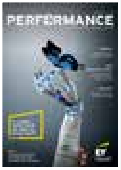
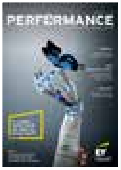


This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Agile GRC: a new approach to governance, trust and risk in the digital age

"Faster, better, more" has become the baseline of expectations in the digital world. Now, it is the time for governance, risk management and compliance (GRC) functions to wake up and participate actively in shaping the future in the digital world. A fresh GRC approach is needed — one that guides and strengthens the core business while providing the agility and flexibility that are essential for innovation and new future business models.



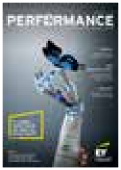
This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Authors

Marcus Götz
Partner, Europe, Middle East,
India and Africa – Risk Transformation,
Ernst & Young GmbH, Germany

Patrick Risch
Manager, Advisory Services –
Risk Transformation,
Global Program Lead Agile GRC,
Ernst & Young GmbH, Germany

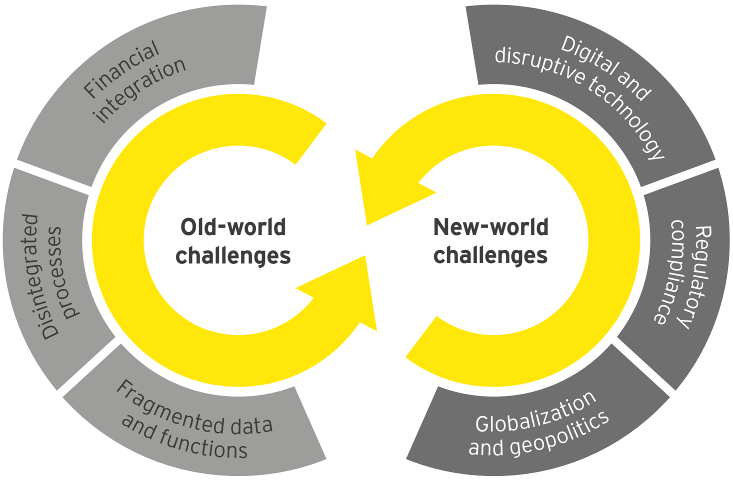
Benjamin Neuberg
Consultant, Advisory Services –
Risk Transformation,
Ernst & Young GmbH, Germany

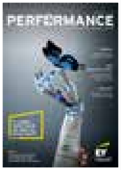


This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Emerging threats in the digital era, such as cyber attacks, competitor shifts or geopolitical crisis, are influencing the future direction of business and forcing their way on to board agendas. As old-world challenges (such as the integration of risk management and financial planning, protecting tangible goods or the fragmentation of data and business functions) collide with new ones in the digital sphere, corporate governance, risk management, compliance management and other "lines of defense" functions need to invest in managing digital risks that matter – and as a result, risk functions need to transform.

Figure 1. The digital economy – challenges everywhere





This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Designing a risk management approach based on agile guidelines and processes, empowered people, cutting-edge technology and analytical capabilities is critical to drive companies forward. It must harness the value of the digital world and protect the organization against the multitude of risks in a volatile and uncertain environment.

The evolution of GRC

Over the past three decades, GRC has evolved in response to a number of large-scale macroeconomic events, as well as the business and regulatory changes they precipitated. In doing so, GRC has continually adjusted its core focus and expanded the scope of risk it covers.

Today, companies face greater uncertainty in a wide array of new and emerging risks. The ever-evolving globalization of competitive markets exposes many organizations to a new breed of risks, many of which were not planned for, nor could have even been anticipated. For these reasons, GRC is entering a new phase in its development, focused on continual monitoring and responsiveness, business decision support and improved shareholder value.

A future-oriented GRC approach can support organizations in multiple ways (see Figure 2).

