Successful Governance, Risk and Compliance within reach

B. Beugelaar
is a director at KPMG IT Advisory responsible for the IRM service line in Internal Audit. She has extensive experience in the financial services sector with regard to IT auditing and IT consulting in the area of IT Risk and Compliance.

beugelaar.brigitte@kpmg.nl

W.A.J. van Loon
is a senior manager at KPMG Advisory, Risk & Compliance. He works in the field of Internal Audit, Operational Risk Management and GRC and has wide-ranging experience in the financial services sector. He also teaches in the EMIA programme at the University of Amsterdam.

vanloon.willem@kpmg.nl

Brigitte Beugelaar and Willem van Loon

In recent years, businesses have clearly been developing initiatives to promote cooperation among, and even integration of, the organizational units charged with the tasks of risk management, internal control, compliance and auditing. These initiatives are often born from the desire and need to establish more transparent and efficient activities related to governance, risk and compliance. Moreover, the legislative and regulatory pressure is increasing, and companies are looking to efficiently and effectively meet the requirements of regulatory and other "control frameworks." Yet not all companies manage to create effective and efficient collaboration between their various divisions. An integrated approach to Governance, Risk and Compliance (GRC) is the solution to this difficulty. This article will provide insight into the manner in which a successful GRC implementation might proceed by discussing the approach, requirements and potential pitfalls. Understanding these issues increases the success rate of GRC, thereby bringing effective, efficient and transparent cooperation and/or integration within reach.

Introduction

Internal control is an issue that applies to every company, and each company approaches the issue in its own way. Over the course of many years, a wide array of function-based units and divisions have been created within companies to deal with various aspects of the control process: internal control, inspection, (operational) risk management, business continuity management, information security, compliance, legal, IT, planning and control and internal audit. All these sub-domains play an important role, but each is limited to its own area with its own specific characteristics. Companies have now learned that this multiplicity of functions and departments is not effective enough, and it is also inefficient. There is increasing pressure from the business community itself (particularly from executive and supervisory boards), including shareholders and regulators, for a clear understanding of the really important risks and their control, as well as for clear and transparent reporting. There is obvious interest in instigating better collaboration among the multitude of risk and "control" functions, or even integrating them entirely.

GRC stands for Governance, Risk & Compliance. On the market, GRC initiatives are also referred to as "risk convergence," "integrated assurance," "E-GRC" and "single view of risks." These terms are simultaneously supported by a large number of (internal) control frameworks[1] and a great deal of GRC software, including SAP GRC, Thomson Reuters, OpenPages and BWise ([Gart09]). All have a common goal: they are meant to eliminate "silo thinking" and reduce currently existing redundancies among governance, risk and compliance activities by implementing a GRC framework, supported by an IT platform and a single application. Improved cooperation among, or complete integration of, the various organizational units responsible for risk management, internal control, audit and compliance is one of the successful outcomes of GRC. Companies that tend to have high legislative and regulatory requirements and a certain role in society experience a greater willingness or desire to bring about collaboration and/or integration. These companies are mostly active in the financial sector, "chemicals" or "energy and utilities." But companies in other sectors are increasingly seeing the importance of integrated GRC, as it enables management to be demonstrably "in control" and creates improved and more transparent insight into the status of risk and control frameworks, while explicitly co-coordinating the tasks and responsibilities of the "silos." The implementation of GRC software can also significantly improve the manner, speed and effectiveness of reporting.

An integrated "control framework" and implemented GRC software only gets you part way there. There are many initiatives that have been undertaken in practice, but these usually do not deliver the desired results over the long term. Different departments often feel too distinct to work together (people feel that laws and regulations, or various codes are best approached from their own area of expertise, on account of which cooperation, not to mention integration, only distracts from the main task at hand). In addition, many of these departments are anxious about discarding any carefully acquired expertise, tooling, methods, reporting structures or developed risk ratings.

Typically, there are various levels of an organization involved in the specifics regarding compliance with laws and regulations, internal control frameworks, risk management, executing internal controls, conducting audits and interpreting governance issues. There is also some discussion about the "three lines of defense" model. All the layers in this model (*i.e.* management, risk and control support services and internal audit) play a role in GRC, and this produces a certain amount of overlap, the characteristics of which will be further explained in this article. In addition, the realization of GRC discernibly and permanently reduces the work involved in the "three lines of defense" and thus makes them more efficient (see Figure 1). A far-reaching implementation of GRC principles shifts the distribution of the various roles of internal control from the second and third line to the first line (management), where most of them essentially belong. The weighting of the internal control activities is represented from left to right in Figure 1 as a function of the extent to which GRC is implemented, ranging from low realization of GRC (left) to high realization of GRC (right).

