Engaging risk: creating a risk-aware culture through a more engaging GRC user experience
Preface

If you are taking the time to read this e-book, it’s likely you have a certain level of interest in governance, risk and compliance (GRC). There's no shortage of information on the subject. A Google search will throw up all sorts of tips, views and best practices designed to help those responsible for these areas. While created with the same purpose in mind, this e-book takes a slightly different slant – we are sharing our view of what it takes to make GRC part of your organization's DNA, and the potential benefits of doing so. So this is really about the user experience and the risk intelligence that is created by a mature risk management culture. To help give this concept meaning, we’ve coined the phrase “engaging risk.”
Introduction: GRC, it’s kind of a big deal

Let’s start with a definition. According to Wikipedia, “GRC is the umbrella term covering an organization’s approach to governance, risk and compliance. It concerns how these activities are increasingly being integrated and aligned to some extent in order to avoid conflicts, wasteful overlaps and gaps. While interpreted differently in each organization, it typically encompasses activities such as corporate governance, enterprise risk management and corporate compliance with relevant laws and regulations.”

The key word here is “integrated.” GRC enables organizations to put common policies and processes in place across their operation. It is believed to be a more controlled and efficient way to manage risk. At the same time, it can also enable the gathering of information that can then be acted on to run a business more effectively. It’s like a central nervous system. It integrates all the information it receives and coordinates the right activity across all parts of the body, keeping you away from harm. If you stray off course or risks emerge, the alarm will sound and it will get you back on track.
So how important is GRC? You only have to look at the events in the financial markets and the challenges that have loomed over global economies for the last few years. Three fundamental risk management failures could be said to have led to the downturn. First, the failure to link strategy with risk. In other words, when generating business models and strategies, many organizations did not give enough consideration to risk. Second, executive boards didn't have the right visibility of their exposure to risk. It was simply not a focus and, often, the level of risk was not communicated effectively to senior management. Finally, risk management was not a disciplined, core competence. Instead, it was something only done periodically. It should have been embedded as part of daily life.

GRC does not mean just financial controls. It also relates to security, trade, the environment, natural disasters, business interruption, mergers and acquisitions, and health and safety. Another good example of where GRC may have been able to prevent a major crisis is the 2013 European horse meat scandal. The meat-processing industry had allowed a long supply chain to evolve without robust risk management controls. When horse meat was discovered, it sent shock waves through the entire processed meat ecosystem. It has cost those involved millions in terms of audits, fines and corrective action.

“Ninety-seven percent of organizations have made progress in linking their risk management objectives and business objectives ... however ... only 16% of the 97% consider them to be closely linked today.”

There's no reward without risk: GRC survey 2015, EY, 2015
But this is not about scaremongering. GRC was not only designed to keep the CFO out of prison; many people don’t appreciate that it can also be an opportunity to find new and improved ways of running your business. If risk intelligence runs through the core of an organization, it can better inform the decision-making process for strategic and business planning. For instance, such insights can help with upside and downside scenario modeling. So, not only could you reduce exposure to negative outcomes, you could be better prepared to exploit the upsides too. Growth is not without risk-taking. Market-leading organizations are leveraging GRC to ensure the risks are better understood and quantified. This means assessing risk versus reward, as well as the most effective mechanisms for protecting existing assets.

So, GRC is kind of a big deal. Nevertheless, many still regard it as just technology or, worse, as merely a project. At its best, GRC is an intrinsic part of an organization’s culture. It’s a safety net that ensures people make the right decisions when no one is looking.

The rest of this document will explore how you could make GRC an everyday part of your business. It’s about how you engage your people in the best risk management practices.

“Companies that think about risk in the context of their business decisions can be better positioned to managed the risks that drive performance.”

There’s no reward without risk: GRC survey 2015, EY, 2015
Section 1: The importance of engagement for successful GRC

Many GRC projects have suffered the same fate as unsuccessful software implementations. This is because they have relied too much on implementing the technology, and not enough on people and process. As we established earlier, GRC is more than a tool. It’s a business practice.

The message is simple. Keep regarding GRC as technology only and you’ll likely have limited success. Same old thinking, same old results. GRC buy-in is achieved when sustained effort and ingenuity is put into reaching out beyond the risk community and into the wider organization. This doesn’t just mean the end users, but the process and control owners too. The bottom line is that GRC should be part of everyone’s job description. An ethical and responsible approach to managing risk should be part of the very fabric of your organization.

