Embedding digitalization into Governance, Risk Management and Compliance activities

CRO Forum GRC Tooling

March 2023

Table of Contents

Summary

Increased digitalization in society is leading to increased digitalization in the insurance industry impacting distribution, product design, underwriting, and operations. In line with this changing landscape, Governance, Risk management, and Compliance activities (GRC) are also becoming more digital.

Given this trend, the CRO forum has decided to investigate the implications of this digitalization on GRC activities and the ways to assist insurance companies to assess their current position and possible future ambition in terms of digitalizing GRC activities. With the aid of use cases from CRO Forum members, the current status, the main challenges, lessons learned, and critical success factors are identified. A survey was held amongst CRO Forum members to gather insights on these topics.

Chapter One introduces how digital technology is changing the insurance industry from product design and distribution, underwriting risks to claims management.

Chapter Two sets out the implications within GRC that the digital transition provides in terms of benefits but also the challenges. The survey results are used to provide insights on how members are digitalizing their GRC activities and where the future focus will lie, for example, the degree of use of machine learning, real-time monitoring and automated controls. The main challenges lie with centralization of data collection and integration of GRC tooling with the rest of the organization, plus ease of use/customization options. Most members say data-sharing between the various control disciplines (Risk Management, Audit, Internal Control, Compliance, Actuarial, Model Validation) is currently ad-hoc and manual.

Chapter Three presents a GRC Digitalization Radar model. This model visualizes the digital positioning of an insurer and its GRC digitalization activities along four dimensions: Functionalities, Data, Technology and Organizational Model. Within each dimension, stand-alone and inter-linked GRC components are identified with a description of high, medium or low use of digitalization since there is not a one-size fits all solution. For example, a low use of digitalization but well-implemented solution that is adapted to an organization could be more efficient and more effective than a high use. Such a model aids an organization to determine its ambition and gives an integrated view on its GRC solutions.

And finally, Chapter Four presents critical success factors for digitalizing GRC activities and three use-cases from CRO members are detailed to demonstrate the issues faced and lessons learned when embedding digitalization within GRC activities.

Key Take-aways

- As well as the usual hard pre-conditions for implementing new software, such as customisation, flexibility, data governance, business requirements etc, since GRC tooling is used by all three lines of defence, successful embedding of GRC tooling requires Senior Management sponsorship (e.g., CFO or CRO).
- Given the wide variety of users across the three lines, other soft pre-conditions for successful integration involve the second line investing in: being able to train all users; maintaining the relationship with the (internal) vendor; staying aligned with digitalization projects in the first line to be able to innovate GRC digital activities as processes or regulations evolve, and gaining knowledge on digital transformation processes such as agile and lean.

These take-aways, together with lessons learned, are illustrated with the use-cases on further integration.

- The first use-case desired more integrated assurance from its centralised solution. Their lessons learned included strong sponsorship; ownership at second line with a strong relationship with IT; and differentiated user profiles with limited workflows. Additional success factors included: shared taxonomy; shared access by all lines and limits on the level of integration.
- The second use-case found that having enhanced data analytic capabilities that functioned on different IT domains was a critical success factor.
- In the third use-case communication and engagement is seen as a critical success factor. This includes: clear communication of goals relevant to each stakeholder, aligning with users to have a good understanding of how embedded first line risk management best practices were across the group, and embedding a 80/20 culture. Special attention was given to the soft skills of the project team members and innovative communication methods used to engage all lines, such as an interactive internal social page and drop-in sessions.

In conclusion, although the practical implementation is complex and challenging, digitalization in GRC is a logical next step as society and insurance digitalizes. In order to achieve this the GRC Digitalization Radar can be used as a best-practice tool to assist an insurer in this task.

1. Introduction

Digital technology is changing the insurance industry

The insurance industry encompasses by nature a massive data collection process. It is a significant competitive advantage to have a quick, broad, and reliable access to data in order to tailor the client offering while ensuring compliance with increasing regulatory activity and complex accounting standards.

Digital technology and the availability of new data sources is bringing about change in the insurance industry and reconfiguring the landscape. The increasing use of data analytics, artificial intelligence, and the Internet of Things (IoT) are expanding the role of data in the insurance business model. It gives new business opportunities, but also increases the operational risks for insurers related to digitalization. Technology therefore will enable the development of new business models, and allows, but also requires, more efficient and effective risk mitigation and prevention.

Digital technology is changing what insurers cover and the ways in which they design and distribute products, underwrite risks, and manage claims[1].

Designing of insurance products

There are more and more examples of how digitalization is changing the nature of insurance products. One example is usage-based insurance or pay-as you-go coverage where insurance companies sell car insurance on a pay-per mile basis.

Distribution of products

Distribution channels are also evolving. While traditional intermediaries, like agents and brokers, still dominate distribution for most insurance sectors, an increasing amount of insurance is gradually moving over to mobile and Internet channels, especially in lines such as motor insurance. Digital technology will eventually enable customers to arrange almost all their insurance needs through remote digital channels.

Underwriting of risks

Underwriting is becoming easier and more effective. New data sources, new platforms to store and analyze data, and fast, innovative technologies to use the data or simply automate existing processes will reduce the length and complexity of risk assessment, improve risk selection and allow for more personalized pricing.

Managing of claims

Claims handling processes can be simplified and streamlined by technology. Automated loss notification, real-time processing of claims, self-service capabilities and electronic payments are increasingly used to make claims management more efficient. Insurance technology startup companies are using advanced analytics, such as machine learning, to create early warning systems and gather practical insights that also prevent accidents. Post-event estimation techniques using drones and sensors for quick and easy claims handling are increasing. Technology applications can also be effective in identifying and mitigating insurance fraud.

Naturally this changing landscape also requires that GRC activities across large swathes of the organization need to evolve. This paper explores the status and expectations of the integration of digitalization within GRC activities, introduces the Digitalization Risk Radar which can be used to visualize an organizations' maturity towards GRC solutions and discusses challenges, lessons learned and critical success factors.

[1] Insurance in the Digital Age, The Geneva Association, September 2018

2. Integration of digitalization in GRC activities

This chapter sets out the implications within GRC that the digital transition provides in terms of benefits but also challenges.

2.1. What do we mean with digitalization of GRC processes?

GRC activities are defined as a set of processes and procedures to help the organization to achieve their business objectives and address and manage uncertainty. GRC has multiple disciplines, including but not limited to the control functions risk management, actuarial, compliance and (internal) audit.

The impact of digitalization in business models and processes also reaches GRC activities in all its dimensions such as the use of automated controls, more use of data, increased computer power and the use of new techniques such as machine learning.

- Digital transformation leads to evolutions in process execution, with an increased reliance on controls performed automatically as the operations are performed. Since manual data entry into back-office systems tend to disappear as business moves towards a seamless integration of systems, the manual checks afterwards by specialized control teams, have to be performed synchronously with the business processes such as underwriting and claims handling so that it doesn't drag on the ability to deliver a good customer experience.
- Risk management can rely on a higher volume of digitalized data to generate risk indicators closer to "real-time" operations and have a stronger monitoring of the development of portfolio exposures.
- Increased computing power, associated with the dissemination of techniques previously considered as "advanced", such as machine learning, enables the insurer to redesign some control activities. For example, antifraud analysis based on predictive modelling can be deployed. In the meantime, the widespread use of digital tools also elevates the risk of systematic fraud by sophisticated actors, with the ability to generate authentic-looking documents and IDs.
- The statistically significant samples that control both permanent and periodic activities to assess the overall compliance and adequacy of processes, can be supplemented by more systematic analysis of available data.

Moreover, as was also one of the conclusions of the CRO Forum's paper on the Three Lines Model the control functions have their own areas and priorities, but more and more these functions feel the need to work together and share data to help building a stronger and better organization. This can be strongly supported by the digitalization of the business processes and opportunities that arise as a result. Digitalization affects all GRC disciplines and provides opportunities to improve quality and achieve more efficiency.

Survey respondents state the main benefits of using GRC tooling are **insight, oversight, more control and efficiency.**

In line with the opportunities just mentioned using digitalization in GRC activities can have major benefits for the organization. The main benefits are:

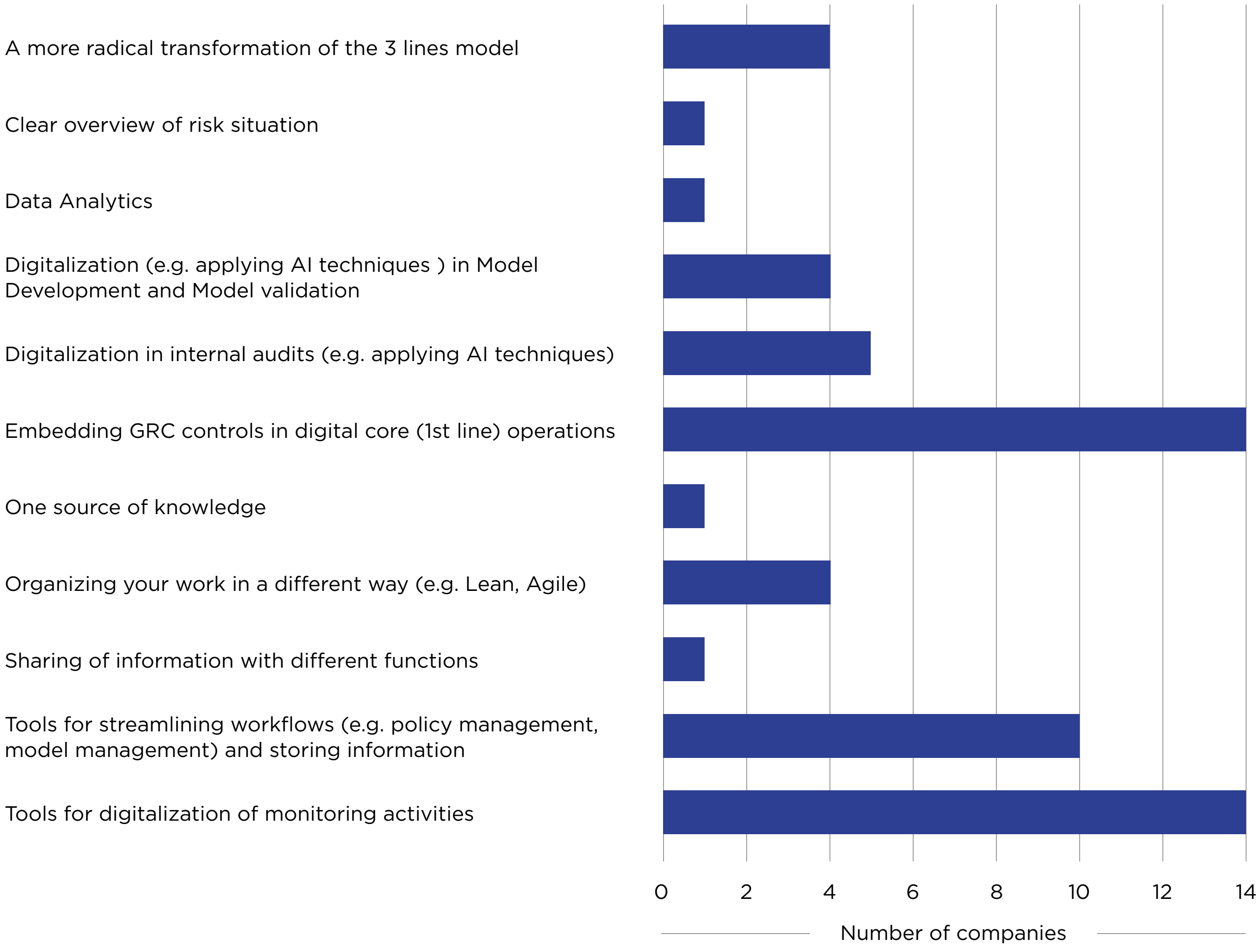
- **Insight.** There is more alignment with digital core business processes for effective and efficient control as controls are integrated in the business processes
- **Oversight.** Get a holistic view of the complete GRC landscape, along with providing insights over the key risks within the organizations.
- **More control.** The level of assurance can be increased as feedback is available more frequently thereby enabling the organization to react immediately.
- **More efficiency.** Overall, more efficiency because of increased integration within the three lines model.

