



BEST PRACTICE

Governance Risk and Compliance

GRC usage and buying trends in the Australian and New Zealand markets

Reference Code: OI00199-003

Publication Date: February 2012

Author: Andrew Kellett

SUMMARY

Catalyst

The existence of an established and stable governance risk and compliance (GRC) strategy is extremely important to public and private sector organisations as they strive to meet an ever-growing range of regulatory demands. It is a major driver for existing and new information security investment. Also, given the current constraints on IT and operational budgets, it is one of the few areas where the vast majority of organisations intend to either maintain or in many cases increase spending. This situation almost certainly results from the predominance of board-level ownership of corporate GRC strategies.

Ovum view

For enterprises there needs to be an integrated approach to GRC that builds on the interdependencies between its three core components. Governance, which invokes culture, policies, processes, laws, and institutions that define the structure by which companies are managed. Risk which focuses on the effects of uncertainty on business objectives, for example risk management is defined as the coordination of activities to direct and control an organisation in order to realise opportunities while managing negative events. Compliance, which concentrates on adherence to, laws, regulations, corporate policies, and associated procedures.

When considering the GRC market the terms eGRC and IT GRC are commonly used. eGRC implies an integrated enterprise governance, risk, and compliance position when working with selected sensor technology; technology that is used to provide protection, monitoring, and management for networks and information systems. For example, eGRC solutions can be used to build collaborative programs across key business areas, to manage risk, demonstrate compliance,

automate business processes, gain visibility, and improve reporting. The specifics of an IT GRC program will vary between organisations and their individual circumstances, it involves pulling together the previously siloed components of IT governance, IT risk management, and IT compliance to provide a holistic view of the IT environment and ensure accountability.

Generically GRC extends across all major business functions. Its combined focus needs to cover key areas such as finance, legal, IT, and business operations. Because GRC relies on accurate and verifiable data, delivering an effective GRC strategy using an integrated approach that covers all these functional areas goes a long way towards streamlining information flows and the avoidance of duplicated effort.

While there remains a stubborn resistance from some areas of senior management to move away from spreadsheets and other home-grown systems to fulfil GRC processes, there is a steadily growing acceptance that specialist enterprise GRC tools are necessary. In Ovum's opinion the growing maturity of the available products can deliver user efficiency and business benefits, which provides the required proof. In today's difficult trading conditions GRC is one of the few areas where organisations are not looking to reduce spending. A very high percentage of organisations expect to spend at least as much or more on GRC activity in 2012 as they did last year.

Historically regulatory compliance has been something of a hit and miss affair, organisations have set themselves up to pass point-in-time inspections, but have not had the facilities in place to maintain continuous compliance. This is a situation that is changing. Our research in the Australian and New Zealand markets identified that almost three quarters of all respondents were working to maintain common standards for their GRC programs. They were looking to continuously satisfy regulations, conform to common standards, make use of the same technology platforms, and importantly apply common processes. All of these responses support the need for specialist GRC tools, the need for automation, and the need to reduce reliance on manual processes.

While there are always differences between the regulatory priorities of enterprises in different industries, GRC pulls together the requirement to integrate processes across key business areas. Close to half of the respondents in the Ovum GRC survey placing GRC ownership at board level, therefore the opportunity to drive initiatives from the top down clearly exists. However, it is less clear how board level objectives will be achieved as there is a significant lack of appreciation of GRC requirements amongst employees and therefore a worrying gap exists between senior management who set policies and the staff who are required to comply.

In the world of business and IT new challenges are never far away. New and emerging areas such as virtualisation and the adoption of cloud raise fresh information integrity issues. The user community is still uncertain about what these issues are, almost a third of respondents were unsure what effect the adoption of virtualisation would have or about its relative importance. Furthermore, when considering cloud usage issues, between 60% and 80% felt strongly that handing over sensitive data to a third-part service provider would present serious GRC issues.

Key messages

- GRC requirements are well understood within senior management circles, but less so by the employees who are required to deliver compliance.
- GRC is a growing area of corporate activity and because of senior management ownership has been protected from budgetary constraints.
- Lack of vision is still a significant issue, with a continuing reliance on spreadsheets and internally developed GRC solutions.
- Changes and updates to rules and regulations as well as the need for regulatory compliance are key drivers, but the need to achieve efficiencies from the use of common processes is of growing importance.
- As well as traditional approaches to GRC technological advances will generate new issues that need to be addressed as organisations take into account changing operational environments.

