Trending topics in GRC tooling

Increasing regulatory pressures and changes have created a new software ecosystem concentrated on providing solutions to manage governance, risk, and compliance processes. Although the ecosystem is still fairly young, it appears to be shaping, and evolving through technology developments like cloud and big data, and responding to changes in the way business wants to manage GRC – from silo to integrated, and from status reporting to real risk insights. Successful deployment of GRC tooling means selecting the right GRC tooling strategy, leveraging the strengths and capabilities of the selected product and sticking to an implementation approach that ensures alignment, speed, agility and confidence.

Drs. G.J.L. Lamberiks RE
is a director at KPMG Advisory.
lamberiks.gideon@kpmg.nl

S.J. Wouterse MSc
is a senior manager at KPMG Advisory.
wouterse.stephan@kpmg.nl

I.S. de Wit MSc
is a senior consultant at KPMG Advisory.
dewit.ivan@kpmg.nl

INTRODUCTION

Since 2002 regulatory changes have forced many organizations to implement multiple oversight functions managing compliance and risk within the organization. This created a new tooling ecosystem focused on risk and compliance functions and internal audit. Since then numerous software vendors have moved into this space, with some organizations having already entered into the second round of selecting a new tool. The tooling market is taking shape and successful and unsuccessful implementations have resulted in a number of key principles to be implemented when embarking on the GRC tooling journey. This article first identifies the ecosystem for GRC tooling, and some key developments in this space. The second part of this article will describe key principles in implementing GRC tooling.

A HISTORY PERSPECTIVE OF GRC

The concept of GRC emerged with the introduction of the Sarbanes-Oxley Act of 2002. Countless other high-impact legislations in combination with various reported large scandals and external pressure from stakeholders and shareholders resulted in companies focusing more on the governance, risk and compliance activities. Because of more strict external demands, companies were and today still are required to provide reliable in-control statements. This requires companies to be able to consolidate and manage different pieces of data required as input for the in-control statements. Risk and compliance initiatives were in many cases setup in silos with each initiative having its own tool and reports, resulting in some cases in contradicting risk reports. Consolidating the initiatives into a single view on risk and compliance is a challenge and requires additional databases and middleware tooling to provide meaningful overviews and management reports.

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 enabling new business opportunities. While evolving through the different maturity levels of integrated GRC the need arises to move from traditional management using spreadsheets to more sophisticated technology. Recent research ([OCEG16]) on the use of GRC tooling within organizations shows approximately 65% of the respondents have implemented GRC tooling in one way or another.

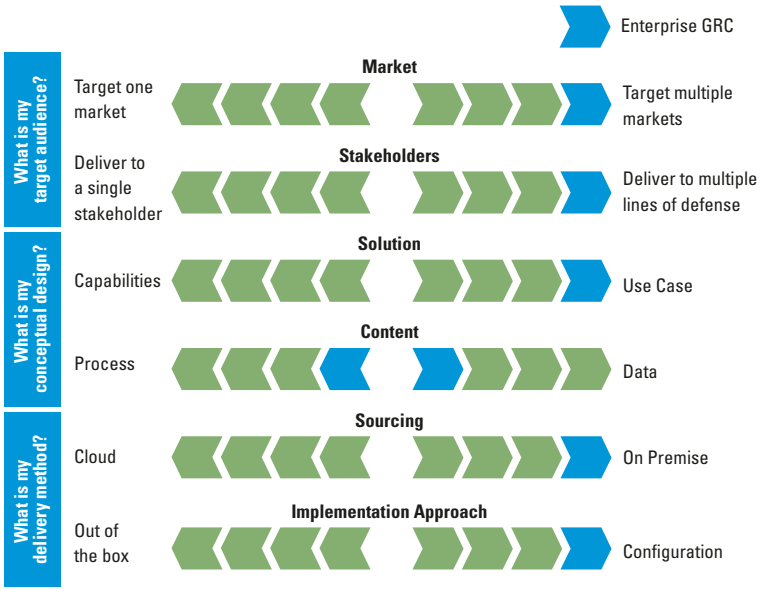
GRC TOOLING ECOSYSTEM

Performing a google on GRC tooling will provide you with a wide variety of vendors. Most of the vendors deliver a variety of what they call plug and play solutions to enable you to hit the ground running. When peeling off the cosmetics, GRC tooling is in fact fairly simple. In its simplest form GRC tooling consists of a database, a document repository, a workflow engine with alerting, reporting and dashboards, web-based and mobile accessibility, and in some cases, a data integration service. By combining these components with common client issues, software vendors provide packages including go-to market use cases, in some cases through an intermediate module layer.