Focus is on embedding GRC controls in **core (first line) operations, tools for monitoring activities and streamlining workflows.**

Based on the survey results the focus of most of the CRO Forum members is on digitalization of GRC controls in core (first line) operations, and tools for monitoring activities and streamlining workflows (e.g., policy management and model management).

Other areas of the GRC landscape such as digitalization for getting a clear overview of the risk situation from one source of knowledge; sharing information with different functions, or the use of data analytics for GRC activities seem to be less top of mind.

Figure 1: What do you think of most when thinking about digitalization of GRC?



2.2. Considerations on tooling available to help digitalization of GRC

For the core GRC activities such as controls, risk analyses and monitoring activities there are two possible directions:

1. A joint GRC system for all stakeholders (business, risk, compliance, audit) with risk identification and assessment, control documentation, incident and losses reporting, action plans and monitoring.
2. A specific solution for each risk discipline (e.g., risk management, audit management, issue management) allowing to deal with granular risk and control information in specific areas and then consolidate for overall oversight.

A little over 40% of respondents report to have an enterprise wide and integrated GRC system. The rest uses department, function or task specific tooling ranging from simple office solutions to specialized in-house built software.

There are real benefits to be achieved if the tools are integrated, by either one tool for the complete GRC environment or linked to each other. This increases the reliability of the data and therefore the efficiency and effectiveness of GRC processes. However, for the majority of the members, the data are not yet shared via a centralized and accessible data pool. For some members there are some linkages but it is not centralized and/or data sharing is still ad-hoc and manual.

Another consideration is whether and how to connect with operations and the relevant data available. Continuous monitoring requires linking the GRC system directly to the source systems, which also guarantees data reliability.

Furthermore, embedding GRC controls in the processes can be implemented by using either an open or a closed loop. In the case of a closed loop, deviations are immediately reported back to the operations as incidents occur so that they can be solved directly, making control activities more relevant, as they are more closely integrated with the business workflow and less based on "cold case", after-the-fact analysis. Monitoring of activities can be done by using data analytics and dashboarding. This gives a more continuous and complete overview and insight to business management and GRC.

Also for the other areas of the GRC landscape advanced technologies are available enabling more proactive risk management by using advanced GRC solutions for developing anticipation and detection capabilities, such as:

- Real time data and analytics provided by satellites, drones, sensors (IoT) to feed risk assessment.
- Computer vision to derive meaningful information from digital images, videos and other visual inputs and take actions or make recommendations based on that information.
- Machine learning to process and understand larger volumes of data and support decisions and insights.
- Non-linear programming (NLP) capabilities can be used in generating natural language such as text summarization, machine translation, spam detection, and information extraction.
- Robotics in its simple process automation branch or more complex and hybrid development.

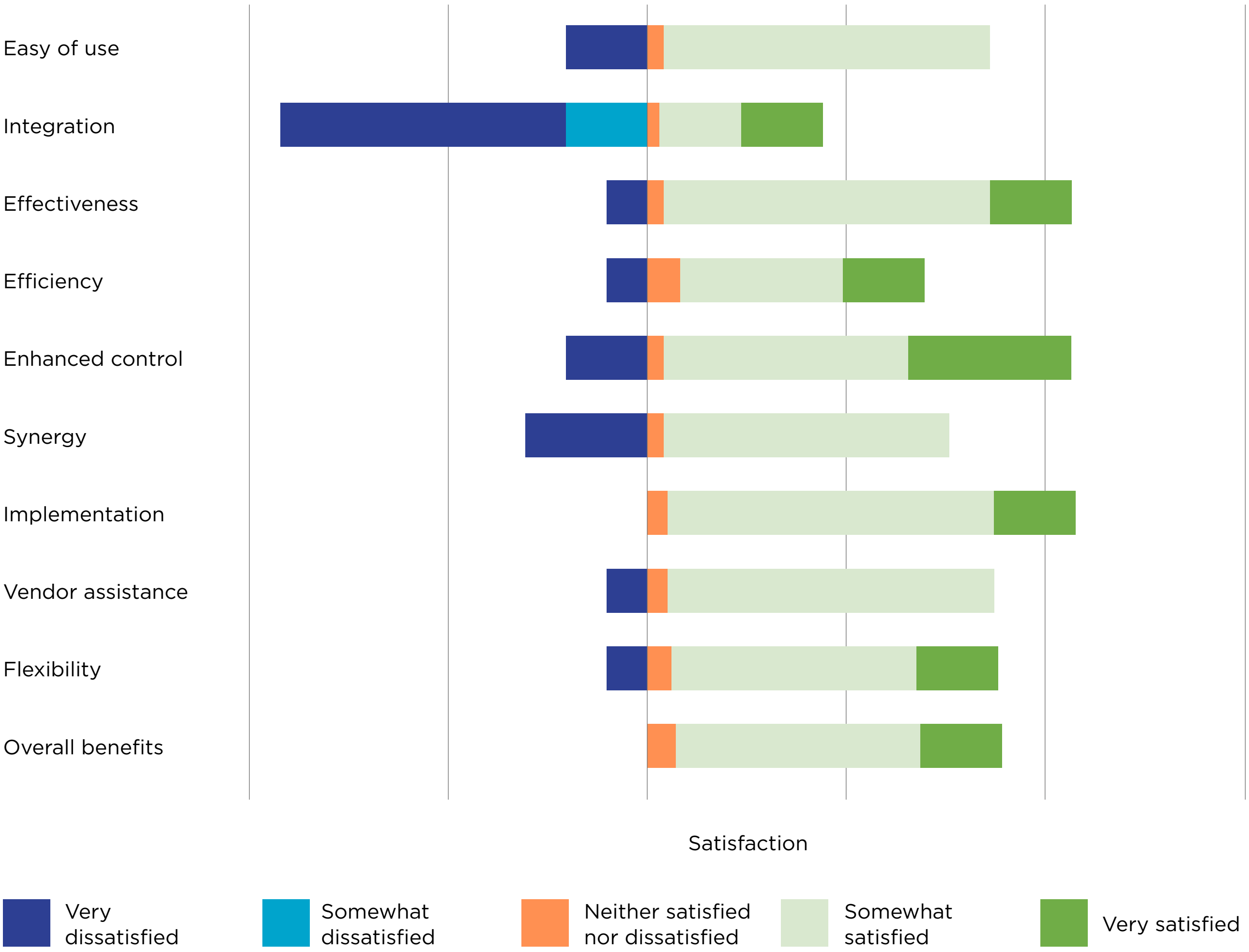
Around 50% of the survey respondents indicated that **they use a form of AI or robotics for GRC activities**.

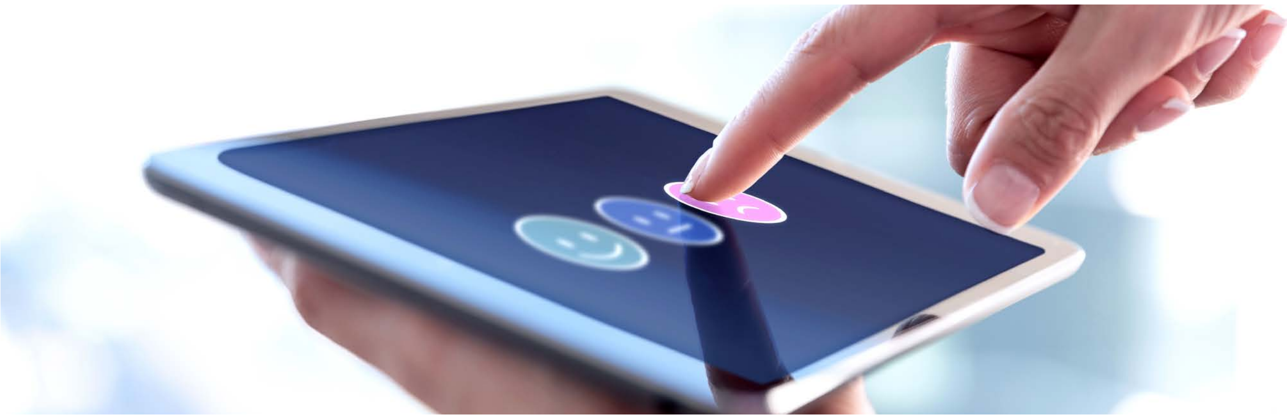
It is important is that there is a common integrated view on the digitalization of the GRC landscape, the GRC system itself but also the interaction with all other additional GRC digitalization initiatives, where applications are complementary and interact. In this way the main benefits for the digitalization in GRC activities are achieved, creating a holistic view of the complete GRC landscape and a more efficient GRC system.

2.3. How satisfied are members with current GRC solutions?

In general, members are quite satisfied with the current application of GRC tooling. In particular, members are satisfied with the contribution that the tooling makes to the improved control level in the organization, the increase in effectiveness and how the tooling has been implemented in the organization.

Figure 2: How satisfied are you overall with your current GRC software tooling on the following subjects?