Figure 2. How a future-oriented GRC approach can support organizations

The market requires a risk solution that:

- Forecasts like controlling
- Creates like information technology
- Enables like learning and development
- Protects like cybersecurity
- Integrates like human resources
- Steers like financial accounting

This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

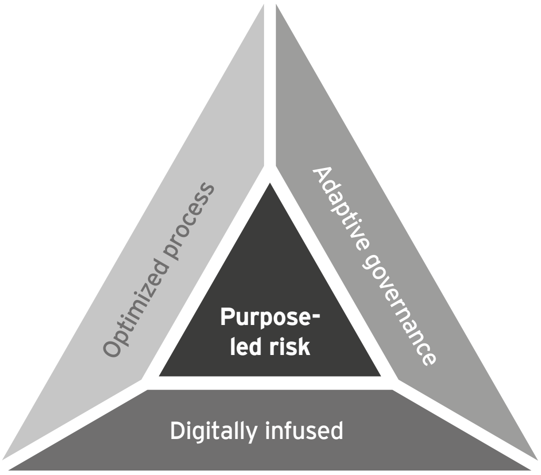
Agile GRC — governance, trust and risk in the digital era

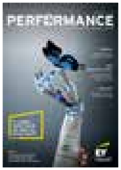
Agile GRC therefore addresses a new way of corporate governance, supported by technology and a spirit of agility and entrepreneurial thinking. For this agile, integrated and future-oriented approach, we defined five key guiding principles that build the foundation for how to operate, empower and make decisions in our next generation of business operations and GRC management:

1. **People first** — business leaders must understand and recognize that properly motivated people are the strongest links in the chain. It is necessary to shape behavior and motivate people to do the right thing; it's not enough to just try to force people to do what they are told.
2. **Purpose led** — it is essential to activate purpose for a changing business landscape and a new GRC environment across the organization. This adds the right insights to help guide decisions.
3. **End-to-end centric** — future success is based on the essential capability of being able to take the customer's perspective (both internal and external) into consideration across all GRC-related functions, activities and outputs.
4. **Multilane speed** — ensuring that the right governance, processes, capabilities and enablers are in place to address the different demands of business models, areas and lines of business.
5. **Fully digitalized** — mobilizing a technology portfolio that digitalizes optimizes all risk and compliance-related activities, embeds them into the organization and end-to-end processes, and engages all stakeholders based on their individual needs.

GRC is entering a new phase in its development, focused on continual monitoring, business decision support and improved shareholder value.

Figure 3. The four key components of Agile GRC



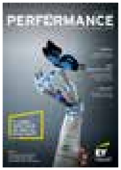


This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Using these key guiding principles, the Agile GRC approach is built on a framework of four components:

- **Purpose-led risk – making risk meaningful:** the purpose-led risk approach aligns the cadence of strategic and business functions with the velocity of risk and opportunities to provide timely information and forecasting on key business drivers and values beyond the financial impact.
- **Adaptive governance – governing performance and risk:** the future of corporate steering and risk governance is based on an integrated and adaptive approach of performance and risk management that is enabled through transparency, agile collaboration and business-centric elevation.
- **Optimized process – managing compliance in a smarter way:** this includes ensuring that regulatory changes and risk recognition are implemented in days rather than in months; securing the integrity of the organization and its people; and governing risk-based steering using holistic control optimization to enable trust and secure relationships in a performance-based manner.
- **Digitally infused – turning data into multispeed action:** excellence through transparency is rooted in a GRC approach based on digitalized and intelligent applications and services. Using technologies such as blockchain and machine learning is just the first glimpse into the future of intelligent risk and compliance solutions.

To understand the full scope of the Agile GRC approach, a closer look at the four components within the approach is necessary; hence, they are examined in the remainder of this article.