SURVEY METHODOLOGY

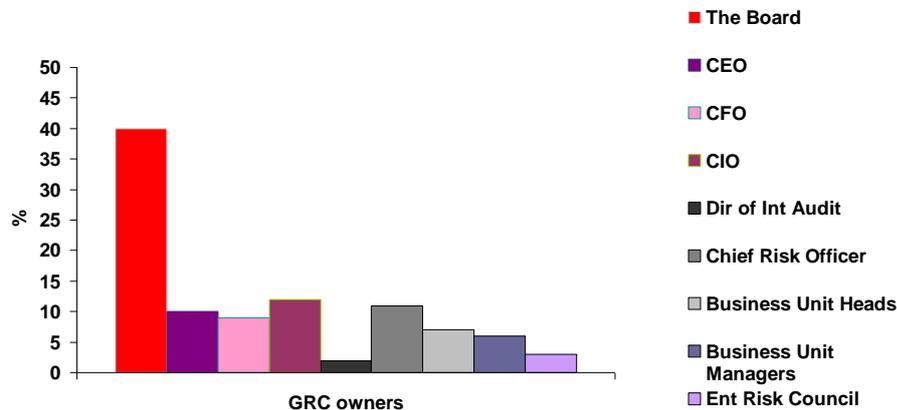
This report has been commissioned by RSA, the Security Division of EMC. Ovum has interviewed 100 senior executives across Australia and New Zealand with responsibility for GRC activities in their organisations. The selected organisations had over 500 employees, and for the purposes of this analysis were grouped into size bands of: 500 to 999, 1,000 to 1,999, 2,000 to 4,999, and over 5,000. We analysed their responses to a range GRC related questions that focused on existing and future requirements and on issues of concern and market adoption.

GRC OWNERSHIP, BUYING HABITS, RISK, AND EXECUTION CHALLENGES

Ownership

GRC requirements are well understood within senior management circles, but less so by the employees who are required to deliver compliance. The GRC strategy of organisations is owned by around nine separate senior management groups including 'C-level' executives. By far the largest of these groups is the board of directors which accounts for 40% of the companies surveyed. Chief information officer (CIO), chief risk and compliance officer (CRCO), and chief executive officer (CEO) were the only other posts that scored double digit percentages; the highest of these was the CIO with 12%.

Figure 1: GRC Ownership



Source: Ovum

Who owns your GRC strategy

Source: Ovum

OVUM

The Australian and New Zealand GRC survey results reflect a predominance of high-level boardroom ownership, which centralises the issue of control far beyond the level of individual business units. This is similar to the responses seen from the USA and Canada, and from France and the UK in earlier surveys. But is significantly different from other areas of Europe including Germany and the Benelux countries where ownership of GRC is often delegated to the CRCO, CFO, or CIO, and Germany in particular where no organisations reported positioning GRC ownership with the board. Germany takes a more technical focus with either an enterprise risk/security council, or the CRCO taking responsibility in over 50% of cases.

The important ownership issue for GRC within the Australian and New Zealand markets is that when board level responsibility is added to 'C-level' accountability over 80% of GRC responsibility exists within the boardroom or is invested in officers who report directly to the board. At the other end of the scale business unit managers look to have little influence and the role of 'enterprise risk security councils' has not taken off within the region.

