



# Managing Governance, Risk and Compliance with ECM and BPM

Sponsored by

OPENTEXT

 **aiim**<sup>®</sup>  
The Global Community of  
Information Professionals

## About the White Paper

As the non-profit association dedicated to nurturing, growing and supporting the user and supplier communities of ECM Enterprise Content Management, AIIM is proud to provide this research at no charge. In this way, the entire community can leverage the education, thought leadership and direction provided by our work. Our objective is to present the “wisdom of the crowds” based on our 80,000-strong community.

We are happy to extend free use of the materials in this report to end-user companies and to independent consultants, but not to suppliers of ECM systems, products and services, other than OpenText and its subsidiaries and partners. Any use of this material must carry the attribution – “© AIIM 2015 [www.aiim.org](http://www.aiim.org) / © OpenText 2015 [www.opentext.com](http://www.opentext.com)”

Rather than redistribute a copy of this report to your colleagues, we would prefer that you direct them to [www.aiim.org/research](http://www.aiim.org/research) for a download of their own.

Our ability to deliver such high-quality research is made possible by the financial support of our underwriting sponsor, without whom we would have to return to a paid subscription model. For that, we hope you will join us in thanking our underwriter for this support:

### OPENTEXT

#### OpenText

275 Frank Tompa Drive  
Waterloo, Ontario  
Canada, N2L 0A1  
Tel: +1 519-888-7111  
Web: [www.opentext.com](http://www.opentext.com)

## Process used and survey demographics

The survey results quoted in this report are taken from a survey carried out between 13 March and 06 April 2015, with 211 responses from individual members of the AIIM community surveyed using a Web-based tool. Invitations to take the survey were sent via email to a selection of AIIM’s 80,000 registered individuals. 76% of respondents are from North America, 14% from Europe, and 10% from elsewhere. They cover a representative spread of industry and government sectors. Results from organizations of less than 10 employees have not been included, bringing the total respondents to 1200. Full demographics are given in Appendix 1.

## About AIIM

AIIM has been an advocate and supporter of information professionals for nearly 70 years. The association mission is to ensure that information professionals understand the current and future challenges of managing information assets in an era of social, mobile, cloud and big data. AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community: practitioners, technology suppliers, integrators and consultants. AIIM runs a series of training programs, including the Information Governance Certificate course. [www.aiim.org/Training/Certificate-Courses/Information-Governance](http://www.aiim.org/Training/Certificate-Courses/Information-Governance)

## About the author

Doug Miles is Chief Analyst at AIIM. He has over 30 years’ experience of working with users and vendors across a broad spectrum of IT applications. He was an early pioneer of document management systems for business and engineering applications, and has produced many AIIM survey reports on issues and drivers for Capture, ECM, Information Governance, Records Management, SharePoint, Big Data, Mobile and Social Business. Doug has also worked closely with other enterprise-level IT systems such as ERP, BI and CRM. He has an MSc in Communications Engineering and is a member of the IET in the UK.

© 2015

#### AIIM

1100 Wayne Avenue, Suite 1100  
Silver Spring, MD 20910  
+1 301 587-8202  
[www.aiim.org](http://www.aiim.org)

© 2015

#### OpenText

275 Frank Tompa Drive  
Ontario, Canada, N2L 0A1  
+1 519-888-7111  
[www.opentext.com](http://www.opentext.com)

# Table of Contents

## About the White Paper

<b>About the White Paper</b> .....	<b>1</b>
Process used and survey demographics.....	1
About AIIM .....	1
About the author .....	1

## Introduction

<b>Introduction</b> .....	<b>3</b>
Key Findings.....	3

## Drivers for GRC

<b>Drivers for GRC</b> .....	<b>4</b>
Risks.....	4
Challenges.....	5
Stakeholders.....	6

## GRC Issues

<b>GRC Issues</b> .....	<b>6</b>
Managing Regulatory and Standards Compliance.....	6
Managing the Policy Lifecycle .....	7
Managing Operational Risk .....	8
Managing Audit.....	9
Managing Supply-Chain Risk .....	9

## Use of ECM/RM/BPM

<b>Use of ECM/RM/BPM</b> .....	<b>10</b>
Role of ECM/RM/BPM in GRC .....	11
Current Usage .....	12

## GRC Solutions

<b>GRC Solutions</b> .....	<b>12</b>
Solution Selection.....	13

## Opinions and Spend

<b>Opinions and Spend</b> .....	<b>13</b>
Spends .....	14

## Conclusion and Recommendations

<b>Conclusion and Recommendations</b> .....	<b>15</b>
Recommendations.....	15

## Appendix 1: Survey Demographics

<b>Appendix 1: Survey Demographics</b> .....	<b>16</b>
Survey Background .....	16
Organizational Size .....	16
Geography .....	16
Industry Sector .....	17
Job Roles.....	17

## UNDERWRITTEN BY

OpenText .....	18
AIIM .....	18

## Introduction

Governance, risk management and compliance, or “GRC”, is increasingly being seen as a key discipline. The corporate misdemeanors of the past decade, and the resulting fines, refunds and brand damage have created a situation where the long-term detrimental effect of “loose governance” is being felt both in business and in government. As a result, organizations in a wide range of sectors are much more aware of potential risks, and the need to assess and measure them, while at the same time, legislators and regulators are imposing more and more laws and rules to tighten up business practice.

By its nature, if GRC is worth doing, it is worth doing well, and our survey respondents agree that good quality GRC practices are generally a positive benefit to the business rather than “a necessary evil”. Operating a best practice GRC regime will involve a number of key steps. Pro-active awareness of changes to laws and regulations; decisions on how to change policies and processes to ensure compliance; documentation and dissemination of these changes; implementation of process changes that embed compliance; recording of actions and due process that are evidence of compliance; and measurement of performance to assure senior management and other stakeholders that risk is under control.

ECM, BPM and RM systems (Enterprise Content Management, Business Process Management and Records Management – sometimes combined as EIM, Enterprise Information Management) all have a big role to play in the GRC equation including: information governance for policies, operational monitoring, risk tracking and compliance auditing. In our survey, we set out to understand which governance, risk and compliance areas are the biggest concern, if and how organizations are using ECM, BPM and RM to solve GRC challenges, and what their plans are to improve their GRC program, processes, and tools.

## Key Findings

### Drivers

- **Reputational risk is twice as big a driver for compliance (44% of respondents) as avoiding fines and penalties (20%).** 32% consider “being a good corporate citizen” to be the prime driver.
- **Keeping policies and procedures up to date is a bigger challenge (40%) than keeping up with new and changing regulations (26%).** Managing the paperwork to demonstrate compliance is given as the biggest challenge by 19%.
- **Security risk (56%) and information privacy risks (52%) are of extreme concern. Then come reputational (48%) and regulatory risk (42%).** Financial and operational risks are rated less highly, but are of extreme concern for 35% of our respondents.
- **There is a very wide spread of roles deemed to “own” the GRC program, with Legal (14%) or the GRC committee (12%) most likely** - although only 27% have a GRC committee.

### GRC Issues

- **Adoption of best practice in managing the policy lifecycle is poor.** 38% have no scheduled reviews, 28% have no central store for policies, and 18% don’t capture employee acceptance.
- **47% struggle with multiple systems to document compliance requirements and 45% use manual processes to track performance against requirements.** 19% use home-grown systems that they admit are not efficient or effective.
- **The biggest issues with managing operational risk are lack of visibility and control (50%) and no way to track key indicators (27%).** Not having a central system for records is an issue for 30%, and 25% struggle to provide management with timely reports.
- **45% of respondents find their biggest challenge with internal audit operations is that processes are manual and inefficient.** Having multiple and disparate systems to manage audit information is an issue for 35%.
- **Managing supply-chain risk is made difficult by vendor information not being stored in one place, nor being up-to-date for 35%.** Gaining risk visibility of vendors and classifying them by risk profile is problematic for 25%.
- **81% support the view that “GRC is good for business”,** although there is crossover with the 42% who consider it to be “a necessary evil.”

### Use of ECM/RM/BPM

- **ECM and RM are used widely for policy management (69%), BPM for tracking and resolution (20%) and GRC tools for managing IT threats (30%),** but all four are used across the range of GRC management.
- **67% see ECM, BPM and RM as essential to solving GRC problems.** 27% would like to use these tools for GRC, but the systems they have are not well optimized for this purpose.
- **40% feel that they are achieving regulatory compliance by using their ECM/RM system,** but 78% feel they could get much more value from these systems.