This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

1. Making risk meaningful

Agile GRC needs a component as its centerpiece. We believe this will be "purpose-led risk" and that this approach will be the next evolutionary stage of enterprise risk management. The objective is to align risk and compliance management initiatives with the organization's purpose to cover all aspects of its strategy. This includes everything from mission, vision, brand and legacy, to culture, values and people. The approach includes frameworks such as The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 2016 enterprise risk management framework[1] and the International Integrated Reporting Council's (IIRC) Integrated Reporting.[2]

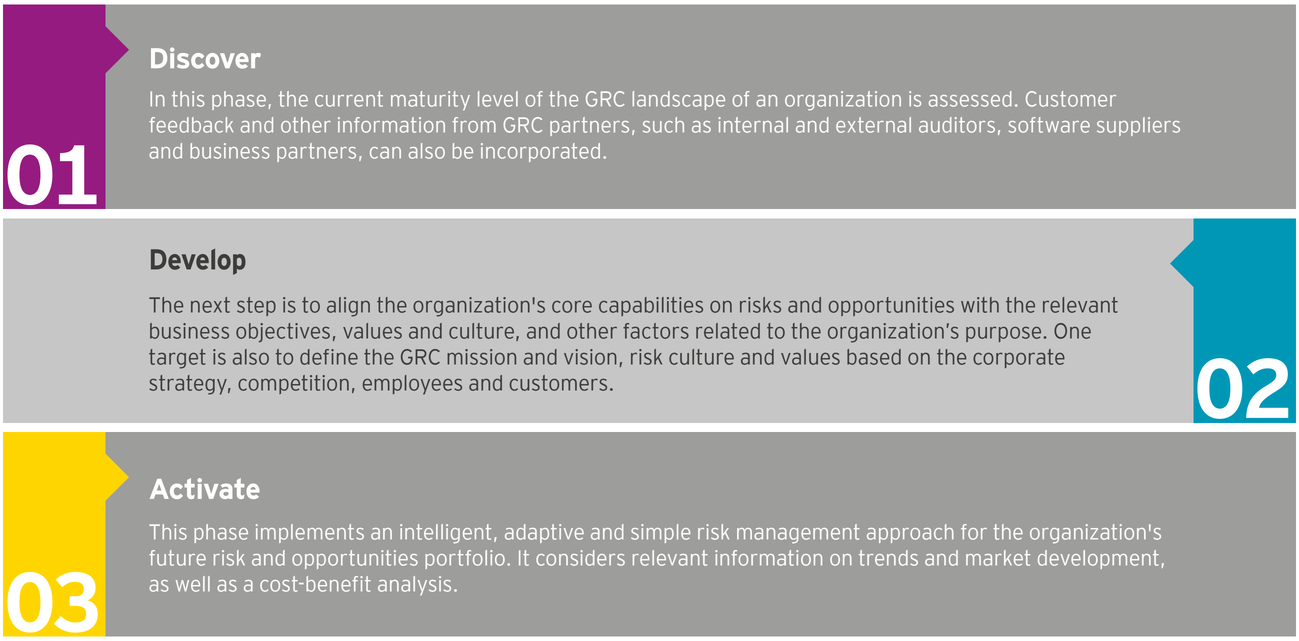
The intention is to create a "single source of truth" that defines one single risk and compliance management approach for the entire organization. It is important to make the approach as simple as possible to secure stakeholder buy-in. Therefore, the EY approach comprises a three-step model involving GRC-affected groups, which we further divide into GRC partners, GRC functions and GRC customers.

What this overview demonstrates is that practically all areas of an organization are affected by Agile GRC.

[1] *Enterprise Risk Management: Aligning Risk with Strategy and Performance*, COSO, 2016.

[2] https://integratedreporting.org/, accessed 14 August 2017.

Figure 4. How to start the journey — the three-step model



Discover

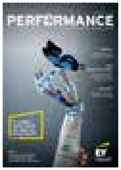
In this phase, the current maturity level of the GRC landscape of an organization is assessed. Customer feedback and other information from GRC partners, such as internal and external auditors, software suppliers and business partners, can also be incorporated.

