

REPORT ABSTRACT

Personalized GRC: Leading Practices from Methodware

A report by Chartis Research, June 2011

An overview

There is little doubt that risk management has begun to assume an ever greater significance in the post credit crunch world. In all the analysis of what went wrong, however, one common theme seems to be emerging: in many cases, there was a loss of individual ownership of risk management practices because of a failure to personalize them.

It was not that firms did not have risk management policies in place before the crunch. Many had a top down approach that effectively imposed procedures on the organization. They also had external bodies, such as auditors and regulators, endorse their procedures and validate their practices. Today, experts are beginning to understand that while centralized control of risk management practices is vital, a personalized approach and distribution of its ownership promote a sense of participation and belonging among staff. Without full staff engagement in the process, a top down approach to risk management is likely to meet stiff resistance from individual departments and staff members.

Before the credit crunch most companies' approach to governance, risk management and compliance (GRC) had remained unchanged for years. Now it is widely acknowledged that this lack of evaluation of GRC practices contributed to firms' inability to respond appropriately to the risks that emerged during the crisis. As regulators and rule makers all over the world have sought to establish new regulations to shore up the financial system, so financial organizations have had to review their GRC practices – which govern the way they approach these regulations. The answer has been to move towards personalization of GRC practices whereby individual business units and staff members can begin to embrace those practices, recognizing their relevance to their own work and that of their department, how they fit into the overall GRC picture and the consequences of any risk management decisions that they may have to take.

This report examines recent trends in GRC practices, including good practices that firms are adopting, some real life examples of how companies' risk management practices failed them in the credit crunch and the need for a more personalized approach. It also considers how ERA Kairos, the latest version of Methodware's GRC software platform, can help businesses meet the personalization challenge and includes two user case studies.

A little more detail

From a functional perspective, GRC incorporates risk management, compliance and internal audit. Ideally, these functions should be independent of each other. The audit function should review and, if necessary, challenge the compliance risk functions to provide assurance to the board of the firm's overall governance.

It has become clear, however, that some of the failings in financial services companies' ability to manage risk emerged out of their lack of insight into how the different types of risk are interconnected and related. Consequently, any attempt to manage them must reflect that rather than being approached on a siloed basis and any consideration of GRC must include other types of risk. For example, it shares many aspects of Enterprise Risk Management (ERM) and is also interrelated with Operational Risk (OpRisk).

The convergence of GRC, OpRisk and ERM practices has led to some confusion in the technology marketplace for both the buyers and sellers of risk management solutions. Fortunately, it has also resulted in the convergence of technologies, so that solutions with roots in one risk management discipline are adding new functionality that crosses boundaries into other risk areas.

Some CEOs are also looking to reduce cost and complexity, which is causing GRC practices to evolve. The objective is to bring together many of the groups that comprise GRC, such as internal audit, compliance, operational risk and IT security, to reduce complexity and provide management with information that can improve performance and efficiency. The convergence of these risk management areas is set to continue, further driving systems and technology sharing and integration.

One of the main factors driving convergence in GRC, OpRisk and ERM is the increase in worldwide regulatory activity. Many countries and regions have enacted laws and regulations, such as Basel II and Solvency II in the European Union and SOX and HIPAA in North America, and adopted new standards that create an overlap. The new regulations and standards have resulted in increased levels of scrutiny.

In the last three years, as awareness and understanding of risk management has begun to pervade organizations, risk officers report that they have made great progress in engaging employees and business units and in being able to gather the relevant data to be able to do their jobs more effectively. Business units have set up specific sub-groups to report regularly to risk officers. They can provide intelligence and insight, but they also gain a sense of their significance in the process.

Companies are also looking to link their GRC and business processes in the belief that understanding and managing GRC issues will help them to improve the business decisions that they make. They recognize that to be successful they must view the process as a method of achieving their stated business goals, rather than simply a box-ticking exercise.

In the aftermath of the credit crunch, reams and reams of analysis have been generated as businesses, experts, risk managers and others seek to understand exactly what went wrong. One of the conclusions beginning to emerge is that although financial institutions had risk management policies and procedures in place, backed up by outside experts, such as external auditors, there was a failure to take individual ownership of risk.

The move is towards individual ownership of risk management by senior management, risk officers, individual business units and employees – whereby more personal responsibility is taken for risk management decisions.

Industry observers say that loss of ownership of responsibility is what characterized many of the firms that made the biggest losses in the financial crisis. While some smaller firms failed, it was the largest firms that suffered the most harm, partly because their risk management decision makers were furthest removed from the consequences of their actions. They were simply too large and unwieldy for them to be able to see the effects of their decisions. In the smaller firms those making the decisions had extensive knowledge and experience, were able to see more clearly what was happening in their own firms and took personal responsibility for their decisions and final outcomes.

**“In the airline industry, the final decision to fly rests not
with the board of directors or the CEO, but with the pilot...”**

So how can firms establish an enterprise wide culture in which individual ownership of decisions and their consequences is encouraged and promoted?

Since knowledge and understanding are key to effective risk management, it is vital that individual workers and teams understand how their work impacts on others throughout the organization and the consequences of any decisions that they make. A siloed perspective must be avoided so that they see themselves in the context of the whole enterprise rather than just their own business unit.

A long established pioneer of risk management software, Methodware has a large and varied client base and a truly global presence. As a leading GRC vendor, it has sought to address the individual ownership challenge with the release of the new version of its GRC software platform, ERA Kairos. A risk, compliance and audit software solution, it allows users to personalize all the GRC functions and to control how data and workflows appear so they meet user requirements and change with the needs of the business.

Recognition of the need for a personalized approach has been a more recent development that is going to require a response and appropriate action from firms. Like an integrated approach to risk management, it may require major cultural and organizational change for it to take effect. So any organization that is already beginning to think along those lines is ahead of the pack.

To download the full report, please visit the Chartis Research website via the link below:

