KPMG

Enhancing the return on investment for GRC implementation

Estimating and truly measuring return on investment (ROI) for Governance, Risk and Compliance (GRC) investments is no longer optional, but rather, it is a business imperative.

Establishing an integrated, enterprise-wide GRC program is a strategic priority for many large and mid-sized organizations. In a dynamic business environment, companies increasingly need highly effective yet efficient risk and compliance management functions to support growth and sustain operations. While risk and compliance professionals readily grasp the potential of GRC-enabling technologies, their executive leadership must carefully weigh the costs and benefits of a GRC implementation just as they do other top organizational initiatives. This careful calculation is driving the need for GRC stakeholders to create meaningful business cases supported by well-defined program and technology costs, as well as to assert both qualitative and quantitative benefits.

Here we discuss how risk and compliance leaders can make the case for GRC investment with intangible and tangible benefits, including a quantifiable ROI.
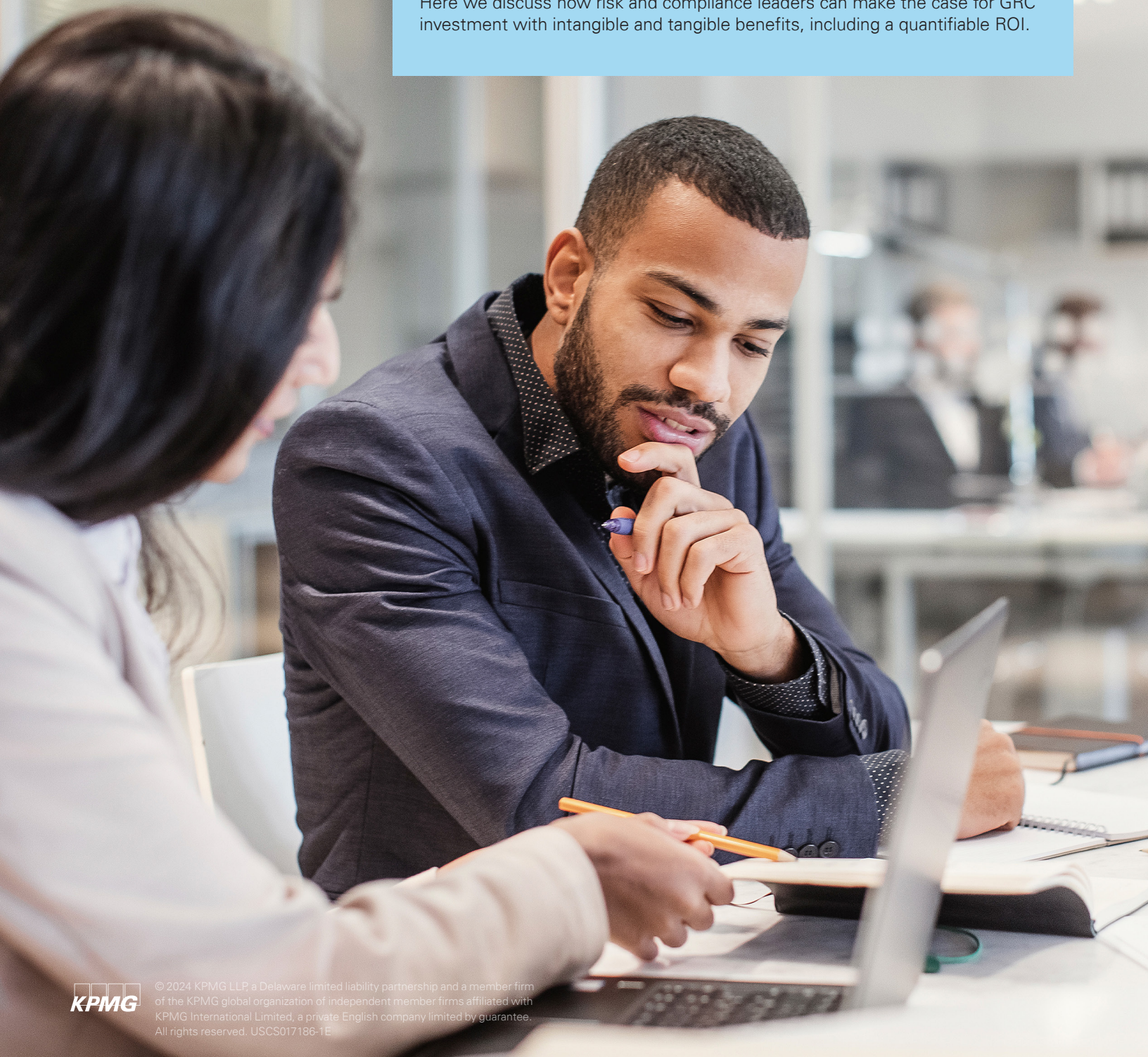
Today's GRC landscape

What is driving organizations to implement GRC?

