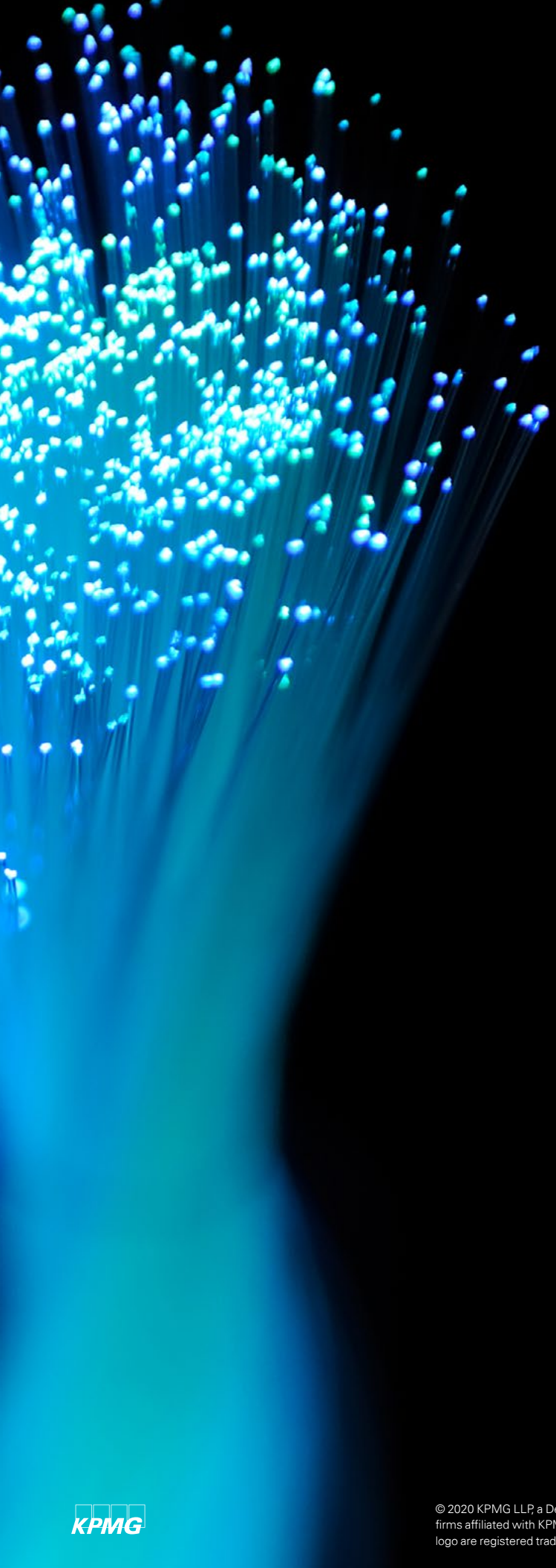
KPMG

Charting the right course

Cultivating a lasting GRC mindset

kpmg.com



Organizations around the world are coming into an adjusted reality after a potent mix of healthcare, economic and political challenges.

It is critical now more than ever to take a hard look at how companies can manage risks and compliance while sustaining a culture that is strong in the face of unprecedented adversity.

A well-established GRC program should have a strong set of foundational principles that can adapt with changing times.

Outlined here are seven topics for organizations to cultivate and practice a forward-looking GRC program that is complementary...

KPMG

Recognize GRC programs are ever-evolving

Standing up a cross-functional capability that thoughtfully brings together a variety of risk, compliance, and assurance disciplines should not be treated as a project with a definite end.

If anything is definite, it is that GRC programs do not have a definite end. It has a general direction of travel to help organizations *enrich the practice of being risk aware* on a repeatable and consistent basis. During this "travel," organizations should expect to set clear intentions, attain milestones, have missteps, and continuously learn from each stage of the program so the organization can be better today than it was yesterday.

We help clients realize this with a practical approach by crystalizing a succinct, long-term vision that sets the tone for the program and its indefinite nature. The vision is shared with all stakeholders—internal business functions, and external regulators and third parties—so they know that they all have a common agenda and a part to play in setting and achieving incremental milestones. This also brings everyone into one fold to establish a culture of trust and reliability, which will come in handy during the thorny portions of the process.

Words and context matter

Oftentimes, as we engage with clients we find ourselves in debates on definitions of risks, threats, and issues. Equally, we find ourselves in situations where the involved parties all have different interpretations of these simple, yet powerful words in GRC.

In our experience assisting clients with GRC programs, we have observed that these words all have distinct meanings depending on the context in which they are used. So yes, words and context matter! Typically, this is a phase in our engagements with companies, where we sift through their existing terms and definitions to rationalize and develop a new risk and compliance vocabulary applicable to all stakeholders.

No matter where you are in your journey, recognize the existing interpretations of key terms and definitions, and establish a clear vocabulary of terms and context in which they should be used. You will soon find that this is an equalizer that lessens ambiguity and helps steer the stakeholders towards the same vision.

KPMG

Encourage diversity

An integrated GRC program, by definition, is a meaningful mix of risk, compliance, and assurance functions. The supporting steering committees and leadership structure should naturally be inclusive of all participating functions, yet also diverse in experience, skills, and points of view.

For example, having a set of linear thinkers or deep experts in risk and compliance is going to inadvertently ignore certain fundamental capabilities required to have a sustainable program. It is becoming increasingly clear that there is a need for experts in data science, analytics, AI/ML and, user experience, as part of a GRC enablement team in addition to a core set of technology risk and control testing professionals. Our more recent client engagements at several organizations—especially those that are highly complex in their organizational setup and needs—have highlighted the importance of having diverse set of skills that are seemingly noncore to GRC domains.

As with any journey that requires drivers, pathfinders, and navigators, it is important to have an open mind about incorporating a diverse set of skills in your programs who can help challenge status quo and set new paths to achieve your goals.

Self-awareness is a good thing

Organizations think about their GRC programs in many ways including world-class, evolved, ineffective and siloed, amongst others. No matter what one thinks it is, one needs to be sure about what it really is. This requires an unbiased and sweeping assessment of the current state of the organization's GRC capabilities. It will give a powerful perspective from where you can re-imagine the program with an eye towards charting a pragmatic course for the GRC program.

As intuitive as it may seem, we find that organizations that are not self-aware about their capabilities often end up with structural issues in their program resulting in irrecoverable investments. On the other hand, client that is fully aware of their capabilities often are able to chart a clear course to success through a practical and goal-oriented set of functional and technological capabilities.

Being comfortable in the eye of the hurricane

In our experience working with organizations, we often find that seemingly complex GRC problems have relatively simple solutions. While this may seem counterintuitive, it is important to get comfortable with this idea, focus on the basics, and start your journey there—similar to responding from within the calm center of the hurricane rather than reacting from the chaos surrounding it.

A surprising number of organizations expect technology products to solve complex GRC programs in a matter of weeks. No complex journey is complete in a matter of weeks. And no such journey is what it seems at the outset. Problems that our clients are solving are frequently buried underneath layers of complexities that first needs to be understood, revealed, and rewired for efficiency and effectiveness. This includes root causes such as programs that lack self-awareness, foundational capabilities, common language, streamlined processes, and communications mechanisms. These collectively manifest as complex problems. Focusing on this manifested problem rather than the root causes is like fighting for calm from the edges of the storm. Staying focused on solving the root causes are much simpler and effective. Successful organizations get comfortable operating in this zone of discomfort to establish foundational capabilities that allow them to respond to the complexities.

Encourage creative confidence

It is hard to avoid a GRC product vendor that says a full-scale program can be "turned on" in a matter of weeks. Little of that is real when it comes to transforming an organization's GRC program because one tool or technology rarely solves all the problems.

While we have observed that our companies today are aggressively adopting new ways of operating their risk, compliance, and assurance programs, current crises have forced many organizations to get more creative than before. With costs being cut, workforces being reduced, and technology being consolidated, there has never been more pressure to push the organization to find creative ways to solve traditional problems. Typically, GRC stakeholders are skeptical about adopting forward-looking technologies because of a potential lack of control of the program and related components. However, at KPMG, we are experiencing a significant uptick in managing risk and compliance in more creative ways than before. For example, shifting from digitizing workflows to AI/ML-based automation, adopting modern product delivery with continuous integration into production, being flexible with gig workforce/contracts, collaborating with industry peers for risk and threat data gathering, and at the same time, emphasizing user experience so that key stakeholders feel welcomed by technologies they use to perform their risk and compliance assessments. With strong indications that the new normal is largely here to stay, it is important to adopt a creative mindset that does not revert back to what was there before, but rather focuses on what should be there in the future under new operating conditions. This will eventually allow organizations to convert GRC programs from cost centers into value drivers.

KPMG

Practice, measure, and repeat

A journey is good only if it has some rewarding experiences. These could be simple milestones and pit stops, and include the ability to find new paths in the event of changes. Similarly, establishing an enduring GRC program should set goals, recognize successful accomplishments, have strategic pauses, and constantly connect with stakeholders to assess their engagement, and ability to adapt to changing environments—be it regulatory, economic, or political.

In working with organizations, this often comes in the context of conversations related to return on investment and the case for change. An effective response to this can be accomplished by establishing objectives, metrics, and continuously measuring progress. A number of tools exist to help, including: objectives and key results, balanced scorecards, key performance indicators, or a combination of those. It is key to remember that this is less about meeting a specific, definite goal, but more about making incremental towards multiple objectives over a period time in the form of an integrated program.

As discussed in this paper, GRC programs are continuously evolving journeys—with a direction of travel that aims to improve an organization's ability to manage the ever-changing landscape of threats including cyber, technology, operational, supply chain, and enterprise risks. It starts with a single step, but it does not have a final step—rather, the journey has to diffuse into your organization's culture and become a way of life. It is usually exciting and sometimes painful, but if you have the right mindset, pragmatic set of roadmaps, and a great band of fellow travelers, it is a rewarding journey that is bound to raise the risk quotient in your organization and contribute to better practices in an organization's management.

Contact us

Prasanna Govindankutty
Principal, Cyber Security Services
E: pkgovindankutty@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