KPMG | servicenow

Raising the bar on risk management

Improving the caliber of your governance, risk, and compliance program

July 2023

kpmg.com/us

Introduction

The technologies and approaches that enterprises use to manage risk and compliance have evolved—and this evolution is creating a moment of opportunity.

When your enterprise gets risk right, it can achieve a more agile and proactive posture that drives organizational value. This creates a foundation of stakeholder trust that makes it possible to realize responsible growth, bold innovation and sustainable performance

Yet the reality is that your legacy risk and compliance technologies may not be adequate to meet the needs of today's world. In the current macroeconomic climate, many organizations are seeking ways to cut costs. At the same time, risk leaders face pressure to support digital transformation with efficient, digitized, and forward-looking programs that anticipate, monitor and respond to business needs and corresponding shifts in the dynamic risk and regulatory environment

Governance, risk and compliance (GRC) vs. integrated risk management (IRM)

For decades, businesses have coordinated their efforts across the functions of governance, risk and compliance (GRC). This approach led to the evolution of technology tools that help businesses manage risk and comply with regulatory requirements.

Today, the acronym GRC is most often associated with those purpose-built tools. As a result, there can be a perception that the term only refers to legacy technology solutions that were built and implemented in silos. In addition, GRC may carry the connotation of a reactive, compliance-oriented approach to risk management. In contrast, the concept of integrated risk management (IRM) has emerged in recent years with a greater emphasis on the organizational benefit of structuring a holistic risk management program across functions and technology to help improve performance and decision-making.

Whether you say GRC or IRM, the critical point is that leading enterprises are increasingly realizing the importance of a programmatic approach to risk and compliance. Such an approach incorporates people, processes, data and technology across a broader range of functions and capabilities — including those outside of traditional risk and compliance teams. These programs are often built on a centralized enterprise platform that unifies operational data from across the company. This enables the three lines of defense to have intentional coordination and alignment, driving organizational value through extensive visibility and a broad view of risk and compliance.

From GRC tools to IRM platform

Modernizing legacy GRC systems and adopting an enterprise-led, programmatic IRM approach can improve the breadth, depth and richness of your organization's risk profile. Enabled by technology, it can promote a proactive risk and compliance posture while enhancing agility and resilience. This allows you to reduce risk and lower costs while surfacing new insights from aggregated data. And you can increase productivity using the modern capabilities of cloud-based platforms.

In this paper, we explore why, when and how companies should modernize their legacy GRC programs to support a **more integrated, collaborative and proactive approach to risk and compliance with IRM.**

Why

Legacy or legendary?

Evaluating your existing GRC technology

Without the flexibility, integration, and automation of a modern IRM program, you may be leaving value on the table. The following questions will help you assess your current risk program to determine whether your legacy GRC technology is still meeting your needs.

1 Are you confident that your GRC technology can support the evolving vision, needs, and risk profile of your business?

In today's risk and regulatory landscape, change is a constant. Legacy GRC tools that may have been adequate a decade ago can no longer keep pace. They often strain under the weight of years of accumulated technical debt, slow and costly feature updates and excessive manual intervention.

In fact, some GRC tools are approaching 20 years old. These older systems lack enhanced reporting capabilities and dashboards. Their interfaces may not conform to current leading practices for usability and accessibility. As a result, these outdated GRC systems can reduce user productivity, and they may even present companies with new risks as the technology becomes obsolete.

Organizations in these situations experience these common warning signs:

- Operational inefficiencies due to manual processes and a lack of automated workflows
- Complex integrations with other tools, or more than one instance of the same tool
- Fragmented data across systems that require labor-intensive data collection and reporting
- Limited ability to glean actionable insights
- Increased audit and regulatory issues and warnings
- Inability to manage the increasing scope and complexity of regulations and their impacts on the business

2 Have your GRC operational costs increased over time?

Over time, legacy systems become expensive to maintain, requiring specialized skillsets and costly infrastructure. Moreover, vendors may no longer offer support for older systems.

The leading causes of increasing costs include:

- Complex customizations and coding
- Extensive re-work on upgrades
- Multiple systems and point solutions

3 How do employees feel about your GRC technology?

The ultimate success and long-term sustainability of your technology solution depends on end-user buy-in, adoption and commitment. If your current GRC tool can't keep pace with changing needs and expectations, employees will often be the first to know. The most common things holding back employee productivity and engagement include:

- Outdated user interfaces
- Poor usability leading to repetitive, complex tasks
- Unreliable data quality, usability, and integrity
- Inconsistent, free-form text fields that obstruct the path to automation
- Lack of scalability
- Rigid workflows with no flexibility
- Limited ability to proactively manage risk.

