

White Paper



IMPROVING THE BOTTOM LINE WITH RISK AND COMPLIANCE
MANAGEMENT

**An Integrated, Unified and Collaborative Approach for Improving Control
over Business Processes | Martijn Iseger and Teemu Lehto, QPR Software Plc**

Executive Summary

Organizations that manage risk and compliance in a project-by-project approach, executed in functional isolation, expose themselves to unnecessary cost and complexity, and are less likely to react to risk in an effective manner. Furthermore, a disconnect with strategy, performance and business process management prohibit risk and compliance management to become the enabler that it should be, for achieving strategic and operational goals.

This white paper proposes the use of a Risk Management and Compliance (RMC) platform that integrates risk and compliance management tightly with strategy management, operational performance management and business process management. RMC platforms provide organizations with a technology framework that enforces a unified and consistent risk management approach throughout the organization, which is aligned with the achievement of strategic, operational, reporting and compliance objectives. An RMC technology platform allows organizations to improve organization-wide awareness of risks, facilitate orchestrated and strategy-aligned risk responses, gain an up-to-date, accurate and complete picture of the organization's ability to achieve set objectives, and comply with regulations in an efficient and cost-effective manner. It provides organizations with the key ingredients for turning RMC from being a cost-driver and often perceived nuisance into a lever for improving stakeholder value.

Table of Contents

Introduction	4
The Need for a Holistic Approach	4
Key Ingredients for Success.....	7
Satisfying Business and Compliance Needs	10
QPR Risk Management and Compliance Solution	12
Conclusion.....	13
Next Steps.....	14
References.....	14

Introduction

Any manager, whether on an executive, business unit or departmental level, will agree that insight in the risks that influence the achievement of set objectives will help in improving the chances of achieving those objectives. In most organizations, however, this insight is lacking or limited to isolated functional or departmental views on risk. The complex nature of risk and regulatory compliance as well as their effect on multiple levels and functions of the organization requires organizations to take a more holistic, uniform and integrated approach.

Common to Risk Management and Compliance (RMC) in most organizations is its' disconnect with strategy, performance and process management, the application of a multitude of approaches executed in as many functional areas of the organization, and a disregard of the cross-functional nature of risk. The resulting lack of transparency regarding the state and completeness of identified risks, implemented controls, and the definition and alignment of response strategies leaves management at all levels of the organization unable to leverage RMC as a driver for achieving organizational success. In this scenario RMC merely remains a cost driver.

This white paper proposes the use of an RMC platform that integrates risk and compliance management tightly with strategy management, operational performance management and business process management. RMC platforms provide organizations with a technology framework that enforces a unified and consistent risk management approach throughout the organization, which is aligned with the achievement of strategic, operational, reporting and compliance objectives. An RMC technology platform allows organizations to improve organization-wide awareness of risks, facilitate orchestrated and strategy-aligned risk responses, gain an up-to-date, accurate and complete picture of the organization's ability to achieve set objectives, and comply with regulations in an efficient and cost-effective manner. It provides organizations with the key ingredients for turning RMC from being a cost-driver and often perceived nuisance into a lever for improving stakeholder value.

The Need for a Holistic Approach

For many organizations, risk and compliance has become a widespread business problem that is driving them to look for new approaches to better

manage it. In an environment of ever increasing competition, organizations are turning to a globalization of operations, business re-engineering, outsourcing and more complex business models that often feature a multitude of diverse partnerships, in order to seek advantages. These internal drivers for gain, however, increase their exposure to risk. Organizational boundaries become more difficult to discern and the level of internal control is affected.

In 2007, toy producer Mattel was forced to recall nearly 1 million products due to one of its contract manufacturers in China failing to adhere to regulations by using lead-containing paint in the production of toy dolls. Apart from the \$30 million cost directly involved with the recall, Mattel suffered the consequences of worldwide negative publicity, just before the 2007 Christmas holiday season.