The Open Compliance and Ethics Group (OCEG) calls this concept “Interact.” It is defined as “enabling the capability with technology to manage information so that it efficiently and accurately flows up, down and across the organization, the extended enterprise and to appropriate stakeholders.” The OCEG emphasizes the need for information that is timely, relevant, reliable and secure to be available to the right audiences, enabling them to perform tasks as well as to shape their attitudes.

“Change is the single greatest challenge for organizations in the context of governance, risk management, and compliance (GRC).”
Every day, we witness examples of how a neglected culture can result in serious implications for an organization, including financial penalties, poor customer or employee retention and diminished brand equity. By positively influencing culture, you can heighten the value of risk and compliance across your enterprise. The workforce can then become your greatest ally in potentially exposing new risks, escalating improper behavior and providing valuable feedback to key decision-makers. Engagement is the key.

"Culture, more than rule books, determine how a company behaves."

Warren Buffett, Berkshire Hathaway
Section 2: Embedding GRC in your culture

As mentioned earlier, organizations that are effective and efficient in managing risks to their assets, as well as their growth opportunities, can outperform their peers. Developing this advanced capability takes time and will undoubtedly mean moving through different stages of maturity. It’s a journey. But you have to take your people with you.

As regulatory and compliance pressures have increased, top executives are often now directly involved in GRC practices. They want greater visibility of risk, not only to safeguard themselves and the business, but also to make better-informed strategic decisions. They need their workforce to play their part. Historically, responsibility for risk minimization and compliance has been something managers enforced on employees. However, a downward diktat driven by fear or coercion is not sustainable. Nor is it the approach generally taken by high-performing organizations.

Efficient GRC processes enabled by an integrated technology platform are essential building blocks. But it’s the development of a GRC-aware culture that can take an organization beyond meeting compliance standards and toward leveraging risk management capability for competitive advantage.
We believe there are seven steps, or the seven Cs, for developing a GRC-orientated culture:

1. **Consumer insight**
   Break down the “consumers” of GRC into groups and consider their needs separately. Run workshops or conduct a survey if necessary. Gaining a real insight into different audiences at the beginning helps develop a relevant and compelling engagement program.

2. **Corporate values**
   For desired values to be embraced, people first need to be able to understand them. And they need to be consistent for the whole organization. Your GRC should be clearly defined as part of corporate values, which includes clearly explaining the expected behavior and codes of conduct for individuals and the departments they work in.

3. **Change management**
   Most organizations invest in robust training programs for functions that are explicitly focused on risk management, such as legal, internal audit and compliance. To achieve real cultural alignment in GRC, a change program focused on people outside these formal functions is needed. The more relevant this is to the risk associated with the role of each individual, along with clear rewards and compensation, the better.

4. **Communication**
   Once the change strategy has been defined, an internal communications plan and a training plan is needed. This includes deciding on goals and targets, strategy and rollout schedule, and defining the resources and materials required. Storytelling is a great way to get personal engagement and a technique used extensively for developing culture. For GRC specifically, it is essential for the right behaviors to be demonstrated from the top down. Senior management needs to set the tone and be authentic if the rest of the organization is going to follow.
**Consumer-grade experience**

Technologies that are more familiar outside work can be deployed to enhance the user experience. They can be a huge differentiator in driving a more ethical, risk-responsible culture by helping increase levels of awareness and adoption. We will explore some of these applications and their deployment in greater depth later.

**Community**

In recent times, employees' natural desire to belong to a community has grown significantly. Creating a community that shares experiences, information and insights can help to break down silos, and foster a stronger sense of collaboration and meaning for GRC. Social platforms can enable communities to grow quickly and increase participation, but the approach should be integrated with wider corporate initiatives for maximum impact.

**Continuity**

Many cultural engagement programs have a start, a middle and an end. But if treated like a campaign that runs for a period of time, momentum can be lost after the initial energy and excitement has died down. Continuity and reinforcement is achieved by incentives and penalties to maximize compliance with laws, regulations, corporate polices and values. These all need to be embedded locally, and monitored and reviewed as part of day-to-day business life.
Section 3: Focusing on the user experience

So what are forward-thinking companies doing to take engagement to the next level? They are looking primarily at the user experience. Here’s the thing, usability is driving the era of modern business. Today’s workforce is more mobile, more collaborative, more social and more 24/7 — some are calling it the “connected economy.” If GRC can exploit this trend, people may take much more interest.

