Galvanize

The journey toward Integrated Risk Management

Four steps to realizing the gains of IRM

Table of contents

The journey toward Integrated Risk Management

Four steps to realizing the gains of IRM

Integrated risk management is the disciplined, unified approach an organization can take to govern all the risks it faces, so that executives can make wiser decisions and drive better business performance.

If that sounds hard to achieve—in all honesty, that's because it is. But the siloed, ad hoc approach to risk management that too many organizations still use today doesn't do them much good either. There are simply too many risks out there, and a fractured approach leaves executives and boards reacting to events, rather than understanding them and then advancing business objectives anyway.

Integrated risk management (IRM) is a better path, but one that depends on strong corporate culture, thoughtful policies and procedures, and shrewd use of technology. Aligning those elements in the right way is a gargantuan task, leaving many to wonder whether IRM truly is a tangible goal that's worth the investment

The purpose of this eBook is to explore that conflict. Business leaders need a better understanding of what IRM can provide, what the business case for it is, and the steps an organization would need to take to reap all the gains that IRM promises. We've outlined how to do this in the following four sections.

First, define IRM clearly

An organization can't implement IRM successfully without a clear understanding of what it is—and nobody can blame risk assurance teams or corporate boards for feeling confused on that point.

IRM is the third significant acronym to streak across the risk assurance world in the last 15 years or so, preceded by GRC (governance, risk, and compliance) and ERM (enterprise risk management). All three encompass the same basic concepts: achieving business and compliance objectives, reducing uncertainty, and acting with integrity.

So what's the difference among the three acronyms? Has a board that's been focused on GRC or ERM for the last few years wasted its time, when IRM should have been the focus?

Not at all. On the contrary, all three are so similar that whatever investment you've already made will still prove valuable for what's next.

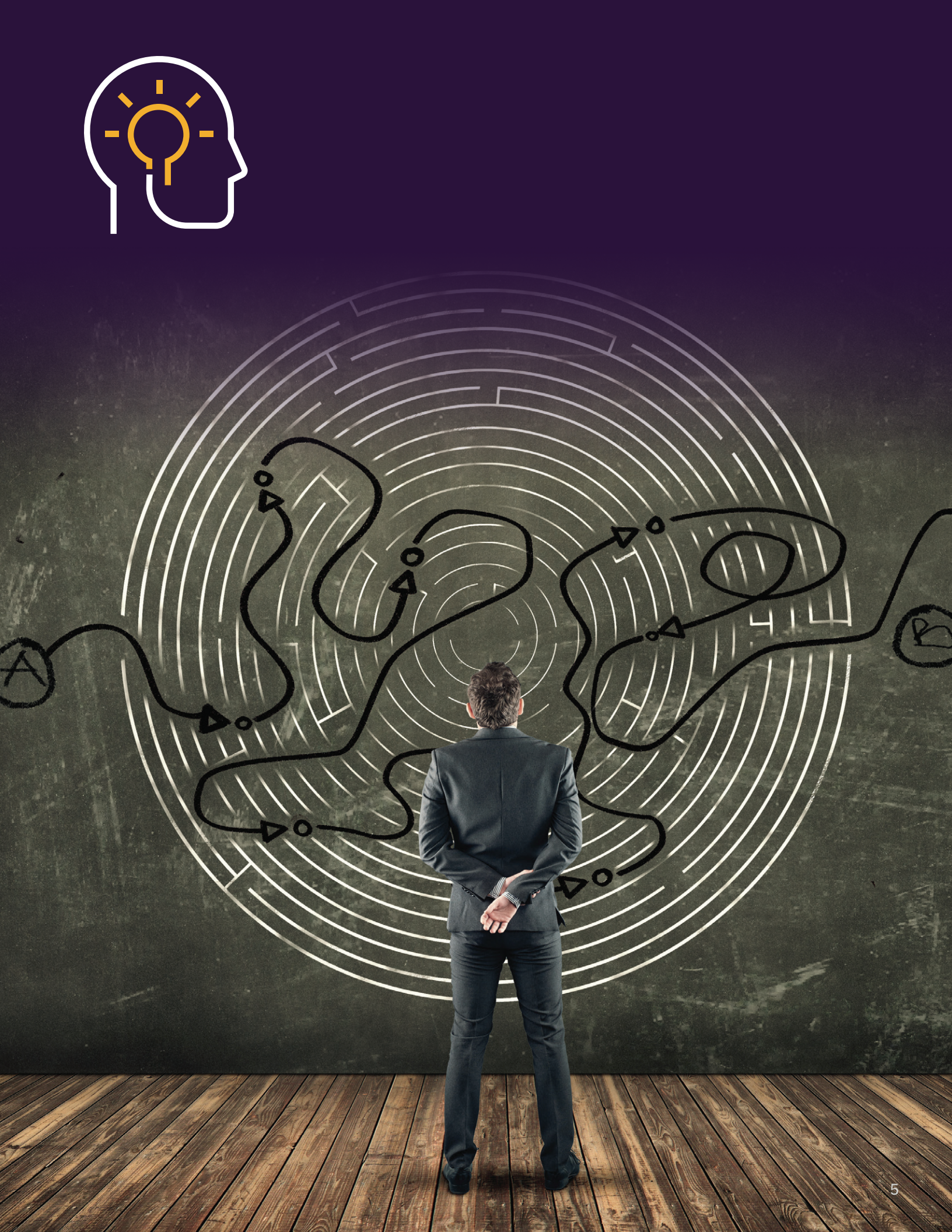
What's next should be an ability to identify, monitor, and manage all enterprise risks according to one larger program; and that program should be integrated into corporate strategy and decision-making. Specifically:

Risks should be mapped to business objectives, so senior leaders can understand the risks they are accepting with their strategic choices.

Internal controls should be tested, remediated where necessary, and monitored, so executives can be more confident as they make risk-versus-reward calculations.

Reporting of risks or internal controls should be robust, so the organization can assure all its stakeholder groups—regulators, investors, employees, customers, business partners—that it does have risks under an appropriate amount of control.

That's how risk assurance leaders should define integrated risk management: as a set of organizational capabilities, more than a sector of the software industry. And those capabilities will let an enterprise thrive in today's highly volatile business landscape.



Second, build the business case for IRM

The previous section defines what IRM is. Then comes the next inevitable question from the board or senior executives: "Why are we supposed to invest in this, exactly?"

Risk assurance leaders can articulate at least three main reasons. (We define "risk assurance leaders" here as any audit, risk, finance, or governance professional; although as you'll see further below, internal audit leaders are especially well-suited to lead this charge.)

01 Financial reasons

The cost of risk failures can be exorbitant, so investing in IRM can be justified on those grounds alone.

For example, the average cost of a data breach in 2019 was $3.92 million; when the breach happened via a third party, the damage jumped to $4.29 million[1]. The average cost of an investigation into violations of the Foreign Corrupt Practices Act is $1.85 million per month—and the average length of an investigation is 38 months![2]

We could go on from there, with statistics on revenue lost from critical system failures, or penalties for price-fixing schemes, or settlement costs for class-action lawsuits over discrimination claims, or many other risk failures. The point will always be the same: that the cost of a risk failure is rising dramatically. All organizations are destined to experience such a failure eventually, and large organizations usually face multiple risk crises at any given moment. Whatever you might spend to invest in IRM, it won't cost anywhere near as much as poor risk management does.

"the cost of a risk failure is rising dramatically."

[1] **IBM,** *2019 Cost of a Data Breach Report*
[2] **Stanford University,** *FCPA Clearinghouse*

02 Governance reasons

Boards, and particularly the audit committee, are overwhelmed with risk issues that they need to oversee. They need a better and more concise understanding of the organization's risk posture, which is what IRM strives to convey.

For example, Protiviti's 2020 survey of enterprise risks (published before the pandemic, we should note) identified the top 10 risks that board directors and senior executives worry about—and survey participants flagged seven of the 10 as "significant risks."[3]

The C-suite and the board are not the only ones demanding a better sense of the organization's risk management. Investors want a better sense of corporate risks, especially around environmental, social, and governance issues. Customers or business partners want more assurance on cybersecurity, including the security of vendors your organization uses. The versatile reporting that should be part of IRM serves all those needs.

03 Efficiency reasons

The plain truth is that many organizations do conduct extensive risk management already, but those efforts are siloed from each other. IRM is about bundling all those efforts together so senior leaders can see the full picture of activity.