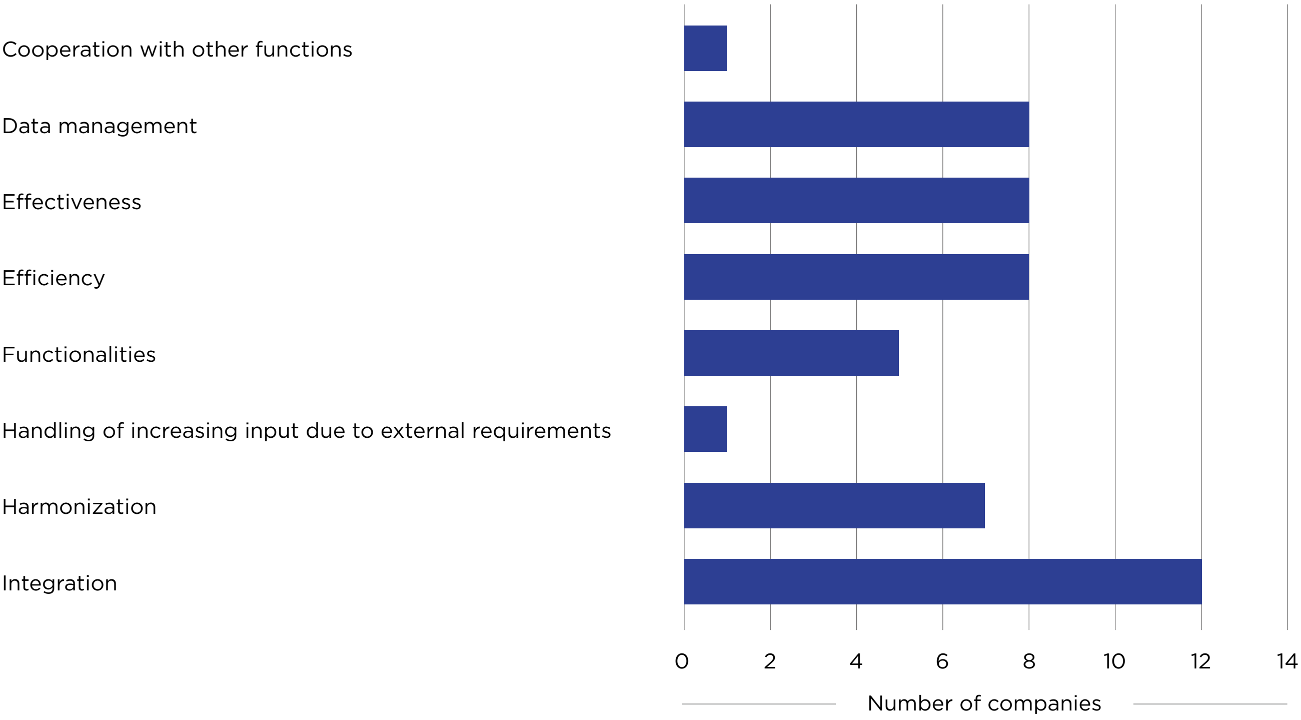
However, there is also room for improvement in the areas of data management and integration:

- **Integration of GRC tooling.** A lack of integration is seen as the main area of dissatisfaction of current GRC tooling among Forum members and at the same time the main driver for modernization and there confirms that having a common integrated view is an important aspect to consider.
- **Central data collection.** Another important topic is to have all relevant data shared in a central place to be able to leverage digitalization for GRC purposes (synergy, data management). Only 15% of the respondents indicate having such a centrally shared and used data solution.

A majority of the organizations plan to further expand and modernize the GRC solutions in the coming years. 40% of the members want to get started with this in the coming years; another 40% in the next 3 to 5 years. In particular, the application of robotics and artificial intelligence are mentioned as solutions to further improve and optimize GRC (50%).

As there is a wish for further improvement, we introduce the GRC digitalization radar in the next chapter which can be used for setting the ambition and creating an integrated view for digitalization of the GRC activities.

Figure 3: What are the main drivers for modernizing your GRC technology solutions(s)?



3. GRC Digitalization Radar

This chapter presents a structured approach for assisting insurance companies to assess their current position and possible future ambition in terms of digitalizing GRC activities and gives an integrated view of its GRC activities.

3.1. GRC Digitalization Radar

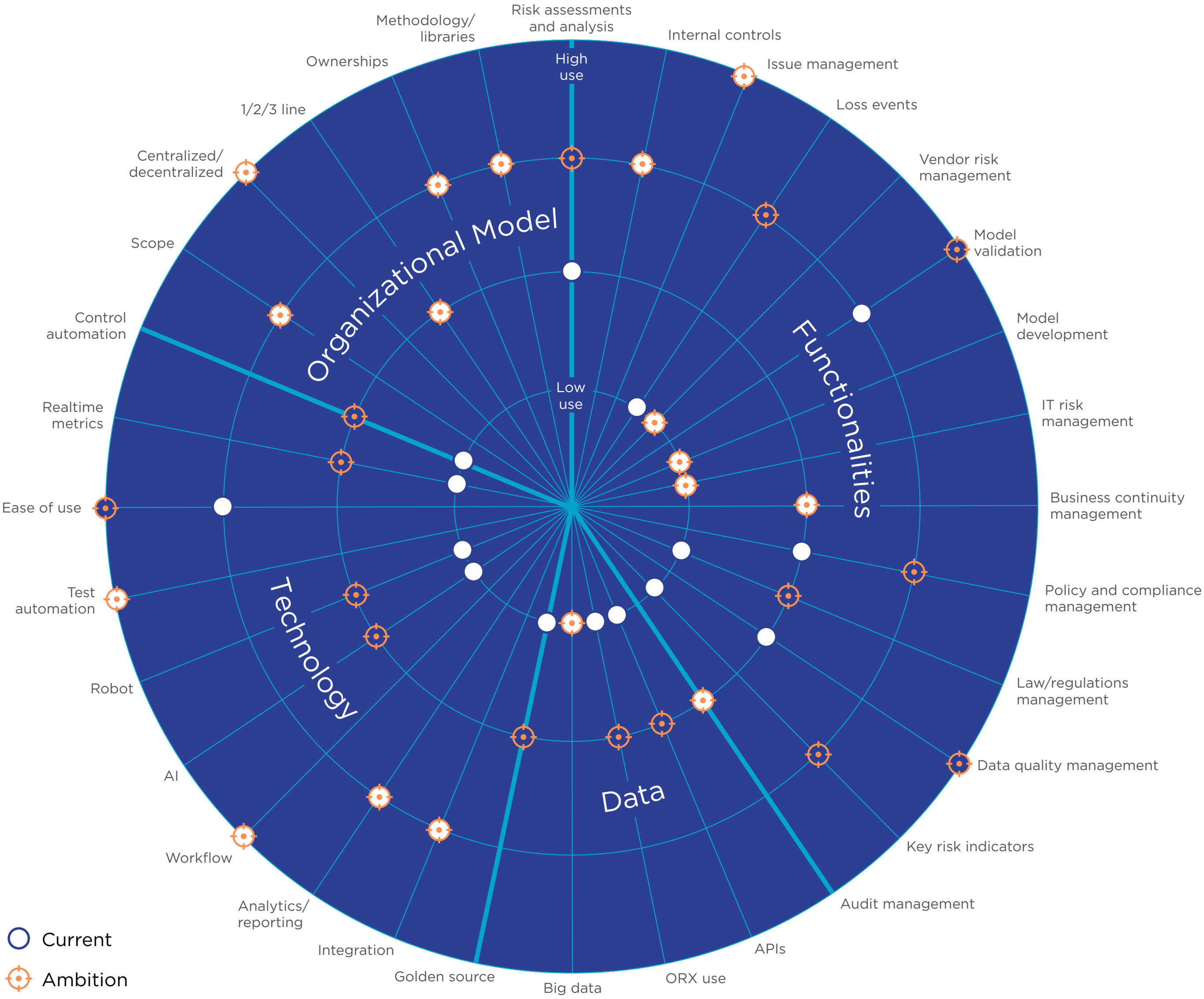
Given the complexity and variety of GRC tooling offerings in the market, the number of modules and customizations available and the fact that each organization aims to define its own GRC strategy, it is very complex (and impossible) to provide a single vision of the best use of a GRC solution that would suit all.

One key assumption made is that there is no value measurement in the concept of 'degree of use': a 'low use' but well implemented and adapted to an organization could be more efficient and more effective than a 'high use'. The degree of use is related to the complexity of the solution adopted and, likely, the time and costs involved to achieve and maintain it. It also often goes with the size of the organization and the team administering the GRC, its knowledge and its customization power.

In order to help organizations to visualize their maturity towards GRC solutions, the GRC digitalization radar was developed (see next page). The GRC digitalization radar helps each organization to position its current use of the GRC tooling across different dimensions and components, and to define its future digitization strategy, based on proven market practices and trends.

This model visualizes the digital positioning of an insurer and its GRC digitalization activities along four dimensions: Functionalities, Data, Technology and Organizational Model. This concept is not meant to be static and will evolve over time with new dimensions or components, however, the radar represents the current situation well. A dimension can be seen as a key axis to analyse the digital positioning of an organization and can fit with other IT tools that are not related to GRC. A dimension combines several components to form a consistent group. Components can be seen as modules that are a further breakdown of the dimension and represent a framework for assessing the desired specifications. Each component within a dimension could be assessed by level of use (high, medium, low, or no use) and is supported by an example of what this usage would be.

Figure 4: Example of use of the GRC Digitalization Radar



Sometimes, components are linked to each other and therefore they need a certain degree of use (low/medium/high) to properly achieve the level of use (low/medium/high) of other components. For example, it is complex to enable a Big Data strategy without APIs (Application Programming Interface), a certain degree of integration and centralization, and efforts related to analytics and reporting.

Per component organizations can plot their maturity from the centre (no use) to the outside of the diagram (high use) in terms of current situation and ambition or desired situation. Detailed descriptions and examples per component from low to high are available in the appendix.

The use of the radar is easy and facilitates in producing an own version of the chart tailored to your organization, by following the steps highlighted below:

1. Understand the concept of level of use, dimensions and components in the following sections
2. If necessary, tailor the radar itself by adding new dimensions or components potentially not covered by this study
3. Perform a self-assessment of the current situation in your organization per component/ dimension
4. Define your ambition level, according to your digital strategy and by inquiring internally with key stakeholders. This step could leverage the high-level stories provided by current GRC users and trigger networking activities across the CRO Forum members.