4 Can your organization proactively manage risk and compliance with its current capabilities?

Legacy GRC technology challenges and pain points can stand in the way of business needs and regulatory demands. Outdated, niche or over-customized tools can't deliver the capabilities of a modern IRM solution. Your organization may be missing out on modern user experiences, data analysis, actionable insights or real-time reporting

Without easy integration with the extensive enterprise data needed to drive continuous control monitoring, legacy GRC tools don't have the flexibility to support ambitious advances. As a result, these legacy systems can stand in the way of achieving program maturity.

If the evaluation of your organization's GRC program surfaces process capability, data and technology inefficiencies, a modernization effort is likely in order. But when is the right time to act? And how do you start? Next, we'll look at when and how to execute a successful IRM transformation.

When to modernize

Is it time to modernize your organization's risk and compliance program?

The timing of your risk and compliance modernization project can have a significant impact on its success. As you consider when to shift from your legacy GRC tools to a modern IRM platform, consider these milestone events to help inform your plans:

- **Technology licenses and contracts**

  As you plan your roadmap, note the timing of any maintenance contracts and renewal dates for software licenses. Planning your data migration with these dates in mind can set you up for a more seamless transition.

- **Platform releases and updates**

  If you are planning to add or incorporate IRM into existing technology platforms, it may be wise to plan around your significant software update releases.

- **Audit and compliance reporting**

  Transitioning to your new program in the offseason, between your annual auditing and compliance cycles, can create the necessary space for change management and end-user adoption.

- **Leadership changes**

  When new executives join the organization or take on new roles, the timing may be right to launch a modernization initiative.

How

Review, reimagine and reframe

Creating a modern foundation for your risk and compliance program

Modernizing GRC capabilities is not a trivial effort—you can't push a button to switch over from one toolset to another. Attempts at this kind of "lift and shift" often result in overinvestment and undervalued outcomes. Instead, successful organizations treat modernization as an opportunity to review, reimagine, and reframe their risk and compliance program, adopting technology and processes that:

- Effect a step-change in program maturity and automation
- Reduce inefficiencies and provide insights for proactive risk management
- Embed a risk-aware culture across the business

Getting started

When you embrace IRM modernization as an exercise for rebuilding your capabilities, you can prioritize your mission, stakeholder experiences, and data-driven insights.

1 Go back to the drawing board

There is no better time to revisit your program's vision than when you are upgrading the underlying technologies. As you begin, examine your processes and foundational data to identify the integrations, capabilities, and skill sets you want to keep, upgrade, or sunset. Moving forward, you can focus on evaluating risks in the wider context of business strategy, working to enable capabilities that meet the challenges of today—and tomorrow.

2 Change the rules

Legacy technology is, by definition, based on program principles that are legacy, too. Organizations that have a legacy mindset often omit important elements like user experience, cloud-based tools, or the processes within the project's scope.

It's important to trade off the "lift and shift" approach for one that refreshes your capability set. True modernization means changing the rules. As a result, your organization can revisit the scope of the program, its strategy, and the technology roadmap.

3 Redesign beyond basics

Organizations have lofty visions. Translating them to outcomes sometimes requires big bets and quantum leaps. Those that go short on execution tend to suffer from value deficit.

By taking the opportunity to redesign from the ground up, you can go beyond your legacy GRC tools—and gain an ecosystem of fit-for-purpose technologies. Specifically, consider an IRM platform that allows for improvements across modern technology capabilities.

This approach to processes and technology will accelerate deployment. Your organization will benefit from standardized code libraries and lower compliance costs over time. Furthermore, you can see improved business performance through actionable insights and better decisions.

4 Remember your data

Organizations tend to underestimate the importance of rationalizing and enhancing data as part of their modernization effort. But it is important to realize that the data supporting your risk program is more relevant than the underlying computing tools.

For that reason, it's important to consider data strategy as an integral part of your migration roadmap. As you move towards an IRM platform approach with a unified data model, you can unlock the value of real-time insights and actionable analytics.

5 Lean into "out-of-the-box" technology capabilities

By reimagining the vision and future-state design, organizations can lean into modern technology capabilities that can easily scale to meet ongoing business challenges, stakeholder growth, and technology changes.