The GRC ecosystem is still relatively young with new entrants and solutions frequently emerging. The innovators (new entrants) tend to focus on emerging compliance and/or risk themes like GDPR, Cyber, Vendor Risk and/or Regulatory Risk, with strong capabilities in data integration and advanced analytics. The traditional players have by now developed a more mature suite of traditional use cases like audit management, operational risk management, SOx (internal control over financial reporting) and are now faced with the challenge of keeping pace with the new technologies being introduced.

Vendors appear to present and position themselves in the GRC ecosystem driven by three main questions and six related design principles (Figure 1). In the remainder of this paragraph we will discuss three main observations defining the GRC ecosystem: point solutions versus eGRC platforms, on premise versus cloud, and from workflow to data driven.

Figure 1. Three main questions and six design principles.



Point solutions versus eGRC platforms

Based on the selected principles and positioning you will find vendors trying to cover the full suite, or vendors with a focus on a specific niche, a so-called point solution.

The enterprise GRC suite is the ERP in risk and compliance. It supports a wide range of use cases generally targeted at supporting the GRC process and methodologies of all risk and compliance functions. The GRC suite vendors offer their product largely independent of the market a company in is. The solution is often delivered on premise[1] and it can generally be configured to match customer requirements.

Point solutions, by definition, focus on a certain point of GRC, e.g.:

- one of the lines of defense like Audit Management software aimed at Internal Audits;
- a common process executed by multiple risk/compliance functions, e.g. Policy Management;
- a specific risk area, for example environmental health and safety or regulatory change;
- specific capabilities, like data analytics.

Both enterprise GRC and point solutions have their opportunities and challenges, see Table 1.

It is very likely that organizations find that there is not just one solution that fits all needs. In general a combination of tools with even some manual process workarounds, should be applied in this respect. Much similar to the ERP ecosystem, the organization must ask itself: what is my GRC tooling strategy? Organizations can apply different strategies, e.g. best of suite, best of breed, point solutions etc.

A best of suite strategy (one eGRC platform from one vendor) requires consensus amongst all the stakeholders as to the goals of the GRC program and the way to achieve these through technological implementation. In many cases it will also result in compromises between stakeholders as not all requirements of a single stakeholder will be addressed – either as a result of specific limitations of the tool, because in an integrated process you don't want (too many) exceptions on because configuration choices made in the GRC platform are applicable to all the parties and stakeholders using it. A point solution obviously is much narrower and will cover specific needs of a process, or a risk and compliance function individually. This is likely to be easier and faster to implement, and in most cases will provide more advanced capabilities compared to an enterprise platform.

The most common strategy toward GRC tooling is one common enterprise GRC platform to cover approximately 70 to 80% of the GRC processes, and implement point solutions to close the gaps. The point solutions generally tend to focus on innovative, content rich solutions in specific pockets, which can be best seen as plugins. Such strategy offers the stability and central maintenance of integrated GRC, while being open and resistant to the rapidly changing pace in GRC. The challenge in this strategy is to locate the right point solution offering the exact piece of required functionality (and no more) to avoid unnecessary cost which can fully integrate (two way) with your existing GRC platform.

1 Some vendors provide managed hosting solutions, but through a dedicated client environment.

Table 1. Opportunities and challenges.

	Enterprise GRC solution	Point solution
Opportunities	• Alignment and standardization of common elements (e.g. organizational hierarchies, rating scales, risk/control taxonomies), resulting in easier aggregation of information and reporting across solutions. • Integration and standardization of common processes (e.g. control testing, issues management) across multiple user groups. • Integration of reporting across multiple functions. • Centralization of vendor interactions and gain economies of scale in licensing agreements; potential for greater leverage for a given expenditure. • Leverage common internal support resources to support a shared platform.	• GRC platforms have historical strengths in certain functions and may be more easily implemented as out-of-the-box solutions for specific purposes (e.g. Internal Audit; Information Security; Regulatory Change Management). • Limited/no process related dependencies across user groups are required to be enabled in the technologies allowing groups to continue working in parallel. • Minimal security concerns as access is limited to finite user groups who may be able to access the full system. • No singular dependency on one vendor to support all risk and compliance functions.
Challenges	• Agreement on organizational priorities and impact on implementation timelines. • Dependencies across user groups – process and data dependencies – pre and post implementation. • Alignment of multiple risk frameworks across the GRC technology platform. • Dependency on a single vendor supporting a technology solution across the enterprise.	• Alignment of common data elements and structures across solutions, resulting in challenges in sharing information across the enterprise. • Aggregation and reporting of management information to stakeholders in a meaningful and consistent way across platforms. • Interaction points with multiple vendors in contracting and support arrangements. • Resources with distinct skills may be required to support multiple platforms.