GRC spending and buying habits

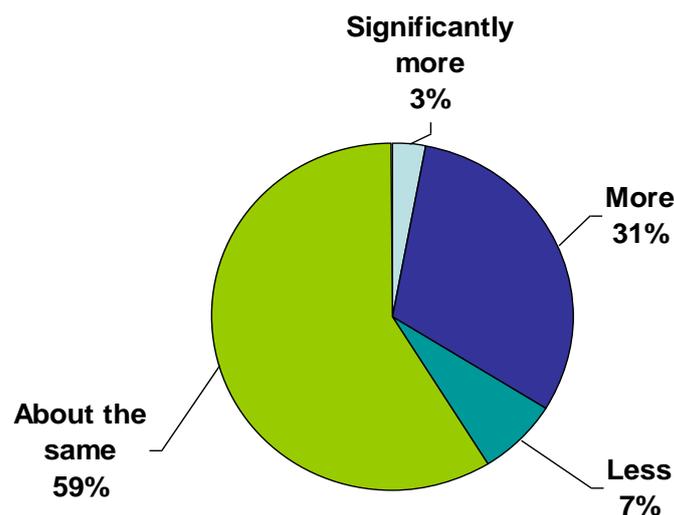
GRC is a growing area of corporate activity and because of senior management ownership has been protected from budgetary constraints.

While very few Australian and New Zealand organisations (only 3%) are planning to spend significantly more on GRC projects during 2012 than they did last year. The overall picture for GRC is extremely positive. Against an industry-wide backdrop of cutbacks, 93% of respondents to

the Ovum buying trends survey expect to spend at least the same or more than last year on GRC, with a third of those organisations planning to spend more.

Board and 'C-level' ownership of GRC is certainly advantageous in today's difficult trading climate, but with almost three quarters of organisations looking to achieve common standards for regulations (76%), frameworks (70%), technology and platforms (72%), and processes (75%) across their GRC infrastructure; the fact that GRC budgets are being maintained and in many cases increased is not surprising.

Figure 2: 2012 GRC spending patterns



Source: Ovum

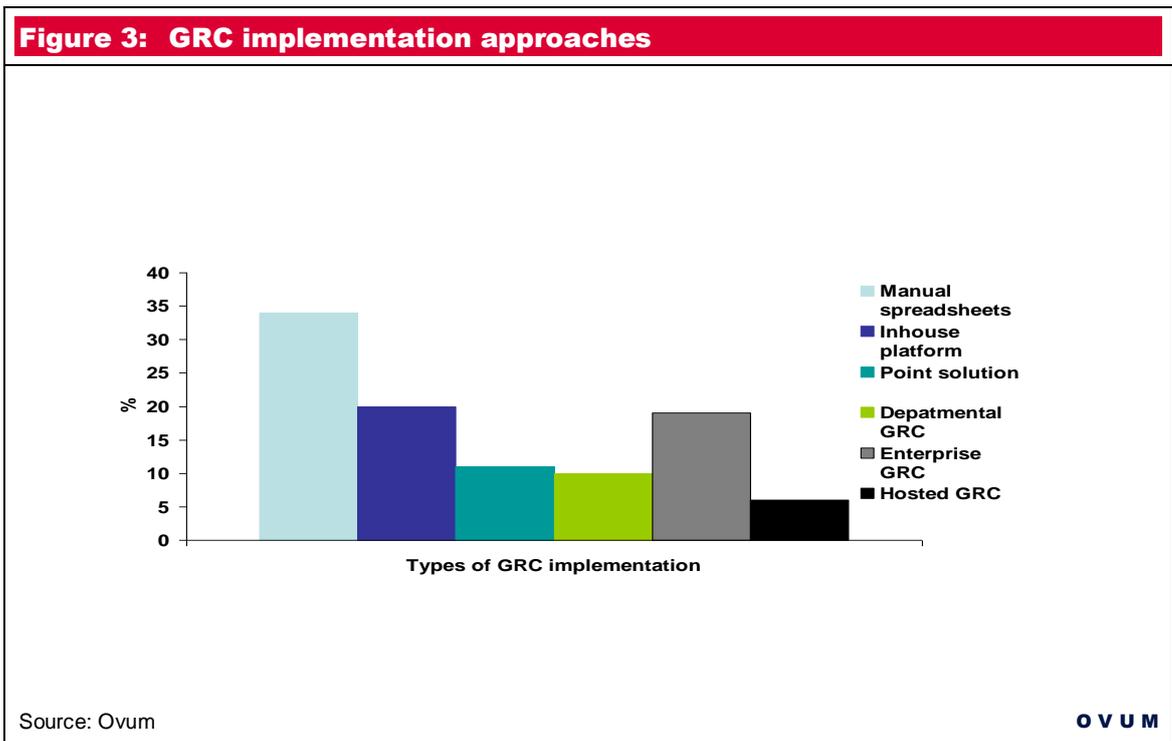
OVUM

Lack of vision is still a significant issue with a continuing reliance on spreadsheets and internally developed GRC solutions.

