KPMG

Vision, strategy & structure

Optimizing Governance, Risk and Compliance Programs

kpmg.com

A vision for GRC

A strong program to manage risk and compliance requires a vision of what a new GRC program is designed to achieve for the organization – what success looks like.

It must address business needs and strategically align to the organization's overall objectives. If the strategic objectives of the organization and the goals of the GRC program are not moving in lockstep, the latter will fail to create the benefits that are expected and may even have a detrimental impact on the organization's risk management capabilities.

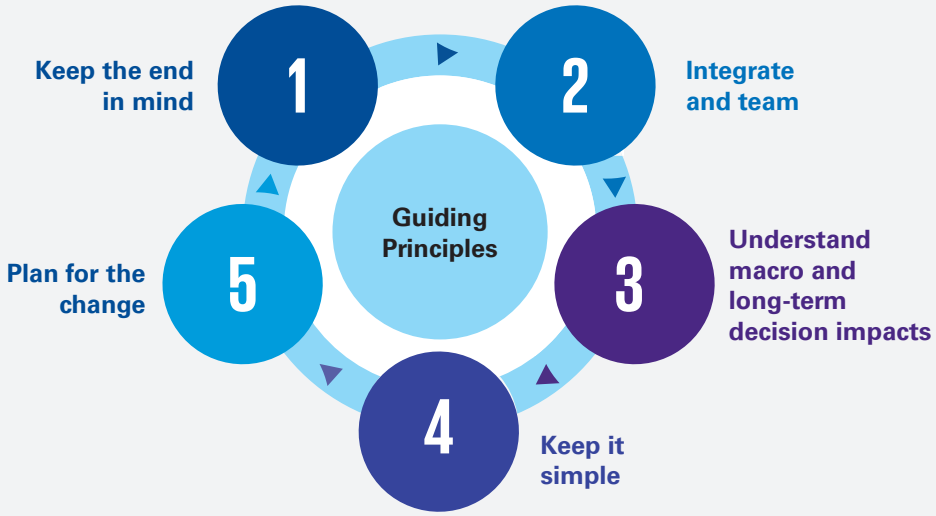
The value of an effective GRC program lies in an integrated approach of risk and control with accurate and timely communication of risk information to the decision makers. There are many critical components to make this happen – including consistent business taxonomies, program governance, process discipline, and always designing your program with the "end in mind". Management needs to understand when risk limits are breached, when new risks arise, and how much risk is acceptable to achieve objectives. This requires an integrated approach where risk and control oversight functions work together by sharing information while still achieving their original mandates. This is a major change for many organizations. Risk functions are more effective if they share information and follow consistent processes that allow them to identify risks and opportunities at a pace matching changes in the market and stakeholder expectations. The value of a GRC program cannot be fully realized unless a shared vision for risk management and compliance is driven by the business.

To create a vision, therefore, requires identifying the different stakeholders who will be expected to participate or contribute to the GRC program. What are their expectations, concerns, and business needs that have to be addressed? While the Board of Directors has oversight responsibility for enterprise risk management, there is a broad range of internal and external stakeholders with a keen interest in the outcome of this program. Although not all stakeholders are likely to be incorporated formally in the process, it is vital that their expectations are taken into account.

Translating stakeholder needs into a plan of action requires a vision that will provide a direction for the GRC program and will set the tone for risk management, and guide compliance activities throughout the enterprise. The vision, aligned with the organization's overall goals, should be understandable and achievable, and contain a set of guiding principles that will operate for the lifetime of the program. These principles define how the risk, compliance, and assurance functions will work together, breaking down barriers to create enterprise value. The principles will encourage business owners to look beyond their span of control and focus on designing a proactive, strategic GRC capability.

The value of a GRC program cannot be fully realized unless a shared vision for risk management and compliance is driven by the business.

Example Guiding Principles



A strategy and roadmap

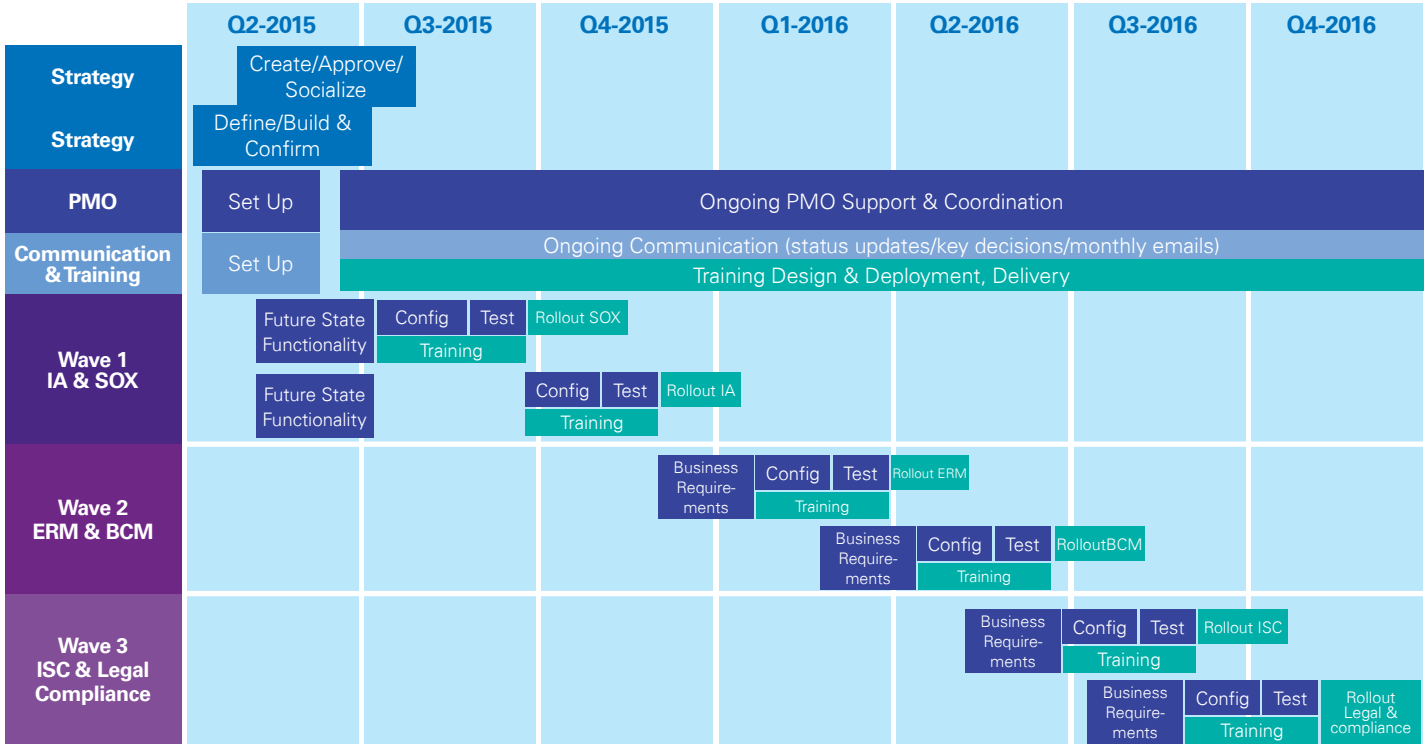
Once the vision has been set and the stakeholders' needs are prioritized, the project team will develop a strategy for the GRC program that will describe the changes to be implemented and the expected effects on the organization's operations.

Critically important is to abide by the shared guiding principles established earlier in the program. As this initiative cuts across many risk and control oversight functions, it may become very challenging to come to common ground on many of the activities needed to successfully integrate risk information across disparate functions. In addition, some compromise will be necessary throughout the initiative; therefore, set the stage early.

Another key component of strategy for a robust GRC program is the design and creation of a roadmap showing how to reach the goals that are set out in the vision and the speed at which the enterprise intends to travel. The timeline of a GRC program is not only controlled by the organization itself, as there may be regulatory drivers. Ideally, the roadmap should be driven by a maturity assessment of the functions that are to be enabled by the GRC technology. A critical success factor is to only enable mature processes. Those risk and control functions that require maturing will be placed further out on the timeline to allow them time to define and operationalize their future state.

There are also a number of foundational elements that should be prioritized and placed early in the roadmap. By definition, these are elements of the technology or common process that all functions will be dependent on and will include the definition of a common taxonomy, common risk and control libraries, and issue management. In addition, often, the GRC technology vendor has not been selected, therefore the timing and activities related to vendor selection have to be built into the plan. How readily the organization adopts and integrates change is the final consideration before putting the roadmap together. The roadmap should therefore enable the vision, incorporate stakeholder expectations, and consider the maturity of the functions to be enabled and the speed of adoption. In addition, consideration should be given to 'quick wins' to show progress and to create positive momentum. This is not an easy task, but critical to allow for visibility of the program, facilitate communications, and budget for costs.

Strategy, vision, and governance roadmap example



A governance structure

A GRC initiative should be seen as a program and not a project. In addition to creating a vision, strategy, and roadmap, there must be a governance structure built for the GRC effort. This is essential. A senior executive, such as the Chief Risk Officer, should be assigned to oversee the program and ensure it fulfils the vision, enabling the program to overcome any significant obstacles in the way of completion. At the top of the governance pyramid sits a steering committee comprised of senior executives from all participating risk and control functions, and they will typically set up a working group to drive work streams and create work products and templates. It is important to include representation from a wide array of risk management and compliance functions to implement a successful GRC program and help ensure maximum efficiency and returns from it.

Building a new GRC program is a complex undertaking that involves many moving parts and a wide array of corporate departments. A project plan is a critical component for implementation, as are roles and responsibilities to clearly assign accountability across multiple stakeholder groups. In addition, a GRC program is intended to be transformational. An effective implementation often entails significant changes to the way people do their jobs. Many stakeholders will be reluctant to change; therefore, a successful GRC journey starts with a stakeholder needs assessment, followed by targeted stakeholder engagement, and stakeholder expectation management. This approach promotes a general understanding that changes are needed, that stakeholders are an integral part of the change process, and that they can adopt those changes in their day-to-day work.

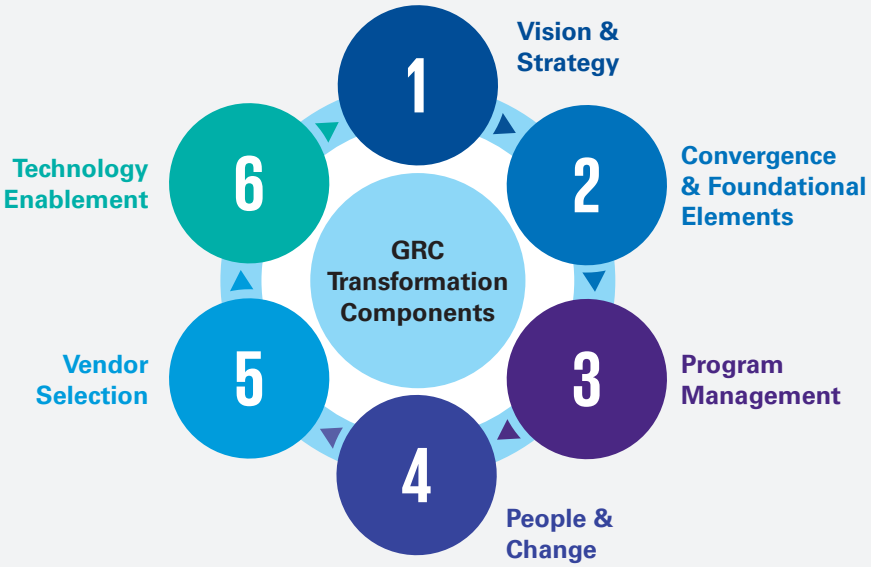
A successful GRC program will not only improve the way an organization manages risk and compliance, but also improve business operations. An organization with a risk- and compliance-aware culture is likely to withstand external shocks and pre-empt threats to its operations and strategy. Business opportunities, risk, and compliance, are simply three facets of a resilient enterprise.

Further details of leading practices will appear in parts two and three of Optimizing Governance, Risk and Compliance Programs. In part two, Governance, Risk and Compliance: The importance of managing change, we discuss the changes required in these areas to attain project objectives. If the company does not successfully manage all of the stakeholders involved in the new GRC program, it won't be possible to coordinate all their processes. Part three, Governance, Risk and Compliance: Implementing the technology, discusses technology selection and implementation issues. Taken as a whole, the three reports provide an overview of the benefits of a transformative GRC program and the pitfalls to be overcome in achieving success.

Business disruptions, the rapid pace of change, and an increasingly stringent regulatory environment has rekindled the debate on alignment and integration of Governance, Risk and Compliance (GRC). Is an integrated GRC an imperative, or simply, a nice to have? For many organizations it has been a costly and painful endeavor, due to a range of causes, including lack of strategy, poor executive buy-in, failed software implementations, poor change management, and a lack of alignment between program outcome and stakeholder expectations. Whatever the cause, organizations need to understand that it is possible to develop a highly successful GRC program with a positive return on investment, provided they adopt certain good program practices. This introductory report, the first of a three-part series, explains how to help maximize the value of a GRC investment, focusing on the importance of establishing a vision, strategy, and governance structure for the GRC program. Part two will delve deeper into process, people, and change management matters, while the last part of the series will discuss technology selection and implementation challenges.

It is possible to develop a highly successful GRC program with a positive return on investment, provided they adopt certain good program practices.

KPMG's Enterprise GRC Life Cycle



1. Strategy

- GRC vision and strategy
- Guiding principles
- Critical success factors
- Executive buy-in
- Governance model
- Functional commitment
- High-level roadmap

2. Convergence & Foundational Elements

- Foundational elements – language across GRC functional areas/ oversight and assurance areas
- Assess maturity of GRC functional area
- Future state process flows
- Convergence opportunities, alignment of shared functionality, and integration points with GRC technology
- High-level business, functional, and technical requirements definition

3. Program Management

- Project goverance
- GRC business case
- Project planning –detailed project plans for each implementation wave
- Budget management
- Scope management
- Project risk management
- Project issue tracking
- Project resource management
- Project plan monitoring and status reporting

4 People & Change

- Stakeholder analysis
- Roles and responsibilities
- Communication plan
- Learning, development and training
- Adoption plan/roll-out

5. Vendor Selection

- GRC business case development
- Buy vs. Build analysis
- Tool selection, RFI/RFP
- Vendor demonstrations, proof of concepts, and RFP scoring

6. Technology Enablement

- Fit-gap analysis and/or traceability matrix – map requiremenbts to technology specifying complexity
- Select implementation approach and detail project plan
- Proof of concept
- Data conversion
- System configuration
- Testing strategy, performance and user acceptance testing
- Deployment check-list

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: **kpmg.com**