On premise versus in the cloud

In principle GRC vendors only license the software or underlying code of the application. Other aspects like setting up the different instances, environments, servers, databases are performed during the implementation project, and are mostly partly the responsibility of the customer. We observe two changes in the way GRC software is delivered:

- Most vendors move away from the perpetual license model to a subscription license model. For financial and other reasons a subscription model is very interesting for the vendor.
- More and more customers demand the vendor to provide an end to end solution (software, infrastructure and management). This demand is mainly driven by the efforts that go into the set-up of the in-house sourcing of the GRC tooling and the need for in-house skills to support the tool.

The combination of the two provide some early indications of GRC tooling becoming fully cloud adopted (delivered as a service). However, for two main reasons we expect GRC tooling to still be delivered in a more traditional way, at least for the next few years. First of all companies will be prudent in bringing sensitive or personal data and/or business critical processes (think about BCM or Incident Management and Response) to the vendor (is it secure?), and secondly, a full multi-tenant delivery model will require significant changes and thus investment in the software code, resulting in vendors more likely focusing their efforts on maturing the software.

We do expect vendors to develop an application management service to support customers in managing the application, and we expect vendors to build partnerships with Infrastructure or Platform Service providers to provide hosting. This means as a customer you can, if you want, outsource the entire stack with the flexibility of cloud. If you decide to go for an outsourced model, be sure to thoroughly investigate the service setup (e.g where is data stored, which parties are involved?), and the available certifications of the providers (e.g. is a SOC2 statement available?).

Extending beyond workflow management

Traditionally GRC solutions can be considered to facilitate risk and compliance processes by integrated tooling and software. Especially because many of the GRC software vendors support easy configuration or tuning of the software to match GRC processes, companies are able to work with implementation partners, or configure new functionality easily themselves. With this focus on processes, much of the GRC tooling can be considered as workflow management systems, that are delivered with well-developed out-of-the-box processes, sometimes even tailorable to the maturity level of the company. For a company which adopted and implemented its processes in GRC tooling, keeping the system up-to-date and filled with the correct data is largely dependent on human interaction. To give a few examples:

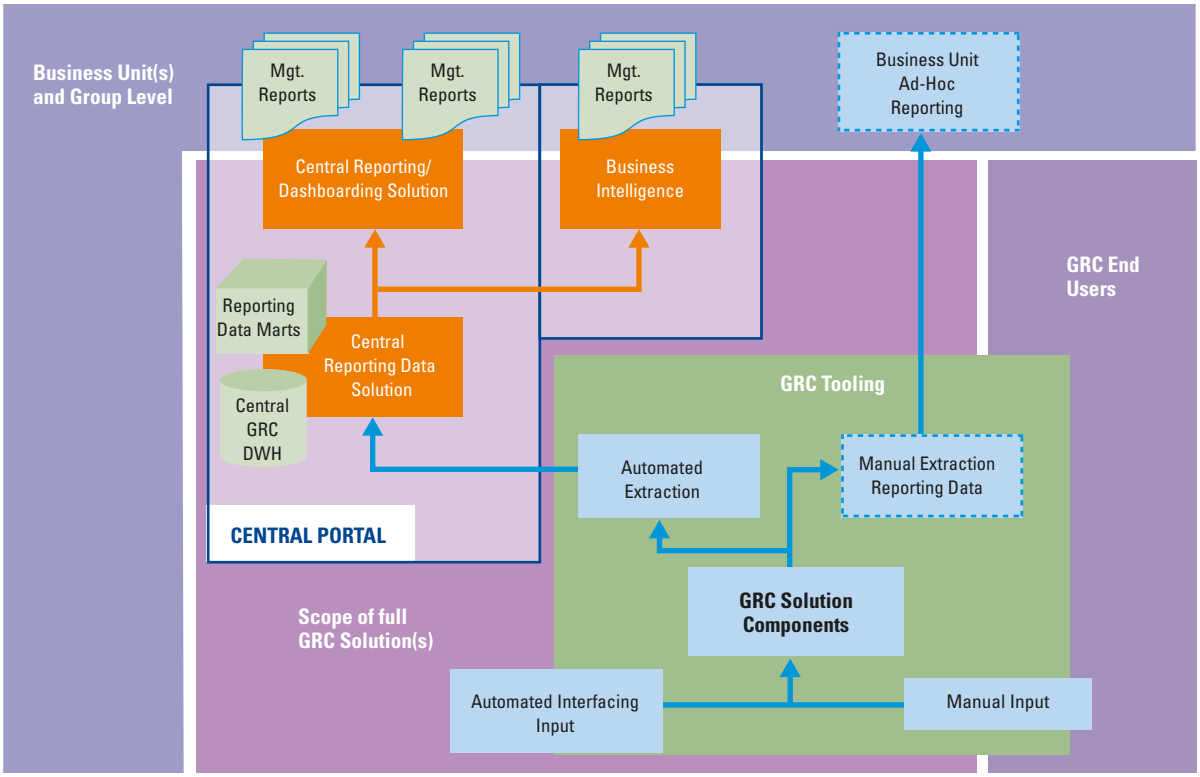
- the registration of Loss Events and follow-up of potential Legal Claims life-cycles;
- performing Risk Assessment and Risk Response for each entity in the organization;
- manual control testing of process level controls including follow-up and validation of findings.