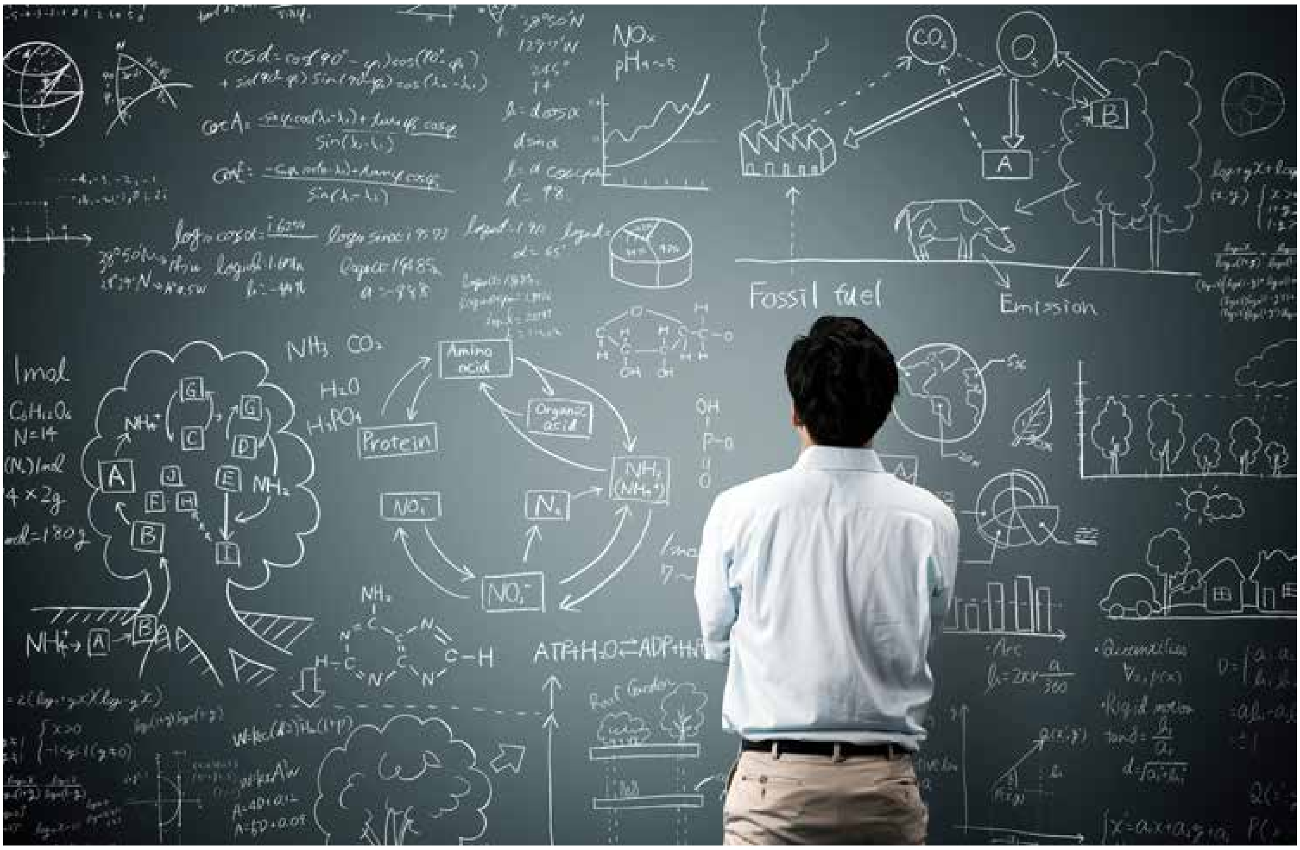
Develop

The next step is to align the organization's core capabilities on risks and opportunities with the relevant business objectives, values and culture, and other factors related to the organization's purpose. One target is also to define the GRC mission and vision, risk culture and values based on the corporate strategy, competition, employees and customers.

Activate

This phase implements an intelligent, adaptive and simple risk management approach for the organization's future risk and opportunities portfolio. It considers relevant information on trends and market development, as well as a cost-benefit analysis.





The Agile GRC approach extends the classic circle of stakeholders relevant to GRC issues. Compared with conventional GRC functions, Agile GRC is an end-to-end approach involving diverse external, as well as internal, sources in the process.

