Pathway to technology alignment

Optimizing Governance,
Risk and Compliance Programs

kpmg.com

Increased scope of regulatory obligations coupled with the pace of the changes being introduced, and disruptive innovations, are causing companies to implement a more integrated and systematic approach to Governance, Risk and Compliance (GRC). A successful GRC program improves the management of risk and compliance, and also helps to strengthen a company's competitiveness. Despite the promise, however, some GRC programs have suffered from poor technology selection, weak implementation, and a lack of alignment between stakeholder expectations and program outcomes. Nevertheless, GRC programs have succeeded thanks to the adoption of certain good program practices. This report, the third of a three-part series, discusses technology selection and implementation challenges and tips. Part one explains how to help optimize the value of a GRC investment, focusing on the importance of establishing a vision, strategy, and governance structure for the GRC program. Part two examines matters relating to process, people and change management.

Key focus areas of this include:

- Navigating to an integrated approach
- Choosing a vendor
- Fitting the technology to the needs of the stakeholders
- Being realistic
- Tips for technology enablement

Navigating to an integrated approach

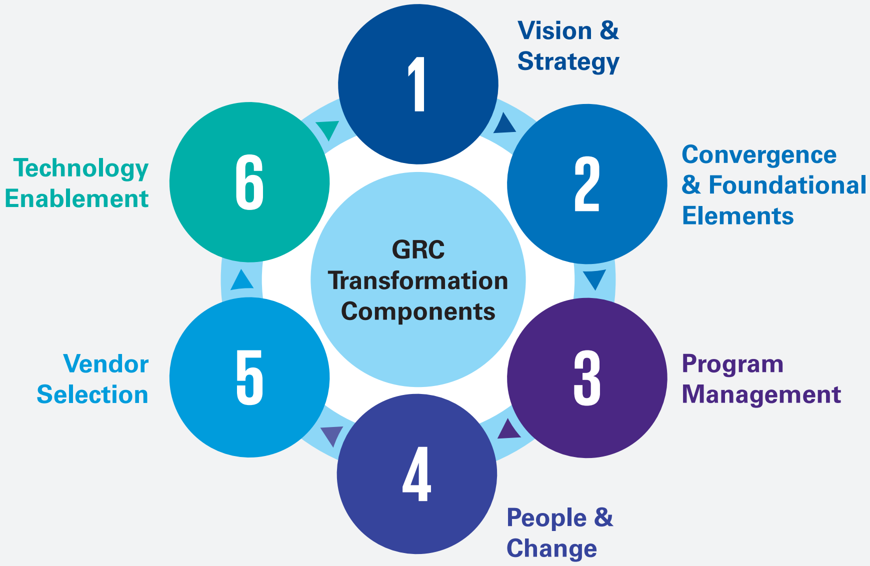
GRC promises an integrated governance, risk and compliance approach that increases risk transparency across the organization, while also enabling more efficient risk and compliance management and driving business. Even with this shared vision, diverse stakeholders typically have varying starting points to their GRC journey, and a bias towards autonomy and unique personal objectives. It is often challenging for diverse stakeholders to sign on to a transformational project in which all must work toward achieving a set of common organizational objectives. Implementing a GRC program is no different. Each stakeholder has his or her own perspective on the program and individual processes that are maturing at different speeds. Similar considerations apply to the implementation of GRC technology. In this respect, the organization must ask itself how it intends to leverage the technology: either in an integrated approach that will cover the entire risk and compliance needs of an enterprise, or one need at a time (i.e., a point solution).

The former is much more ambitious and requires a consensus among all the stakeholders as to the goals for the GRC program and the way to achieve these through technological implementation. The latter is a narrower solution that will address the specific needs of risk and compliance functions individually. Internal Audit, for example, might have an urgent need for a new GRC technology. This is likely to be easier and faster to implement than an enterprise-wide solution, but the two—integrated or point solution—are not mutually exclusive. In fact, in the experience of KPMG LLP, it may be better to launch a new GRC implementation program with the ultimate understanding that this solution may one day support an enterprise-wide approach to governance, risk and compliance; however, start with smaller more mature use cases that can lay the foundation for the enterprise-wide program.

This entails a design that envisages an enterprise-wide GRC program in, say, three years, but begins more narrowly with technological implementation by individual Internal Audit, risk and compliance functions. The design should provide a road map for the entire organization that outlines how and where the program begins, and then shows how, where and when it broadens to encompass other functional areas in an integrated platform. The map, therefore, should not be too broad at the outset, but neither should it be designed to prohibit others from coming on board further down the road. This design will depend on the organization's priorities, the technological needs of each department, and where the individual functions stand on the five-point maturity scale (discussed in the previous two reports) from a GRC perspective.

In choosing a GRC technology platform, organizations are likely to find that there may not be a solution that fits all parts of the enterprise. They need to take a practical approach to this matter. Although organizations may not find a single GRC tool that can cover all business activities and use cases, it will be possible to aim for a technology that meets 70-80 percent of an organization's needs, with the remainder covered by one other solution, either another technology or manual process workaround. The aim should be to achieve a successful GRC implementation with a combination of tools that will provide coverage across the enterprise that supports integrated reporting based on a common language and agreed foundational elements.

KPMG's enterprise GRC life cycle



Choosing a vendor

For the process of selecting a technology vendor, organizations should start by drawing up the request for proposals (RFP) based on the functional requirements and use cases of each stakeholder group. These requirements, which should be weighted and prioritized, are intended to facilitate each vendor's demonstration of the GRC tool's capabilities by guiding their alignment with what the organization is looking for. In addition to evaluating RFP responses and out-of-the-box vendor demonstrations, organizations should also develop a proof of concept. This will allow for hands-on experience with the vendor's technology in a "sandbox" environment, in which the organization's stakeholders can evaluate the tool in a realistic way. This is preferable to selecting the technology first and then afterward providing users with their first hands-on experience.

When selecting a GRC solution, organizations should also consider whether the vendor provides leading-practice processes (such as tailored risk assessments or regulatory change management workflows) that align with industry standards, and which can be integrated with relevant content sources, such as regulatory information feeds. For each vendor demonstration, establish a consistent agenda with specific use cases included so that vendor capabilities can be easily compared. This prevents the vendor from highlighting only the best capabilities of their software. In creating a score card to evaluate each vendor, include attainable criteria that allow for the comparison of the vendors' experiences with similar-sized clients, industry peers, and organizations that have similar uses for the tool and similar user groups. In the evaluation, determine whether the tool will be maintained in-house or by the vendor. Be sure to request references that can speak to the vendors' capability to support your organization's intended maintenance model.

An organization's roadmap should set a sequence of use cases based on maturity, that include realistic measurements of success criteria and that are not too complex; include no more than five use cases or two user groups at a time. As more vendors move toward agile methods of implementation, it remains best practice to capture the most important requirements and to validate the vendor's system accordingly. Many organizations configure their GRC platform in excessive detail, so at the outset agree with the vendor on clearly established complexity classifications for mapping the stakeholder's requirements to the capabilities of the technology.

RFP response scorecard

Attribute	Vendor1	Vendor 2	Vendor 3
Hierarchies, taxonomy, and control inventories	◔	●	◑
Policy management	●	●	●
Risk assessment, testing, and issues management	◔	◔	◑
IT risk	◑	◔	◑
Reporting, dashboards, and KRIs	◑	◑	●
Solution usability	◑	◔	◑
Ease of solution configuration	●	◔	◑
Technical foundation	◑	◑	◑
Implementation history	●	●	◑
Summary rating	◑	◔	◑

Legend

● Fully mapped - % of attainable requirements

○ Partially mapped - % of unattainable requirements

Fitting the technology to the needs of the stakeholders

In deciding which technology to select, it is important to gain agreement among the stakeholders on the future use of the GRC system. Try to cast the net as widely as possible in order to understand who the primary stakeholders are and what they see as the most urgent needs to be addressed by the technology. Control testing, for example, is vitally important because it is used by several different functions (i.e., Internal Audit, Compliance, Financial Controls) that need to reach agreement on which capabilities will be needed from the system.

Next, determine the functionality to be optimized. In certain areas, the organization might perform a simple risk assessment, but the aim with the new technology will be to make the risk assessment more robust, using interconnected data and quantitative metrics that move the assessment, for example, to a higher level of maturity. It is important to build into the roadmap the expectation that the technology will enable the organization to move up the maturity curve.

It is also necessary to revisit the risk and compliance process workflows to understand if the new system is enabling the GRC process. In the past, GRC information was shared among the functions by telephone call and email. In the future, the organization is going to build higher functionality into the new system that helps ensure that risk assessments, control testing, and issues management move seamlessly from one user to another. But, don't underestimate the amount of time it takes to ensure the workflow is properly constructed and is enabled by the technology. The organization wants to avoid users falling back on e-mails and telephone calls after the new system is implemented. We encourage organizations to routinely reflect on their initial strategies and desired outcomes to help ensure that we do not fall back on poor behaviors. But even after the new technology is implemented properly, this does not obviate the need for the functions to have robust conversations about risk and compliance. These never go away.

Each stakeholder has a unique perspective on the GRC process.

Being realistic

Building a strong GRC program is a work in progress; there is always room for improvement. The important point is to make sure the organization knows where it wants to be in three to five years' time and is not taking a shortcut to fix an isolated problem. All the relevant stakeholders must understand and agree upon the organization's GRC priorities, and as they go through the process of selecting the vendor, they need to be honest about where the organization is on the maturity curve and where they should reasonably expect it to be in the next three to five years.

This ties back to the point outlined in the first report, that the organization must create a strong vision and strategy around the GRC program and design a realistic roadmap based on this. The aim is to achieve an integrated GRC program, not just an automated one. The ultimate objective is a robust GRC program that enables the organization to move up the maturity curve and to become more resilient and competitive as a result.

Tips for technology enablement

The implementation of a GRC solution is typically driven by the organization's risk and compliance functions; however, care should be given to help ensure that the "Nuts and Bolts" of a technology implementation are not forgotten along the way. The information below identifies some Key GRC Implementation Activities that should be considered within each major phase of the GRC Lifecycle.

GRC Lifecycle Phases and their Key GRC Implementation Activities:

Program and Project Management

- Establish an integrated project plan with key activities, resource allocations and realistic milestones
- Continually monitor progress against the agreed timeline and adjust based upon strong change management principles

Foundational Elements and Business Requirements

- Align core data structures, establish a roadmap for obtaining key content and identify plans for closing content gaps
- Map business requirements to the chosen GRC solution, and identify and prioritize potential functionality gaps
- Review the solution design documents as provided by the vendor, and gain an understanding of how the technology aligns with the business requirements

Development and Configuration

- Actively engage business partners in periodic reviews of the solution throughout the development and configuration activities
- Develop a plan for data migration, and include steps to assess the completeness and accuracy of data prior to updating within the GRC solution

Testing and Defect Management

- Establish an integrated testing plan including sequenced testing activities and resources
- Develop end-to-end testing scenarios that account for both positive and negative testing, as well as access validation
- Define and agree "Go/No-Go" criteria for the implementation
- Document deployment checklists to guide the implementation activities

Training and User Adoption

- Perform a broad stakeholder needs analysis and align training to meet end-user needs
- Create user support guides and FAQs to carry the training into the field

Production Support

- Define and agree levels of production support
- Establish realistic timeframes for providing post-production enhancements, and ensure these follow strong change management principles

Parting thoughts

As discussed throughout the series, the establishment of a GRC program is a holistic journey. The end result may lie more than two years off, but it is best if the implementation program is designed to achieve meaningful quick wins. In this manner, the organization will be able to experience the benefits from an early stage and celebrate them. The people who have their needs met in this way will then be able to pass on the positive lessons to their colleagues and act as champions for the initiative. The enterprise will benefit from a virtuous circle of improved governance, risk and compliance that helps enable business improvements. As we noted in the first report in this three-part series, success will be achieved by aligning the goals of the GRC program with the strategic objectives of the organization. This is not easy, but it is well worth the effort.

Contacts

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

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

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.