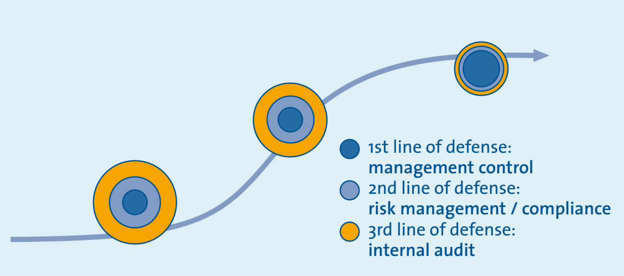

1st line of defense: management control
2nd line of defense: risk management / compliance
3rd line of defense: internal audit

Figure 1: **Distribution of roles involved in the "three lines of defense" in relation to greater GRC commitment**

A number of factors affect the successful deployment of GRC within organizations. This article will furnish answers to the following questions:

- What is the importance of successful GRC? Why should organizations strive to integrate GRC?
- What are the steps that an organization should take in a successful roll-out of GRC?
- What are the advantages of integrated GRC?
- What are the conditions that make for a successful roll-out of integrated GRC?

The importance of successful GRC

Proliferation

There are many reasons why organizations are desperately seeking an effective and efficient structuring of the entire control framework around governance, risk and compliance. However, the importance of successful GRC can only be properly appreciated by examining why these organizations have, in principle, allowed multiple control functions to proliferate. After all, no organization deliberately chooses to perform activities that appear to be similar or overlap, result in loss of a clear and comprehensive picture (*i.e.* transparency) and are undertaken without understanding the total costs. The reasons for the proliferation are shown in Table 1.

Importance

The problems identified above show how important a successful GRC initiative can be. According to AMR Research

[1] Various frameworks for the internal control of organizations are currently in circulation, such as COSO-ERM, COCO, Cadbury, Cobit and ITIL.

Due to fraud, trickery and deceit ...	In the past, there have been some companies – and we need not here go into the details of cases such as Enron, Ahold, Parmalat, Worldcom and Credit Lyonnais – that have interpreted laws and regulations rather freely, not to mention such concepts as ethics and integrity. The result was the failure of the company, dissatisfied shareholders, decreasing consumer confidence and an increasing call for more legislation, regulation and supervision.
... new laws, rules and codes ...	In many ways and in many areas, new laws, regulations and codes have been introduced that are intended to: • win back consumer confidence (Sarbanes Oxley) • protect shareholders (corporate governance codes and the Turner report) • regulate and protect financial markets (Basel II and Solvency II) • increase transparency and comparability between companies (IFRS) • show customers that they, in fact, come first (MiFID, duty of care) • eradicate the financing of terrorism and money laundering (FATF recommendations) • and so on... These laws, rules and codes have not been introduced all at once as a single package, nor were they all created in an appropriately coherent and coordinated manner. The consequence is that every organization implements any new law, regulation or code as a "requirement" dealt with in a separate project. Often, the relevant law or regulation is implemented and integrated by regular staff departments. Sometimes the implementation and further integration within the organization occurs by means of a department specifically established for such a purpose. The existence of numerous "SOx" and Basel II-risk departments testify to such practices. Given the often extremely confining time constraints on implementation and the great complexity of the measures involved, many of these projects were initiated without considering available opportunities to increase efficiency. For instance, in response to the introduction of the Sarbanes Oxley Act, frameworks were initially set up to deal with financial reporting risks, "key controls" and test plans without making proper use of what actually already existed in organizations in terms of operational and monitoring controls. As a result, many managers came to focus on the many extras that had to be implemented, over and above what they were already doing, which was not sufficiently apparent.
... resulting in overlap and non-transparency ...	This unrestrained growth in rules, laws, internal and external governance codes, various control frameworks, etc. has unquestionably led to less transparency, convoluted risk and control structures, redundant (and often double) internal control activities and uncoordinated reporting of risk. What is more, the business front line (the people in the field serving the customer) has the impression that too much time is being spent on GRC activities and the allocation of responsibility for them. There are other causes of non-transparency: the use of different risk definitions and ratings by different departments; the adoption of multiple "control frameworks"; the use of multiple recordings and recording mechanisms with regard to specific issues, events and losses; and the inconclusive demarcation of roles, tasks and responsibilities.
... but with the same purpose.	Ultimately, the various functions assigned duties in the areas of governance, risk & compliance have but one goal: to adequately control the organization in order to conform to internal and/or external laws, regulations and established codes. Laws and regulations do not always come into effect in a logical sequence, and this sometimes inhibits efficient implementation. Some regulations are very similar to each other but differ sometimes in detail. The result is risk and "control frameworks" that often closely approximate each other, while displaying slight differences. Thus, the same controls appear in different "control frameworks," leading to potential inefficiencies when executing the control procedures, taxing the business on multiple occasions instead of reducing the load through better planning.

Table 1: **Causes of proliferation**

([AMRR08]), the importance of successful GRC lies in the following drivers (listed in order of importance):

- better risk management and control in the business
- reduced total costs of GRC activities
- automation of GRC activities and the continuous application of them
- provision of internal and external transparency
- risks and costs of non-compliance
- creation of a defensible information environment

The problem is that these drivers are often insufficiently quantified. In fact, there is insufficient clarity about the current "cost of risk," "cost of control" and "cost of compliance." To clear this up, an inventory has to be made of all GRC-related costs incurred within an organization. We are not just talking about the costs of external and internal audits, but also about the costs of the first and second "lines of defense" and the costs of operational controls, including the costs expressed in hours spent on GRC activities. The latter often constitute hidden costs

An integrated "control framework" and implemented GRC software only gets you part way there

because they are incorporated in regular business processes. In addition, many of the control procedures are inadequately classified as "operational controls" and "monitoring controls" ([Klum09]), and there is a lack of insight regarding the extent to which controls are automated or performed manually. It also appears that many organizations are unclear about the amounts of time (and money) that are spent on corrective actions in response to detected shortcomings in performance. See Figure 2 on the components of control costs.