2. Governing performance and risk

The objective of "adaptive governance" is to guide all aspects of corporate governance, risk and performance management, as well as compliance and regulatory aspects. It can manage the risk and opportunity portfolio of programs, projects and operations, align their purpose and consider the risks. Therefore, adaptive governance can make GRC operations leaner and more integrated into governance and process capabilities, enabling agile collaboration and multispeed modes to manage an organization's risk portfolio and support strong corporate performance.

Figure 5. Purpose-led risk as key to a stable core

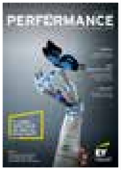
1 **360-degree view:** enabling better business performance through a 360-degree risk integration in objectives, processes and capabilities

2 **Purpose-based risk traceability:** measuring strategic objectives and their achievement, and gaining risk and opportunity insights for the right path

3 **Dynamic risk appetite:** promoting a well-defined dynamic risk appetite into risk policies to balance business objectives and prudent risk-taking

4 **One approach to truth:** embedding a GRC process, based on one common approach, in decisions for all three lines of defense, providing early warning indicators for leadership

5 **Risk optimization:** influencing the likelihood of positive and negative results along the risk bell curve to achieve risk optimization (one of the primary objectives of Agile GRC)



The intention is to create the "single source of truth" that defines one single risk and compliance management approach for the entire organization.

GRC operating models need to support the organization's benefits and commercial management function to leverage investments in building capabilities and solutions – and they will achieve this by acting as the business process, information and organization management governance office. This fresh setup also helps to deal continually with the digital ecosystem, its risk and opportunities, and ensures that the relevant stakeholders are more focused and engaged over the long term.

Adaptive governance demands a change to conventional GRC functions that are based on divisions and run by a hierarchical line organization – instead, GRC functions will become part of a hybrid organization that supports an agile, fully connected network structure with more integration and guidance.

The new hybrid organization changes the classic "three lines of defense" model. Due to better connections between the internal GRC functions, GRC partners and GRC customers, the siloed thinking between the lines of defense will soften. The first (operative management) and second (i.e., risk management, compliance management and quality management) lines in particular will blend. This allows the organization to react faster and be more efficient – and because of the wider involvement within the organization, as well as with the business partner network, GRC operations will become more visible. This can be further enhanced if the GRC model is equipped with an innovation center and a solution hub. Business process management and business information management can be centralized to speed up internal discussions and solution-finding processes.

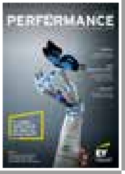
3. Managing compliance in a smarter way

Many GRC functions still conduct risk and compliance processes in a manual, ad hoc fashion. Standardization and optimization of processes is one of many steps that can improve GRC efficiency and effectiveness, while maintaining the agility and flexibility needed by the multilanes principle to provide the business units with the freedom they need to be successful in the market.

The objective of optimized processes is, through standardization, to make processes leaner and more enriched with agile methodologies. This requires a rethink of conventional risk functions and business operations, such as establishing formal procedures for functions, including third-party due diligence and partner screening, or adopting ISO 31000 to manage risk more holistically and consistently.

Accordingly, the optimized processes element of Agile GRC can also be applied to cybersecurity, resilience, and identity and access management so that it is more risk-