Organizations seek technology-enabled GRC programs in order to avoid critical pitfalls, from multiple inconsistent sources of data and high risk exposure to siloed risk management processes, just to name a few. GRC is an investment not only to avoid future failures, but to augment strategy, process and culture in a way that supports proactive risk management, increased transparency and informed decision making.

As organizations seek better decision making at the top of the house and continue to navigate the dynamic regulatory environment, investing in GRC will be increasingly critical for operational health and strategic development. GRC transformation can be a significant investment and a heavy lift for any organization. But at the same time, this valuable activity unifies an organization's GRC approach, clarifies the risk and control environment across an organization, and promotes more effective oversight.

Opportunities and challenges

Data is key in aligning and improving transparency in the actions the business performs and reports to management. An organization's ability to create a unified risk and compliance environment depends in great part on its ability to leverage integrated data to develop strategic insight and provide more meaningful oversight of the organization's risk profile, ultimately leading to improved business decisions and outcomes across the enterprise.

The GRC landscape is further complicated by the many capable software solutions available externally, and competing values and concerns within organizations.

Finally, organizations are at different stages in their GRC transformation, and many fall into one of two distinct categories. Those in the first group have started incorporating technology but have yet to create a unified, actionable vision for the GRC organization they want to build. Many in this category have begun to implement GRC technology in several verticals, and are therefore using more than one technology. The second group has not yet undertaken the journey, and therefore has not deployed GRC technology in any meaningful way.

Internal headwinds to GRC implementation

As organizations navigate the global business environment, as well as disparate and dynamic regulatory pressures, there is a strong case for investing in GRC. So what is holding organizations back from pursuing the benefits of a unified GRC vision?

In our experience, organizations that have not successfully implemented an integrated GRC program typically face one of three realities:

- The benefit and return on investment from GRC transformation is unclear, and therefore they have not pursued moving forward from their current functional state despite it being painful and inefficient, and yielding less-than-desirable outcomes.

- One or more internal champions are trying to move the organization toward a unified GRC vision but encountering resistance from leadership around the impact, value and cost of GRC.

- The organization tried several technologies, often across various departments, and failed to create an enterprise vision and solution. They have become frustrated with one or more of their solutions, and the GRC brand is suffering for it.

In each case, there is a lack of clarity in approach, impact and outcome for the organization. Often, internal resistance to GRC transformation is tied to financial concerns around the time and cost associated with standing up an enterprise-wide GRC solution. Additionally, the competing priorities of key stakeholders may delay the implementation of a cohesive platform, reducing the potential benefits.

GRC transformation proponents must be able to answer one key question from leadership: "What return can I expect from investing in GRC?"

Demonstrating returns on a GRC transformation

The benefits of GRC transformation are both tangible and intangible

Ideally, an investment in GRC transformation offers a return that is recognized across the organization, principally in saving work hours associated with various processes, fewer hours overseeing multiple technologies, reduced training time, less leg work in collecting and organizing data, and fewer resources needed to run GRC functions overall.

A successful GRC implementation could result the following:

- Savings through operational efficiencies (e.g., streamlined processes: risk assessment, control testing, issues management)
- Labor cost savings
- Long-term IT cost reductions (e.g., legacy tools)

As a direct result of these benefits, organizations can repurpose their valuable resources to perform value-added risk analysis, deliver process and control enhancement activities, and focus on forward-looking initiatives, all of which can help drive business performance.

GRC program leaders are often required to predict and measure the promised tangible benefits of their GRC transformation initiatives. While there is no one-size-fits-all approach, GRC program leadership can take the following meaningful steps to build their business case for investment.

Listing tangible benefits is easy; quantifying these benefits is the hard part.