Without that larger view, audits of various risks might be duplicative. That drives up costs and exasperates executives in the First and Second Lines of Defense: "We have to answer all these questions again? Didn't we just do this?"

Even worse is the opposite: risks that go overlooked, either because nobody told internal audit that the risk had changed or because people believed somebody else was responsible for monitoring it: "Why did our controls not work? I thought we handled this!"

So for multiple reasons, and to multiple audiences, the business case for IRM is compelling—at the conceptual level, at least. Then come the details of exactly what IRM should do.

[3] **Protiviti,** *'Executive Perspectives on Top Risks,' December 2019*

Third, develop the capabilities of your IRM program

An effective IRM program will use technology in several ways to streamline the assessment and monitoring of risk, as well as testing and remediation of internal controls, as much as possible.

Better risk mapping.

An IRM program should map the organization's risks—compliance, financial, operational, security, litigation, and more—based on their importance to business objectives. That helps risk management teams understand what risks pose the greatest threat to the organization's goals, so they can prioritize mitigation efforts appropriately.

For example, a nonprofit charity might have the objectives of raising money from donors, preserving cash for its charitable cause, and staying in compliance with regulatory obligations. Cybersecurity is a risk for all three objectives; a breach could result in regulatory attention, and money spent on IT recovery, and a tarnished reputation with donors. So clearly cybersecurity should be a high priority for risk assurance.

Better mapping of controls.

IRM should also help audit or risk teams map internal controls to various risks, so audit and risk teams know which issues should go to the front of the remediation line.

For example, user access controls are critical to reduce fraud, protect data, enable remote working, and achieve segregation of duties. So at the least, audit teams would know that testing and monitoring user access controls is important; and that remediating any weaknesses in access controls should be a priority. Understanding how important a control might be for multiple risks might even spur questions about control design. (Say, embracing single sign-on and multi-factor authentication, rather asking employees to remember multiple user IDs and passwords.)

Better remediation.

An IRM program should dovetail with internal control testing and remediation. Where controls are found to be lacking, audit teams can develop remediation plans and assign specific remediation steps to control owners. As remediation work proceeds, that should feed into the mapping of risks and controls so the depictions are always up to date.

Better monitoring.

Another goal is the development of key risk indicators, based on mapping risks to objectives as outlined above. Then the IRM program should monitor those risks. For example:

- How many vendors with access to confidential data, without a vendor security audit complete?
- How many resellers or distributors in high-corruption countries with due diligence checks incomplete?
- How many complaints about workplace harassment or discrimination as a percentage of all internal complaints?

The company should have predetermined tolerance levels for each of those risks. The IRM program should then pull relevant data from across the enterprise to monitor those risks, so executives can view the current state of each risk at a glance. Whenever one of those risks exceeds tolerance levels, automated alerts should go to relevant executives so they can investigate and decide how to proceed.

Better reporting.

IRM is about providing assurance; that includes reporting. IRM allows senior leaders to see all the risks the company faces and its progress on various risk management efforts. That comprehensive sense of things can help the board and the C-suite make better strategic decisions, and help operational executives understand the risks they face—and the precautions they should take—on a day-to-day level.

Meanwhile, IRM also allows the organization to provide documentation of its efforts to other parties as well: regulators, auditors, investors, or even consumers. So IRM can help the organization to meet the more demanding expectations of stakeholder groups, providing the data more accurately and more quickly.