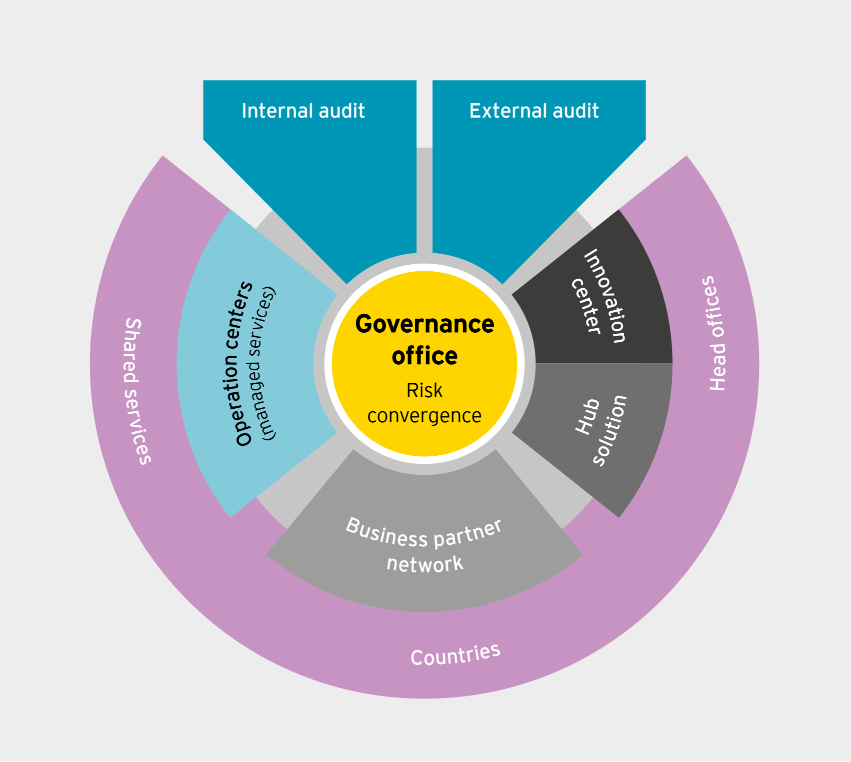
This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

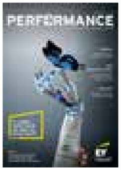


based and agile. Simultaneously, internal control systems, compliance management and risk management can be more standardized and enriched by forecasting, steering and dimensional planning, while Agile GRC is embedded into business operations, thereby better integrating it rather than it merely sitting on top of existing processes. Reward and incentive measurement and multilayer reporting can be enabled through technology and people behavior to provide more risk insights to the organization.

Meanwhile, the most important objective is to embed risk management activities in day-to-day business operations through SMART controls, risk- and regulatory-enabling assessments or risk insights in decision processes – for example, in third-party risk management, simplified deal selling or bidding processes, as well as IT risk and vendor management. Making processes simpler and more standardized, and encouraging people to act with more integrity and be risk-oriented, is crucial. In the age of digital, the involvement (and empowerment) of people is more important than ever before, and so it is for GRC operations.

