

COMPLIANCE WEEK



# RISK MANAGEMENT

## Benchmark Survey



# Poll shows gaps in integrated risk management

Many organizations' enterprise risk management capabilities aren't as integrated as they need to be, leaving them vulnerable to legal, financial, regulatory, and reputational risks, according to a new GRC benchmark report. **Jaclyn Jaeger** explores.

Compliance and risk professionals know that having an enterprise-wide view of risks is far more effective than trying to manage risks in a fragmented way, and that achieving this objective through automation is far more efficient and cost-effective than manual processes and controls. Even knowing that, however, many organizations' enterprise risk management (ERM) capabilities still aren't as integrated as they need to be, leaving them vulnerable to legal, financial, regulatory, and reputational risks.

That was just one of many key findings to come from a recent governance, risk, and compliance (GRC) benchmark report conducted by Compliance Week in partnership with Riskconnect, an integrated risk management solutions provider. The survey polled 113 compliance, risk, and audit executives from around the world—including the United States, Europe, Asia-Pacific, and Latin America—to get a better sense of the state of organizations' risk management capabilities; how effective they are at mapping risks; what GRC metrics they track; and much more.

According to the findings, 44 percent said they have "standardized some processes and use of technology but not across the entire enterprise," while another 35 percent said their processes and technologies remain largely siloed. Only 20 percent said they have integrated processes and technology across the organization.

Most respondents (65 percent) further indicated they are only "somewhat confident" in their organization's ability to map each control it has to a given risk or requirement. Another 21 percent of respondents said they are "very confident," while 14 percent said they are "not confident."

"In my experience, most organizations rely on localized and manual solutions for all kinds of risk management needs," says Quin Rodriguez, vice president of strategy and innovation at Riskconnect. "This amounts to complex, confusing tangled webs of IT systems and data sources that can't support effective enterprise risk management."

"If integrated risk management is the corporate goal, a key strategy to get risk management working effectively and efficiently throughout the enterprise is to adopt a unified framework and create a common risk vernacular," Rodriguez says. The follow-up question, then, is how to go about integrating those processes and technologies, he says.

That is where an integrated risk management solution, like the one offered by Riskconnect, comes into play. Riskconnect's integrated risk management solution consolidates in a centralized dashboard information from multiple sources, automates routine processes, and uses sophisticated analytics to turn complex data into actionable intelligence. In this way, the comprehensive, Web-based system supports

---

"In my experience, most organizations rely on localized and manual solutions for all kinds of risk management needs. This amounts to complex, confusing tangled webs of IT systems and data sources that can't support effective enterprise risk management."

Quin Rodriguez, Vice President, Strategy and Innovation, Riskconnect

risk, compliance, and internal audit, delivering deep visibility to better manage things like vendor risk management, health and safety, policy management, and claims administration.

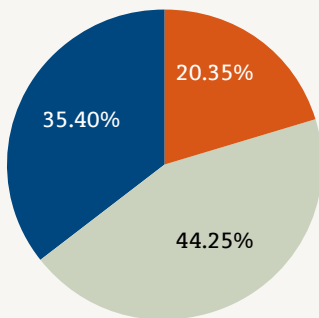
An integrated risk management solution also helps compliance and risk functions track key metrics. According to the survey, the top five key performance indicators respondents said they track are the number of substantiated allegations of misconduct; risk coverage; number of control violations; number of control-test failures; and total cost of risk, compliance, and control activities.

### Risk ownership

Risk managers and risk owners are another important part of a best-in-class risk management program. When asked who leads strategy around integrating GRC processes, 29 percent answered the chief compliance officer, while 21 percent said the chief risk officer, and 17 percent said they had no such role. Fewer said it was the chief executive officer (15 percent) or chief audit officer (8 percent). Here, it all depends on “who has the most visibility across the organization with access to leadership,” Rodriguez says.

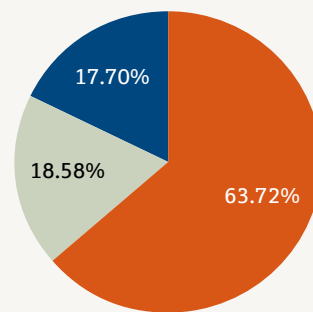
What is imperative to a robust ERM program, however,

Pick the statement that best describes your organization's state of integration of GRC capabilities. (The more integrated you are, the more you share information and use standardized approaches.)



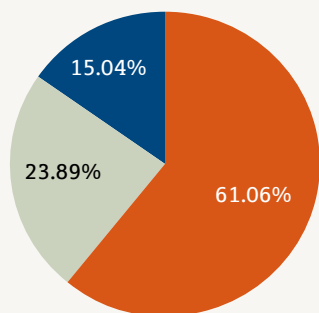
- We have integrated processes and technology across many or all organizational silos of operation
- We have standardized some processes and use of technology but not across the entire enterprise
- Our processes and technologies remain largely siloed

How confident are you in your organization's ability to map risks to the drivers of each risk across all risk functions?



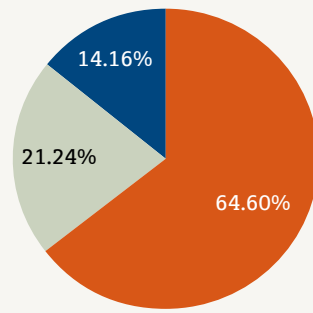
- Somewhat Confident
- Not Confident
- Very Confident

How confident are you in your organization's ability to map ownership of each risk, requirement, and control to specific individuals/roles, ensuring oversight of operation and consideration of need for design or application changes?



- Somewhat Confident
- Very Confident
- Not Confident

How confident are you in your organization's ability to map each control it has to a given risk (or risks) or requirement(s) and track changes that would trigger the need for a change in the control?



- Somewhat Confident
- Very Confident
- Not Confident

is having the ability to map ownership of each risk, requirement, and control to a specific individual or role. This helps ensure proper oversight of a specific operation.

When asked how confident they are in their organization's ability "to map ownership of each risk, requirement, and control to a specific individual or role," however, 61 percent said they are only somewhat confident, while another 15 percent said they are not confident at all. This is concerning, because "if you don't designate an owner of a risk, then how do you manage it?" Rodriguez asks. "Who do you hold accountable?"

Furthermore, most respondents (64 percent) expressed just mediocre confidence in their organization's ability to map risks to the risk drivers across functions, while 19 percent said they are "not confident." Just 18 percent said they were "very confident." To ensure that risk drivers are properly mapped to each function, many organizations today delegate responsibility for risk-information gathering to several risk owners across the various business functions, with the process overseen by a central risk team.

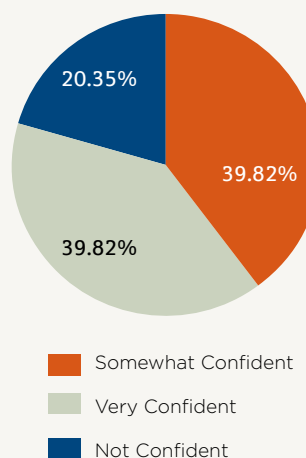
Not surprisingly, many respondents indicated they have the least amount of confidence in their organizations' ability to identify vendor and other third-party risks, with 26 percent saying they are "not confident" in their ability to do so. The types of third-party risks organizations should watch out for include reputational/social media risk; financial; cyber; operational; and supply-chain.

Effective third-party risk management (TPRM) helps companies identify high-risk behaviors and situations, monitor vendor risk levels over time, and compare the risk levels of vendors against one another. When TPRM is integrated with sophisticated technology and the risk posture of the organi-

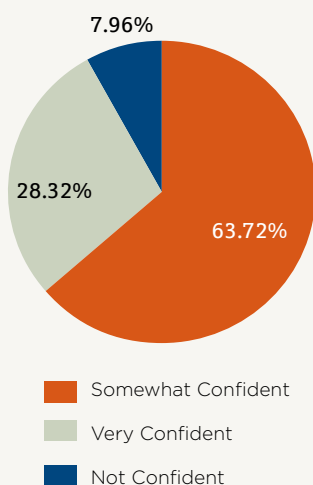
zation, it provides even greater visibility, risk reduction, and cost savings. In a 2018 Compliance Week on-demand Webcast, Riskconnect further discusses how an integrated approach helps solve TPRM challenges.

"Having the ability to integrate more points of the business allows organizations to really automate the risk controls process," Rodriguez says. "It allows people to see the risk landscape far better than they ever had before and understand the impact it has on their organization." ■

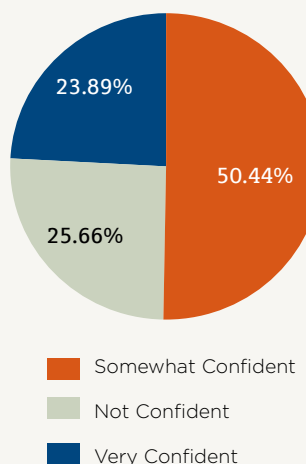
**How confident are you that your governing authority (board or other oversight committees) gets adequate information about risk and compliance to use in establishing objectives?**



**How confident are you in your organization's ability to identify threats that give rise to risks and compliance needs?**



**How confident are you in your organization's ability to identify vendor and other third-party risks and compliance requirements?**



### What key GRC metrics/KPIs do you track? (select all that apply)