1 Estimate current state costs.

- Identify the priority risk and compliance processes (use cases) that will be enabled by the GRC program and supporting technology.
- For each use case, document the current activities performed (e.g., prepare risk assessment matrices, facilitate risk assessment, document and aggregate results, prepare executive dashboards/reporting, etc.).
- Identify participants for each activity and the associated level of effort in hours to accomplish the noted activities.
- Establish a reasonable metric for internal cost associated with each participant. Where organizations do not have a standard metric, a flat rate of $100/hour may be applied. This same variable must be used to estimate future-state labor costs.
- Calculate the total level of effort and corresponding spend across all current-state activities.
- Identify supporting technologies associated with the execution of the use cases and all associated technology costs including vendor licenses, infrastructure and support costs.

Tangible benefits

- Increased transparency
- Ability to proactively manage risk
- Integrated processes and platform
- Enhanced decision making

Intangible benefits

- Efficient risk and control assessment activities
- Enhanced traceability of transactions
- Greater reporting and data integrity
- Minimized legacy technology expenses

2 Estimate future state costs and benefits

- Identify the implementation costs for the GRC program initiative, including licensing, implementation partner and internal project costs.

- For each GRC-enabled use case, document the future activities to be performed.

- Identify all anticipated participants for each future-state activity and the new associated levels of effort. The expectation is that both the number of overall activities (e.g., reconciling data sources), as well as the level of effort associated with future-state activities, will be lower going forward.

- Leveraging the same internal cost metric as the current state analysis, calculate the total level of effort and corresponding spend across all future-state activities.

- Identify the ongoing annual maintenance costs, including annual vendor spend and infrastructure and support costs.

Forward-looking companies often realize some of the following benefits:

Time reduced towards steering committee reporting

Time reduced to manage issues

Time reduced to evaluate vendors

Time reduced to report, triage, and investigate incidents

3 Calculate expected ROI and measure actual results.

- Leveraging the data from the current and future-state analysis, calculate the expected differential in both fixed (e.g., software licenses) and variable costs (e.g., control testing efforts).

- Using the expected differential estimates, establish metrics for key risk and compliance activities enabled in the GRC platform and consistently measure the actual future-state results to determine whether the anticipated value is being realized.

The metrics could include the following:

Financial Metrics

- **People:** Reduced manually intense labor requirements allowing workforce to focus on forward-looking initiatives

- **Process:** Risk reduction leading to reduced penalties incurred due to non-compliance

- **Technology:** Reduced costs by eliminating multiple siloed tools; Eliminate licensing cost; Eliminate infrastructure cost; Eliminate process administration cost

Operational Metrics

- Percentage reduction in audit findings across different compliance programs due to risk reduction

- Percentage reduction in incidents due to early identification of risks

- Percentage reduction in time to manage various governance, risk, and compliance functions

- Manage issues

- Evaluate vendors

- Investigate incidents

- Risk and Compliance reporting

Account for the intangible benefits.

In addition to tangible, quantifiable benefits, the "intangible" benefits and value of establishing and empowering an enterprise GRC program include the following:

- Improved transparency and collaboration driven through use of a common language, converged processes, and an integrated technology platform

- Automated risk and compliance processes and a structured common workflow

- Early warning indicators that enable the organization to anticipate potential events and proactively respond to mitigate and avoid unwanted surprises

- Enhanced insight to enable risk-informed decision making

- Improved issue identification and remediation

- Integrated view of issues and risks to support effective risk management

- Increased business performance through meaningful reporting

- Capability to proactively and efficiently manage compliance to a variety of regulations and industry standards

- Coordinated platform governance including a change management program with defined roles and responsibilities

- Gained operational efficiencies and a consolidated view of risk and compliance activities.

Define the business value.

GRC enables your organization to understand and operate within identified and well-articulated parameters designed to help the business thrive. Ultimately, the development of a business case should answer the question, *"Will our GRC investment enhance functionality and deliver business value?"* To answer, there are several key frames to consider:

- Does our GRC program vision align with our organization's vision, mission and values?

- Does our desired future state help us, as a whole, to deliver additional value to our customers, stakeholders and partners?

- Does the incorporation of an enhanced and intentional GRC program further our organization's strategic business objectives? Examples include:

- Profitability, including enhanced operational savings

- Positive market reputation, including ability to attract and retain talent

- Strong internal control environment, including compliance with laws and regulations.

Each of these factors will be unique for each organization, and the list of criteria will vary. More importantly, the GRC team must be able to act against the defined criteria and realize the value and ROI that is outlined. This cannot be accomplished by simply implementing a GRC technology solution in a vacuum; the GRC team must maintain close adherence to the program's vision.