Often our experience with technology outside of the workplace is far better than what we get inside it. The experience of doing even the most difficult or mundane task can be made enjoyable with a more usable and attractive tool. For some, GRC practices and policies can be unexciting and hard to understand, and this is why it is even more important to work at making them appealing.
The “engaging risk” principle is about achieving synergy by combining cultural change with the right technology, helping enable everyone in the organization to participate in, adopt and embrace GRC practices. By using fresh, elegant-looking mobile applications, dashboards, interactive games, social platforms and video, as well as training, GRC can be brought to life, made more accessible and, if combined with the right communications around values and behaviors, potentially more entertaining for the workforce. With increased adoption, the benefits sought from GRC initiatives are far more likely to be realized.

The technology emphasis is not about being “bleeding edge.” Instead, the focus is on the integration of engaging tools and interfaces with existing technologies to build solutions that employees can enjoy working with more. Traditionally, most GRC technologies and deployments have focused on managing the back end complexity of GRC. But advances in user experience interfaces, social media tools and the general consumerization of IT in the workplace provides a great opportunity for GRC.

“The ‘engaging risk’ concept was recognized by GRC 20/20 in its 2013 GRC Technology Innovation Awards.”

GRC 20/20
Section 4: In practice – tools and tactics that can help enhance the user experience

There are a variety of tools and tactics that can be employed to help increase user engagement. We focus here on three of the most widely used techniques for helping companies engage risk.

1. GRC reporting and dashboards

Dashboards are a great mechanism for helping find the “needle in the haystack” quickly. They can allow users to participate with GRC information in an intuitive and business-friendly way. They are the front end of an effective technology infrastructure that helps the right information to get to the right people in a timely fashion. They distil information in a form that helps people to understand the risk associated with a particular decision.

Dashboards are a great way to communicate with senior stakeholders. They provide a reporting layer, helping executives to govern risk and compliance using indicators that monitor performance. Dashboards can provide consistent and transparent real-time insights across the enterprise, helping to develop smarter, more risk-aware strategies.

With a more holistic view, it is possible to take a preventative approach to risk to help protect against future vulnerabilities caused by rapidly shifting conditions.

“Respondents identified ‘more effectively leveraging technology across the organization to efficiently manage risk’ as one of the top priorities to enhance the way their organization manages risk.”

There's no reward without risk: GRC survey 2015, EY, 2015
2. Adobe interactive forms

Adobe forms are an effective way to interact with users in order to “crowdsource” their risk intelligence using technology (i.e., Adobe PDFs) that many are familiar with. Crowdsourcing is the practice of obtaining ideas or content by soliciting contributions from a large group of people, especially from an online community.

This approach can make it simpler to encourage users to participate without knowing they are actually inputting into the GRC system. It provides a closed-loop mechanism that allows automation of the aggregation of risk intelligence.

Perpetuating the use of electronic documentation can support security and compliance. It can also help drive greater efficiency. For instance, by using digital signatures, organizations can fully automate business processes, such as filing regulatory paperwork online or conducting legal transactions, without having to print and process forms.
3. Mobile applications

Mobile applications (or apps) are increasingly being developed for business use. Gartner predicts that, by 2017, half of employers will require workers to use their own devices for work. It also believes that over 38% will stop providing devices to workers by 2016.³

Tapping into this trend is key. And let’s face it, apps are powerful vehicles for employee engagement. They can help boost productivity by making it easier for users to participate in GRC-related activities. Authorized employees could have timely access to the systems they need to do their jobs. Managers could review and approve time-sensitive access requests from their mobile device. People can often be more productive as a result. They can perform tasks while they are on the move and approvals happen much faster, helping work flow more quickly across the organization.

A mobile platform can also be harnessed to support “social GRC,” where risk communities connect and collaborate through social networks. For this, the appropriateness of rewards for completion that are visible to all players needs to be considered.
Section 5: The ROI of engagement

The cost considerations for ROI from GRC are not much different from other IT projects. They should certainly include software, hardware, maintenance, implementation and ongoing support. However, the returns can be greater from GRC programs that truly engage the workforce. Of course, you’ve got to give them the tools and develop the right processes. But the focus has to be to support people everywhere in the organization to be more risk aware and understand the risk element in their decision-making. Achieve this, and you could see a better return in each of the three main areas below.

- **Operational efficiency:** By creating a common risk management approach, it is possible to potentially to consolidate processes, remove redundancies and reduce duplication and effort. Through automation, manual intervention can also decrease.

- **Risk mitigation:** If the level of risk is reduced in your organization, then it stands to reason that there will be less of it to manage. Audit costs and regulatory fines can come down, as well as the cost of corrective actions, incident management, reporting and data manipulation. It is also possible to realize some indirect benefits such as lower insurance payments and cost of capital.