The integration of different "control frameworks" is often a good first step in remedying this lack of oversight, but it certainly does not go far enough.

The business case ([AMRR09]) for a successful implementation of GRC is certainly solid, but needs to be prepared. The challenge lies in determining the estimated benefits (or reduced costs). This can be expressed in terms of a number of factors such as:

- reduction in the number of FTEs responsible for GRC tasks
- increased productivity through a more efficient execution of GRC tasks, for example, by automating a number of "controls"
- streamlining and optimizing business processes
- joint performance of reviews and audits by various teams, thereby reducing redundancy
- improved risk management and GRC reports (dashboards)
- faster availability of management information through the use of GRC software and therefore improved transparency

The estimated benefits (or reduced costs) have a quantitative but also a qualitative character. Successful implementation of GRC also requires investment. Therefore it is important to formulate a sound business case, detailing an approach to successful GRC.

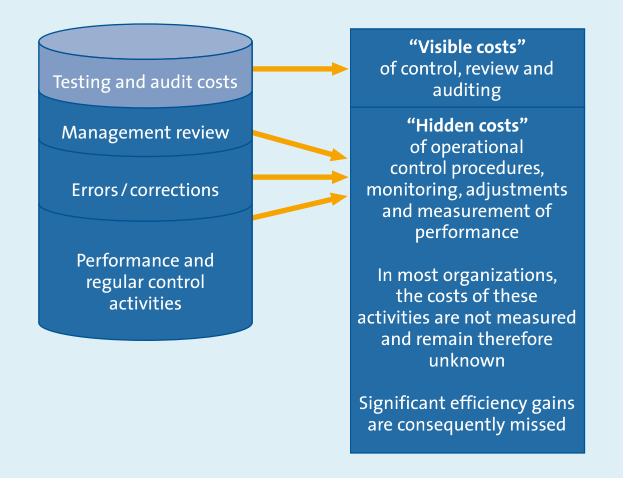

Testing and audit costs
Management review
Errors / corrections
Performance and regular control activities
"Visible costs" of control, review and auditing
"Hidden costs" of operational control procedures, monitoring, adjustments and measurement of performance
In most organizations, the costs of these activities are not measured and remain therefore unknown
Significant efficiency gains are consequently missed

Figure 2: **Control costs components**

Toward a successful roll-out of GRC

A vision of integrated GRC

For a successful roll-out of GRC, it is important that organizations develop a corresponding GRC vision. This entails clearly identifying where the organization is currently positioned in terms of GRC and how it would like to grow (the target). This target may be approached from various points of view. A competitive advantage may be achieved by faster, sharper and better informed decisions. But the desire to be the first to have internal control demonstrably up and running may also be a target. It may also be desirable to have an integrated solution for all risk and control functions in situations where supervision is carried out by regulatory bodies or where rating agencies are constantly looking over your shoulder.

All of the above demonstrates that GRC is not just "joint" execution of certain operations. It is a fully integrated manner of thinking and working in accordance with an efficient and effective business model in which all GRC activities, ranging from strategy to final reporting and performance measurement, are unambiguous, subject to appropriate cooperation and coordinated with activities outside the GRC domain.

Figure 3 illustrates this integrated approach. GRC is accordingly defined as:

- the integrated "framework" that, based on organizational goals, establishes
- a link between the functions of "governance, " "risk," "control," "compliance" and "assurance"
- in order to implement a uniform, consistent and comprehensive approach to GRC
- throughout the entire organization.

Within this approach, processes are based on a series of successive development, implementation and result components.

The mission, which encompasses the expectations of the organization's stakeholders, will be translated into a strategy concerning "governance," "risk," "control," "compliance" and "assurance" tasks, as well as the values and convictions to be shared. The business model for the GRC activities will be connected to the organization's overall business model. The "value drivers" ultimately determine the success of the GRC activities, based on the organizational goals.

The "Governance, Organization and Infrastructure" category is also called "hard" governance. It unambiguously determines