3.2. The components of the GRC Radar

In this section a brief explanation is given on its importance and the different components for each of the four dimensions of the GRC Digitalization Radar. For each dimension an example is recorded of the maturity scale for one component. The full table with an overview of all components of the four dimensions can be found in the appendix of the paper.

Functionalities

The first part of the GRC Digitalization Radar deals with the functionalities or modules of GRC solutions an organization selects. Consider which functionalities or modules make most sense for your organization. Should it be for only one specific use (e.g., risk and control assessments) or for several? The footprints of GRC tools have considerably improved over the years and currently offer solutions for a wide panel of use. It is then very likely that other units or departments in your organization are in fact looking for solutions that a GRC solution can achieve.

An understanding of the information that will be required from the GRC is an important factor in the design process in order to ensure effective future engagement with the GRC tool. Activities lending themselves to digitalization include risk & control self-assessments, the recording of risk & loss events, and the documentation and tracking of the remediation of control weaknesses. Tooling may also provide capabilities to capture and report upon key risk indicators, seek attestations of policy compliance, and support the control testing activities.

The design of the system needs to consider the end users, and agreement will be needed on areas such as risk definitions, “heatmaps” and scoring, and mandatory fields. It is important to consider business users when designing screens and minimize the number of data capture fields to complete. It is also best to avoid speculative “future proofing” and focus on real business needs. Tooling itself introduces standardization but consideration must also be given to the impact of standardization on smaller businesses and the potential overhead that this may create.

An example maturity scale of risk assessments and analysis component (see full table in appendix):

Risk assessments and analysis *“A module of the GRC that allows the entities to perform on a regular basis risk evaluations and analysis on the (operational) risks, monitoring of the risk mitigation and reporting of the risk exposure”*					
HIGH	Performance of Risk Assessments fully integrated in GRC and automated results reporting, integration with other modules and leveraging on other inputs (internal control results, KRI etc.).	MEDIUM	Performance of Risk Assessments in GRC but with limited possibilities - medium level of manual effort for data reporting readiness. Usage of external tools and minimum connection with other modules.	LOW	Performance of Risk Assessment and Analysis out of the GRC (e.g., Excel, own templates) but results uploaded in the tool.

Data

The second part of the GRC Digitalization Radar deals with the approach to the available data to consider when implementing a GRC solution.

GRC tooling requires a data model to support its effective operation. This is highly important and should fit the overall data strategy of organizations. Will the GRC solution connect to existing data sources (directories, master data, controls results, chart of accounts …) or be based on a standalone database?

The design of data model and hierarchy is a fundamental to GRC tooling, and it is worth investing significant time in getting it right before starting to build it into a GRC tool and certainly well ahead of going “live” with a system as it will immediately become “legacy”, and difficult to unpick once the system is in production. Similarly, it is important not to over-engineer the data model, focusing on the factors that you wish to measure rather than seeking to manage everything. An iterative approach may be required for this, and any complexity may be difficult to reverse out of. It is also likely that the data model will also need to evolve over time, and data models should not be over complex to limit the ability to change.

An example maturity scale of Big Data (see full table in appendix):

Big Data *"The GRC tooling is used to collect high volumes of data for the purpose of data analytics"*					
HIGH	Large, clean data is contained within the system and updated to ensure relevancy and timeliness. Key data analysis can be undertaken providing business insights. These insights can be extracted and used across businesses and group-wide functions or interrogated further to provide bespoke results.	MEDIUM	Fairly clean data across most areas of interest which lacks completeness in parts or updated sources. Used for limited trend analysis and decision making but would need corroboration for key decisions.	LOW	Unstructured limited data input into the GRC system which provides the basis for further confidence assessments.

Technology

The third part of the GRC Digitalization Radar deals with the digital strategy of an organization. it is important that the GRC tooling fits within the organizational IT architecture. Certain choices should be driven by certain technologies: is this the right moment to go for AI?

This part of the radar deals with aspects as the level of interoperability of the different functional modules (e.g., Risk Assessment, Loss Events, Audit Management, BCM, …) of the GRC solution, enabling data alignment and process automation, the level of use of the reporting capacities of the GRC, the level of use of Artificial Intelligence related to the GRC tooling and ease of use to customize the GRC system in order stick to companies' processes, while keeping a high-end user satisfaction and aspects as real time metrics and control automation.

An example maturity scale of AI (see full table in appendix):

AI *"Level of use of Artificial Intelligence related to GRC tooling"*					
HIGH	Validated, compliant and monitored AI techniques are embedded into systems to deliver Realtime decisions and information to the GRC process. Self-learning aspects of these systems are continuously monitored and controlled for compliance and validity. State of the art methods like deep learning and neural networks are applied to reach optimal and smooth performance beyond human capabilities. Methods and techniques are in line with EU regulations and regulatory guidelines.	MEDIUM	AI techniques are used for decision support and guidance. Integrated AI applications process and analyze data using less complex models to generate indicators, scores and other results. These results are used by humans to assist in decision making, especially in situations where data volumes and number of variables are high.	LOW	AI techniques are used ad-hoc and decentralized to analyze distinct use-cases or incidents, sometimes in the form of pilots. Outcomes are helpful to understand and analyze data and risks. Outcomes can be used to amend key risks and controls or to re-evaluate and gather extra risk and control data. Tooling is open source, local and not fit for production purposes.

Organizational Model

Finally, the fourth part of the GRC Digitalization Radar deals with the organizational model with respect to the choices around the integration of the GRC and how it penetrates the organization. Will the three lines be using it? The whole organization or risk management only? Could one single GRC solution cover the entire organization?

It is important from the outset that there is clear understanding of the business need for GRC tooling. Each line of defense has different information needs, and consensus is required to ensure all stakeholders will be able to source the information that they need. Focus on the design of reports and management information outputs from the outset for all stakeholders will also help “buy in” to the GRC tooling from the first line. Conducting an internal survey to collect the needs before defining the strategy often pays off.

In this context it is important to consider the “use case” for the first line - how will the GRC tooling improve their risk management capabilities and the insights into their risk landscape; and more importantly, how much time can the first line save thanks to the GRC tooling? The perception by the first line of how data within GRC tools may be used by the second and third lines must also be recognized as a factor that may inhibit engagement, with clear communication on the data purposes of the second line and third line.

In terms of users of the GRC tooling, a sound and clear role matrix could be developed allowing for segregation of duties between the three lines and where possible, this segregation is enforced via pre-fixed workflows.

An example maturity scale of centralized/decentralized (see full table in appendix):

Centralized / decentralized *“Measures the degree of centralization of the GRC solution”*					
HIGH	There is a single GRC solution across the Organization handled by a single central team to leverage resources. Any new component (e.g., acquisition of an organization with a legacy GRC) is forced to fit in the global tool thanks to the sponsorship of top management.	MEDIUM	A main GRC solution exists as a reference. There are however other tools doing the same thing with a high integration level (e.g., same granularity, taxonomy …).	LOW	There is a manageable number of diverse GRC solutions that enables to consolidate outcome from the different sources to get the full picture. The logic is to keep/promote GRC locally developed to fit with very different needs

The Use Case 1 presented in the next chapter illustrates a high level of use for centralization.

4. Challenges, lessons learned and critical success factors

This chapter describes the challenges, lessons learned, and critical success factors in the digitalization and automatization of GRC activities. It is reflective of experiences and learnings and by its nature is backward looking.