Fourth, how audit teams can lead the way

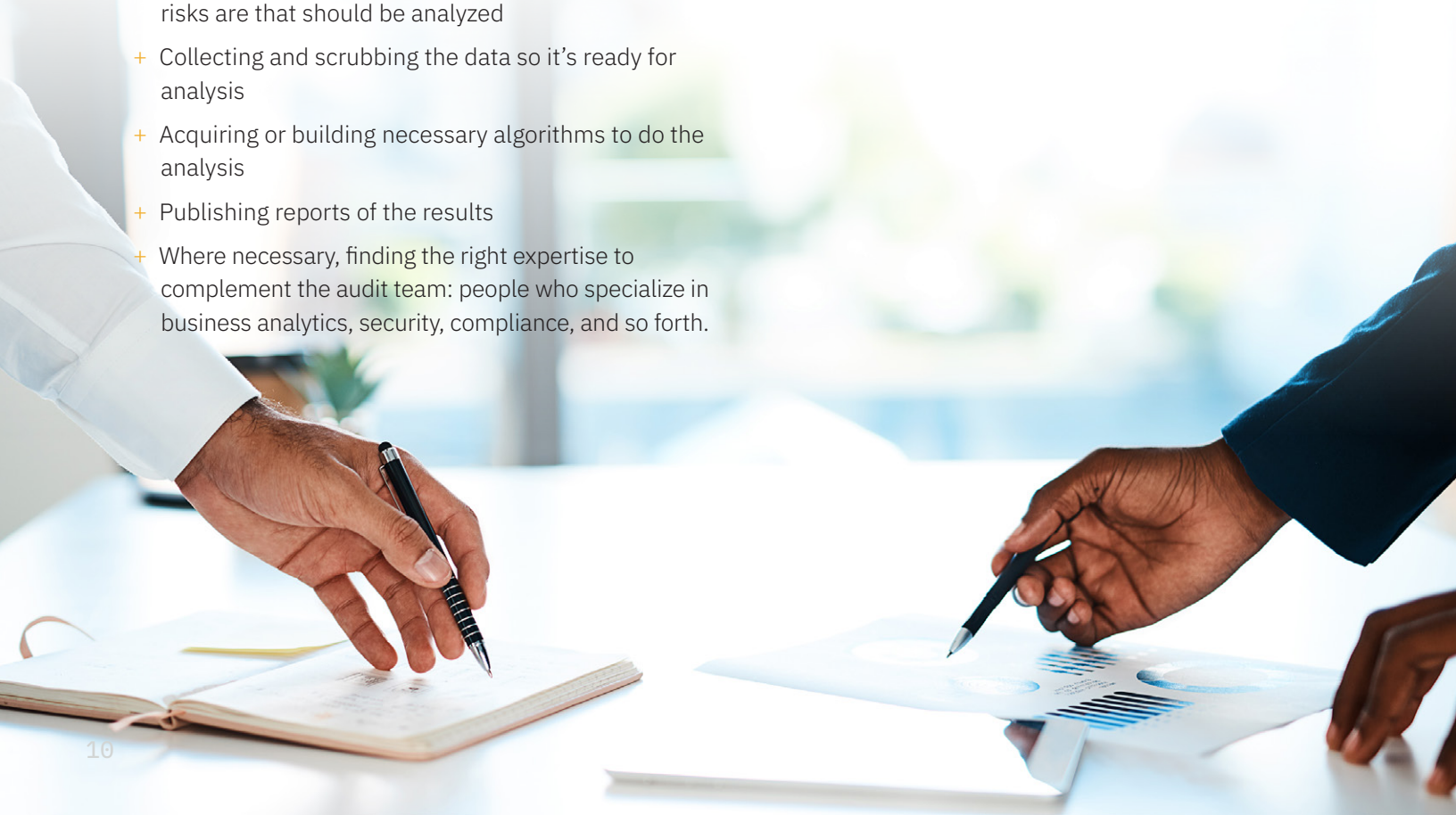
One significant obstacle to IRM programs is that too often, nobody has clear responsibility and competency to get such a program launched. Internal audit leaders are ideally suited to that challenge.

First, **internal audit functions have already been evolving along these lines for some time**. The constant push for more data analytics, demands from the board for better information about emerging risks—those are precursor steps to what IRM can deliver. Audit leaders can build on their prior experience here to lead the IRM charge.

Take the push for data analytics as an example. The challenges for using analytics include:

+ Working with business units to understand what the risks are that should be analyzed
+ Collecting and scrubbing the data so it's ready for analysis
+ Acquiring or building necessary algorithms to do the analysis
+ Publishing reports of the results
+ Where necessary, finding the right expertise to complement the audit team: people who specialize in business analytics, security, compliance, and so forth.

Those are all the same building blocks for integrated risk management. Indeed, audit executives already know what happens next with data analytics once those steps are done: you give those algorithms and analytical tools back to the business unit, so they can monitor the risk themselves. Then audit might circle back the following year to see how risk management is going, or intercede whenever the data shows an unusual pattern that merits immediate attention.



