EBOOK

THE POWER OF INTEGRATING **Risk** and **Resilience**

riskonnect.

Risk management and resilience have long operated in parallel universes. The risk team identifies and manages potential threats to the organization, and the resilience team maintains business continuity when the unexpected happens.

While both teams are charged with protecting the organization, each views this mission through its own lens, with its own goals, its own language, its own metrics, and its own reporting structure. Roles and responsibilities are clearly defined, and there is little cross-team interaction.

That siloed approach doesn't work anymore.

Risks are more numerous, more damaging, more connected, and more volatile than ever. Organizations are constantly fending off challenges from supply-chain problems, geopolitical tensions, market volatility, regulatory changes, economic uncertainty, cyberattacks, and more. The accelerating pace of change makes disruptions harder than ever to predict, even as they grow in frequency and severity.

Risk doesn't live in silos. And neither can the teams tasked with managing it.

Risk and resilience working together are a powerful combination. Removing the walls unlocks knowledge, eliminates duplicate work, and aligns strategic priorities. Closer collaboration helps risk teams think more practically about potential outcomes. And it helps the resilience team bring a strategic focus to continuity planning.

This ebook will help you understand the power of integrating risk and resilience, what might be getting in the way, and how to build a strong connection.

CONTENTS

What Is GRC?

Governance, risk, and compliance – GRC – is a set of processes and procedures to help organizations achieve business objectives, address uncertainty, and act with integrity. GRC focuses on high-level strategic risks.

What Is Resilience?

Resilience – also known as business continuity management, BCM, or business continuity and resilience – ensures that critical operations can continue during disruptions and normal operations can quickly resume. Resilience focuses on operational realities.

A Tale of Two Perspectives

The risk and resilience disciplines started from two different places with two different mandates:

The discipline of governance, risk, and compliance emerged when organizations expanded their view of risk management beyond risks that could be insured to enterprise risks, compliance, third-party risk management, internal audit, IT risk management, and more.

The discipline of business continuity and resilience was spurred into existence to counter external societal threats like Y2K. Over the years, it has expanded to comply with growing regulatory requirements designed to prove that the organization has concrete plans to keep the business running through disruptions, while minimizing the impact.

Over time, the separation has been exacerbated by:

Structural divides. Organizational silos create natural divides. GRC typically reports into legal, audit, or finance. Resilience, on the other hand, is often part of IT or operations. As a result, they've grown up with different mandates, different toolsets, different frameworks, different stakeholders, and different reporting cadences.

Cultural divides. Each discipline has its own definition of success. GRC is judged on how well it anticipates and informs strategic decisions. Resilience is judged on how fast the organization can recover and adapt from a major disruption. Those fundamental differences are baked into the way each team operates.

Governance divides. Risk and resilience have had separate forums, separate budgets, and separate risk languages. No one was accountable for connecting the dots, which goes largely unnoticed – until something goes wrong.

THE FORCES PUSHING RISK AND RESILIENCE TOGETHER

The separation between risk and resilience is no longer simply inefficient. It increasingly impacts corporate performance. The four main forces accelerating integration include:

Regulatory pressures. The message from regulators worldwide is clear: Identifying risk and risk mitigations are not enough. You must demonstrate that you can continue to operate with unified risk and resilience when high-impact risk events occur.

Executive expectations. Boards and the C-suite expect one narrative about threats to the business and the impact. They want assurance that resilience is systematically built into strategic planning and not just reactive in nature. When risk and resilience are disconnected, leaders are left with fragmented plans, redundant assessments, and no clear path for enterprise-wide readiness.

> **Siloed reports don't add to intelligent decision-making processes. They only add to confusion.**
>
> *Dr. Phil Moulton, global chief risk and compliance executive advisor, author, and thought leader*

Fatigue from drained resources. Siloed functions mean the risk team and the resilience team are doing separate risk assessments, separate workshops/exercises, and separate reports, which may reach conflicting conclusions. Not only is this inefficient, but it can create dangerous blind spots when things fall through the cracks.

Misalignment between risk priorities and risk capabilities. Disruptions have exposed the gap between strategy and response resulting in missed signals, duplicated efforts, and a fragmented response when a crisis hits.

Important Regulations

DORA

EUROPEAN UNION

The Digital Operational Resilience Act (DORA) combines risk management, technology risk, third-party risk management, and business continuity to prevent, detect, respond to, and recover from ICT risks.

OSFI

CANADA

OSFI's Guideline E-21 combines risk management and business continuity to enhance the ability to prevent, detect, respond to, and recover from risks and threats.

APRA

AUSTRALIA

APRA's CPS 230 combines risk management, business continuity, and third-party risk management to prevent, detect, respond to, and recover from risks and threats.

THE HIDDEN COST OF DISCONNECTION

Disconnection between risk management and resilience can undermine both functions – with real cost implications for the organization. Here's why:

Conflicting priorities. Risk teams prioritize risks based on likelihood and impact, often relying heavily on past experience. Resilience teams prioritize efforts based on the plausibility of a scenario and whether it is credible even without historical evidence. It's a problem when these priorities are at odds.

Language barrier. Are risk and resilience teams using the same term to measure different things – or different terms to measure the same thing? Something as simple as one team using "people" and the other using "employees" can cause time-wasting confusion. Terms to watch out for:

- Incident/crisis/disruption
- Threat/risk
- Supplier/vendor/partner
- Location/area
- Applications/products
- Organizational risk/organizational resilience/operational resilience

Agreeing upfront on taxonomy and criteria can speed up communication and minimize misunderstandings.

Measurement misalignment. Resilience teams look at impact tolerance – the amount of disruption the organization can handle before customers, employees, the business, and markets are intolerably harmed – and recovery time objectives – the maximum acceptable amount of downtime. Risk teams measure risks against risk appetite – the amount of volatility acceptable to achieve goals – and risk tolerance – the acceptable level of operational risk by category.

When the resilience and risk concepts are considered in isolation, it's difficult to assess the true impact of a risk or which controls are most meaningful. Two stories also make it difficult for the board to understand what to focus on.

Redundant work. Both teams asking others for the same – or almost the same – input on vendors, risks, impacts, etc. wastes time, squanders resources, and slows response to emerging threats. And the requests can be extra annoying if more work must be done to adjust the data to fit the peculiarities of each team.

WHAT GRC AND RESILIENCE CAN LEARN FROM EACH OTHER

Bringing the risk and resilience teams closer together and encouraging them to learn from each other will help the organization better plan for the unexpected. It will help build up response capabilities in advance and improve your chances for long-term success.

A clearer picture of enterprise risk

Resilience activities like business impact analyses and scenario testing can reveal operational gaps that risk management alone might miss. Working together allows insights from both teams to filter up to the enterprise risk portfolio, so leaders can see the full spectrum of risks and potential impact on the company.

Less duplication of work

Shared assessments, controls, and data reduce administrative work for both teams, as well as risk owners charged with completing risk assessments. Coordination also ensures resources are used effectively during a crisis, speeding up critical response times.

Audit readiness

Unified heat maps, dashboards, and other documentation make it easier to create reports, comply with regulations, and answer auditor questions.

A stronger risk culture

Shared language and metrics promote collaboration, minimize misunderstandings, and get everyone working together for the greater good of the organization.

HOW TO INTEGRATE GRC AND RESILIENCE

One of the biggest challenges in integrating risk and resilience is that the teams operate differently on a daily basis. The GRC team is scenario-driven, strategy-oriented, and often focused on financial, reputational, or regulatory issues. Business resilience is procedural, operational, and concerned with keeping people, processes, and systems running under stress.

Moving from parallel functions to an integrated risk and resilience program doesn't require a total rebuild. Start off with a few basic – but important – initiatives:

1. **Create a cross-functional team.** Put together a team with representation from both functions. This group can work together to identify risks, prioritize actions, and develop solutions. They can establish common workflows that bake in cross-collaboration from the start. You may even find that with your combined efforts, data gathered for one requirement can be leveraged to comply with another, saving everyone time and effort.

2. **Establish a regular cadence for talking. Don't wait for trouble to happen.** Get the cross-functional team together on a regular basis as a forum to raise issues, discuss solutions, and build trust.

3. **Decide on a common language and metrics.** Come together to institute a common taxonomy and measurement criteria for all stakeholders – including both the risk and resilience teams and internal partners. Jointly define what "critical" means for products, services, systems, and suppliers – and ensure that both the enterprise risk register and BIAs reflect the same assumptions. Shared objectives and KPIs can also motivate teams to collaborate on solutions. And a common language will help eliminate discrepancies and misunderstandings – which is especially important when facing the pressures of disruption.

4. **Establish a joint governance structure.** A shared steering committee keeps risk and resilience aligned with business strategy and ensures consistent communication up to leadership and the board. An executive sponsor who can champion the cross-functional group's work is a bonus. This person will have the authority to garner broad leadership support and secure necessary resources.

5. **Leverage GRC data to prioritize resilience testing.** Use the enterprise risk register to prioritize resilience testing scenarios. For example, if a specific supplier or facility appears in the top risk tier in GRC, that should drive tabletop drills and recovery testing.

6 **Translate risk appetite into recovery objectives.** GRC teams set the tolerances. Resilience teams operationalize them. Align recovery time objectives with stated risk appetite to bridge strategy to operational execution.

7 **Align risk registers with business impact analyses.** While these tools are often developed in silos, they are really two sides of the same coin. If a critical risk is in your risk register, it should be mapped to a BIA priority and vice versa. That will reveal your real risk exposures.

8 **Run joint exercises.** Don't limit scenario testing to just the resilience team. Involve the cross-functional team to help everyone think beyond their roles and share different perspectives for making improvements. Co-led exercises and after-action reports allow both risk and resilience to validate assumptions, surface blind spots, and jointly communicate outcomes to executives and boards.

9 **Sync metrics and dashboards.** Connect key risk indicators with operational recovery performance. Shared dashboards can show when thresholds are breached – and how quickly the organization recovers.

HOW SOFTWARE CAN HELP BRIDGE THE DIVIDE

Today's GRC and business continuity and resilience software gives both risk and resilience teams access to the same high-quality data so they can exchange knowledge and collaborate on actions. It reinforces the agreed-on vocabulary, standardizes processes, and establishes one source of truth for all, from frontline management to the board.

Here's what to look for:

Purpose-built solutions for GRC and for resilience. Beware of specialized vendors that try to oversell expertise in a discipline they know little about. Look for software that is built specifically for the practice of GRC and specifically for the practice of resilience – that also are tightly integrated with each other. That way, each team gets the best solution for their needs with the added benefit of a seamless information exchange.

A shared data model. What starts as, say, a data breach at a critical vendor, can lead to operational risks, cyber risks, compliance risks, and more. Look for software that brings all risk-related data into one place that's easily accessible to all stakeholders. Data can be entered once and used by all, which saves time, reduces the likelihood of errors, and adds transparency.

Interoperability. Combine things like risk exposures, KRIs, and risk appetites from the GRC perspective with business continuity metrics like RTO performance, BIA outputs, and recovery assurance levels. Look for software that puts them in one view, one voice, and one context, so you have the overall picture and can see whether critical risks and the response plans have been properly exercised.

Workflow automation. Integrated technology automates routine tasks, workflows, and follow-up, saving time, improving accuracy, and adding consistency. Look for software that not only streamlines everyday work in each discipline but that also automatically triggers cross-functional actions. For example, a risk flagged in a cyber audit would immediately trigger a business impact review and continuity plan check. Or a regulatory requirement for resilience would directly feed into your GRC framework, with controls mapped, tested, and ready to go.

Reporting and analytics. Boards want to know that the organization is ready for whatever obstacles pop up. That means reporting testing outcomes, recovery capabilities, and gaps in a way that reflects enterprise resilience. Look for software that helps the cross-functional team identify gaps, determine an action plan, assign responsibility, and set a timeline for completion.

AN INTEGRATED FUTURE FOR RISK AND RESILIENCE

The challenge now is to advance the organization from a narrow focus on governance, risk, and compliance to a longer-term strategic view of the entire environment, including unplanned crises.

Organizations that embrace integration between GRC and resilience will recover faster from disruption – and ultimately become more trusted by the market.

This will require a fundamental change in how organizations make decisions. Resilience must be woven into that decision-making process, not tacked on as an afterthought.

By codeveloping scenarios and walking through the real impacts across people, processes, and technology, both teams gain a deeper understanding of how strategic risks translate into operational disruptions and vice versa. This creates a shared vocabulary and helps ensure that the scenarios being used to guide risk, appetite, and resilience planning are grounded, holistic, and testable.

Don't let calm lure you into complacency

Crisis doesn't happen every day, and it is all too easy to forget about the importance of resilience between disruptions. When it's business as usual, deprioritizing investment in resilience is a common – but dangerous – reaction. The organization, the market, and the data are constantly changing. True resilience requires constant care and feeding to keep up.

AI and advanced analytics further strengthen the connection between risk and operational readiness. Instead of looking at risk registers or manual BIA results, for instance, leaders get real-time insights into questions about exposure relative to risk appetite, the risk profile of a vendor, and how quickly the business can recover from a disruption.

Instilling an enterprise-wide approach to risk and resilience is essential to thrive in any form of crisis. The organization will know how to navigate disruptions, emerge stronger, and gain an advantage over less-agile competitors. And customers, investors, employees, and regulators will be assured that you can keep your promises even when times are tough.

That's the power of integrating risk and resilience.

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific. To learn more, visit riskonnect.com.

riskonnect.

CONNECT NOW →

INTEGRATED RISK MANAGEMENT SOLUTIONS:

INSURABLE RISK
- Risk Management Information System
- Claims Management
- Billing
- Policy Administration
- Health & Safety

ACTIVE RISK MANAGER

HEALTHCARE RISK & PATIENT SAFETY

BUSINESS CONTINUITY & RESILIENCE
- Business Continuity Management
- Operational Resilience
- Emergency Notifications
- Crisis Management
- Threat Intelligence

GOVERNANCE, RISK & COMPLIANCE
- Enterprise Risk Management
- Third-party Risk Management
- Environmental, Social & Governance
- Compliance
- Internal Audit
- Internal Controls Management
- Policy Management
- Project Risk Management
- IT Risk Management
- AI Governance
- Business Strategy