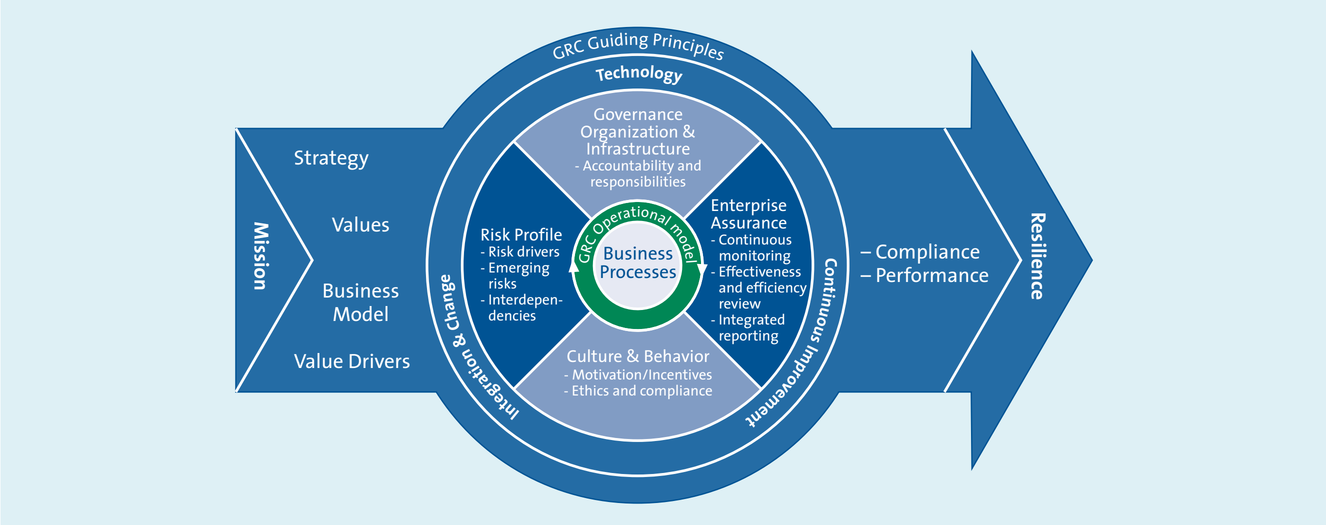


Figure 3: **KPMG's holistic GRC model**

the management and supervisory structures for all the necessary approaches to risk and coordinates them with each other. For example, it leads banks to create an unambiguous structure for credit, market, liquidity and operational risk. Roles and responsibilities are determined and a strategic choice made concerning the use of (IT) systems and supporting applications for GRC activities and reporting. Suitable specific GRC software is available on the market.

"Culture and Behavior" is also called "soft" governance. Robust GRC works only when things like integrity, motivation, discipline, communication, responsibility, independence and transparency are fully embedded in the organization and its people. The corresponding culture and behavior must be rooted in the hearts and minds of employees. The importance of a clear and positive culture cannot be stressed too often. It is one of the most important conditions of successful GRC. Within this culture, issues are identified and disseminated, such as "tone at the top," training, awareness sessions, compensation and incentive plans, "soft controls," as well as open, honest and clear communication.

Automated methods of analysis can make important contributions to an efficient and effective system of internal control

The "risk profile" is drawn up at least once a year by means of an "assessment" that is compiled using all the areas of expertise in the organization. This "assessment" therefore covers all fields of work in the culture. It will create a clear and comprehensive picture of the "risk universe" and an unambiguous assessment of risks connected to the mission and strategy of the business. A uniform risk measurement in each risk category is of crucial importance in the translation of the risk profile into follow-up activities, monitoring and reporting.

The "operational model" and "business processes" are the lifeblood of GRC. They are where operational activities take place. It is therefore important to manage risk in respect of activities such as procurement, sales, production, R & D, HR and accounting, while taking account of the established "risk profile." This "heart" is where GRC activities occur and where the "control framework" for risk management is established. The regular GRC activities are varied: policy making; maintaining "risk and control frameworks"; recording and monitoring incidents, issues and "losses"; teaching management; conducting awareness programs; and implementing and accompanying approval processes for new products.

All monitoring, review and internal audit activities are brought together under "enterprise assurance," where they are performed in a coordinated manner in order to secure the organization's goals (as embodied in the mission and strategy and translated into tactical and operational objectives). This "enterprise assurance" can be formulated in a highly efficient and effective manner. The concept of "embedded testing" ([Klum09]), again emphasized by the COSO organization in its latest guideline on monitoring in COSO ERM ([COSO09]), produces an efficient design for the entire internal control and accountability structure. Its basic principle consists of attributing the task of monitoring the implemented operational controls to a level as close to management as possible. If this arrangement is effectively put in place and policy has been set, the review function (second "line of defense," such as risk management and compliance) only has to have a supportive and evaluative role. Internal audit can then examine the proper design and operation of the "second line of defense." When this "line" does its job well, you only have to use internal audits to determine if management is adequately performing its monitoring role and to run spot checks on the "operating effectiveness" of operational controls. Furthermore, automated methods of analysis and continuous monitoring / auditing can make important contributions to an efficient and effective system of internal control. In this respect, consideration should be given to software such as Idea, Approval, SAP GRC Process Controls and ACL. Based on predefined parameters, deviations in trends and bandwidths will give rise to further analysis. The "enterprise assurance" toolbox should also contain tools for capturing, tracking and monitoring issues, incidents and errors. Examples include GRC software like BWise, OpenPages, Thomson Reuters, Axentis and Qumas ([Forr07]).

If everything is properly supplied and operational, the organization will perform adequate reporting procedures (*i.e.* reporting in an efficient, effective and timely manner) for performance and the extent of compliance with internal and external laws, regulations and guidelines (compliance). As a consequence, the flexible (resilient) organization will be able to respond quickly to future internal and external developments.

GRC and COSO-ERM

Viewed properly, GRC and COSO-ERM share much in common. The above-described holistic GRC paradigm encompasses all COSO ERM activities, all objectives and all levels of the organization. In addition, the ERM approach establishes an unambiguous and coherent process based on all categories of risk. Figure 4 shows the components of COSO ERM, namely the eight activities (front), the layers within the organization (the right side) and objectives (top). There is one difference, however. COSO ERM specifically indicates which activities have to be performed in order to achieve which objectives, and how they are distributed over the various organizational levels. In contrast, the holistic GRC model shows precisely *how* an integrated approach and enhanced cooperation can be organized, and how such a method will work. Both models complement each other well.

