

## BEST PRACTICE

# Corporate eGRC update

## Ovum research for EMC

Reference Code: CYIT1450

Publication Date: December 2010

Author: Graham Titterington

---

## THE OVUM VIEW

E-Governance, Risk and Compliance (eGRC) strategy is of immense importance to organizations in both the private and public sectors. It has consistently registered as one of the major drivers for information security investment for many years. As leading organizations adopt more mature eGRC processes, and integrate their eGRC systems more closely with their business systems, it is now an appropriate time to review how far enterprises have come and determine their future priorities.

Leading organizations are moving eGRC strategy to the board and coordinating policy around risk management. eGRC is broader than security management. eGRC activities span the finance, operations, IT, and legal functions. Integrating activities across these functions can streamline processes and avoid duplication of effort. Integrated processes, well supported by appropriate technology, pay dividends with more efficient operations, more accurate and consistent reports, and enhanced reputation.

eGRC empowers trust and drives many corporate initiatives in areas such as sustainability and social responsibility. It relies on accurate and verifiable data relating to these business processes and it is therefore advantageous to integrate its implementation with business processes, both to enhance accuracy and to gain operational efficiencies.

Ovum interviewed 340 senior executives with responsibility for eGRC activities in their organizations, across seven countries in North America and Western Europe.

There is heartening evidence that eGRC processes are maturing. One problem with compliance as it is practiced today is that it is too heavily based on periodic inspections, and organizations drift



out of compliance between audits as a result of their evolution. We were therefore particularly pleased to find a growing intention to integrate continuous controls monitoring into eGRC processes.

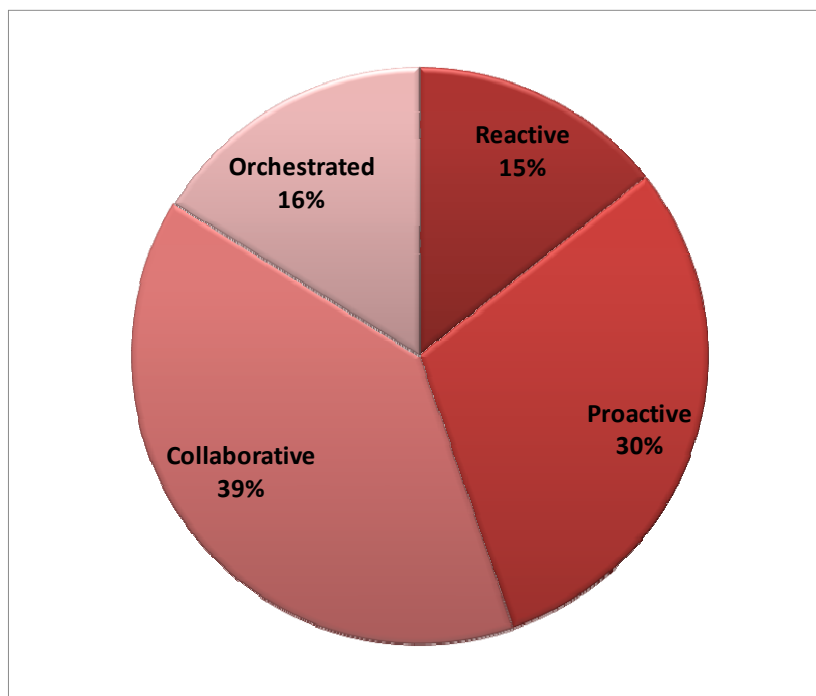
eGRC faces new challenges as emerging IT technologies such as virtualization and the adoption of cloud services raise new issues relating to information integrity. The user community is still uncertain about what these issues are, and about their relative importance.

While the main driving force behind eGRC implementation is the raft of legislation emanating from the US and EU governments, about 20% of the programs are motivated by a desire to adopt best practice, and a small but significant portion is driven by internal polices within the organization.

## RESEARCH FINDINGS

### Integration of eGRC activities

Organizations painted an optimistic picture of their journey into eGRC, with 69% believing they have arrived at either the “proactive” or “collaborative” level in the process maturity model. 16% have achieved the highest level of an “orchestrated” approach.