- **Business performance:** With a more risk-savvy culture, decisions impacting investments, productivity, partnerships, mergers and acquisitions, and growth could all lead to better financial performance.
Given the huge range of benefits and returns, it's difficult to provide any hard numbers as examples for the kind of ROI you could typically expect from GRC. It's essential that you work with every relevant business function, particularly those that will benefit most from GRC, to identify the potential savings and performance gains. If you can then develop long-term projections (a minimum of three years to create), it is possible to create a compelling business case for GRC.

“Twenty-one percent of respondents indicated risk activities are well coordinated today, whereas 67% indicated they expect risk activities to be well coordinated within three years.”

There's no reward without risk:
GRC survey 2015, EY, 2015
Summary

We’ve explored the importance of GRC, the potential benefits and what it can take to make it a source of real competitive advantage. Undoubtedly, establishing a culture in which people do the right thing at the right time is the very essence of GRC.

No matter how strong the business risk processes and controls, the people in the organization won’t make the right decisions unless doing the right thing just comes naturally. This cannot be taken for granted. It has to be a conscious and sustained effort to help build a culture that reinforces ethical standards of behavior.

Enhancing the user experience by harnessing consumer-grade technology is a good way to engage the workforce in GRC. This is because it aligns with how people now access and consume information through more enriching, easy-to-use interfaces. Yes, these are just tools. But many now believe usability is the key to driving adoption.

Make sure the user experience is at the heart of your GRC cultural change program, and it is possible to significantly increase chances of success.
References


2 The GRC Technology Solutions Guide 2011 (version 2.1), The Open Compliance and Ethics Group (OCEG), 2011.

3 David A. Willis, Bring Your Own Device: The Facts and the Future, (Gartner, April 2013).
Want to learn more?

*Insights on governance, risk and compliance* is an ongoing series of thought leadership reports focused on IT and other business risks, and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please view our *Insights on governance, risk and compliance* series at [ey.com/grcinsights](http://ey.com/grcinsights).

---

**There's no reward without risk:** EY's global governance, risk and compliance survey 2015  
[ey.com/grcinsights](http://ey.com/grcinsights)

**Maximizing value from your lines of defense**  
[ey.com/lod](http://ey.com/lod)

**Centralized operations: the future of operating models for Risk, Control and Compliance functions**  
[ey.com/grcinsights](http://ey.com/grcinsights)

**Step up to the challenge: helping Internal Audit keep pace with a volatile risk landscape**  
[ey.com/iarisks](http://ey.com/iarisks)

**Expecting more from risk management: drive business results through harnessing uncertainty**  
[ey.com/repm](http://ey.com/repm)

---

**Unlocking the value of your program investments: how predictive analytics can help in achieving successful outcomes**  
[ey.com/prm](http://ey.com/prm)

**Harnessing the power of data: how Internal Audit can embed data analytics and drive more value**  
[ey.com/iaanalytics](http://ey.com/iaanalytics)

**Metrics matter: how Internal Audit can help organizations assess performance measurement**  
[ey.com/grcinsights](http://ey.com/grcinsights)

**Megatrends 2015: making sense of a world in motion**  
[ey.com/megatrends](http://ey.com/megatrends)

**Creating trust in the digital world: EY's Global Information Security Survey 2015**  
[ey.com/giss](http://ey.com/giss)

**Enhancing your security operations with Active Defense**  
[ey.com/grcinsights](http://ey.com/grcinsights)
Contacts

Marcus Götz
Partner, Advisory
marcus.goetz@de.ey.com
+49 89 14331 23471

Gavin Campbell
Partner, Advisory
gavin.campbell@ae.ey.com
+971 4 332 4000

Werner van Haelst
Partner, Advisory
werner.van.haelst@nl.ey.com
+31 88 407 1167

Martyn Proctor
Executive Director, Advisory
mproctor1@uk.ey.com
+44 20 7951 3989
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY’s Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small and medium-sized enterprises, EY Advisory works with clients – from strategy through execution – to help them design better outcomes and realize long-lasting results.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with their clients, as well as an ecosystem of internal and external experts, to create innovative answers. Together, EY helps clients’ businesses work better.

The better the question. The better the answer. The better the world works.

© 2016 EYGM Limited.
All Rights Reserved.
EYG no. 01985-162Gbl
BMC Agency
GA 0000_05058
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/sap

Follow us on Twitter: EY_SAP