As the examples above clearly show, these activities require multiple roles to actively enter the GRC system and create or enrich content, with both first, second, third, and maybe even fourth line of defense participating. Although having this input is very important for management reports and eventually the end state of the in-control statement, lots of manual work is needed to get there. Also, getting the right information out of the system could be a difficult exercise.

Getting the right information out of the system could be a difficult exercise

Where GRC processes can generate huge amounts of data with individual risks or controls labeled against many different attributes, GRC tooling can be limited in functionality to support more advanced dashboarding and reporting (for an example, see Figure 2). Most GRC tooling is not able to identify complex patterns or to implement even algorithms to analyze data, while these insights often add most value in steering on GRC themes. This is where we see the need for additional functionality or more sophisticated business intelligence tooling and where a larger need for automation comes into the picture.

Figure 2. Example of extended usage of GRC data for dashboarding and business intelligence.



Different vendors are already offering automated analytic tools, where risk and compliance status data can be automatically derived, based on for instance log files or other automated outputs. By setting up the right interfaces providing input into the GRC solution, more meaningful data can be combined giving better insights and reducing human intervention and the associated errors. Some trending concepts commonly used like data mining or process mining in combination with automated control testing or continuous control monitoring are more and more adopted by companies on top of the existing GRC solutions. By applying these technologies, manual activities to verify whether controls are executed correctly can be automated and performed continuously.

KEY PRINCIPLES IN IMPLEMENTING GRC TOOLING

Based on the collective experience of the authors in multiple implementation projects, we have identified a number of key principles to a successful implementation:

a. Align before you design
b. Begin with the end in mind
c. Stick to the standard
d. Apply an agile approach
e. Manage the change

a. Align before you design

In essence a big part of a GRC implementation relates to processes to support different groups of people (e.g. Risk Managers, Project Managers, Control Testers) in executing their day-to-day activities according to a predefined workflow. The implementation brings together those parts of the organization which used to work quite independently using their own tools, processes and ways of working. The selected GRC tooling itself also comes with its own terms and definitions, workflows and (implicit) logic.

It is essential to have a common definition and common understanding of both the key definitions and taxonomy of GRC and of future state processes from the start of the project. These can be as basic as 'What do we mean by residual risk?', 'Are we going to use a 5-point or a 9-point scale to assess risk?', or 'Who can be the owner of a risk or control and how do we define this?'. Decisions on taxonomy and definitions can have big implications on the governance and responsibilities within your organization and can jeopardize your GRC initiative if brought up too late. It is good practice to record the key decisions in relevant policies and standards and to translate these into practical ways of working within different parts of your organization.

Some of the most successful implementations have consistently applied the starting point to use out-of-the-box functionality

Making these processes explicit by drafting them in the form of process 'swimming lanes' is a very useful instrument right at the beginning of the project. They can be more easily related to by business representatives and they form the basis for defining functional requirements and for the translation to modules within the selected GRC tooling. These processes also serve a purpose during (functional) testing and more importantly during the business implementation.

Not all activities in a GRC related process will be executed in or supported by the selected GRC tooling; some activities will remain outside the tool. In defining the 'GRC processes' it is relevant to make a distinction between both of these. During business implementation the activities that are supported by the GRC tooling can be more easily translated into a training program. However, it is just as important to also define the desired and expected behavior ('way of working') for activities not directly performed in the tool.

b. Begin with the end in mind

Speaking the same language and being aligned on taxonomy and the scope of the GRC initiative are all very important, but it is now time to ensure that all stakeholders have confidence in the tool. During the selection of the GRC tooling the teams will have obtained a broad understanding of the capabilities of the tool. It is good for your organization to now understand what the strengths, but also the limitations of the tool are. This is to ensure that you are aware of what the tool can support very well, what it can do after some modifications and what you should really not use it for.