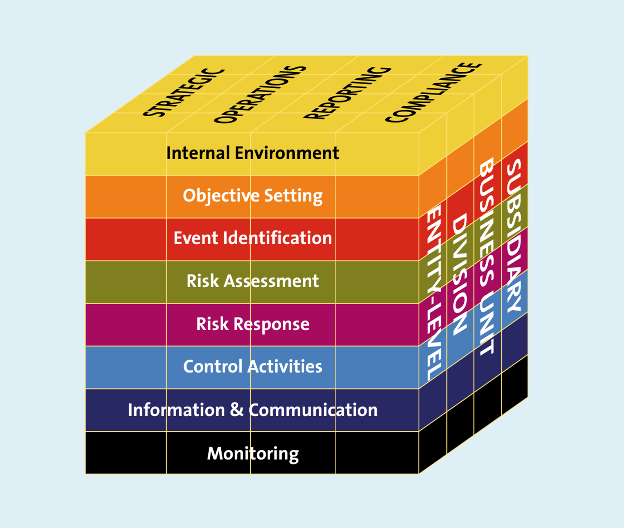


Figure 4: **COSO-ERM framework**

Complexity of implementing GRC

Despite the clearly obvious benefits, the solidity of the business case and the clarity of the vision (see holistic model), actually implementing GRC in practice turns out to be complex and often either fails or has to overcome enormous pitfalls on the road to success.

But why does the implementation of GRC encounter so many obstacles in practice? If you are involved in one of the risk and control functions (such as risk management, compliance, IT, IT security, business continuity management or internal audit) or if you are active in the business, you will undoubtedly recognize the following objections.

1. Often, risk and "control" functions are only responsible for a defined area of internal control. Usually, the task requires specific knowledge and skills and there is a prevalent view that the activities involved cannot be performed by others or that collaboration does not provide an effective contribution to the specific field of work.
2. The individuals performing these functions follow the instructions of a departmental head, an independent manager who assumes the responsibility for the specific department. This department contains a certain number of employees. Collaboration and (worse) integration often leads to fear about having to surrender autonomy, independence and a number of people under the manager's charge.
3. In recent years, each of the function-based units have been carefully working on developing appropriate procedures, processes, IT systems, applications, reports and methodologies in their own field. Collaboration and integration mean that these developed methodologies, databases, applications, *etc.* have to be adjusted, or else their contribution in the new GRC environment will become negligible.

In general, calls for greater collaboration and reduced duplication more frequently come from business and "corporate." The advantages of collaboration have been recognized within each of the function-based units, but such recognition is often only translated into small (though often good) improvements, including the coordination of schedules and concerted action regarding “risk and control self-assessments.” The managers of each of these risk and control departments shall have the collective task of finding a better and more expansive solution enabling the advantages of collaboration to be fully exploited.

GRC scan

As indicated, implementation of GRC in an extensive and comprehensive project often proves to be unworkable. Therefore we advocate the initiation of a GRC scan in order to determine how a successful roll-out of integrated GRC can be achieved. This will remove the obstacles standing in the way of successful implementation, identify them as early as possible and enable a phased implementation of GRC to be started within the latitude provided by the organization.

An approach to a successful roll-out of “integrated GRC” starts by determining the current status of GRC in the organization, along with the organization’s target level with respect to GRC (desired state). It is then important to understand those elements of GRC that will provide the maximum benefit for the organization as a whole. These benefits may be defined in monetary terms, or in terms of increased transparency and speed of decision-making, or even in terms of reduced redundancy and less “harassment” of the business. Running a GRC scan enables the organization to examine a number of issues. The results of such a GRC scan partially form the basis for preparing the business case and the implementation plan for a phased and “sustained” transition to integrated GRC.

In general, a GRC scan provides answers to the following questions:

- What is the current status of GRC in the organization?
- What is the GRC target level?
- To what extent is the organization ready to initiate GRC?
- What are the steps for achieving the target level, and in what order should they be implemented?

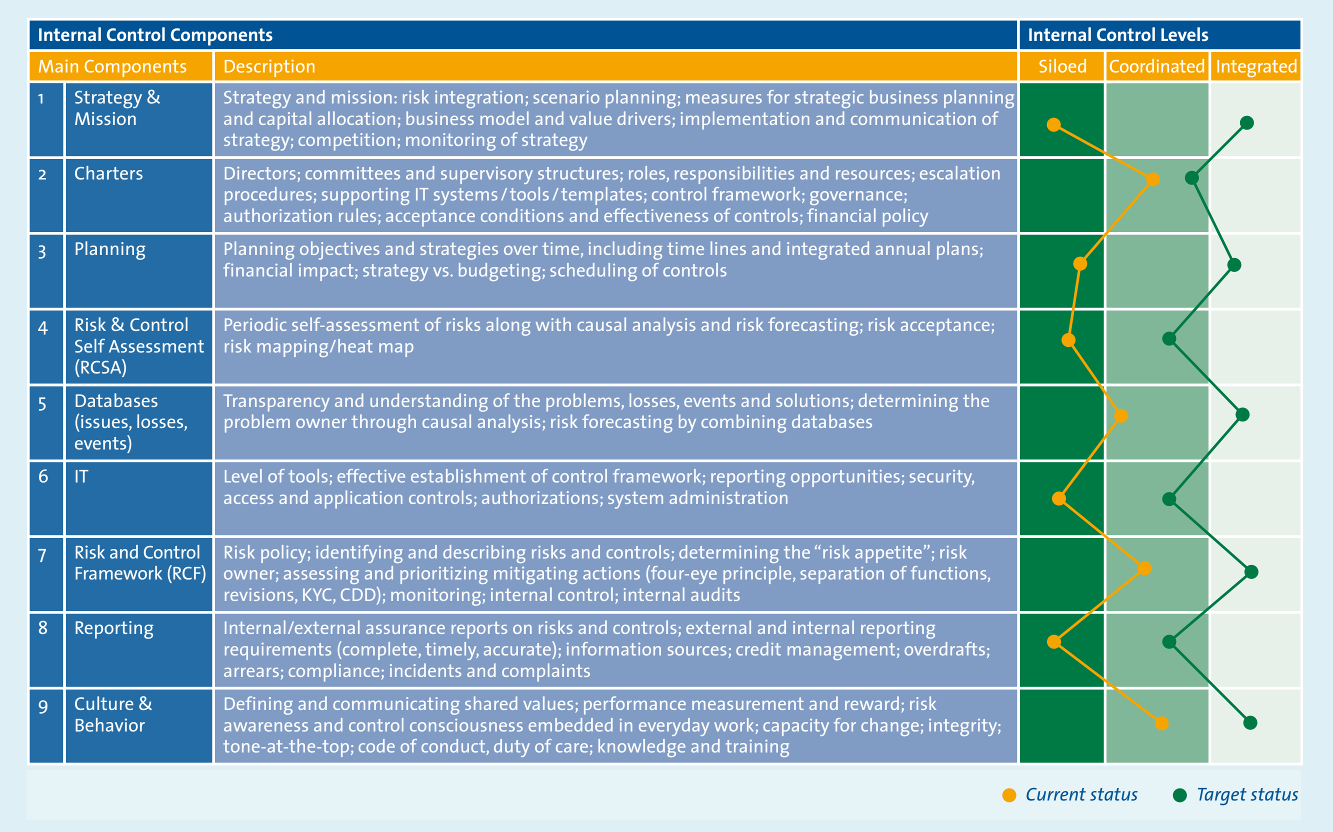
These issues should be clarified by conducting targeted interviews using a questionnaire. Only then is the organization ready to unpack the successes of GRC into more wide-ranging successes for the organization. The advantages of the GRC scan include the phased development and roll-out of the various GRC components. In this respect, it is important to start with those components considered the most likely to deliver the greatest benefits for the organization or to furnish risk and control functions. Based on the readiness for change in the various departments and the importance of rolling-out these high-value components, the sequence of implementation and the parties involved in the roll-out can be determined. Gaining insight into the “quick wins” at this point is one of the key drivers for continued success. During the GRC scan, an analysis will be made of the components that can be created relatively quickly and at sufficiently low costs. These quick wins will pave the way for subsequent successes.

Prior to conducting the GRC scan, all GRC activities will be clearly organized, categorized pragmatically into nine groups and explained by means of the questionnaire. These activity groups contain activities performed in every governance, risk and control function, but almost all of them are customized in a distinct and specific manner. These nine activity groups are fully compatible with KPMG’s holistic GRC model. However, the holistic GRC model is not based on the grouping of activities, but the subsequent development, implementation and outcome components of GRC. See Figure 5 for the activity groups covered by the GRC scan. By determining the status, ambition and willingness to change, as well as the pros and cons for the organization in each of these areas, the organization can make an informed choice regarding the anticipated manner of growth required to achieve an integrated GRC environment throughout its discrete segments.

These activity groups are:

1. *Strategy & Mission.* This component further details such elements as the compatibility of business goals with the appetite for risk, as well as the general goal regarding risk integration. Furthermore, in this component the risk business model is further developed, as are the communication channels to the rest of the organization.
2. *Charters*. This component relates mainly to the further structuring of function-based units, roles, tasks, responsibilities and the commitment of resources and other tools.
3. *Planning.* This component involves the way that the planning activities of each of the function-based units are carried out, and the extent to which they can be integrated or cooperation among them enhanced.
4. *Risk & Control Self Assessments.* This component explores the RCSA’s commitment and progress within the organization when dealing with new products, in reviewing existing processes and in investigating incidents.
5. *Databases (for issues, losses and events).* This component concerns in particular the quality of available data, accessibility of data and the presence of a stand-alone or integrated IT solutions.
6. *IT.* This component explores the current IT infrastructure in terms of platforms, applications and other existing or desired

Quick wins will pave the way for subsequent successes



Internal Control Components			Internal Control Levels		
Main Components		Description	Siloed	Coordinated	Integrated
1	Strategy & Mission	Strategy and mission: risk integration; scenario planning; measures for strategic business planning and capital allocation; business model and value drivers; implementation and communication of strategy; competition; monitoring of strategy	🟠		🟢
2	Charters	Directors; committees and supervisory structures; roles, responsibilities and resources; escalation procedures; supporting IT systems / tools / templates; control framework; governance; authorization rules; acceptance conditions and effectiveness of controls; financial policy		🟢 🟠	
3	Planning	Planning objectives and strategies over time, including time lines and integrated annual plans; financial impact; strategy vs. budgeting; scheduling of controls	🟠		🟢
4	Risk & Control Self Assessment (RCSA)	Periodic self-assessment of risks along with causal analysis and risk forecasting; risk acceptance; risk mapping/heat map	🟠	🟢	
5	Databases (issues, losses, events)	Transparency and understanding of the problems, losses, events and solutions; determining the problem owner through causal analysis; risk forecasting by combining databases		🟠	🟢
6	IT	Level of tools; effective establishment of control framework; reporting opportunities; security, access and application controls; authorizations; system administration	🟠	🟢	
7	Risk and Control Framework (RCF)	Risk policy; identifying and describing risks and controls; determining the "risk appetite"; risk owner; assessing and prioritizing mitigating actions (four-eye principle, separation of functions, revisions, KYC, CDD); monitoring; internal control; internal audits		🟠	🟢
8	Reporting	Internal/external assurance reports on risks and controls; external and internal reporting requirements (complete, timely, accurate); information sources; credit management; overdrafts; arrears; compliance; incidents and complaints	🟠	🟢	
9	Culture & Behavior	Defining and communicating shared values; performance measurement and reward; risk awareness and control consciousness embedded in everyday work; capacity for change; integrity; tone-at-the-top; code of conduct, duty of care; knowledge and training		🟠	🟢

🟠 *Current status* 🟢 *Target status*

Figure 5: **The components of KPMG's GRC scan**

IT-related solutions, such as the use of GRC software and the possibility of running all risk and control functions on the same server, thus enabling data exchange to occur more easily.

7. *Risk & Control Framework.* This component principally examines the existing control frameworks, their overlap and integration, and the deployment of GRC tools.

8. *Reporting.* This component mainly concerns reporting structures, quality and speed of reporting, as well as the availability of accurate, timely and complete information in order to make informed choices and decisions.

9. *Culture & Behavior.* This component explores the willingness to change within each of the organization's segments, their culture and behavior regarding GRC and how people deal with their responsibilities.

Once the actual state and target state are determined and each of the areas is assessed in terms of the extent to which it contributes to the goals of the organization as a whole, then the route to the target level can be plotted (the roadmap). Both the benefits of and obstacles to integrated GRC will be clear for each of the areas. As an example, Figure 6 provides an overview of the possible obstacles and benefits for the "Strategy & Mission" component.

The perceived benefits and obstacles for each of these groups can be plotted on a graph (see Figure 7) in which the elements in the top left corner provide the greatest "benefits" for the organization while involving the fewest predicted obstacles during implementation. GRC development and deployment will therefore be initiated in these areas.

The benefits and conditions for a successful roll-out of integrated GRC

The big question now concerns how to determine when the roll-out of integrated GRC has been successful. The important characteristics of a successful roll-out will be measured based on the realization of the prepared business case. Various GRC implementations in practice have given rise to the following benefits in particular ([KPMG]):

- Organizations that improve their business performance with GRC will find that they increase their flexibility to cope with changes in the environment while being able to enhance their "corporate" reputation and improve shareholder value.
- Cooperation among internal-audit, risk-management and compliance-related functions is improved, while front-line management is less frequently tasked with overlapping issues and functions.

- The use of GRC and continuous monitoring / auditing software improves understanding about the extent to which processes, risks and issues are controlled, while insight into the actual state may be obtained online by means of “executive dashboards.” In addition, costs are further reduced by the concerted action of the various business functions combined in these dashboards.
- Better integrated risk and control frameworks reduce the overlap in activities as well as the quantity of the required controls, or a rationalization of the controls enables the business to be less encumbered by them.
- The organization has better control and is seen to be in better control.
- The organization can respond quickly and flexibly to changes in environmental conditions in areas such as legislation and regulation, customer needs and new products (but also to internal changes).

A case study

At a major international financial institution, the decision was made to increase the efficiency and effectiveness of the internal controls used in some of the risk and control departments by improving the cooperation among the departments and even integrating them. Seven of the second and third line departments (Inspection, Operational Risk Management, Compliance, SOx, IT Security, Process Management and Internal Audit) participated in this initiative. Significant opportunities for improvement were identified in six components that could be translated into actions increasing the effectiveness of internal control and the efficiency of risk mitigation. These involved 1) the integration of the charters, 2) the integration of risk and control frameworks, 3) the development of a GRC application, 4) the further coordination of risk & control self-assessment activities, 5) rationalization of the issues, losses and incidents databases and 6) establishing a system of non-financial risk reporting.

The prepared business case and roadmaps for further implementation yielded the following principal advantages:

- Improvement of risk management by focusing on key controls and using the best risk management methods
- Increased central management of risk and control activities, leading to lower insurance premiums, reduced risks to reputation, and enhanced clarity in assessing risk.
- Increased effectiveness of operational activities through the efficient maintenance of controls, reduction of stratification in risk assessments and a reduced number of IT applications.
- Cost reduction due to smaller number of FTEs, use of uniform IT technology and reduced redundancy.
- Risk reduction resulting in improved resource allocation, increased responsiveness to incidents and an increase in risk awareness.