Increasing complexity in business models mandates a need to ensure awareness of and compliance with quality standards, internal policies, codes of conduct, laws and regulations and a requirement to protect the organization and its stakeholders from the increased exposure to risk. A globalization of operations results in geo-political, regulatory and environmental factors gaining in influence. International sanctions imposed on nations, trade embargos, military strikes, hurricanes and floods all can severely affect business. On top of this, global operations expose organizations to a large and exponentially growing number of geography and jurisdiction-specific regulatory demands. An identified failure to comply with an imposed regulation can have a devastating effect on an organization as sanctions can be as severe as a shutdown of operations and imprisonment for responsible executives.

Traditionally, RMC has been managed in silos of functions, departments and business units. The lack of risk communication between these silos often leads to organizations managing risks in a reactive manner. This means that the organization has identified and is aware of the risk but is unable to avoid or mitigate it with the implementation of effective controls. Take the example of an organization that is relying on a single supplier for raw production materials. To mitigate the fluctuating risk of a disruption in supplies effectively, requires the purchasing, production, finance and sales functions to co-operate. Purchasing may choose to look for alternative suppliers, finance to implement controls, for example a reserve in available funds to ensure timely payments, production to establish a minimum inventory level and sales to make sure it does not promise delivery dates it cannot live up to. One of the leading steel manufacturers in Europe is mitigating the risk of cyclical price fluctuations of its product by increasing the share of special products in its own output, by improving supply chain management and delivery accuracy and by aligning production to profitable

demand in each market situation, thus recognizing the need for an organization-wide approach.

"Organizations are to establish a platform that maintains a system of record for Governance Risk and Compliance. This enables disparate governance and compliance technologies to combine into a coherent regime for managing GRC across the enterprise"

- Forrester¹

The silo approach inevitably leads to a multitude of applied methods in identifying, describing, documenting, assessing and reporting on the status of risks and risk mitigating controls, which in turn makes it significantly harder for management on a higher level of the organization to obtain a clear view of the total picture and leads to long reporting cycles. Reporting to auditors becomes a race against time and despite all the effort, management is in most cases left with incomplete and outdated information on risks, controls and regulatory compliance to base its' decisions on.

What further complicates the problem is the dynamic aspect of business. Operations change constantly, which introduces new risks to be managed, may invalidate earlier identified risks and affects implemented response strategies. This facet is however not just related to internal changes as also the external economic, political, environmental and regulatory landscapes are subject to constant change. Organizations therefore have a need for a periodically reoccurring organization-wide risk and control re-assessment and identification process, something a silo approach simply does not support.

Finally, a silo approach leads to significant amounts of effort being duplicated as organizations often deal with compliance mandates on a project-by-project basis, where often multiple regulations are overlapping each other. Here, the wheel is re-invented over and over again in different parts of the organization, which results in a significant waste of effort and resources.

"Move compliance from a tactical reaction to strategic imperative. Firms can no longer afford to approach compliance as a periodic or tactical project like meeting the Sarbanes Oxley deadline"

- Forrester²

A growing amount of organizations is realizing that a fragmented approach to RMC is inefficient and becoming a huge cost driver. In order to improve risk awareness, communication, mitigation and reporting on an organization-wide scale, organizations are moving toward the use of RMC platforms. These platforms enforce a uniform, systematic and consistent risk management across functional areas and integrate risk and compliance management with strategy and operational processes.

Key Ingredients for Success

An RMC platform by itself provides no guarantees for success. RMC is a continuous, organization-wide process and the software platform is merely an enabler for making that process more effective. Apart from a technology platform to enable an effective RMC process, there are four key ingredients to successfully managing risk and compliance imperatives: Awareness, preparedness, proof and methodology.

Awareness

Effective RMC starts with achieving awareness of the current strategic, operational, reporting and compliance risks, as well as all risks that fall into their subcategories (reputation, competitor, supply chain, financial, environmental, occupational health risks etc.). It requires organizations to implement a periodically executed process for doing risk identification on an organization-wide scale. This process has to be organization-wide as it's important that all risks to the organization will be captured and different departments and roles in the organization will have different perspectives on risk. A marketing manager is likely to identify a different collection of risks than an IT manager, even when discussing about the same topic, such as risks related to the Customer Relationship Management (CRM) system. This process needs to be periodic as business and its environment changes constantly, thus affecting the risk profile of the organization.

Awareness also requires that risks are assessed in some consistent manner across the organization, so that each business unit not only has a good picture of what risks affect its operations and goals but also to what extent they do this. It helps to be able to compare risk assessments between business units, functions and departments and to be able to drill-down into

risk assessments in order to ensure that a certain risk has actually been assessed throughout the organization.

Finally there needs to be an effective means for communicating risk information throughout the organization. Bearing in mind that the average organization will identify thousands of risks, it becomes important to communicate risk information by relevance. A production manager will only be interested in the risks that affect his role and goals in the organization, a Human Resources manager will have a significantly different interest and a CEO will probably only be interested in a higher level, overall view of risks.

Preparedness

Just being aware of the risks that affect business is not enough: It is often cheaper to fix a potential problem than to fix an occurred one, and if you only fix problems as they surface, the flow of future problems is sure to keep you busy. Preparedness is about making sure that each functional, departmental and business unit follows up on the risks that were identified and assessed. This is done by making consistent decisions across the organization for risk response: i.e. what risks to accept, eliminate, outsource and reduce. Accepting a risk means to do nothing about it. It makes sense when risk likelihood and impact are very low or when the cost for controlling the risk is exorbitant, for example trying to mitigate the risk of tsunami destroying a sales office. Eliminating a risk often means deciding not to do a certain thing, like cancelling plans for a new product line or deciding not to enter a new market. Outsourcing means the organization shares the risk, for example by taking up insurance for it, while reducing a risk means to implement procedures and policies that are aimed at reducing the likelihood and/or impact of a risk. In the case an organization chooses to accept or reduce a risk then still it needs to be prepared for the risk occurring, which means the definition of contingency, business continuity and disaster recovery plans.

Preparedness requires an organization to communicate its risk appetite and risk tolerance. Risk appetite is about the level of risk an organization is willing to take. Some managers may be more risk taking than others and there needs to be a guiding line on what the organization considers acceptable, especially when deciding on risk response strategies. Risk tolerance is about the level of risk an organization is willing to tolerate after implementation of risk mitigating controls. Should the residual risk level be higher than what is tolerated, then the team that is responsible for the implemented control should have another look at improving the situation.

Insight in defined response strategies across the organizations is another preparedness requirement as it allows the organization to ensure that these risk strategies are aligned with each other and also with the business strategy of the organization. Naturally there needs to be an accurate,

complete an up-to-date picture of the risk and compliance profile of the organization: Things change and knowing where you are in terms of risks and defined response strategies allows management to make better decisions, and provides the confidence that everything is really as much under control as the organization says it is.

Proof

An effective RMC process is an asset to any organization as it provides an extra degree of reliability to all the stakeholders of the organization. Investors obtain an extra assurance that their money is invested in a trustworthy enterprise that complies with all regulations, exercises good governance and is aware and prepared for dealing with any event that jeopardizes the achievement of defined (and communicated) objectives. Decision makers are more assured that the operational and strategic decisions they make are based on trustworthy information. Customers and business partners are assured that the organization follows all regulations and is ready to cope with risks in order to protect their interests. The ability to demonstrate the quality of the RMC process is not only a regulatory requirement, it should also be seen as something that makes the organization more attractive to its stakeholders and therefore qualifies as a key ingredient for success.

Being active in high-risk operations in several countries on the African continent, South African stock-listed mining company African Rainbow Minerals (ARM) had a need to demonstrate the effectiveness of its risk management process to International underwriting companies, which ARM relies on for insurance. The ability to prove to auditors that ARM's risk management process was state of the art and far ahead of any of its competitors resulted in ARM now paying 30% less in insurance fees than the industry average.

Methodology

As with any process, the success of its outcome is often decided by the application of a tested and well thought through methodology. For quality management the application of the Six Sigma methodology is a good example of such, while for performance management, methodologies like Balanced Scorecard or Malcolm Baldrige have proven their value in organizations worldwide. For RMC there exist a number of available methodologies, like AS/NZ 4360 and the COSO Enterprise Risk Management Integrated Framework, which has been accepted worldwide as the de-facto risk and compliance management standard.

COSO ERM provides organizations with guidance on how to set up an effective RMC process. It defines RMC as a process that is executed in strategy setting, in other words: it serves the achievement of strategic, operational, reporting and compliance objectives. It specifies a number of essential risk and compliance management components and activities, and recommends that these activities are executed on all levels of the organization with clear lines of communication between those organizational entities. Taking COSO's view on effective RMC it becomes clear that strategy, performance and process management need to play a prominent role in facilitating effective management of risk and compliance.

Satisfying Business and Compliance Needs

There are several ways in which organizations approach RMC. Some organizations' operations consist of high risk activities and therefore have a clear need to have all risks covered by appropriate controls. Nuclear power plants, oil rigs, mining companies and steel manufacturers and the likes, would fall into this category of operational risk focusing companies. Then there are those organizations that have identified risk management to provide a positive influence for the achievement of strategic and operational objectives. These organizations are looking at risk management from a business-driven perspective. Often these are organizations that already have a strategy or performance management system, such as Balanced Scorecard in place. Here the organization wants to identify those top 10 or 20 risks that influence the achievement of key objectives, increase organization-wide awareness of these risks by cascading them from enterprise to departmental levels, implement procedures for managing those risks and make sure everything is monitored and reported on a regular basis. Finally there is the group of organizations that turn to RMC because of a multitude of regulations they need to comply with and report on for auditing purposes. Here the compliance-driven need takes prominence. These organizations want to make sure that all compliance related risks are documented and covered with appropriate controls. These controls need to be tested periodically and there needs to be effective reporting processes in place to satisfy the needs of auditors and management.

In order to satisfy both business and compliance related needs, RMC needs to be applied on an organization-wide scale and encompass a multitude of risk and compliance imperatives in a unified and efficient way. This is

where the RMC technology platform becomes the enabling factor as it tightly integrates the discipline of risk management with strategy, performance and business process management in order to provide a number of significant business benefits.

Firstly, it makes the process of identifying risks significantly easier. Looking at the business-driven need to risk management, here the identification of risks is closely related to the objectives of the business. These objectives are typically defined top-down, starting with strategic objectives for the enterprise as a whole and translated into objectives on business unit and departmental levels. Identifying risks here requires people to have insight in the objectives related to their role in the execution of strategy. This is the domain of strategy and performance management and particularly Balanced Scorecard. The compliance-driven need focuses strongly on how things are done in the organization. Therefore insight in the “as is” processes becomes an important enabler for identifying those processes or parts of processes that pose a risk in terms of compliance to a regulation.

Integrating risk and compliance with strategy, performance and business process management furthermore improves strategic and operational decision making. Insight into risks is a key ingredient for improving the quality of strategic choices. Risk and compliance platforms provide top-level decision makers with an accurate, up-to-date and complete picture of the risk profile of the organization that has been compiled over a long term, whereas without such, their decisions are forcefully based upon ad-hoc risk identification and assessments. Managers on lower levels of the organization benefit in their decision making from a clear picture on objective and process related risks and the degree to which those risks are mitigated.