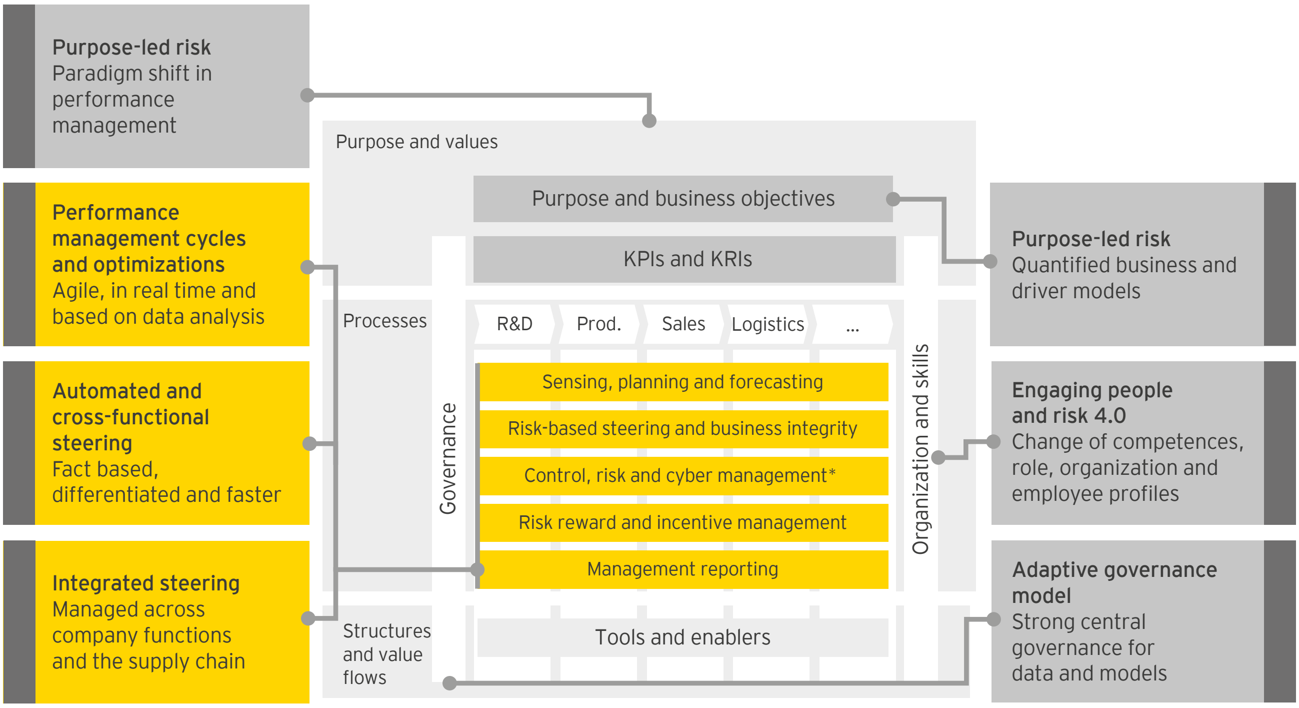
Figure 6. The hybrid GRC function of the future





This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Figure 7. Embedded GRC operations



Purpose-led risk
Paradigm shift in performance management

Performance management cycles and optimizations
Agile, in real time and based on data analysis

Automated and cross-functional steering
Fact based, differentiated and faster

Integrated steering
Managed across company functions and the supply chain

Purpose and values

Purpose and business objectives

KPIs and KRIs

Processes

R&D | Prod. | Sales | Logistics | ...

Governance

Sensing, planning and forecasting

Risk-based steering and business integrity

Control, risk and cyber management*

Risk reward and incentive management

Management reporting

Organization and skills

Structures and value flows

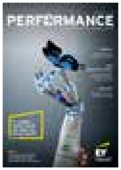
Tools and enablers

Purpose-led risk
Quantified business and driver models

Engaging people and risk 4.0
Change of competences, role, organization and employee profiles

Adaptive governance model
Strong central governance for data and models

* Including advanced identity and access management.



This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

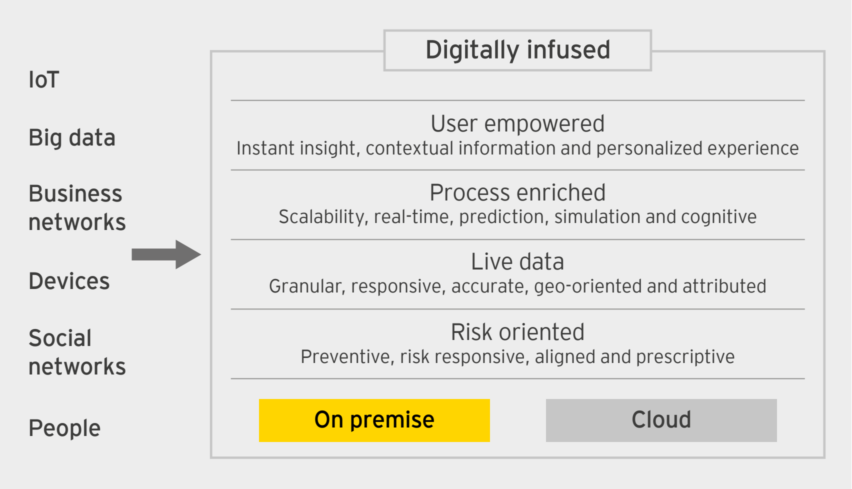
The next generation of GRC architecture makes all GRC functions fully digitalized and connected to allow the best transparency, efficiency and agility for process operations.