Examples of obstacles of GRC		Examples of benefits of GRC	
Strategy & mission			
No	Obstacle	No	Benefit
1.1	Fear of reduction in resources/ functions	1.1	Work can be done in a more efficient and effective way
1.2	Regulatory restrictions on integration possibilities/ opportunities	1.2	Different functions can depend on each other’s work
1.3	Resistance to change	1.3	Better cooperation
1.4	Difficulties in aligning GRC proposition with business objectives	1.4	More information sharing
1.5	Difficulties in aligning GRC proposition with organizational complexity	1.5	Employees understand each other better because they speak the same “language”
1.6	Insufficient support from top management	1.6	Better insight in how the balance is made up between risk and return
1.7	Difficulties in aligning the objectives of the different functions		

Figure 6: **Potential benefits and obstacles – Strategy & Mission**

However, a number of factors need to be addressed as conditions for obtaining these benefits and successes. Some of these conditions are:

- The willingness to change of managers and employees within the various units (culture and behavior).
- A phased approach based on the results of a GRC scan in which the components yielding the highest expected benefits for the organization are performed first.

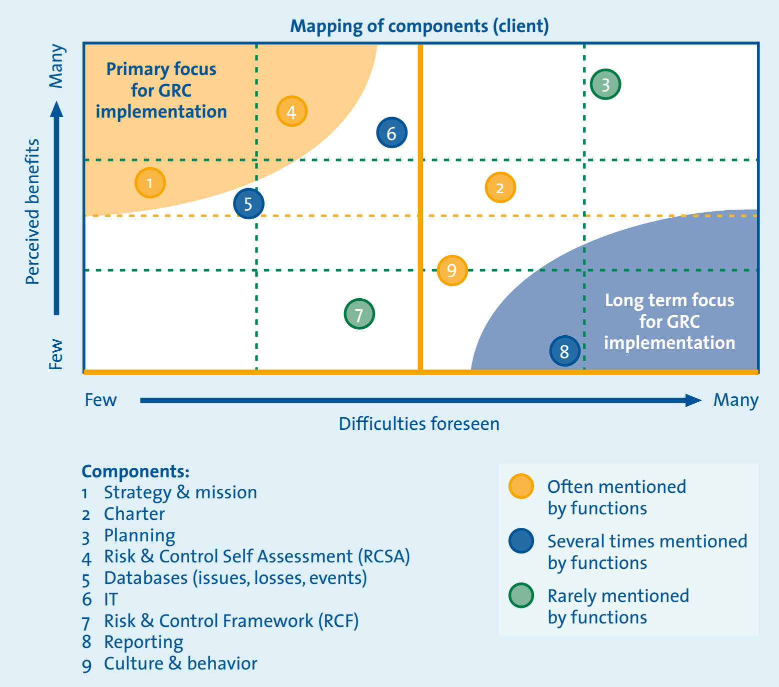


Figure 7: **Priority matrix for GRC**

- Development and implementation of a solid communications plan, under which everyone is promptly and transparently informed about progress and the impact of changes on each individual.
- Commitment from the organization's management, without which successful GRC will not occur.
- Time and money available to invest in GRC. GRC means that a number of items involved in risk and control will be identified and radically transformed; since such an overhaul will require development time and money, it must be budgeted and assigned as the responsibility of senior management.
- Change management. Throughout the program, attention is focused on the changes that have to take place; without this vigilance, people will tend to continue their current activities, and fear of the new will get in the way.

Conclusion

Successful GRC is achievable. Understanding the current status of the various GRC components within the organization, the organizational goal with respect to each of these GRC components and the willingness of the various units to change will make it possible to provide sound advice concerning the steps to take. A further assessment of the perceived obstacles arising when each component is developed and rolled out will result in a clear idea of how the organization can achieve integrated and successful GRC.

The GRC scan is an appropriate means to identify all these matters. The scan results lead to a widely-supported and transparent implementation plan (roadmap) under which the components that meet the fewest obstacles and are the best for the business are chosen to be performed first. Obviously, successful implementation will ultimately only be achieved if certain preconditions are met, including the deployment of a robust communications plan and the commitment of senior management.

References

[AMRR08] AMR Research, *The Future of GRC*, 2008, presentation by John Hagerty.

[AMRR09] AMR Research, *The GRC Imperative – A Pragmatic Guide to Jumpstarting Your GRC Project*, November 2009.

[COSO09] *Internal Control – Integrated Framework, Guidance on Monitoring Internal Control Systems*, COSO, January 2009.

[Forr07] The Forrester Wave™: *Enterprise Governance, Risk, and Compliance Platforms*, Q4 2007, For Security & Risk Professionals.

[Gart09] Gartner, *Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms*, Q3, 2009.

[Klum09] C. Klumper, *Toepassing van de Monitoring component van het COSO-raamwerk*, MAB, March 2009.

[KPMG] KPMG, *The Evolution of Risk and Controls; From Score-Keeping to Strategic Partnering.*