Another key benefit is that complementing business process management (BPM) with RMC provides an important extra driver for continuous process improvement. Traditionally, BPM solutions have approached process improvement only from a performance perspective, aiming to reduce process cycle times, cost and improve agility with improved insight in and control over cross-functional business processes. So far, most of these solutions have ignored risk and compliance or even strategy as necessary considerations when improving processes. One can only truly speak of a process improvement when the total sum of changes to cycle time, cost, strategy alignment, risk and compliance is favorable.

Finally, RMC platforms enforce a unified and consistent approach for the entire organization and provide a single point of access to risk and compliance information. Compared to the often seen situation where information needs to be extracted for reporting requirements from a

multitude of systems, applications and file formats this enables a significant reduction in the time and costs associated with compliance audits.

QPR Risk Management and Compliance Solution

The QPR Risk Management and Compliance Solution covers all phases of the RMC process by providing an effective and unified means for identifying and assessing risks on an organization-wide scale, consolidating risk assessments, implementing controls as well as continuous monitoring and reporting of risk information. By allowing employees on all levels of the organization to participate in the risk identification process and providing them with strategic, performance and process-related context, it enables organizations to capture all the risks that are relevant from both a business as well as a compliance perspective in a convenient way.

With a long history in RMC, QPR recognizes that each organization has its own specific requirements for RMC and that even inside a single organization there exist a multitude of business unit or departmental-specific requirements. This is why we designed the QPR Risk Management and Compliance Solution to provide enough flexibility to match the needs of our customers. Whether an organization is looking for a technology framework to support a COSO ERM, AS/NZ 4360, Balanced Scorecard, EFQM-driven or its own approach, QPR Risk Management and Compliance facilitates a technology foundation that will allow it to focus on the correct application of the methodology without being distracted by technology implementation issues.

This flexibility is prominent in all phases of the RMC process, allowing organizations to decide the way to assess, rank, document, categorize and allocate risks that best matches their needs, communicate and provide access to risk information based on user rights, decide on monitoring intervals on a risk-by-risk basis and customize reporting content and formats.

The QPR Risk Management and Compliance Solution combines a process management and performance measurement approach, which allows organizations to enrich process maps with risk, control and policy information while providing a direct link between documented risks and controls, their measurement and status. To ensure effective follow-up of identified problems, risk information is communicated in a role-based manner and complemented with alerting functionality, accountability

setting, initiative management and the ability to launch and track progress of control activities.

All information is stored in a central repository, which provides different users with views into the information that matches their specific needs. Examples include risk dashboards by regulation, risk category (environmental, strategic, occupational health etc.) or business unit, risks by a specific process, risks ranked by importance for a specific viewpoint, launched control activities by deadline and status and so on. In addition, the solution provides the ability to drill down into information and do analysis in order to effectively assess the overall risk and compliance profile of an organization. Because all user activities are logged and the system always provides easy access to all information, it provides organizations with a reliable foundation for decision making and internal control.

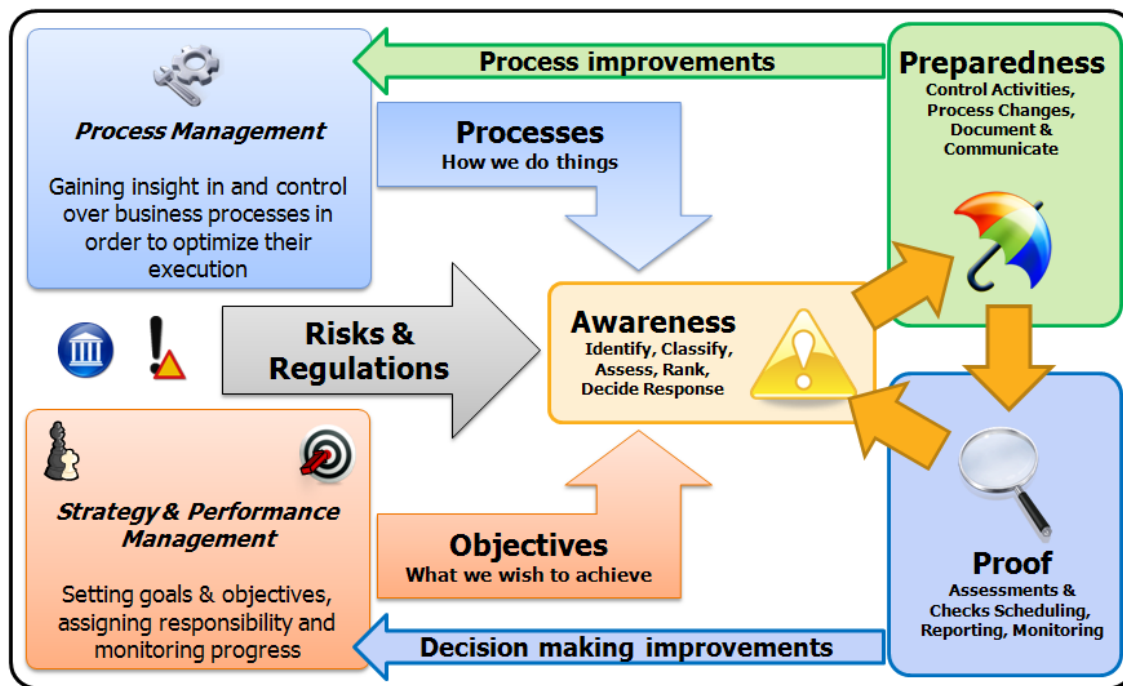


Figure 1: The QPR Risk Management and Compliance Solution provides a platform for managing risk and compliance that integrates it with process, performance and strategy management.

Conclusion

As shown in this white paper, effective risk management reduces costs, improves quality and ensures strategy execution. Cost reductions emerge from the holistic and systematic approach where the RMC platform is used

to align the efforts of multiple silos including functional units and regulation based projects. Quality improvements are reached by integrating the risk management efforts with continuous process improvement. The cornerstones of executing the strategy include communication to all employees and the ability to foresee the possible risks and prepare for them in advance.

Key ingredients for success in RMC are awareness, preparedness, proof and methodology. Awareness means appropriate risk identification and assessment in all organizational levels and for all risk categories. Preparedness includes the decision about proper risk appetite and based on that the selection of risk response for each identified and assessed risk. For various stakeholders and for many businesses the proof of being in control is mandatory for being in business. To tie the individual efforts together every organization needs to deploy a framework suitable for them for risk management. One of the most common frameworks includes COSO ERM.

Best RMC platforms are capable of supporting the business and strategy driven risk management needs as well as the compliance driven needs. This is achieved by integrating risk management with strategy, performance and business process management resulting in cost savings, improved quality and successful strategy execution.

Next Steps

To learn more about QPR Software's Business Risk Management and Compliance solution please visit <http://www.qpr.com/qpr-rmc-solution.html>

To learn more about testimonials from other organizations in your industry about QPR Software's Business Process Management solution please visit <http://www.qpr.com/rmc-customers.html>

References

- 1) Forrester, March 16, 2006, "The Forrester Wave: Governance, Risk, And Compliance Platforms, Q1 2006"
- 2) Forrester Research, July 14, 2005 "Business Complexity Challenges Compliance"

QPR Software Plc

QPR Software Plc is an international, highly regarded partner for enterprises and public sector in process development and business performance improvement. QPR's mission is to help people and organizations to take control of their business processes and achieve their goals.

QPR software has been implemented in more than 1,500 organizations across the globe and is provided in more than 20 languages. QPR was founded in 1991, has its headquarters in Helsinki, Finland and co-operates with an extensive network of talented partners in over 50 countries worldwide.

QPR Software Plc

Huopalahdentie 24
FI-003350 Helsinki, Finland
www.qpr.com

Tel. +358 290 001 150

Fax: +358 290 001 151

QPR Customer Care

Tel: +358 290 001 155
customer care@qpr.com