This step is targeted at creating a first prototype or concept of the full GRC solution to be implemented. The definition of a 'full GRC solution' in this context is flexible in that it can be the implementation of a complete new framework to manage risk and control activities or it can be much smaller and targeted, for example on the management of third party risk. The goal of this phase is to create confidence that the selected tool will enable and support the target GRC state. This is achieved by having this first understanding of the final product early in the project and by already starting to execute some of the GRC activities using 'real' data. Finally, a conscious GO/NO GO decision is typically made to either continue, revise the approach or stop the GRC initiative.

c. Stick to the standard

In the previous step the teams have obtained a good insight into the full capabilities of the GRC tooling, and have understood its complexity. It would not be the first time that the out-of-the-box capabilities of the tool initiate a review of existing processes and requirements. Some of the most successful implementations have consistently applied the starting point to use out-of-the-box functionality of the selected GRC tooling, unless there are very strong reasons to deviate from this. Following this principle you can leverage the in-built good practices of the tool, it can provide an effective way to close otherwise lengthy discussions and it forces you to make a conscious decision about deviating from the standard (are we as a company so different that we need to deviate?).

d. A more agile project approach to drive value

When the big picture is confirmed and the key gaps to be closed are defined, the next step is tuning the GRC solution to the target process and maturing the full solution so it is ready for a wide use within your organization. Unlike in the first step where the entire GRC solution is covered, the maturing of blocks of functionality (e.g. risk assessment) is best done for each building block.

Most of the GRC tooling that is available in the market is flexible, in that it can be relatively easily configured and tailored to your needs and processes, while leveraging the capabilities of the GRC tooling. This allows you to apply an agile or iterative project approach, where you work towards the final GRC solution in iterations/cycles continuously expanding and building on the product, resulting from the previous iteration/cycle. Some of the main advantages of applying such an approach is that you get an impression of the final solution at an early stage, that you see it grow and develop and that you are able to reprioritize your requirements with each iteration/cycle focusing on items which add most value. Often, requirements which appear very important upfront, are later given a lower

priority and may even end up not even being included. An effective agile team includes only a few business representatives for the domain in scope, who are mandated to make design decisions and 'own' the requirements on behalf of your organization. Needless to say, they should also act according to the mandate they have.

It is useful to pilot completed blocks of functionality within a representative part of your organization to not only validate the robustness, completeness and practical use of that building block, but also to test the business implementation approach. Can users practically work with it? Is it intuitive? What elements require additional explanation or training? Lessons learned from the pilot(s) are used to functionally complete a building block and to refine the business implementation approach.

e. Manage the change

An integrated view of risk is a cultural change for many organizations with enormous impact, and should therefore be guided by an organizational change process. The final phase focuses on the so-called business implementation where not only the GRC solution, but also the new or changed ways of working in question are implemented throughout your organization. The approach and duration of this phase vary widely across GRC implementations, depending on the amount of change your organization can handle, the level of senior management support, the phasing out of existing GRC tooling or solution and the existence and strength of a compelling event. As with any (IT) implementation, it is only during this phase that the true benefits start getting achieved, so it is important to measure this achievement and adjust either the GRC solution or implementation approach if the benefits are lagging behind.

FINAL CONSIDERATIONS

Although the GRC tooling market is taking shape, it is not yet mature. IT developments such as cloud and big data will continue to influence and maybe drastically change the GRC tooling ecosystem in the coming years. The rising stars of the past need be careful and continue to innovate their product to keep pace with the young, innovative and ambitious new entrants. Organizations will very likely need a combination of tools to cover all requirements, with one tool to rule them all. Selection and deployment of GRC tooling will focus on standard out-of-the-box functionality and configuration, with highly agile methods of change.

Organizations will need a combination of tools to cover all requirements, with one tool to rule them all

Reference

[OCEG16] OCEG, *2016 OCEG GRC Technology Strategy Survey.*

About the authors

Drs. G.J.L. Lamberiks RE is a director at KPMG Advisory. He supports clients in defining their GRC journey and with the selection, design and implementation of GRC tooling. In addition, he is an expert in the field of assurance integration and service organization control.

S.J. Wouterse MSc is a senior manager at KPMG Advisory. He assists clients in defining their GRC strategy and supports and drives the setup, execution and delivery of GRC tooling implementations. He also manages the KPMG EMEA alliance with GRC tooling vendors.

I.S. de Wit MSc is a senior consultant at KPMG Advisory. As a design lead and business analyst he supports clients in implementing and continuously improving GRC tooling implementations. He also participates in external IT audits, cloud risk management projects and security awareness engagements.