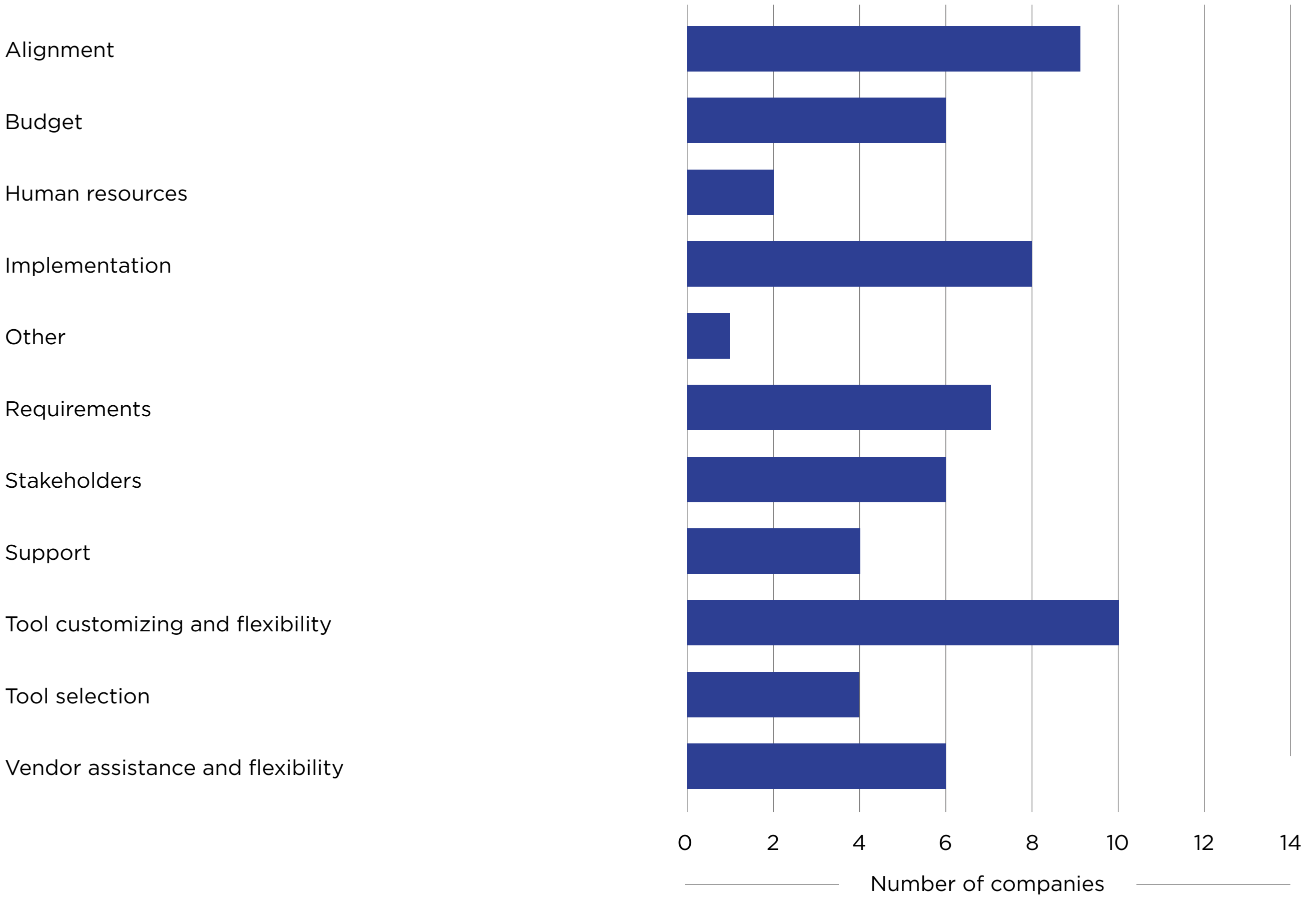
4.1. Main challenges

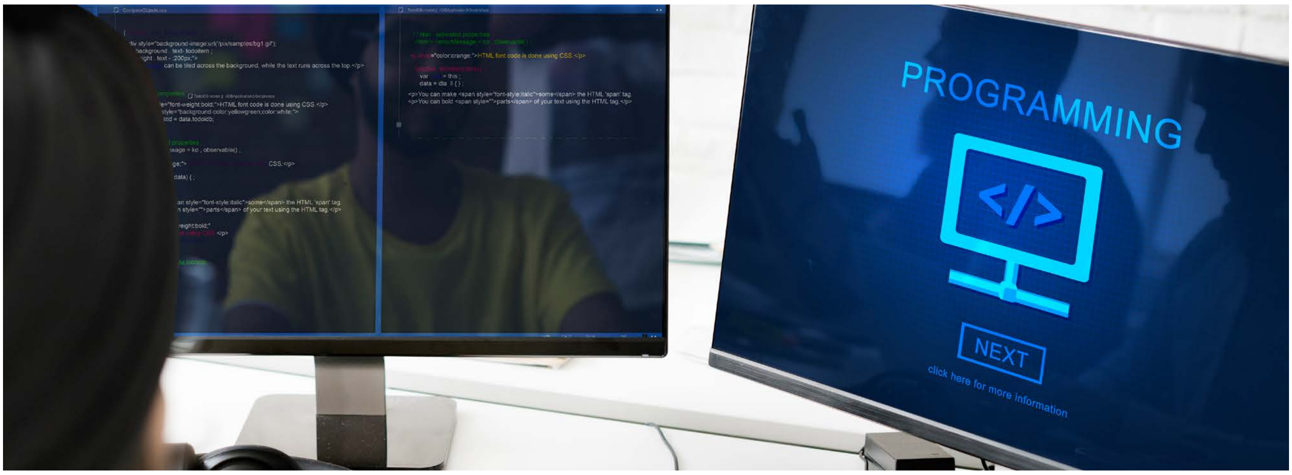
Most respondents in the survey indicated that **the tool customization and flexibility, alignment across all lines of defense, implementation and defining requirements** are the main challenges in using GRC tooling.

Generic IT hard preconditions such as tool customization and flexibility, alignment with users and business requirements are also hard preconditions for a successful GRC tooling implementation. These are included in the Digitalization Radar.

However, apart from the hard preconditions there are also a number of soft preconditions which are critical success factors in the digitalization of GRC activities. In the remainder of this chapter some of the important aspects of these soft preconditions are addressed. In addition, three use cases are described which highlight the different considerations, as also presented in this paper, and illustrate that there is not a one size fits all solution.

Figure 5: What are the main challenges in implementing and using GRC tooling in your organization?





4.2. Soft preconditions

Senior Management Sponsorship

When initiating GRC tooling, Senior Management/ Executive sponsorship outside of the immediate risk function is an important factor in successful delivery. It provides a clear statement that the tooling is something the organization wishes to have in place. More broadly, as part of the implementation, business user group forums can be established, as a conduit for explaining, to the first line, key aspects of the GRC tooling, taking their feedback and refining the GRC tooling proposal.

Second line should maintain relationship with (internal) vendor

The implementation of GRC tooling can be run like any other IT program with the second line used in evaluating the different proposals against the organizations needs and maintaining the relationship with the vendor or in-house IT developers to ensure the tool continues to evolve as risk management practices develop.

The IT support model needs to be clear, with a well-defined system administrator and user support roles. The use of first line IT helpdesks (as used for other applications in the organization) enables users to engage with the resolution of simple IT problems. The second line, however, should seek to retain a deep understanding of the system, and where appropriate have the capability to engage with IT to resolve issues and support further development of the tooling.

Second line should provide customised user training

Significant planning, risk management knowledge and expertise is beneficial for the implementation of GRC tools, even where the proposed systems is an “out of the box” solution.

Having determined the approach to tooling, it can still take considerate time to design the data structures, the operating model, the user work flows and “end user” experience. Whilst technologies are increasingly intuitive for use by users, there is also still a need for detailed training by second line, aligned with the different roles that users will be expected to play in the system operation.

Second line should keep up with digital transformation techniques

Change of digital (core) business processes often take the form of agile projects that are executed in swift and incremental changes. Over 60% of respondents indicated that agile methods and processes are also used for change projects in the GRC domain. On the other hand, the majority of respondents indicated that GRC departments did not change their organization, structure or working methods to align with modern digital change processes in the business. While this is not a must there is a risk of not being able to keep up with the first line from a second and third line perspective. For example, dynamic pricing of insurance policies via AI has implications for GRC topics like model valuation and privacy. Being in the loop at the right moment in case of important changes in the organization is critical for effective GRC functions and might require changes in the way these functions are organized. In addition, training staff in modern digital change methods and mindsets is a precondition to ensure effective oversight in the future.

4.3. Real life experience in practice from CRO Forum members

In this final section three real-life experiences from CRO Forum members are presented to illustrate the considerations discussed in this paper.

Use Case 1

An ambitious program to implement risk-based internal control capabilities

"…While we were equipped with solid operational risk management including regular risk assessment and risk scenarios, risk events collection, KRIs monitoring, risk remediation actions follow-up, we launched an ambitious program to implement risk-based internal control capabilities. The objective was to complement our operational risk management to contain operational risks through efficient and documented controls along the value chain and processes. It was clear that a GRC tool was required to accompany both first line in their responsibilities to operate and monitor a proper control environment over their identified risks, and second line in their challenge and monitoring responsibilities.

We started the journey over GRC tooling providing all functionalities to support operational risk management and internal control for core risks and key controls, for first and second lines users, across the group operations, in a **centralized solution**. However, we clearly had a view that we need to go further to integrate other sources of risk and controls, focused on specific risks such as security, compliance, data privacy …

This move towards integrated assurance embeds the challenge to optimize the coordination of the responsibilities of the three Lines and the capacity to seamlessly consolidate the various inputs.

It should result in avoiding or at least reducing 'information overkill' or conflicting information, minimizing disruption to the business (business fatigue), enabling better decisions based on a common view of risks, and ultimately increase efficiency and reduce costs for all three Lines.

We are progressing along the different stages of integrating assurance with some significant landmarks. Creating a **shared taxonomy** for risks categories, risk assessment approach, control documentation and efficiency assessment is one. Embedding these risk assessments, incident reporting, KRIs, control deficiencies, action plans monitoring in a single GRC with access for all three lines of defense is another area where we are gradually making progress (ref diagram). However, we have set clear boundaries to this platform to keep the focus. Operational risk is an umbrella to an increasing number of subject matter risk frameworks (information Security, Compliance, Data Privacy, Operational resilience, …). The decision to integrate these frameworks came with a limit to what was worth integrating to build a meaningful risk profile and overall assessment of controls. Experts must keep granular risk and control assessments, day to day operational incidents in dedicated and appropriate systems for all necessary detailed information (e.g., detailed security controls per platforms, servers…).

We identified several factors that allowed us to successfully move forward. Strong sponsorship is one of them with the conviction across second line functions of the benefits of building combined risk and control assessment capabilities notably for our common objective to empower first line to fully own and manage risks and controls.

User focus is critical, identifying the different roles and defining user profiles with optimized course of actions in the system, giving specific attention to the **user experience** for non-frequent, and thus mostly first line end users.

We set clear responsibilities among those profiles for example to monitor remediation actions or validate risk assessment with deliberately **limited workflows** steps to streamline processes.

Then we set **ownership** of the GRC system within Risk Management, having a direct relationship with the team in charge of the application, very close to our needs and ambitions, sharing our expertise and translating it in an agile mode in the GRC tool.

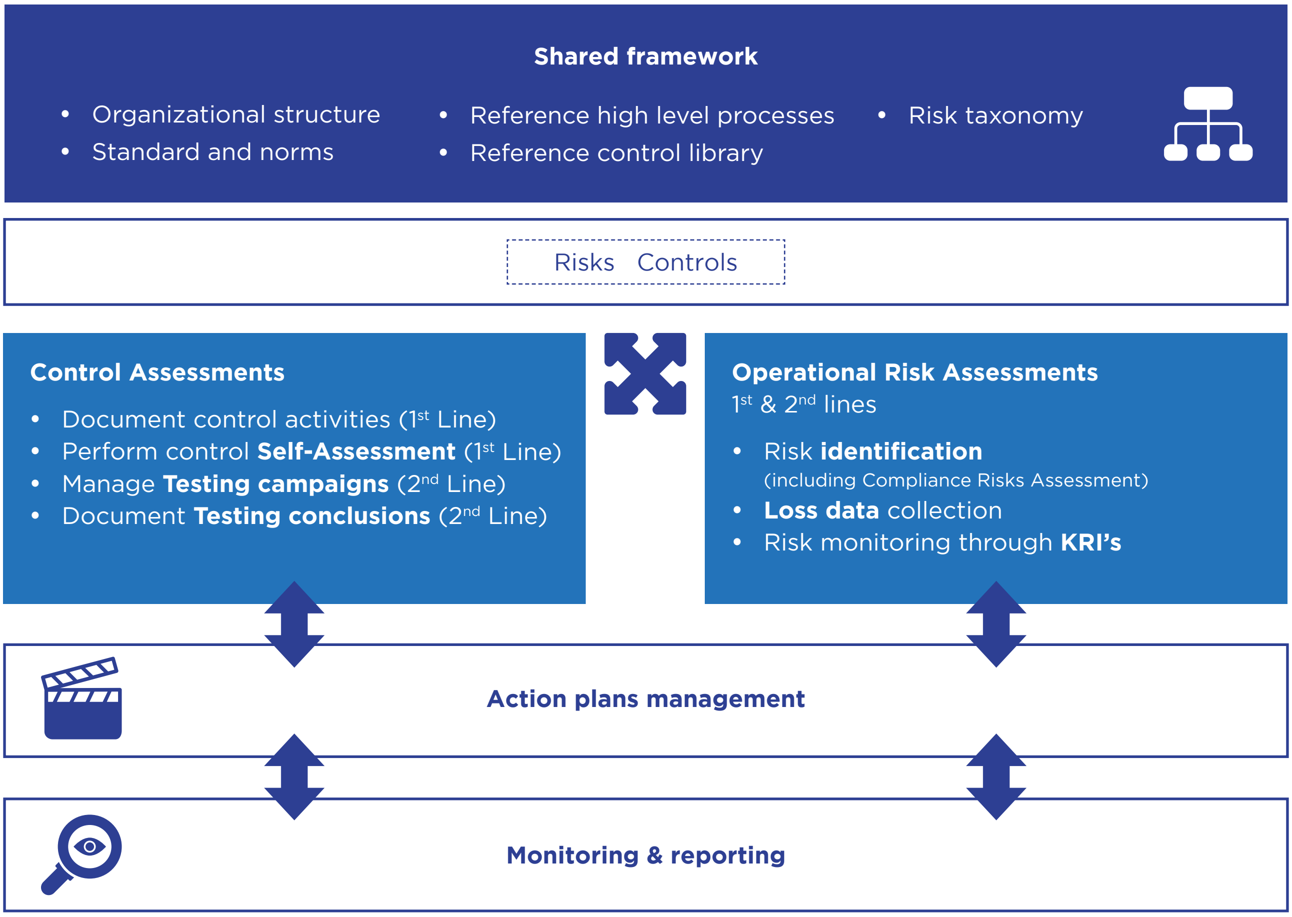
To serve our ambition for one source of knowledge allowing for digital monitoring of risk and control environment, we have split our reporting and analysis capabilities. In the GRC system for standards reporting, which is available for all users from all subsidiaries, the tool supports the day-to-day activities such as monitoring of risk assessment campaigns or KRIs collection, and then separately we have additional data analytics and data visualization environments and tools to explore, analyze, complement with other sources of data.