Out-of-the-box functionalities may include native integrations, built-in workflows, dashboards and reporting, mobile interfaces, intelligent automation, machine learning, continuous monitoring and generative artificial intelligence (AI). Taking advantage of these capabilities will allow you to

optimize processes, enable leading practices, reduce implementation efforts and minimize the impact of future upgrades. With this approach, organizations can achieve faster time to value and build a stronger foundation to evolve future capabilities. At the same time, they can reduce technology debt through innovation and modernization.

6 Inspire adoption

Any initiative is only as good as the adoption rate by the stakeholders involved. This can be a crucial factor that derails the success of an IRM implementation.

To modernize your risk and compliance program, you must reprogram stakeholder mindsets along the way. For example, it is important to collaboratively develop and share the project's goals and vision. Then, offer continued progress updates to all key stakeholders. Finally, position your project as an opportunity to learn new skills, build new competencies, and align across business stakeholders.

Bringing the stakeholders and users along with you—from visioning through execution, then post-implementation—increases the odds of success.

These considerations can help guide your organizations through its modernization efforts. As a result, you'll gain the opportunity to enhance trust among stakeholders—including regulators, customers, third parties, employees, and the communities in which they work.

Tips

Launching your transformation

Three steps to IRM success

A compelling case for change outlines the critical drivers for transformation. It can establish consensus among stakeholders, building the support you need to position your journey for success. Follow these steps to begin a successful transformation from GRC tools to a modern IRM platform.

1 Develop a strategy and roadmap

A platform maturity roadmap should incorporate organizational priorities, readiness, platform capabilities and documented process optimization opportunities. Integrating these factors into your roadmap can help to minimize business disruptions and scope-in improvements or advanced IRM capabilities.

2 Collaborate with stakeholders

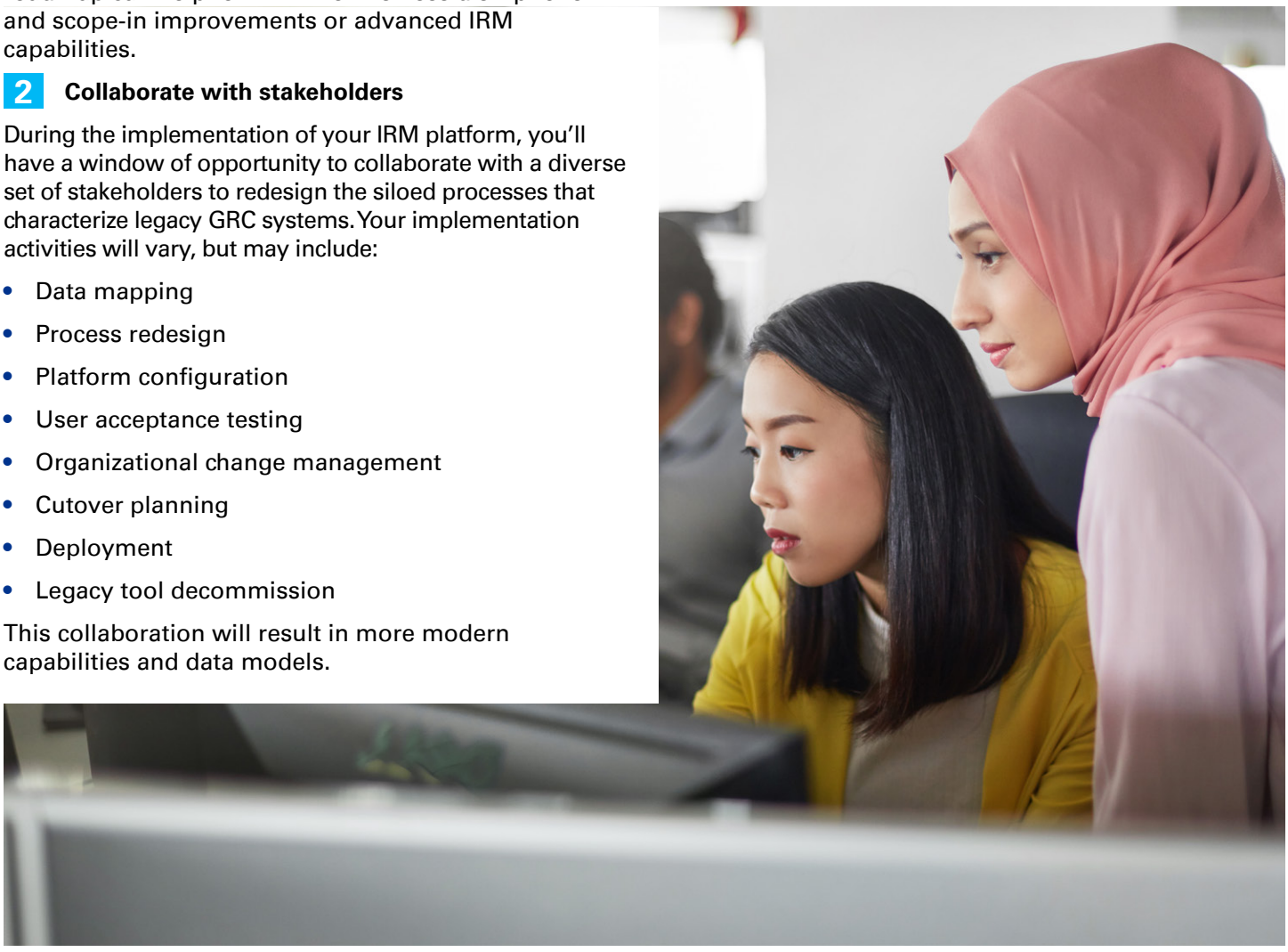
During the implementation of your IRM platform, you'll have a window of opportunity to collaborate with a diverse set of stakeholders to redesign the siloed processes that characterize legacy GRC systems. Your implementation activities will vary, but may include:

- Data mapping
- Process redesign
- Platform configuration
- User acceptance testing
- Organizational change management
- Cutover planning
- Deployment
- Legacy tool decommission

This collaboration will result in more modern capabilities and data models.

3 Enhance governance and operations

To maximize the effectiveness of your IRM transformation, your organization will need robust ongoing governance and operational support. Executive-level governance provides a formal forum for escalation, transparent communication, and high-impact program and design decisions. Meanwhile, operational teams manage the platform day-to-day, addressing the evolving business requirements of stakeholders and in some cases interfacing with external managed service providers.



KPMG Powered Risk + ServiceNow

Reach new levels of IRM maturity

With KPMG Powered Enterprise | Risk enabled by ServiceNow

Organizations that effectively migrate to a modern IRM platform can unlock tremendous benefits to the enterprise. Yet many organizations do not have the time, resources or in-house capabilities to perform a comprehensive assessment and modernization of their legacy GRC technology.

KPMG can help. With our Powered Enterprise | Risk methodologies and ServiceNow IRM technology, you can proactively manage the risk/return equation to:

Inspire stakeholder confidence	Gain insights and flexibility	Drive efficiency and value
Cultivate and maintain the trust of your stakeholders with an integrated, automated and data-driven approach to risk.	Inform new strategies and improve upon existing ones with relevant, forward-looking insights.	Deliver speed to value and get the most out of your risk and compliance data.

Our approach helps businesses to realize value quickly, avoiding the challenges that are typical of traditional transformations. With access to the leading practices we've developed from working with many risk organizations — and pre-configured tools and processes that can be customized to your needs — you can build a more agile IRM operating model and technology stack. As a result, your organization can integrate and orchestrate its risk activities using the ServiceNow platform, existing Configuration Management Database (CMDB) data and other key IT processes.

This holistic approach unifies your platform and data to streamline processes for identifying, assessing, mitigating, monitoring and reporting on risk and compliance exposure. With more accurate and reliable data, your organization can form strong insights on your risk and compliance posture, making you better prepared to respond to changing conditions — while building and maintaining stakeholder trust.

KPMG Powered Enterprise | Risk is a transformation solution enabled by ServiceNow IRM technology. It helps you reduce time spent on worry so you can spend more time thinking about the business.

Out-of-the-box functionalities:

- Built-in workflows
- Chatbots
- Dashboards and reporting
- Role-based mobile apps
- Common, enterprise-grade data model
- Artificial intelligence (AI)
- Machine learning (ML)

Potential Benefits:

- Market-leading, agile, cloud-based capabilities
- Industry-leading risk management processes
- Support with migrating key policy, compliance, risk and issues content
- An array of assets and accelerators
- A global network of experienced practitioners
- Transformative outcomes with reduced delivery risk and increased speed to value

Contact us

Contact us to find out how our methodology can help your organization reach its next stage of IRM program maturity.

Angie Leggett
Advisory Managing Director
Cyber Security Services
T: 614-579-7141
E: aleggett@kpmg.com

Nick Schweitzer
Advisory Managing Director
GRC Risk Transformation
T: 717-816-2112
E: njschweitzer@kpmg.com

James Patten
Advisory Managing Director
GRC Risk Transformation
T: 312-665-1000
E: jamespatten@kpmg.com

Sean Barrins
Managing Director
US ServiceNow Alliance and Sales Leader
T: 206-913-6747
E: sbarrins@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia