# Governance, Risk and Compliance (GRC) software
## Business needs and market trends

**David Cau**
Director
Business Risk
Deloitte

The importance of a holistic view of risk and compliance issues and the difficulty to achieve it is often recognised as a weakness for many organisations. As an indication that significant improvements may be required at many organisations, the recent Deloitte Global risk management survey (eighth edition) reveals that when asked about their capabilities of their data strategy and infrastructure, no more than one-third rated them as extremely or very effective in any area.

As an organisation progresses in developing its risk management, internal audit and compliance practices, the issue of investing in an automated solution to improve efficiency will arise sooner or later.

### Tools for governance, risk and compliance functions

First of all, it is important to clarify the concept of GRC. Although various definitions do exist, the definition proposed by Nicolas Racz, Edgar Weippl and Andreas Seufert in their recent research paper 'Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)' provides a rather comprehensive view of the concept. In this paper, GRC is defined as "*an integrated, holistic approach to organisation-wide governance, risk and compliance ensuring that an organisation acts ethically correct and in accordance with its risk appetite, internal policies and external regulations through the alignment of strategy, processes, technology and people, thereby improving efficiency and effectiveness*".

The primary purpose of GRC software is therefore to automate much of the work associated with the documentation and reporting of the risk management and compliance activities that are most closely associated with corporate governance and business objectives. The primary end users include internal auditors and the audit committees, risk and compliance managers, and accountable executives. The key functions of GRC software are usually the following:

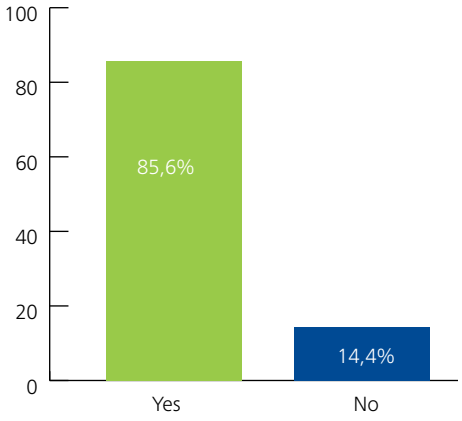
- Audit management functions that support internal auditors in managing work papers, and scheduling audit-related tasks, time management and reporting
- Policy management features that include a specialised form of document management that enables the policy life cycle from creation to review, change and archiving of policies; mapping of policies to mandates and business objectives in one direction, and risks and controls in another, as well as the distribution to and attestation by employees and business partners

- Compliance management functions that support compliance professionals with the documentation, workflow, reporting and visualisation of control objectives, controls and associated risks, surveys and self-assessments, testing and remediation. At a minimum, compliance management will not only include financial reporting compliance (e.g. SOX compliance), but can also support other types of compliance, such as industry specific regulation (e.g. ISO 9000) and compliance with internal policies
- Risk management functions that support risk management professionals with the documentation workflow assessment and analysis reporting visualisation and remediation of risks (as defined in ISO31000). This component focuses generally on risks and incidents follow-up but may also collect data from risk analytics tools (Credit Risk, Market Risk, etc.) to provide a consolidated view of risks