**Figure 1: Maturity Level of GRC**

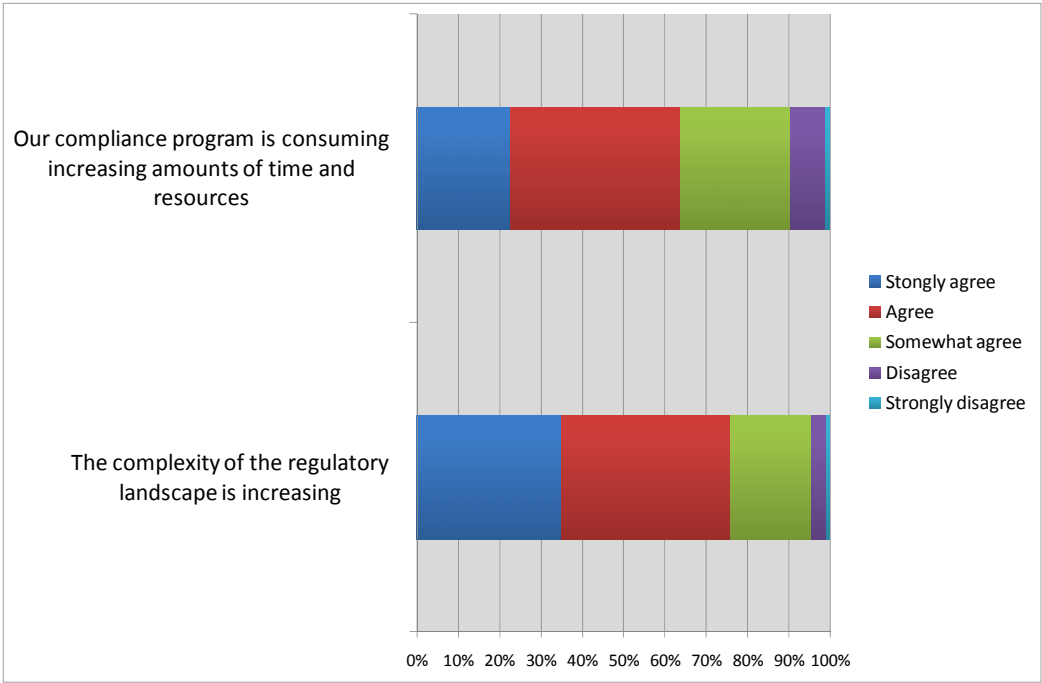
Process maturity is both a stimulus to adopting an integrated and comprehensive approach to eGRC delivery, and a consequence of a coherent and consistent view of the subject. This is a two-way deal. We found that the level of maturity of the process correlated with the level of integration of the supporting eGRC tools – whilst only 15% of respondents overall rated their process “reactive”, this rose to 31% amongst the organizations that relied on manual processes and spreadsheets. Conversely businesses are being driven forward by the state of maturity of their processes – for example, 42% of those with an orchestrated process are looking to integrate their quality management process with eGRC within the next 2 years, and 44% of them are looking to integrate continuous controls monitoring.

**Ownership of eGRC strategy**

We found a diverse view about who is responsible for eGRC strategy. The largest group of organizations put responsibility on the board (30%), but significant numbers operated the strategy under the ownership of their heads of business units (14%), the CIO (12%), a Chief Risk and Compliance officer (11%), or the CEO (11%). However when we looked into enterprises with an orchestrated eGRC strategy there was a clearer sense of direction with 47% placing responsibility on the board. This is consistent with the view that establishing a clear line of responsibility is a necessary preliminary for a coordinated delivery strategy.

**Drivers for eGRC activities – now and in the future**

eGRC activities are under stress. There is general agreement that the complexity of the regulatory landscape is increasing, and that the compliance program is consuming increasing amounts of time and resources. While budgets are growing, demands are outstripping resources. Over 90% of interviewees said that compliance was taking an increasing amount of time and resources, while 96% said that the complexity of the regulatory landscape was increasing. There was less agreement about the way forward.



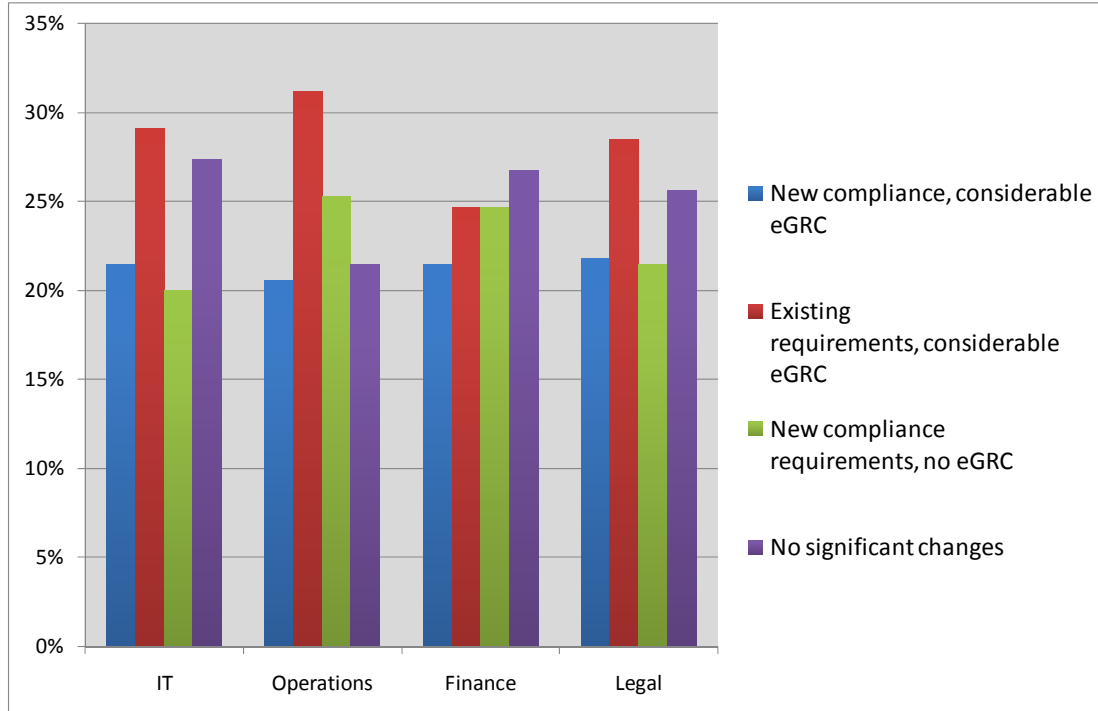
**Figure 2: eGRC complexity and cost**

Opinion is evenly divided about whether additional eGRC response will be needed over the next 2 years as a result of new or existing compliance requirements. The Legal, IT and Operations functions expect to have to increase their eGRC activities, while the Finance function believes that its existing eGRC response will be adequate for the medium term future. We believe that this is because the Finance function has been the focus for many of the recent initiatives on compliance. We have found in other research that there is a widespread problem of "partial compliance" and that most organizations are trying to catch up with the legal and regulatory framework. This survey showed that resource constraints are forcing many organizations to stretch their existing effort to close these gaps.

However we found that eGRC budgets are generally growing. 42% of organizations are increasing their eGRC budgets this year, while 51% are maintaining their current level of spending. Just 7% are planning to cut their eGRC budgets, and nearly all of these by only a modest amount.

In Europe there is a stronger focus on compliance with process management standards and in many cases these get incorporated into an organization's internal practice standards. However the US has stronger penalties for non-compliance, which gives external statutes greater urgency than process improvement initiatives.

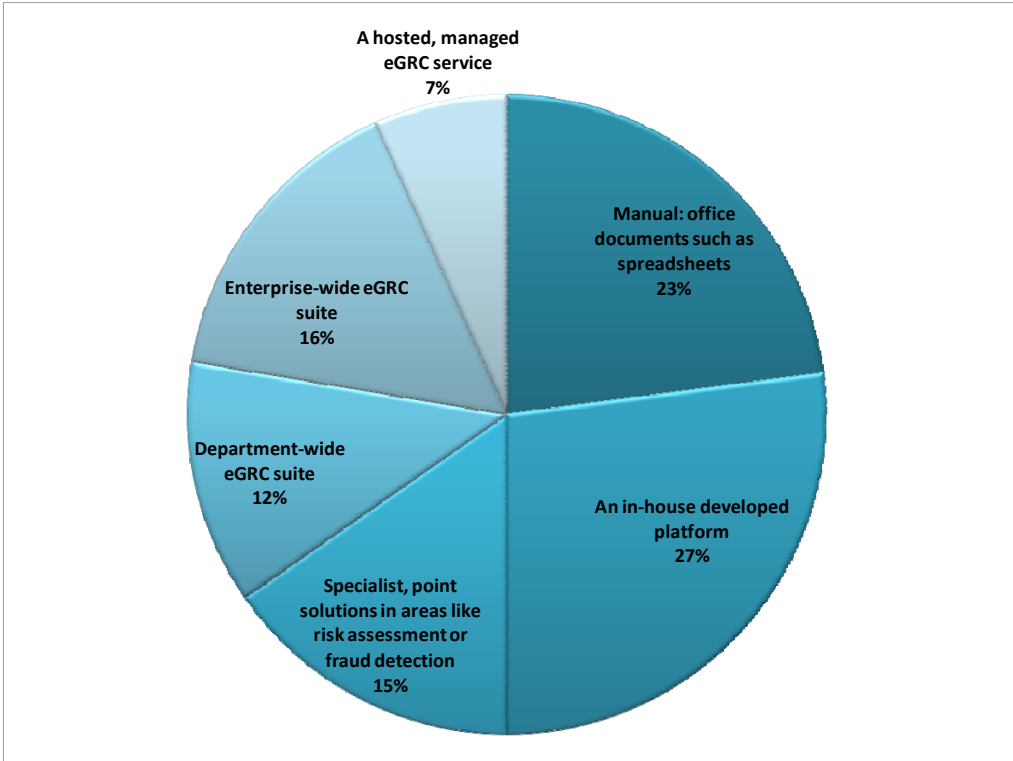
The spectrum of enterprise plans for the next two years, including efforts to address new requirements and to "catch up" on some existing requirements, is illustrated in figure 3.