All these key success factors need continuous attention when expanding the GRC tooling. We need to continue to develop and improve User experience, sharing of data, performance of **analysis and reporting capabilities** while federating second and third line expertise. Regulation is pushing for more and more granularity with specialized authorities asking for dedicated frameworks (AML, ABC, Conduct, …) and we must demonstrate the value of shared frameworks and integrated assurance…"

In relation to the GRC digitalization radar:

- Functionalities covered: Risk assessments and analysis, internal controls, issue management, loss events, key risk indicators
- Golden source for operational risks and internal control information and reporting
- Integrated data across the modules
- Analytics and reporting capabilities real time in the tool
- Access provided to the 3 Lines is role-based
- Reference libraries, taxonomies are structuring the solution to enforce consistency

Figure 6: Core GRC system



Shared framework

- Organizational structure
- Standard and norms
- Reference high level processes
- Reference control library
- Risk taxonomy

Risks Controls

Control Assessments

- Document control activities (1st Line)
- Perform control **Self-Assessment** (1st Line)
- Manage **Testing campaigns** (2nd Line)
- Document **Testing conclusions** (2nd Line)

Operational Risk Assessments
1st & 2nd lines

- Risk **identification**
  (including Compliance Risks Assessment)
- **Loss data** collection
- Risk monitoring through **KRI's**

Action plans management

Monitoring & reporting

Use Case 2

A journey that started nearly 20 years ago

"...We have been operating a GRC system to support our operational risk framework for many years - and our journey started nearly 20 years ago when we recognized that the increasing complexity of our manual processes was drawing upon the time of our risk professionals to the detriment of more value adding risk management activities.

Our early GRC systems were built "in house" and focused on the documentation of key business processing risks and business attestations that key controls were operating, as well as the capture of risk events, issues, breaches and losses.

We moved to a vendor solution in 2010, using the learnings from our "in house" systems to select a tool that would fit the needs of our different businesses. Most vendor solutions we considered mirrored the basic functionality of our "in house" tools; therefore, the key factors in package selection were more focused on usability. This included workflow and how we could use it to ensure first line engagement in the system. The flexibility to build a data model that reflected our different businesses and enable changes in the future; and the plans and capabilities of the vendor to continue to develop the tool as risk management practices evolved. Other important factors related to data analytic capabilities; the ability for the first, second and third line to use the system such that all risks and issues were captured in one place; the ability for the service to be hosted allowing the service to be delivered across different IT domains.

Today we have around 1,000 users engaging with the system each month. The information collected, from a combination of control attestations, risk event and issues, provides good insight to the operation of the internal control environment. However, we are recognizing that operational risk is an umbrella for several risk disciplines including operational resilience, third party management and IT security and data privacy, and that trying to drive detailed risk management activities for these different disciplines is complex. Therefore, where practical we are building in detailed control tasks into first line systems that support these activities, and using data analytic tools to pull data from these systems and our GRC tool to provide a holistic view of our risk and control landscape. This has the benefit of users completing control tasks on the systems they use every day, and we can leverage the first line purchasing power for new systems. This does, however, require access to data analytic skillsets and this is an area we see as being increasingly important to ensure we understand the data that we now are able to source..."

Use Case 3

Adopting an eGRC system - A corporate communications and culture change exercise

"…In September 2022, we launched the initial phase of an eGRC platform with approximately 2000 users across the Group. The design, configuration and testing stages were completed within 12 months with 'Step 1' of the system (Operational Risk Module) delivered into the business on time for our annual Operational Risk assessments.

Approach

The aim of this implementation process, and the embedding of a new system, was implemented on a foundation of design principles and core aims:

- Replace current manual processes that do not add value
- Provide a standard and centralised Risk and Control library
- Support alignment of non-financial risk methodology
- Increase the use of common data and assessment
- Free up time for business and second line teams for more value-add activities
- Enforce clear business ownership and transparency of data and reporting
- Provide digitally enabled efficiencies

These aims and drivers were guidelines to be monitored for success whilst keeping the platform open for future integration with shared objects and processes across other business functions on the eGRC roadmap.

Lessons learned

During the 12-month development cycle, there were several technical challenges around data, permissions, workflows, and in-system decisions. The main hurdles for this case study, however, will center around implementing change and communicating effectively across the businesses. The core lessons learned around these topics were as follows:

- Ensuring the 'end (or interim) goal' is communicated effectively and clearly, even if this may change in the future.
- Understand how much progress has been made with Risk Management best practice across the Group and pitching the solutions accordingly.
- Acknowledge that there will be uncomfortable changes to ensure future alignment of processes, and try to identify these early.
- Embed a culture of the 80/20 rule; perfection can be the enemy of success.
- Ensure the businesses and key representatives are involved in the process.
- For each workstream, understand which stakeholders i.e. Regulators, CROs etc. need to be communicated with.

The importance of the delivery team

The Project Team, responsible for the design and adoption of the initial platform, recognized that the project had been started several times previously without success. A new and innovative delivery and communication methodology would be required to ensure delivery success; Working Groups at all levels of the business were created to ensure first and second line engagement from project commencement. A highly interactive internal social page was created containing update articles, videos, and training aids along with drop-in sessions to provide access to all those that would need to ask direct questions along the journey.

This level of close engagement relied heavily on the efforts, values, and characters of the Project Team. The make-up of this team was carefully selected to ensure a mix of skillsets to deliver this innovative approach.

Whilst the roadmap is in its infancy, the initial signs of adoption are promising, supported by analytical assessment of in-system and off-system data points. Key considerations for future integration will be understanding how future modules and shared objects will interact with the Operational Risk module…"

Appendix

Components / Modules

Risk assessments and analysis "A module allowing entities to perform on a regular basis risk evaluations and analysis on the (operational) risks, monitoring of the risk mitigation and reporting of the risk exposure."	HIGH	Performance of Risk Assessments fully integrated in GRC tooling and automated results reporting, integration with other modules and leveraging on other inputs (internal control results, KRI etc.).
	MEDIUM	Performance of Risk Assessments in GRC tooling but with limited possibilities - medium level of manual effort for data reporting readiness. Usage of external tools and minimum connection with other modules.
	LOW	Performance of Risk Assessment and Analysis outside of GRC tooling (e.g., Excel, own templates) but results uploaded in the tool.
Internal controls "Module that allows entities to perform controls, on processes and risks and reporting of the internal control performance."	HIGH	Performance of First and second level Internal Controls fully integrated in GRC, automated control creation, link with BPM and automated results reporting, integration with other modules and leveraging on other inputs (internal control results, KRI etc.). High frequency/real time dashboard updates.
	MEDIUM	Performance of Second level Internal Controls in GRC but with limited possibilities - medium level of manual effort for data reporting readiness. No or very limited connection with other modules (e.g., Input for Risk Assessments). Limited frequency of dashboard updates.
	LOW	Performance of Second level Internal Controls and out of the GRC (e.g., Excel, own templates) but results uploaded in the tool.
Issue Management "Level to which the issue management function is used across the organization."	HIGH	There is an ambition to handle all issues and recommendations arising from any source (first, second, third line, external audit, regulators …) with the GRC. Potential use by all the organization including externals. Action plans to remediate one or several issues are also documented. Custom workflows and fields are offered to the functions raising issues to fit their categorization and follow-up needs. Issue sources from other tools are interfaced with the GRC for reference. There is a regular and automated reporting on issues to different management levels. The reporting to governing bodies does not require manual walkarounds.
	MEDIUM	Issues and recommendations related to selected GRC components (e.g.,, controls, processes) are managed in the GRC. It is used directly by personal detecting the issue (including first line). This requires a significant training investment for non-risk professionals and quality reviews from the knowledgeable risk team to ensure data consistency.
	LOW	Issues and recommendations related to selected GRC components (Controls, processes) are managed in the GRC. It is mainly used by second line of defense that have a good understanding of the GRC hence limiting training efforts, misunderstandings, and licenses costs. The reporting to governing bodies cannot be achieved without completing GRC outcomes with other sources.