ROI throughout the GRC lifecycle

A successful GRC transformation relies on six key lifecycle components, each with its own ROI considerations. GRC programs that fail to manage and execute against them can struggle to realize their projected returns.

01 Vision and strategy

Description

Supporting the organization's vision while defining and managing a GRC vision that is in perfect alignment with the organization's key objectives and strategies

ROI considerations

- Establish GRC business case, including investment and benefit targets
- Define and align ROI measures and metrics with key objectives and strategies

02 Convergence and foundational elements

Description

Thoroughly reviewing and refining taxonomies, frameworks, future state process flows, and convergence opportunities.

ROI considerations

- Identify anticipated efficiencies gained via process and taxonomy alignment (i.e., process optimization potential)

03 Program management

Description

Designing and implementing project governance, including reporting, project planning, timeline management, and resource management.

ROI considerations

- Identify anticipated efficiencies gained via process and taxonomy alignment (i.e Establish investment and benefit measurement and reporting requirements throughout the project

- Routinely measure actual project performance vs. targets, research variances, and identify improvement opportunities., process optimization potential)
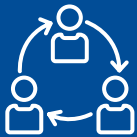
04 People and change

Description

Engaging stakeholders, defining and managing a communications strategy, developing tailored learning and development programs, and guiding a human-centric roll-out.

ROI considerations

- Define specific measures for education and awareness to help ensure that stakeholders are actively participating in and learning from their GRC training

- Consistently measure program and technology performance to determine whether user adoption is in line with expectations. Ensure action is taken, including additional communications and/or training, should performance be below target.

05 Vendor selection

Description

Defining criteria and understanding the capabilities of various vendors and solutions; realizing the business case through technology.

ROI considerations

- Obtain examples of historical investment and benefit projections from potential vendors
- Define performance metrics for the vendor and include within your contracts
- Measure vendor performance both during and after the implementation

06 Technology enablement

Description

Guiding and driving technology deployment including design, configuration, and acceptance testing to ensure business outcomes.

ROI considerations

- Define and measure implementation (configuration) and testing (defect) metrics
- For each use case, establish clear historical performance metrics, cost to implement and future-state target metrics; and then measure post-implementation to track real return

In conclusion

Company leaders are demanding ROI on significant company initiatives, GRC implementation included. It's not enough to simply build a strong business case for an enterprise-wide GRC program; compliance and risk professionals have to project and show the results.

Determining ROI on GRC transformation is a challenging but achievable proposition. By establishing clear financial and operational metrics for today and the future, capturing the value of intangible benefits and focusing on the entire GRC lifecycle, organizations can project an ROI despite often hard-to-quantify value.

Armed with demonstrated financial returns, GRC professionals can advocate across the organization for what they know: GRC transformation can reap a host of benefits, including cost savings that will outweigh the initial investment.

How KPMG can help

The pursuit and realization of a GRC transformation is a critical and often complex undertaking. The effort requires a clear vision, as well as investment in both time and financial resources. As with any investment, management must weigh the initial spend versus the return not only in performance but also future cost savings.

KPMG helps organizations set their long-term GRC vision and progress toward achieving their goals by leveraging our established Enterprise GRC Methodology and the deep experience of our professionals. Our seasoned GRC team helps companies conduct the initial visionary work that sets the stage for a successful GRC transformation; identifies and helps put into place GRC best practices; and works with organizations through execution so that efforts adhere to the program's vision and realize a return on investment.

We also can help assess current state programs and costs, evaluate future state capabilities and solutions, develop a realistic business case for GRC, and assist in the enablement of a holistic GRC program. Ultimately, KPMG works with organizations to identify where they want to take their GRC programs, helping them achieve real and measurable results.

Contacts

Lisa Rawls
Principal
Enterprise GRC Advisory Services
T: 804-306-2182
E: lisarawls@kpmg.com

Nickolas Schweitzer
Managing Director
Enterprise GRC Advisory Services
T: 703-286-8282
E: njschweitzer@kpmg.com

Melinda Mothander
Managing Director
GRC Services, KPMG LLP
T: 703-286-8669
E: mmothander@kpmg.com

James Patten
Managing Director
GRC Services, KPMG LLP
T: 312-665-1000
E: jamespatten@kpmg.com

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

Learn about us: [in] | kpmg.com