**Figure 3: External regulatory requirements: changes & reactions**

### State of implementation of eGRC

Organizations still rely too heavily on manual processes supplemented by isolated tools such as spreadsheets, as shown below in figure 4.



**Figure 4: Implementation of eGRC initiatives and systems**

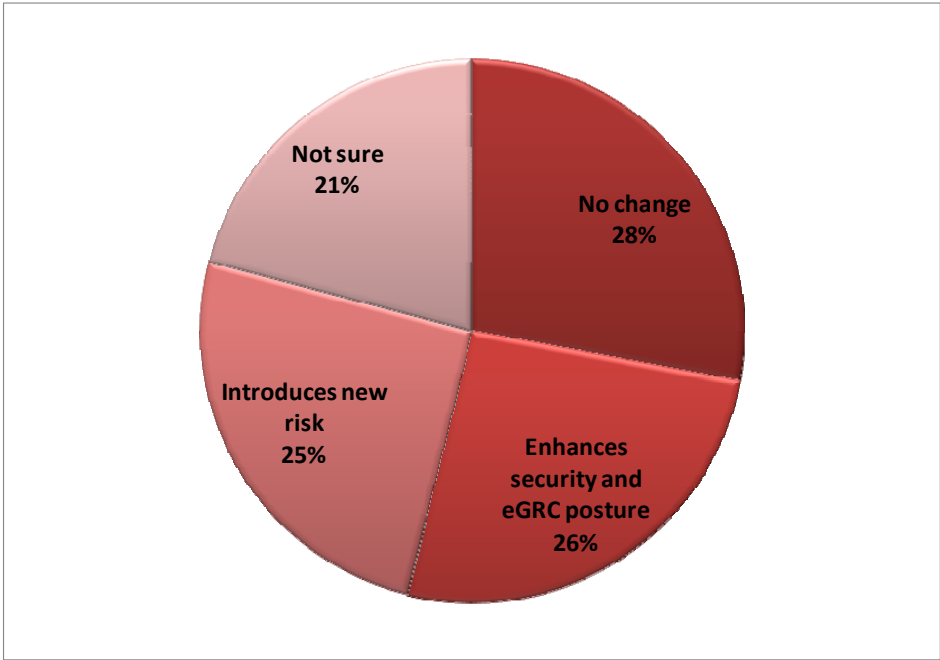
There is a widespread understanding that it is necessary to integrate a wide range of business systems with the eGRC system. The priority list is headed by risk analytics (89%), followed by accounts and HR systems (81%), identity and access management (78%), documents and records management (79%), auditing and logging systems (76%), business continuity systems (72%), anti-fraud systems (67%), asset management (67%), and supply chain management (60%).

Risk management is inherently a difficult task because it involves a multitude of unknowns that are difficult to estimate. When reviewing the types of strategic activity that constitute an eGRC program, assessing and monitoring risk is considered to be the biggest eGRC challenge, ahead of the tasks needed for unified policy management. The greatest concerns in the execution of eGRC activities are keeping up with regulatory changes and mapping them onto control frameworks, managing information captured in decentralized and disjoint systems, and the gap between people who set policies and those who apply them.

Moving forward there is widespread enthusiasm for integrating more assessments into the eGRC process, headed by environmental, health and safety assessments, corporate and social responsibility assessments, continuous controls monitoring, quantitative risk analysis, and privacy assessments. This reflects the increasing importance of privacy in corporate consciousness.

**New technologies, such as virtualization and cloud computing, cause concern**

There is widespread confusion about the impact of server virtualization on risk management and eGRC, with opinion evenly divided about whether risk will increase or decrease.



**Figure 5: server virtualization - impact on risk management & eGRC**

The cloud is generally seen as a high risk development. This concern focuses on handing sensitive data to third parties, followed by the lack of ability to prove compliance in a cloud service, the lack of transparency of cloud service providers' operations, relinquishing control over business processes, and integration of in-house systems and cloud services.

Surprisingly the US respondents were more concerned about proving the physical location of data than their European counterparts. The US respondents registered 25% more concern on this issue



than the European and Canadian respondents. However it is important to remember that corporate law in the US places responsibility on senior management concerning the location of information relating to their organization that goes far beyond the control of personal data.

## **APPENDIX**

### **Author**

Graham Titterington, Principal Analyst, Information security, Ovum

[Graham.titterington@ovum.com](mailto:Graham.titterington@ovum.com)

### **Disclaimer**

All Rights Reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the publisher, Ovum (a subsidiary company of Datamonitor plc).

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.