Loss Events "Data on internal losses entered, collected, stored in the GRC, feeding RCSA and reporting."	HIGH	Loss data directly input to the GRC in a specific module integrated with other modules, e.g., Risk Assessment, to improve quality of the evaluations. Reporting available on demand and customized, integrated with other modules. Data collected in real time with all the information related to the event.
	MEDIUM	Loss data directly input to the GRC, in a specific module that is not connected with other modules. Standard reporting available but not integrated with data of other modules. Upload possible in real time (based on the events). All the key details are captured in the system.
	LOW	Collection of loss data out of GRC but uploaded in the system massively, working only as a repository. Upload made periodically. Basic details on the characteristics of losses (related event, amount, date of occurrence).
Vendor Risk Management "Module of the GRC that collect the data on vendors and contracts (e.g., financial stability, blacklists compliance checks) to incorporate first line information and perform analysis and reporting, leveraging on a Risk Assessment approach."	HIGH	Vendors' data directly input to the GRC in a specific module able to define a synthetic scoring on the Vendor risk and to perform analysis on the contracts' risks. Module integrated with other modules, e.g., Risk Assessment, to improve quality of the evaluations. Reporting available on demand and customized, integrated with other modules, able to produce Key Risks indicators.
	MEDIUM	Data on vendors and contracts directly uploaded to the GRC on demand, in a specific module not connected with the others. Standard reporting available but not integrated with data of other modules. Upload possible in real time.
	LOW	Data collection on vendors and contracts performed out of GRC but uploaded in the system to contribute to RCSA and reporting purpose.
Model Risk Inventory the critical digital solutions (Models, EUCs) and assess quantitatively the risk to use. It also enables to ensure appropriate mitigants are in place and calculated the residual risk."	HIGH	An entire module is administered by a dedicated team to manage the framework. Relationships are established with existing GRC components to assess the model risks and report on it regularly.
	MEDIUM	There is an ambition to recognize that model risk justifies a dedicated treatment (e.g., for regulatory purpose). However, a customization of existing GRC modules is sufficient to handle it.
	LOW	As being a subset of operational risk, the model risk is assessed in the same way as the other risks. Nothing specific developed.
Model Development "Model refers to the architecture of the system and how the eGRC is positioned in the organization to provide value. Not to be confused with Model Risk." Functionality for the Development of internal and other models.	HIGH	A full working plan is established with executive buy-in, established long term budget plans and sponsorship. Clear implementation plan with module drop-ins across an agreed time period. Data plan in place to ensure cleanliness of system. Roll out and adoption plans in place to ensure first line buy in.
	MEDIUM	A coordination committee is established and some consideration for 'final state' has been discussed. Exact plans are unavailable, but a general direction of travel is agreed with a timeline for adoption and implementation of future modules and capabilities. Executive sponsorship exists.
	LOW	Low level of coordination with module developments. Independent progression of modules with little consideration for future integration and alignment. Differing agendas, budgets and intentions allow for limited implementation OR adoption.

IT Risk Management "This model focusses on the management and setup of IT risks within the organization."	HIGH	IT risk management is considered a value driver and proactively used for day-to-day decision making and pursuit of opportunities. KRIs and predictive risk analytics are proactively used to identify and monitor IT risks. Advanced and sophisticated IT risk management processes are used.
	MEDIUM	The organization is proactive in IT risk management. IT risk management is consistently and fully implemented across the organization. Key risk indicators are used for major IT risks. IT risk management processes are monitored and reviewed for continues improvements.
	LOW	An IT risk management framework exists with defined and documented IT risk management principles. IT risk management applied consistently throughout the organization. Some processes in place and implemented.
Business Continuity Management "Business Continuity Management module including BIA, third party options and recovery plans. Incident, issue, action and remediation objects available."	HIGH	BCM is an integrated module which allows for update within other module objects. BCM data fields form part of any Operational and non-financial risk elements. BCM policies and recovery times are built into incidents and automatically trigger notifications to internal stakeholders on input. There may also be an external notification option to third party providers.
	MEDIUM	BCM is a standalone module within an eGRC platform and requires separate input from any other module i.e. OpRisk. The benefit of this standalone module allows for independent assessment across BCM data fields and allows for cross business and country assessment and trends.
	LOW	BCM is not a standalone module in an eGRC system but data from an Operational Risk module. In particular incidents, issues, impacts are extracted for BCM reporting and analysis. Although not specifically referenced as BCM data, cross business and country data can be extracted for reporting and analysis.
Policy and Compliance management "This module aims to manage internal policies and/or guidelines."	HIGH	The GRC is the central place where all the policies are consistently stored and updated. The staff completes regular policy attestations. Policy exceptions are reported. The Policy framework is integrated with related processes and controls.
	MEDIUM	Key policies are stored in the GRC. Targeted staff access directly the relevant documents according to their location/activity. The lifecycle of the documents is also supported by the GRC.
	LOW	The GRC is used to store some Policies and Guidelines related to preexisting GRC objects (e.g., controls).
Data Quality Management "This module aims to manage the data quality risks in the GRC."	HIGH	An entire module is administered by a dedicated team to manage the framework. It allows to visualize the dataflows and transformation steps of key business data. The reports demonstrating that each key data across the organization is accurate, appropriate and complete are generated by the GRC, thanks to the data/controls relationships. It includes processes to prioritize data.
	MEDIUM	There is an ambition to recognize that data quality risk justifies a dedicated treatment (e.g., for regulatory purpose). However, a customization of existing GRC modules is sufficient to handle it.
	LOW	As being a subset of operational risk, the data risk is assessed with the same way than the other risks. Nothing specific developed.

Key Risk Indicators "Module to collect different risk indicators from difference sources, stored in the GRC, feeding Risk Assessment and reporting."	HIGH	Key Risk Indicators fully integrated in GRC, automated results reporting, integration with other modules and connection with external databases.
	MEDIUM	Key Risk Indicators partially calculated in GRC and partially coming from outside; limited possibilities - medium level of manual effort for data reporting readiness. No or limited connection with other modules (e.g., training courses delivered; sanctions; allegations).
	LOW	Key Risk Indicators recording in GRC (e.g., Excel, own templates) but results evaluated outside the GRC.
Audit Management This module allows management of internal audit activities (from the proposal to the execution) - reviewing and tracking the results with the capacity planning and scope of the engagement - and report all results through issues and remedial actions monitoring."	HIGH	All data related to the Audit Management phases are input to the GRC in a twofold mode: massively or directly on the System, in an agile and user-friendly manner. The Audit Management phases are coordinated and managed with an automatic workflow, allowing interaction between both internal members and external / business contacts. The reporting templates are automatically pre-filled based on information input (text, image, table, etc.) and the document review is performed directly on the system. The results are exported and connected to external Tools in an easy way in order to effectively share data.
	MEDIUM	Audit Management activities are managed in GRC through a workflow that can be customized according to methodological requirements and countries' exceptions. For reporting purposes, the System provides pre-filled templates with only text entered in the dedicated fields.
	LOW	All data related to the Audit Management are just stored in GRC, but the workflow is managed outside: the GRC works just as a data repository.

Data

APIs "The capability of the GRC solution to be easily integrated with external systems to manage automatic inbound / outbound data flows."	HIGH	The GRC solution provides a very wide set of defined and documented APIs, that support the online event-driven or batch scheduled interaction with other systems for all the use cases throughout the supported processes, such as the full automation of the controls performed by first and second line of defense.
	MEDIUM	The GRC solution provides a limited set of defined and documented APIs, that support the online event-driven or batch scheduled interaction with other systems for key use cases, such as the import of the legal entities data and their organizational structure, or the import/ export of ORX data.
	LOW	A minimum set of automatic data extracts are available, such as periodic scheduled feeds towards a data warehouse/data lake for reporting and analysis.
ORX Use "Integration of the external losses data collected by ORX consortium into the GRC."	HIGH	ORX data directly uploaded to the GRC via connection with ORX tool, in a specific module integrated with other modules, e.g., Risk Assessment to improve quality of the evaluations. Reporting available on demand, customized and integrated with other modules' report.
	MEDIUM	ORX data directly uploaded to the GRC via connection with ORX tool, in a specific module that is not connected with other modules. Standard reporting available but not integrated with the other modules' report.
	LOW	ORX data uploaded in the GRC massively even if collected externally.
Big Data "The GRC tooling is used to collect high volumes of data for the purpose of data analytics."	HIGH	Large, clean data is contained within the system and updated to ensure relevancy and timeliness. Key data analysis can be undertaken providing business insights. These insights can be extracted and used across businesses and group-wide functions or interrogated further to provide bespoke results.
	MEDIUM	Fairly clean data across most areas of interest which lacks completeness in parts or updated sources. Used for limited trend analysis and decision making but would need corroboration for key decisions.
	LOW	Unstructured limited data input in to the GRC system which provides the basis for further confidence assessments.
Golden Source "The GRC is used as golden source or to determine where the golden source is for each critical data."	HIGH	The eGRC system is fully embedded, trusted and provides tangibles outcomes for decision making and risk/control awareness. As such, it is the golden source of information and the first place for risk information within the organization.
	MEDIUM	There is general confidence in the system, but this is not entirely used across all geographies or in all businesses. Certain modules may be trusted more than others and a golden source for some. Inconsistency of approach means the system is not established and fully adopted.
	LOW	eGRC system is utilized to support some decision making and information analysis but is seen as an input for consideration only and not a source of truth that can be relied upon.

Technology

Integration "The level of interoperability of the different functional modules (e.g., Risk Assessment, Loss Events, Audit Management, BCM, …) of the GRC solution, enabling data alignment and process automation."	HIGH	All the data that are needed across more than one functional module are shared and managed in order to grant the overall coherence of the different views, enabling advanced reporting and data analysis from different perspectives. Moreover, versioning of the different data snapshots is supported, so that historical data are fully managed across the different functional modules.
	MEDIUM	Most of the data that are needed across more than one functional module are shared and managed in order to grant, for that data, the coherence of the different views, enabling standard reporting and data analysis from different perspectives.
	LOW	A minimum set of data are shared across the functional modules, e.g., only the alignment of the legal entities' hierarchy is enforced.
Analytics/ Reporting "Level of use of the reporting capacities of the GRC."	HIGH	There is a real time reporting culture in the organization, a large part of the required information is directly available upon request with reports and dashboards. The internal report writing resources are sufficient to develop complex report and dashboards from the GRC data and other sources. AI based & advanced data analytics techniques are being explored/developed to explore GRC data. Most of the reports doesn't require any manual proceeding to meet the requirements.
	MEDIUM	The tool and the internal administration team are capable of simple report writing based on the GRC data. Complex reports are handed over to reporting specialists. Some reports / dashboard could be directly used during workshop or committees or to meet internal and external reporting standards without reworking. There is no ambition to develop AI based data analytics.
	LOW	The reporting from the tool is provided out of the box. For requests demanding more, data dumps are available to process the linkages outside of the tool (e.g., in Excel, Power BI …). There is no ambition to develop internal report writing capabilities. The data has in most of the cases to be processed or formatted manually or semi manually to meet the internal and external reporting requirements.
Workflow "Level of use of Workflow capabilities provided by the GRC."	HIGH	The GRC workflows are used to handle business topics of the first line such as approval of deals, pavement of claims, authority management … The central team offers customized workflow developments for business use cases.
	MEDIUM	A central team handles relatively complex workflows on GRC objects (several branches, number of approvals depending on object fields and conditions). The scope is limited to the GRC objects.
	LOW	Out of the box basic workflows exists and are in use to ensure basic tasks such control assessments or issue validation. The roles are simply defined. The workflow rules (e.g., number of approval steps, conditions) cannot be easily changed.