In other words, so far in our example internal audit has used data analytics and collaboration to build siloed risk management—data-driven and continuous risk management, to be sure; but still siloed.

The next logical step would be to bring all those siloed efforts into one consolidated layer of oversight: integrated risk management. That integrated view would let senior executives see what risks exist for the business objectives they have, and how well various parts of the enterprise are monitoring and managing those risks.

Moreover, when any risk grows too great, or some new risk emerges, IRM would let that issue come to the surface quickly, where senior executives can make better decisions about how to handle it: new policies, more training, new controls, or perhaps no action at all, other than to accept the new risk.

Second, there is another benefit of internal audit leading the adoption of IRM: **it makes internal audit a more strategic asset to the business**. Frankly, if internal audit doesn't lead this evolution—who else in the organization can?

No other part of the enterprise has the requisite knowledge of risk assessment, control testing, remediation, and working with other parts of the business. Plus, other crucial actors in IRM include the CISO, the heads of IT and HR, the compliance officer, the general counsel, and the CFO; internal audit already does (or should) work closely with that group anyway. IRM is an excellent way to bring internal audit's expertise closer to the First and Second Lines of defense, and senior executives, and the board.

Conclusion

Integrated risk management is the natural evolution of what organizations have wanted to do—and been trying to do—for years, regardless of the specific label we've put on those efforts.

IRM is about understanding all the risks the organization faces, how those risks might affect its ability to achieve objectives, and what decisions should be made in response to those risks.

Every board and C-suite wants that type of insight; businesses today operate in a world that is too complicated to prosper otherwise. Every organization of any appreciable size now lives in a world that is highly interdependent and highly regulated, with risks coming from all directions.

Audit teams are ideally suited to help the organization achieve IRM because, fundamentally, IRM is about doing four things continuously and comprehensively: risk assessment, monitoring, mitigation, and reporting.

That's what audit teams have provided for years in piecemeal fashion, one audit at a time. Modern technology and data analytics now allows organizations to do the same at an ever accelerating pace—until, eventually, it all blurs into integrated risk management.

This isn't one possible future for risk management, that might happen. This is the future, inevitable. The only question is whether organizations will make a disciplined march toward IRM, or stumble toward the same capabilities in fits and starts. Strategic advantage will go to the former.

Key Takeaways

DEFINE IRM CLEARLY,

so boards and the C-suite understand it. IRM is a disciplined, unified approach to understanding and governing all risks the organization faces, so executives can make better decisions.

ARTICULATE THE BUSINESS CASE FOR IRM,

because it's compelling. Effective IRM will save the organization far more money than it will cost, enhance governance at the board level, and improve efficiency at the operational level.

DEVELOP IRM'S CAPABILITIES.

IRM should map risks to business objectives, map controls to risks, guide remediation and monitoring, and provide versatile reporting.

YES, INTERNAL AUDIT CAN DO THIS.

Internal audit teams are ideally suited to lead an IRM project. Their experience with risk assessment, remediation, and reporting, as well as their collaboration with other parts of the enterprise, is exactly what's needed.

REMEMBER: IRM IS INEVITABLE.

All executive teams and boards already do risk management; some just do it less deftly than others, struggling with one silo of risk at a time. Collaboration and astute use of technology will bring about the same end, more quickly and effectively.

Galvanize

ABOUT THE AUTHOR

Matt Kelly
CEO, Radical Compliance

Matt Kelly is an independent compliance industry analyst and consultant who studies and writes about corporate compliance, governance, and risk management issues.

He maintains a blog, RadicalCompliance.com, where he shares his thoughts on business issues, and regularly speaks on compliance, governance, and risk topics.

In 2018 he won a Reader's Choice award from JD Supra as one of the Top 10 authors on corporate compliance. Before starting Radical Compliance, Matt was editor of Compliance Week, from 2006-2015.

ABOUT GALVANIZE

Galvanize delivers enterprise governance SaaS solutions that help governments and the world's largest companies quantify risk, stamp out fraud, and optimize performance.

Our integrated family of products—including our cloud-based governance, risk management, and compliance (GRC) solution and flagship data analytics products—are used at all levels of the enterprise to help maximize growth opportunities by identifying and mitigating risk, protecting profits, and accelerating performance.

wegalvanize.com