY INTEGRATED VIEW

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 platforms. 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, if engaging with a cloud service provider presents a security risk, that's both a digital risk and a third-party risk. And if that risk isn't addressed, it may result in issues across multiple areas, from business disruption to compliance. 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. Think of this as a *horizontally* integrated view of risks that needs to be managed.

...AND A VERTICALLY INTEGRATED VIEW

A horizontally integrated view is important—but incomplete. The other part of the picture is a vertically integrated view that connects strategic and operational 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, however, 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 a great example. At RSA, we talk about Business-Driven Security™,[4] which puts security-related IT incidents in a business context and makes it possible to calculate the business impact of a security event—and vice versa. This kind of interrelationship allows organizations to bridge the gap between security teams and their business counterparts, creating an environment in which they can reduce the risk that security incidents will negatively affect the business or that business decisions will negatively affect IT.

The interrelationships between strategic business goals and operational events are becoming increasingly impactful. A decision made at the strategic level will cascade down and affect the organization's ability to manage a risk in 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—as illustrated in the accompanying graphic—is essential to truly understanding, and addressing, the obstacles to achieving business objectives.

An integrated view of risk includes both a vertically integrated view connecting strategic to operational risk and a horizontally integrated view across operational functions.

THE GOAL: INTEGRATED RISK MANAGEMENT

As views of risk management broaden to include both a horizontally integrated view across risk areas and a vertically integrated view through business and IT, organizations will become better able to adapt their risk management strategies to address the scope and complexity of risk today. For RSA, this is the thinking that underpins the evolution of RSA Archer® Suite from a GRC-centric technology solution to an integrated platform for managing multiple dimensions of risk.

When compliance was the primary driver of risk management, and when compliance was primarily the domain of IT, there was no real need for an integrated approach to risk management—at least not beyond the integration of risk management with governance and compliance. But today, the integration represented by the original vision of GRC is no longer enough. GRC must move toward a more expansive definition of integration that addresses a diverse set of risk areas and includes both business and IT risk.

Data from the RSA Cybersecurity and Business Risk Study[5] indicates that an integrated IT security and business risk approach is important to successfully moving risk strategies forward today. The study included a survey, commissioned by RSA and executed by Enterprise Strategy Group (ESG) in June 2018, of 306 IT GRC professionals working at large (1,000 or more employees) organizations in North America. In the survey, 69 percent

RSA

of respondents agreed the relationship between business risk and IT security can be difficult to coordinate, and 70 percent agreed that business risk and IT security personnel tend to use different tools and language, making communications between these groups challenging. This points to the value of an integrated approach to risk management, with a common risk taxonomy, standardized tools and consolidated key data.

What does it mean specifically to adopt an integrated approach? It means being able to tackle a particular risk challenge and then extend the solution to additional elements of risk using an integrated set of processes and an integrated technology platform. According to the Gartner IT Glossary, IRM is a set of practices and processes, supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organization manages its unique set of risks.

Under the Gartner definition, IRM has certain attributes, and technology is among the six it lists:

1. **Strategy:** Enablement and implementation of a framework, including performance improvement through effective governance and risk ownership
2. **Assessment:** Identification, evaluation and prioritization of risks
3. **Response:** Identification and implementation of mechanisms to mitigate risk
4. **Communication and reporting:** Provision of the best or most appropriate means to track and inform stakeholders of an enterprise's risk response
5. **Monitoring:** Identification and implementation of processes that methodically track governance objectives, risk ownership/accountability, compliance with policies and decisions that are set through the governance process, risks to those objectives, and the effectiveness of risk mitigation and controls
6. **Technology:** Design and implementation of an integrated risk management solution (IRMS) architecture[6]

ON THE HORIZON NOW: DIGITAL RISK MANAGEMENT

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.

With so many organizations moving toward some form of digital business today, shifting the focus to digital risk management makes sense. Digital risk management is the integrated management of risk that is associated with digital business areas such as cloud, mobile and the internet of things (IoT). This scope makes it one of the most consequential forms of integrated risk management today—and the right place to start.

RSA

Digital transformation is about speed, and risk can't be allowed to hinder organizations as they move forward with it. As you keep moving toward digital, you have to move toward integrated risk management at the same time. Otherwise, you'll find your organization struggling to manage digital 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 a digital world.

Learn more about the path to integrated risk management at rsa.com/irm.

[1] 2018 Digital Business Survey, IDG, April 3, 2018

[2] "IDC Forecasts Worldwide Spending on Digital Transformation Technologies to Reach $1.3 Trillion in 2018," IDC Media Center, December 2017

[3] "Current employees remain the top source of security incidents," PwC, The Global State of Information Security Survey 2018

[4] RSA® Business-Driven Security™ Solutions, rsa.com

[5] ESG Custom Research, Cybersecurity and Business Risk Survey, June 2018

[6] IT Glossary, Integrated Risk Management, Gartner