AI "Level of use of Artificial Intelligence related to the GRC tooling."	HIGH	Validated, compliant and monitored AI techniques are embedded into systems to deliver Realtime decisions and information to the GRC process. Self-learning aspects of these systems are continuously monitored and controlled for compliance and validity. State of the art methods like deep learning and neural networks are applied to reach optimal and smooth performance beyond human capabilities. Methods and techniques are in line with EU regulations and regulatory guidelines.
	MEDIUM	AI techniques are used for decision support and guidance. Integrated AI applications process and analyze data using less complex models to generate indicators, scores and other results. These results are used by humans to assist in decision making, especially in situations where data volumes and number of variables are high.
	LOW	AI techniques are used ad-hoc and decentralized to analyze distinct use-cases or incidents, sometimes in the form of pilots. Outcomes are helpful to understand and analyze data and risks. Outcomes can be used to amend key risks and controls or to re-evaluate and gather extra risk and control data. Tooling is open source, local and not fit for production purposes.
RPA	HIGH	RPA is deployed on a large scale to support GRC tasks and control automation. RPA runs automatically in the background on enterprise IT infrastructure. There is mature governance around management, compliance and IT security of RPA solutions. An example can be the automated screening and redacting of content on databases for privacy issues.
	MEDIUM	Proofs of concept are set up for isolated and non-production environments. These cases concern Robotic Desktop Automation (RDA) that can perform defined or recorded human actions under human supervision. RDA works visibly and on screen on the user's PC or laptop.
	LOW	Proofs of concept are set up for isolated and non-production environments. These cases concern Robotic Desktop Automation (RDA) that can perform defined or recorded human actions under human supervision. RDA works visibly and on screen on the user's PC or laptop.
Test Automation "Measure how far the organization can run tests by robots."	HIGH	Many test cases are defined, covering roughly 80% of the used processes and functionalities within the GRC tooling scope. These test cases are run automatically by a dedicated test team before an implementation of a new release, but it can be run any time, or on a continuous basis if required. Test cases are adapted continuously in case of functionality and use case enhancements. Individual tests by users are limited to few individual specific tests not covered by test automation. The goal is to reduce dedicated user testing as much as possible, ensure high-quality deliverables, and could detect exceptions very quickly. Test case results are automatically produced and stored for audit purpose.
	MEDIUM	A list of test cases is defined, covering roughly 30% of the most used processes and functionalities. These test cases are run automatically or partly manually before an implementation of a new release to ensure quality and stability. Specific user testing is still needed but limited. The goal is mainly to increase the base quality of the deliverables.
	LOW	Test cases are defined for a few critical cases. They are run automatically or manually by scripts before an implementation of a new release to avoid severe malfunction. Enhanced user testing is still heavily done to ensure the quality of the deliverables. The goal is mainly to deliver a release to the test persons without critical errors.

Ease of Use “Measures the efforts invested to customize the GRC system in order stick to companies’ processes, while keeping a high-end user satisfaction.”	HIGH	High adaption is ambitioned to customize the system for a very good user experience according to the needs of each group of end users and to have the tool fitting with the risk management practices. Depending on different profiles (e.g., line of defense, business unit, use case ...), the end user is immediately directed to what matters for him. The system is sufficiently flexible to allow a central team having the capacity and the skills to modify its look and feel (views, filters ...), include targeted guidance, dashboards and reports. Satisfaction surveys on the user friendliness are regularly conducted and analyzed for continuous improvement. Active discussions with the vendor are led to report improvement collaboratively.
	MEDIUM	Basic customization is possible to internally influence the end user experience. Compromises / balance should be found between customization costs and adaptation to risk management practices. The views are adapted to the public using it (e.g., differences between first, second and third line). The guidance is mainly given by means of dedicated training and is not integrated.
	LOW	The system is mainly meant to be used out of the box with limited capacities to modify the look and feel. The selection of the tool already integrated the end user experience. Modifications of the views are very limited (e.g., limited to the new fields created) and mainly done by the vendor by means of new releases. All users (including admins) use the same interface. The risk management practices should often be adapted to fit with the logic of the tool.
Real time metrics “Audit Management is a solution that involves multiple applications and allows to manage internal audit activities (from the proposal to the execution) - reviewing and tracking the results with the capacity planning and scope of the engagement - and report all results through issues and remedial actions monitoring.”	HIGH	The eGRC system has automated data inputs or timely updates by proficient users to ensure real time metrics can be produced or read off an eGRC dashboard or report. The data sources are verified and trust in the system is high with high adoption across the organization.
	MEDIUM	Real time metrics provide some key metrics within the organization. This, however, is limited and only accessible (useful) to some for onward reporting. Inputs are sporadic and inconsistent with reminders needing to be sent to ensure 'real time' status achieved in practice.
	LOW	Limited metrics in the system highlight certain areas of health or insights within the organization. This is limited to 1 or 2 locations and not adopted by personnel due to lack of timeliness and trust.
Control automation	HIGH	Most controls are automated via the control by design principle. Controls are embedded in systems and applications where they naturally occur. The automated controls are therefore part of the regular IT governance and management. Reporting on controls is fully automated, real-time and always available.
	MEDIUM	More controls are automated using RPA and other techniques. There is a periodical reporting connection to an enterprise control management system. An example is the automated control and reporting on mandatory employee training programs.
	LOW	Some examples of control automation are present, mainly in the IT department. Some IT controls such as patch management for non-critical infrastructure are fully automated and reported. There is no connection to an enterprise control management system.

Organizational Model

Scope “Defines to what extend the use of the GRC is seen as an expansion factor.”	HIGH	The GRC is seen a central asset for the organization. For every main key project (new entities, business …) there is a systematic impact analysis on the potential to include or connect the GRC to it.
	MEDIUM	Some modules of the GRC outside of its initial purpose have been, or are being developed in the area of Governance, risks and compliance.
	LOW	There is an appetite to integrate other modules to the GRC, but not systematically. The priority is given to the functionalities offered by tools rather the expansion of the GRC.
Centralized / decentralized “Measures the degree of centralization of the GRC solution.”	HIGH	There is a single GRC solution across the Organization handled by a single central team to leverage resources. Any new component (e.g., acquisition of an organization with a legacy GRC) is forced to fit in the global tool thanks to the sponsorship of top management.
	MEDIUM	A main GRC solution exists as a reference. There are however other tools doing the same thing with a high integration level (e.g., same granularity, taxonomy …).
	LOW	There is a manageable number of diverse GRC solutions that enables to consolidate outcome from the different sources to get the full picture. The logic is to keep/promote GRC locally developed to fit with very different needs.
1/2/3 line “Measures the degree of penetration of the GRC in the organization across the 3 lines model.”	HIGH	Any person of the organization uses regularly the GRC (e.g., to pledge adherence to the code of conduct). This includes personal that are not necessarily risk owners. The GRC is also used by third parties (Regulators, auditors, rating agencies …).
	MEDIUM	The business (first line) completes tasks in the GRC on a regular basis. Some business processes/ use cases are directly integrated in the GRC.
	LOW	The GRC is used by specialists such as risk management, compliance, actuarial and audit functions, but the business do not directly use it.
Ownerships “Measures how the ownerships of the organization are enforced by the GRC.”	HIGH	It is intended that the GRC contains all key roles and responsibilities of the organization as a golden source (not limited to processes but also to business units' owners, CEOs, legal entities). To some extent, it extends the organizational/legal aspects (Org. chart, legal org. chat).
	MEDIUM	All Key GRC stakeholders (e.g., process, risks, control owners) are listed in the tool and are aware of their responsibilities. However, the GRC only contains ownerships related to its scope.
	LOW	GRC tasks are sent to the responsible persons, but there is no ambition to have a comprehensive list of ownerships in the GRC.

Access Management “Defines the flexibility and granularity how access can be granted to specific use cases, functionality, objects, controls and processes. This includes a powerful role-based access concept, dynamic UI based on the access rights, handing confidentiality of data on reports and data extracts. Based on the access rights individual users are allowed to create, edit, delete or read the data.”	HIGH	The role-based access control on multiple levels like use cases / functionality, objects, controls, and processes is fully implemented at a high granularity. Access roles of all users are regularly monitored, yearly validated, and signed off. Dedicated group of people handles the access, following segregation of duty principles. User interface is dynamically set up to show features, fields and data referring to the access rights. Restriction on confidential data is fully supported. Admin access is very limited to small number of people.
	MEDIUM	Role-based access control is implemented, but more generally handled on either functionality, controls, legal entities, or processes. Users may get more access rights than needed. Access is granted by a dedicated group verifying the access requests.
	LOW	Access is granted more generally by providing a dedicated group of people the same access. Access rights are clearly distinguished between create, edit, delete and read access to data. Admin access is limited to small number of people. People trying to access restricted pages and data get an appropriate message.
Methodology/ Libraries “Defines to what extend the concept of libraries (i.e. place where to find templates, or blueprints of GRC objects) is used.”	HIGH	It is mandatory to use certain library objects (Processes, risks, and controls) based on clear criteria’s (e.g., upon decision of a business unit head). The library is kept up to date and triggers on update synchronization of related elements (e.g., when the description of a control is updated in the library, the places where this controls is instanced are also updated, with appropriate notifications). Hence libraries play here a key role on driving consistency of practices across the organization.
	MEDIUM	A complete library exists for items requiring a common taxonomy as a reference (e.g., risk library, regulation library…). It is not intended to streamline the operations with the library.
	LOW	Simple libraries of GRC objects are available (e.g., used as examples of processes, risks, or controls). The use is voluntary and the library doesn’t claim for completeness.

Disclaimer

Dutch law is applicable to the use of this publication. Any dispute arising out of such use will be brought before the court of Amsterdam, the Netherlands. The material and conclusions contained in this publication are for information purposes only and the editor and author(s) offer(s) no guarantee for the accuracy and completeness of its contents. All liability for the accuracy and completeness or for any damages resulting from the use of the information herein is expressly excluded. Under no circumstances shall the CRO Forum or any of its member organisations be liable for any financial or consequential loss relating to this publication. The contents of this publication are protected by copyright law. The further publication of such contents is only allowed after prior written approval of CRO Forum.

The CRO Forum is supported by a Secretariat
that is run by KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org