4. Turning data into multispeed action

Beyond process and governance improvements, technology implications will extend the scope, consistency and efficiency of existing GRC efforts. This will empower users to support faster decision-making, enrich processes with controls, real-time actions and cognitive intelligence, use live data in response, and be risk-oriented and streamlined. This can be achieved through digitally infused and intelligent GRC technology.

The next generation of GRC architecture makes all GRC functions fully digitalized and connected to allow the best transparency, efficiency and agility for process operations. The enterprise GRC platform has the capability to manage an integrated architecture across multiple GRC areas in a structured strategy, process, information and technology architecture, and leverages the scalability of the cloud to fulfil the needs of a fast-changing environment.

Figure 8. The digitally infused environment



IoT

Big data

Business networks

Devices

Social networks

People

Digitally infused

User empowered
Instant insight, contextual information and personalized experience

Process enriched
Scalability, real-time, prediction, simulation and cognitive

Live data
Granular, responsive, accurate, geo-oriented and attributed

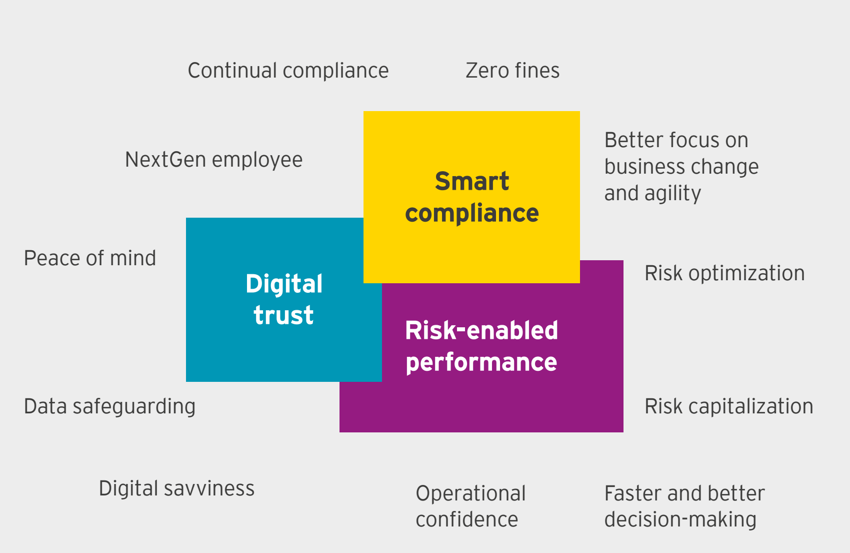
Risk oriented
Preventive, risk responsive, aligned and prescriptive

On premise

Cloud

This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**

Figure 9. The competitive value of Agile GRC



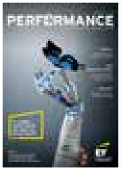
It is important to understand that, in this context, one platform doesn't mean one solution — it can comprise a variety of best-of-breed tools, harmonized by a common platform architecture and data lake for all relevant information that needs to be processed.

In addition to specific GRC technology, the approach is enhanced with other technology, such as using robotics to monitor user access behavior and customer interactions. The use of SMART analytics, artificial intelligence and real-time collaboration in applications such as psycholinguistics, relationship mapping and outlier analysis can result in better insight and a higher speed for more effective considerations of risk and compliance implications in strategic decisions (e.g., mergers and acquisitions, third-party risk scoring or fraud surveillance).

With the rise of new technologies, such as blockchain and other digital-experience tools, GRC functions will probably undergo another step change, encouraging organizations to increase transparency, and change the way they make business decisions and how they will achieve compliance. This will drive GRC and your organization into the next century of business.

Agile GRC creates the desired competitive values

In summary, Agile GRC could help address the most significant market demands and benefits in any digitally disrupted economy. ■



This article is an extract from *Performance*, Volume 9, Issue 3, May 2017. The full journal is available at **ey.com/performance**