### The GRC software market: the business need

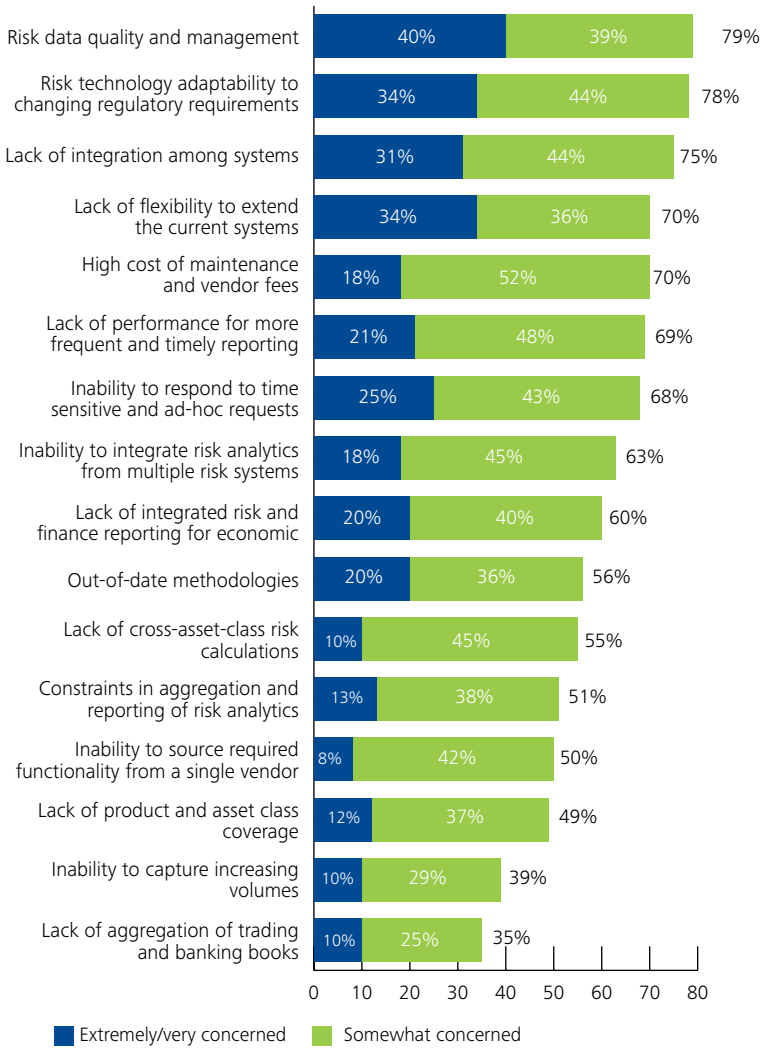
- Most organisations are aware of the need for a significant improvement in the way they manage their risk, internal audit and compliance functions through better automation of data and information. As illustrated by an OCEG survey, 85% of companies interviewed are convinced that they would benefit from integrating the use of technology for their GRC activities. The need for a GRC technological solution is there, but the question remains: which technological tools will be able to provide the appropriate solution?
- In the eighth edition of the 'Deloitte Global Risk Management Survey', organisations cited a number of concerns about their risk management information technology systems (Figure 2)
- Among the main concerns addressed, the ability of organisations to easily upgrade or revise their systems risk technology, 78% of companies are extremely, very or somewhat concerned about their ability to adapt to changing regulatory requirements, as well as the lack of flexibility to extend the current systems. Related to this issue, 75% of organisations are extremely, very or somewhat concerned about a lack of integration among systems and 63% of the organisations have issues with an inability to integrate risk analytics from multiple risk systems. Many organisations maintain different information systems for specific products or geographies, sometimes due to past acquisitions, and it can be difficult and expensive to combine their output or else to replace them with an integrated information system
- Moreover, the pace of regulatory change has put the emphasis on the ability of organisations to have risk systems that can respond quickly to new requirements. This appears to be a concern especially for larger institutions: 40% of large institutions said they were extremely or very concerned about the ability of their risk technology to respond to new regulatory requirements, as did 44% of mid-size institutions and only 12% of small institutions
- Some of the other top priorities for investment include risk analytics and risk reporting: risk analytics (53%), real-time risk monitoring (51%) and risk dashboards (44%)
- But the fastest growing business need relates to risk data quality and management, with 79 % of institutions at least somewhat concerned, including 40% who are extremely or very concerned. Creating consistent data standards is a challenge for organisations, which often source data from multiple locations with incompatible data formats. Further, departments within an organisation may not realise that they both have a relationship with the same counterparty as each may do business with a different business unit or subsidiary

Figure 1: Would your organisation benefit from integrating and streamlinning use of technology for GRC activities enterprise-wide?




The need for a GRC technological solution is there, but the question remains: which technological tools will be able to provide the appropriate solution?

Figure 2: How concerned is your organisation about each of the following issues for its risk management information technology systems?



## The GRC software market: the offering

### Market overview

The GRC market as defined by the technology industry is about 10 years old, and buyers have high expectations for the performance of GRC software.

Up to now, from a technical perspective, organisations have generally opted for risk management systems installed in-house, whether developed internally or by vendors, rather than hosted externally. Indeed, according to a recent Deloitte survey, roughly 40% of organisations said they were likely to make a major investment over the next 12 months. Among these organisations, 45% were considering internally-developed applications, while 41% would rather opt for third-party vendor applications installed in-house (41%). Third-party vendor applications hosted by a vendor (20%) were cited less often as a target for major investment. Data privacy concerns around confidential information being hosted off-site may well be a reason this last approach seems to be adopted less often.

The GRC software market is dominated by key players like IBM, RSA Archer, Thomson Reuters, SAP or Oracle. Deloitte has established strong strategic and technical alliances with these key players in order to better serve the clients that have opted for these softwares. But the market is still offering a significant place to niche players (e.g. MetricStream, Sword, Checkpoint, Mega and Aris). Moreover, the GRC market seems to be thriving, as more companies realise that they pretty much have to invest in this area, and so the market landscape might rapidly evolve as a result.

It is important to mention that this market segmentation is more a question of size of vendor rather than a significant price differentiation. Price is key, as sometimes the business case for GRC software is often strongly questioned and budgets for GRC software are often limited in most of the companies and licence fees or, more globally, the Total Cost of Ownership (TCO), namely the cost of development, implementation, licence fees and maintenance of a GRC solution is usually similar.

Most of the recent market studies forecast an annual rate of increase of 10% over four years. Indeed toward the end of 2011, after the market had grown 18% in 2010, Forrester Research data suggested a CAGR of 14% or so through 2015. TechNavio, for its part, has recently forecast that the Global GRC software market will grow at a CAGR of 9.2% over the period 2012-2016, driven by *"increasing demand for comprehensive solutions"*, which seems to favour the biggest players in the industry, such as EMC, IBM, Thomson Reuters and the big ERP players (SAP and Oracle), though it is worth mentioning that projected growth rates in previous years have been even higher.

A strong consolidation, with a shift from best-of-breed players to well-established vendors will also be a key market trend. This consolidation trend will be driven by the need for greater investment in complex risk analytics to face the 'big data' problem of the vast majority of organisations.

Differentiation today is also about the ability to deliver against multiple use cases, and provide advanced risk management functionality, with analysis of the impact of risks on strategic objectives and business performance, domain expertise in multiple highly regulated industries, ease of use—including mobile capabilities—and configurability.

**GRC software market view in Luxembourg**

The GRC software market is still emerging in Luxembourg, but the situation is rapidly evolving and differs among sectors.

In Luxembourg the banking sector is already well equipped with various niche solutions covering one specific aspect of risk (market risk, credit risk, operational risk, liquidity risk) and compliance. This sector is facing the issue of a lack of integration of its various solutions and has difficulty in migrating or integrating the various applications into an overarching structure. However, the recent CSSF circular 12/552 is already contributing to the development of the GRC market as this new regulation recommends more and more efforts on common governance on risk and compliance issues.

Investment management, a key sector in Luxembourg, is up to now significantly underequipped with GRC software. The main reason seems that investment management sector is highly fragmented with various actors, who are still overwhelmed by the operational management/set up of regulations, such as AIFMD or EMIR. Moreover, it has to be said that the vast majority of GRC players is not offering the appropriate solutions to this sector: both pricing models and key features proposed by GRC vendors are not yet fully adapted to this market.

The insurance sector is increasingly interested in GRC solutions, but either local players are part of international groups and have to use (or wait for) the corporate solution or they are small and cost is often perceived as a key hindrance for a the implementation of a GRC software.

The industry and public sector is increasingly ready and interested in GRC software and is generally starting its GRC project with the implementation of an operational risk application/module. New regulations such as REACH, CLP or quality-related recommendations are also pushing the industrial sector to enhance its holistic approach of risk, internal audit and compliance.

**Key trends affecting the GRC software market**

The functions of GRC software are evolving on the basis of several trends, which include:

- A growing need for internal audit features as organisations face increasing regulatory requirements, GRC oversight and demands for more business performance audits
- An increasing need for regulatory content services and change management to deal with regulatory proliferation. In the aftermath of the 2008 global financial crisis, GRC has to support the transparency objectives of regulators and decision making by business leaders. Currently the regulatory focus of the software is on anti-corruption and bribery
- The development of risk analytics to support integration of risk management and performance management
- The emergence of third-party risk management to ensure that third parties do not present unacceptable compliance and risk
- A focus on operational technology and critical infrastructure protection, which increases the variety and volume of risk and control data ('big data' management)

Moreover, the GRC market seems to be thriving, as more companies realise that they pretty much have to invest in this area, and so the market landscape might rapidly evolve as a result

## GRC software selection

### Usual approach: vendor selection based on 'quadrants'

Most companies that are opting for third-party GRC software tend to base their GRC software selection on GRC market 'quadrants' analysis, mostly performed by Gartner and Forrester. Instead of simply showing statistics or ranking companies in lists, GRC market 'quadrants' use a two-dimensional matrix to illustrate the strengths and differences between vendors.

The most common criteria used by these quadrants are the ability to deliver GRC functions (audit management, compliance management, policy management and risk management) and a credible presence in the marketplace (an existing enterprise GRC client base, a growth strategy and brand, support capabilities, a strategy for and investment in continued innovation in GRC solutions and related products, geographical reach and financial strength).

However, these quadrants may lead companies to limit their GRC tool selection process only to the vendors mentioned in the quadrants, or even only consider players from the leader's quadrant and initiate their choice only from an IT standpoint, rather than also considering the business needs.


### Deloitte holistic approach

The key driver for the holistic approach of a GRC software selection process is the agnostic position of Deloitte regarding technological solutions.

The main purpose is to find the solution that gives the best value for money for clients. Deloitte uses a well-proven methodology that will guide the client through the evaluation process for software options, allowing the client to make a decision based on a sound analysis. The selection process generally encompasses seven phases (as illustrated in figure 3).

It will be important to start a GRC selection project with a deep analysis of the client's business needs and context in order to formalise the functional coverage. Then, a clear view on the client's current IT environment (existing specialised solutions or enterprise solutions—ERP) has to be obtained. These analyses will help to see if the best option will consist in developing a new solution internally, buying a packaged solution or opting for a best-of-breed solution. These reviews will also enable to evaluate if, given the current situation, the implementation is realistic.

If the best option identified consists in the implementation of a third-party/vendor solution, it will be necessary to see how we can identify the best solution on the market from the wide range of software currently available. Five key areas of criteria will enable to select a list of potential candidates that will be able to make live demo (based on specific client requirements). Lastly, price negotiations and final technical adjustments discussions will come into play in order to select the target solution.

Deloitte's specialists will therefore help clients throughout their selection process, providing specific support when it comes to performing an analysis of requirements, and helping to draft calls for tender, conducting research on the software market and offering a selection of appropriate suppliers or making the final decision through coaching, support and analysis.

In a nutshell, integration is the key idea regarding the current and future situation of GRC software. There is a need for integration of the decision process within the organisations. Too often, decisions concerning GRC technical solutions are taken at department level and only cover a specific aspect of the GRC spectrum. There is a need for technical integration, as most of the companies have to deal with existing solutions. There is also a trend for integration among the GRC solution providers, driven by the need for greater investment in complex risk analytics to face the 'big data' problem of the vast majority of the organisations. In fact the need for integration is rather logical as it is the essence of GRC itself.

Figure 3

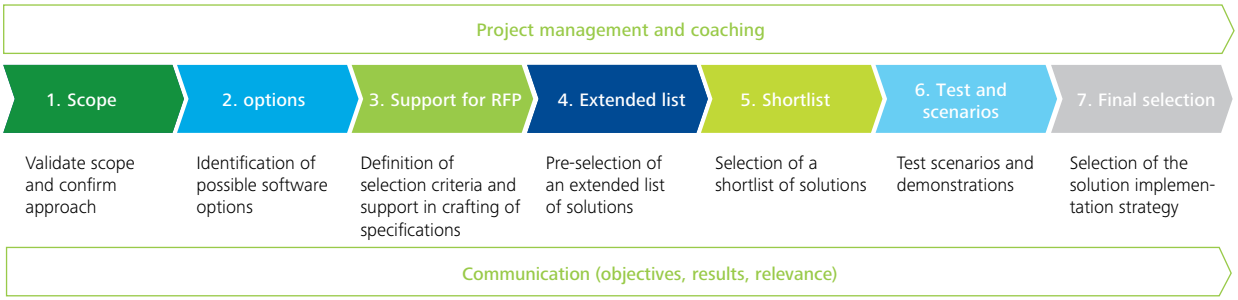



Figure 4

### 1. Functional coverage

- Are the answers regarding specific functions clear or are they deliberately vague?
- Functional coverage is not perfectly matching with the expectations

### 2. Technical architecture

- Is the software available in multiple versions for multiple environments (Windows, Linux, Unix, etc.)?
  This demonstrates the suppliers's experience working in various technical environments
- Is the solution modular?
  This will facilitate further development (sustainability)

### 3. User friendliness

- Design of screens
- Predictive text input
- Number of entries required for the operation
- Level of customisation of reports

### 4. Costs

- Is the implementation of the solution clearly described (e.g integration of existing data, time required for setup, time and cost required for the customisation of the solution)?
- Is the cost of consultants that will implement the solution clear (fixed price? travel costs?)?
- Is the cost of licenses clearly defined?
- What does the maintenance contract exactly cover?

### 5. Vendor characteristics

- Has the vendor replied in a timely manner? This is a measure of the seriousness of the supplier and available resources
- Does the vendor understand the requirements?
- Are the vendor references comparable? Some vendors have many references... in other continents... or other products.
- Is the vendor a 'market maker' or a 'market follower'?