It remains disappointing, although not out of line with our findings in other parts of the world, to find the level of reliance on spreadsheets and in-house developed legacy platforms. Amongst the major concerns in GRC execution is the need to keep up with and maintain regulatory changes and map these onto control frameworks. Information captured in local, often home-grown systems, present potential continuity problems between those who set policies and those who have the need to apply them.

There may be a general understanding that it is necessary to integrate a wide range of business and security systems within GRC including key areas such as risk analytics, accounts, HR, documents and records management, asset management, supply chain management, audit management and logging systems, business continuity management systems, identity management, and antifraud. However, the evidence suggests that only around a fifth of

organisations have deployed enterprise wide GRC suites with 10% using departmental GRC suites, and a further 11% purchasing point-based risk assessment or fraud detection solutions.



Risk management and the assessment of risk

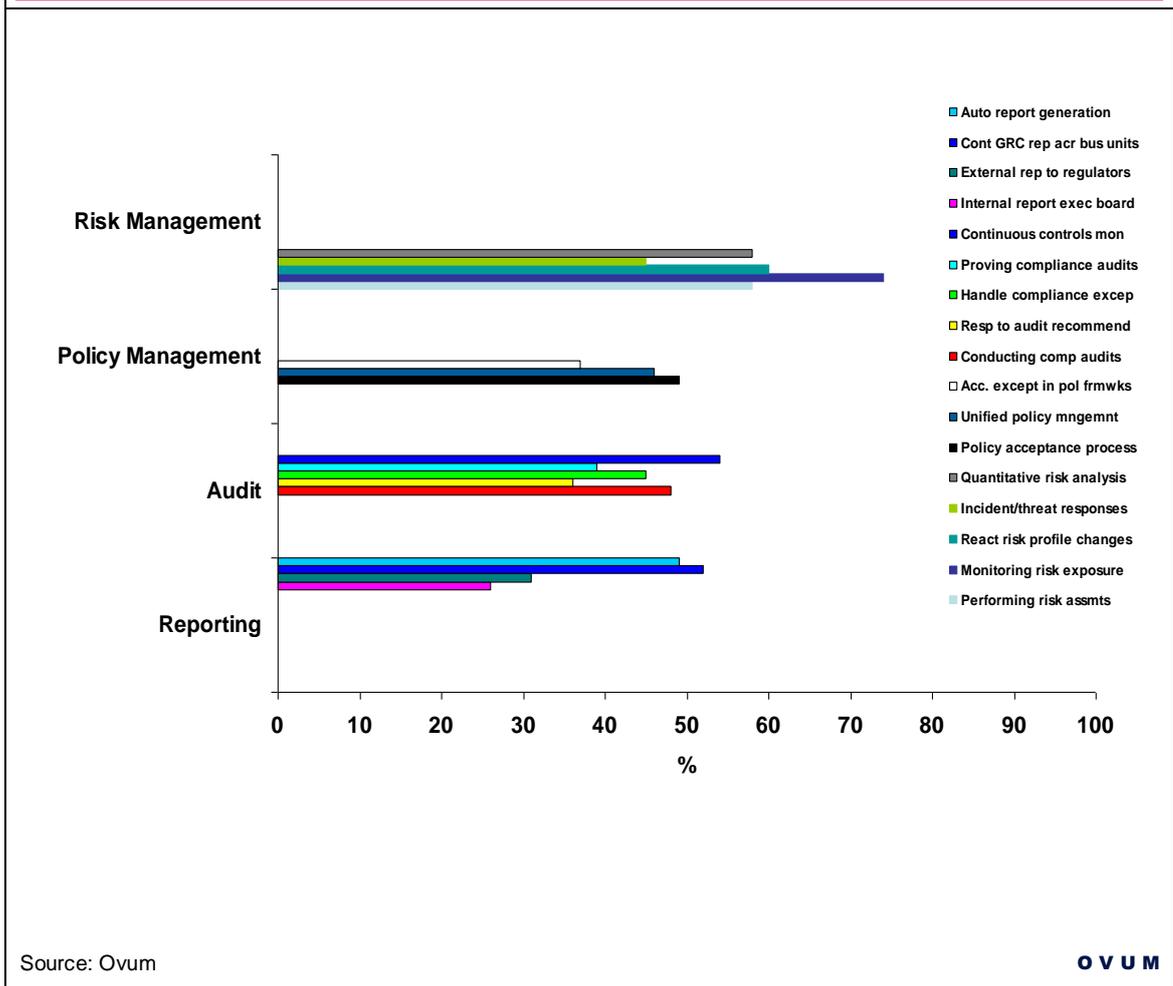
Effective risk management is difficult to achieve. It involves many different tasks, some of which will not be obvious. Our interviews confirmed this to be the case when we asked organisations what their biggest GRC strategy challenges were.

The four GRC strategy areas assessed were: risk management, policy management, auditing, and reporting. Figure 4 shows that respondents identified risk management as the most challenging area. Four out of the top five most significant GRC challenges came from risk management. The fifth element came from the auditing area where 'continuous controls monitoring' was seen as providing serious problems. This was not unexpected because of the need to keep up with constant regulatory and business changes.

Within the risk management options there were five areas of assessment. Ovum identified that the number one GRC challenge for Australian and New Zealand organisations is the monitoring of risk exposure, almost three quarters of respondents saw this as a key challenge. It was followed by the need to react to changes in risk profile, the performance of risk assessments, and the ability to provide quantitative risk analysis.

Elements of policy management - policy acceptance processes; auditing - with the high profile elements of continuous control monitoring and conducting compliance audits; and reporting - where the connection of GRC reporting across business units and automating report generation, were also seen as significant obstacles.

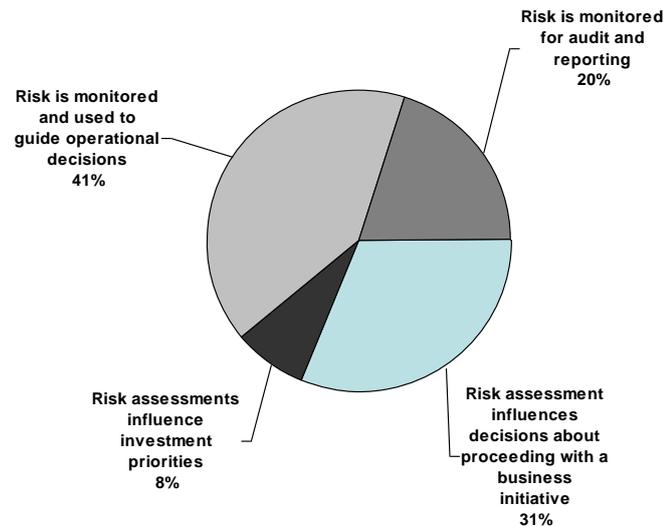
Figure 4: The most significant GRC strategy challenges



Risk assessments have an impact when making business decisions

Risk assessments have more of an impact on operational judgements than they do over investment decisions. On a priority basis clients were asked about their risk assessment usage priorities. Over 30% of respondents said that most importantly risk assessments are used to influence business decisions, and hold sway on whether to proceed with new business initiatives. A further 41% confirmed that risk assessments are used to guide operational decisions. However, there was a very low response when clients were asked if risk assessments influence investment priorities, only 8% said they did. Finally, one fifth of respondents confirmed that risk is monitored for audit and reporting purposes.

Figure 5: The impact of risk decisions



Source: Ovum

OVUM

GRC EXECUTION

As well as making provision for traditional GRC controls, technology advances will generate new issues that need to be addressed as organisations take into account changing operational environments.

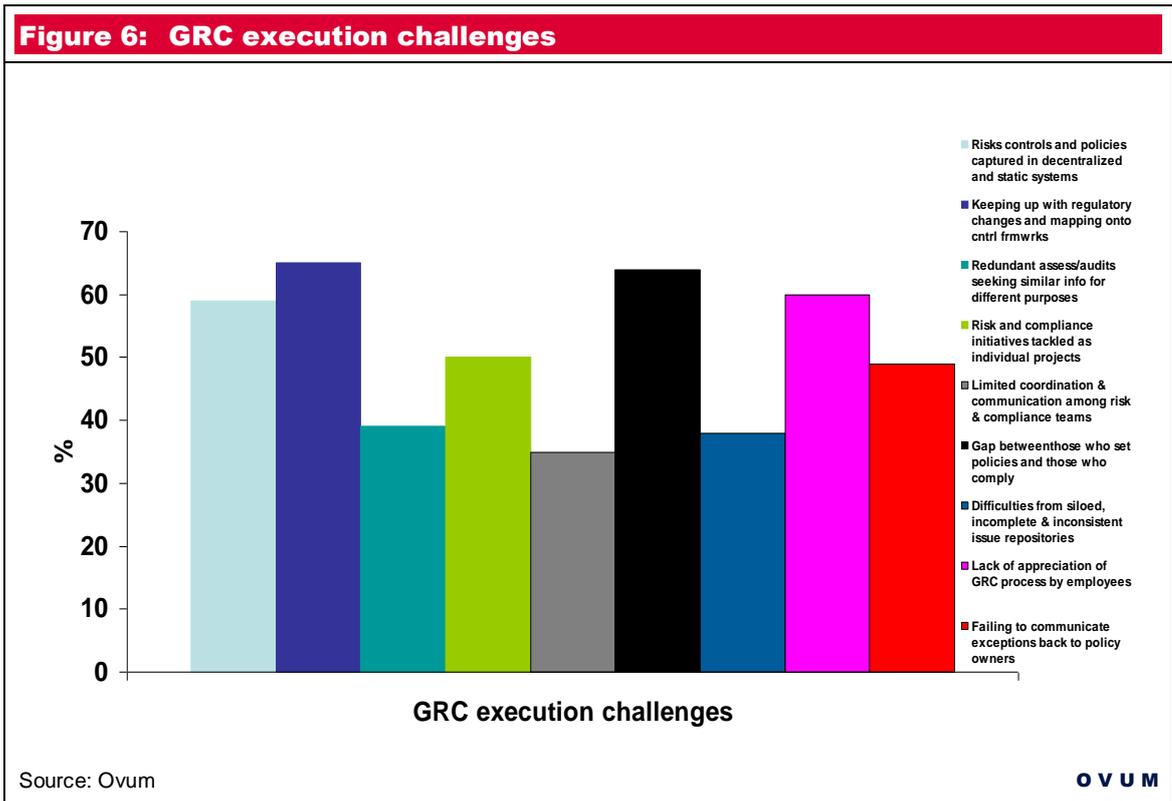
Execution - regulatory compliance challenges

Changes and updates to rules and regulations as well as the need for regulatory compliance are key drivers, but the need to achieve efficiencies from the use of common processes is of growing importance to GRC strategies. When asked to look across the business and determine the most significant GRC challenges that organisations face, the number one priority reported by over 65% of respondents involved the problem of keeping up with regulatory changes and mapping these changes into their control frameworks.

This is not a surprise because so many of those same GRC frameworks are not integrated and were either home-grown, spreadsheet based, or founded upon a combination of the two. Less than 20% of Australian and New Zealand organisations operate an enterprise-wide GRC strategy. For the execution elements these issues were further compounded by the high number of respondents who confirmed that major problems were caused because risks, controls, and policies were captured and maintained in a series of decentralised and disconnected systems.

Further to the reported systems issues that relate to how GRC is operated and maintained, two particular business usage problems were seen to be of significant concern. 64% said that the gap between senior management, who set GRC policies, and employees, who are required to comply, is problematic. This situation was confirmed by the 60% of organisations who said that there was a

lack of appreciation of GRC processes by employees. These elements were clearly high-level execution challenges.

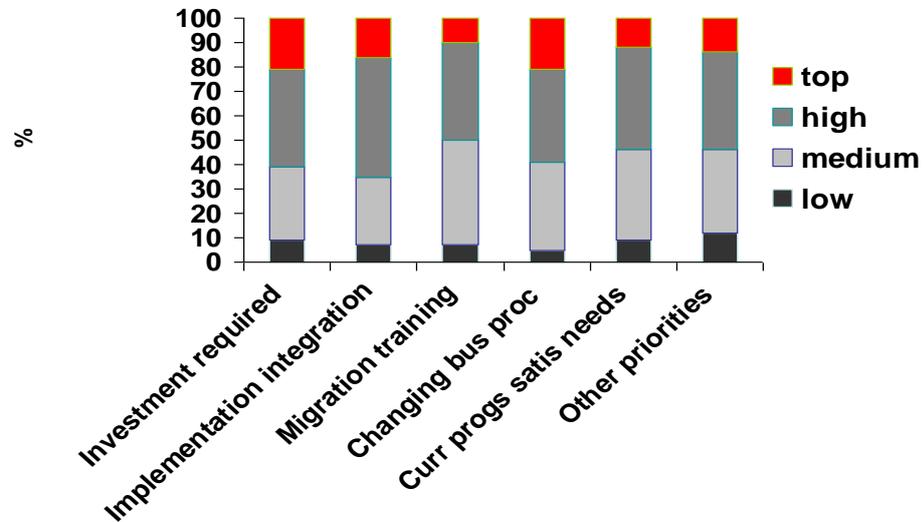


Execution - GRC Adoption challenges

The most significant obstacles to adopting new GRC systems and strategies involve implementation and integration issues. Included within the scope of implementation is the associated need to change existing business processes. Required additional investment was also identified because, in today's difficult trading climate, all budgetary additions are subject to close scrutiny. However, as previously mentioned, senior management ownership of GRC strategies makes it more likely that approvals will be given. Which is the established position, as GRC budgets are generally being maintained, or as reported by a third of respondent organisations are increasing.

The downside of this argument comes from the high number of organisations that appear to be reasonably happy with their existing GRC approaches with over half saying that their current programs and systems meet or at least satisfy their needs and a similar number suggesting that no changes will be made because other initiatives are being prioritised. Again this position is in line with earlier budgetary findings as more than two thirds of respondents reported that they would be spending about the same on GRC in 2012 as they did last year. This is a position that can be maintained if the same or similar facilities are being used and major changes are not planned.

Figure 7: Obstacles to GRC adoption



Source: Ovum

OVUM

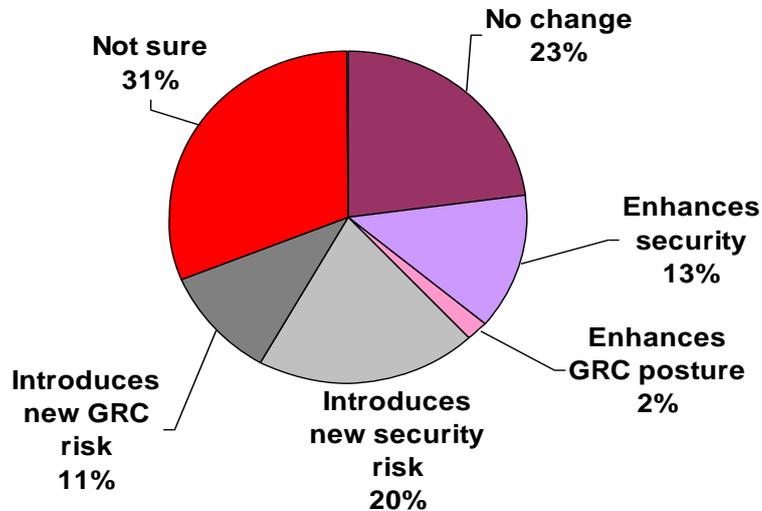
Execution - GRC and virtualisation

GRC faces new challenges as emerging technologies, such as virtualisation, raise new issues of information integrity. Ovum research shows that the user community is still uncertain about what these issues are, and about their relative importance. Opinion was divided about whether risk will increase or decrease as a result of adopting server virtualisation technology.

Almost a third of Australian and New Zealand respondents fell into the 'not sure' category which is 10% higher than the results from a global survey carried out a year before. This could indicate that the use of virtualisation technology is not as widespread and therefore a higher number than expected do not have enough information available to give an opinion.

Organisations that have taken up the virtualisation challenge were evenly split in their views on whether the technology's adoption impacts on risk management and GRC. Almost a quarter (23%) took the no change position, but almost the same percentage said they felt that virtualisation introduces new security risks and a further 11% considered that new GRC risks would exist. In line with general security concerns about virtual and cloud environments only a small number of organisations felt that using new technology enhances either their security or the general GRC posture.

Figure 8: Virtualisation Challenges



Source: Ovum

OVUM

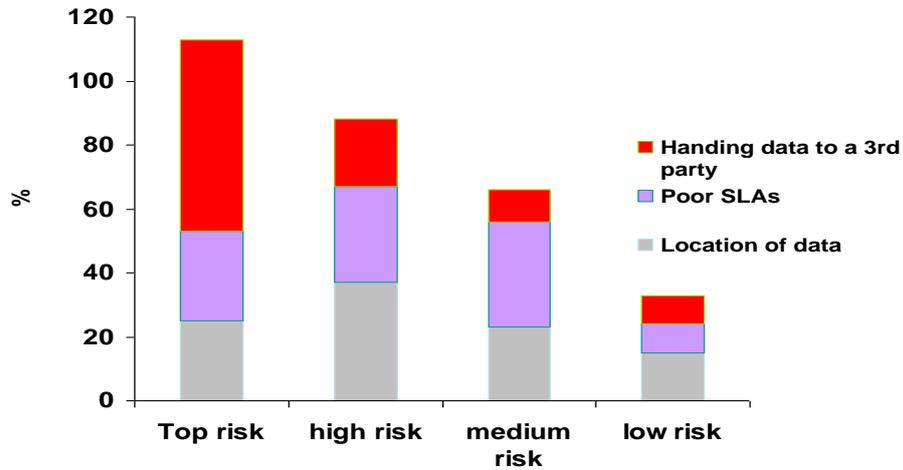
Execution - GRC and cloud computing services

From an information security perspective the cloud is seen as high risk. In line with this business view, over 80% of survey respondents said that handing sensitive data to third party service providers is a major inhibitor to the adoption of cloud services and is a significant GRC issue. 60% put this into the top risk category and were supported by a further 21% that considered it medium to high risk. These risk numbers far outweighed any of the other cloud issues that organisations were concerned about.

For example only a quarter of respondents said that proving the physical location of their data was of the highest concern and only one fifth had major worries about relinquishing control over business processes. However, the continuing issue that business has with service level agreements (SLAs) was seen as a significant concern. 28% positioned SLAs as a major cloud inhibitor and the numbers increased to nearly 60% when taking into account those organisations that see SLA issues as a medium-to-high concern.

The responses from Australian and New Zealand organisations match those of their European and US counterparts, where handing sensitive data to third parties was also seen as the largest single cloud-computing issue. Again in the European and US markets this was followed by the lack of ability to prove compliance, and the lack of transparency of cloud service providers' operations and the SLAs provided. One associated element that was surprising was that Australian and New Zealand organisations shared the European view and were less concerned than US respondents about proving the physical location of data.

Figure 9: Main cloud computing issues



Source: Ovum

OVUM

APPENDIX

Definitions

Governance

Governance is the culture, policies, processes, laws and institutions that define the structure by which companies are managed.

Risk

Risk is the effect of uncertainty on business objectives; risk management is the coordination of activities to direct and control an organisation in order to realise opportunities while managing negative events.

Compliance

Compliance is the act of adhering to, and demonstrating adherence to, laws, regulations, corporate policies and procedures.

Policy Management

Centrally manage corporate and IT policies, map them to objectives and guidelines, and promote awareness to support a culture of corporate governance.

Risk Management

Identify risks to your business, evaluate them through online assessments and metrics, and respond with remediation or acceptance.

Compliance Management

Document your control framework, assess design and operational effectiveness, and respond to policy and regulatory compliance issues.

Enterprise Management

Manage relationships and dependencies within your enterprise hierarchy and infrastructure to support eGRC initiatives.

Business Continuity Management

Automate your approach to business continuity and disaster recovery planning, and enable rapid, effective crisis management in one solution.

Audit Management

Centrally manage the planning, prioritisation, staffing, procedures and reporting of internal audits to increase collaboration and efficiency.

Author

Andrew Kellett, Senior Analyst, Infrastructure Solutions

andrew.kellett@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@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 (an Informa business).

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.