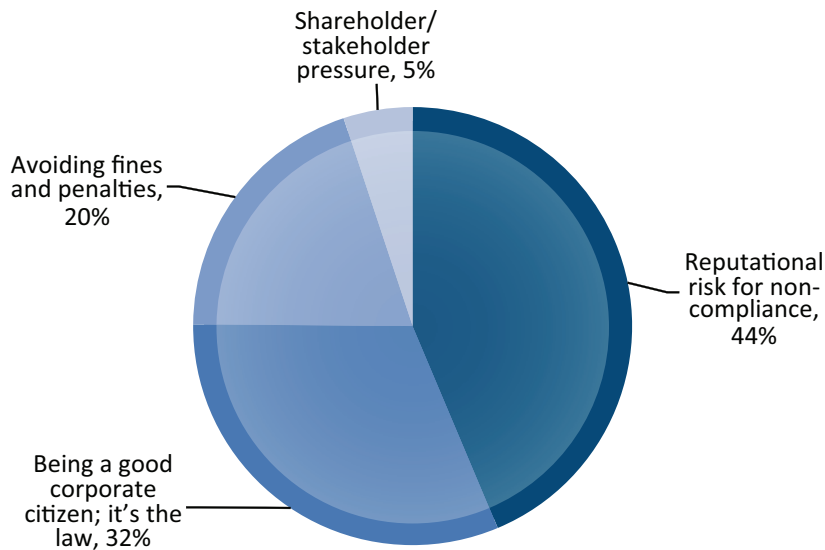
### GRC Solutions

- **Ability to integrate with existing infrastructure (43%) and ease-of-use (35%) are given as the most important selection factors for GRC solutions,** along with price (37%).
- **46% of the organizations surveyed plan to spend more on GRC software or services in the next 12 months,** including 15% spending more on software licences, and 19% on vendor implementation services.

## Drivers for GRC

The traditional justification for investment in compliance has been to avoid fines and penalties from regulators, but as customer perception of the “brand” has shifted from the controlled media world of advertising and publishing to uncontrolled social media and rolling news, the need to present a clean and responsible image has become paramount. For non-commercial organizations, citizen power and political criticism create just as strong an imperative to protect the brand. As a result, we can see in Figure 1 that twice as many respondents (44%) consider reputational risk to be the prime driver for GRC in their organizations rather than avoiding penalties and fines (32%). In between are 32% who consider it part of good corporate stewardship.

**Figure 1: What is your organization’s main driver for regulatory compliance?**  
(N=197, one answer only)

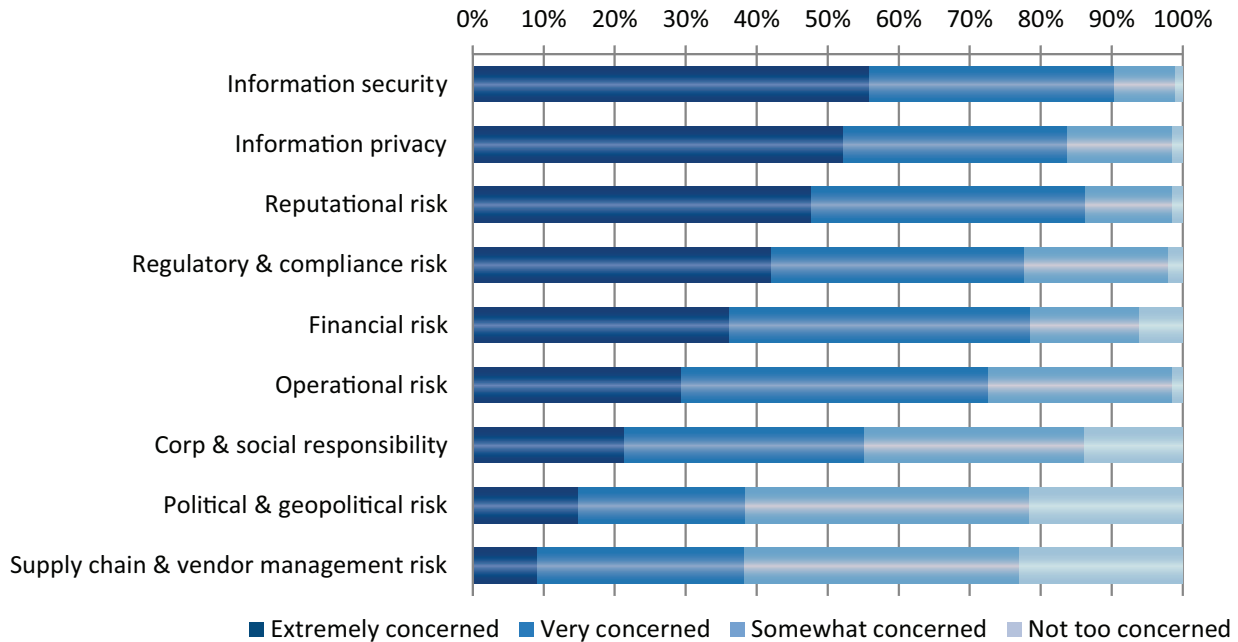


## Risks

Risk management has also become more sophisticated. It is hardly surprising that banking and insurance businesses would take a more measured view of compliance costs versus compliance risks – risk balancing is what they do every day as part of their core business. However, they would also be keen to quantify risk, and to ensure that any risk exposure is both measured and monitored. Many of the huge fines incurred in the banking sector have been the result of over-eagerness to win business, as well as poor monitoring of process. Underestimating the potential fallout from data breaches, price-fixing, money laundering, environmental failures, etc. has proved very damaging to some very large corporations, and strong and durable GRC practices can be an important buffer against poor business decisions.

When rated for significance, information security and privacy are the risks that raise most concern, greater, in fact, than financial or operational risk. With the aggressive growth in digital data and resulting increases in compliance obligations, this finding is not surprising. Reputational risk and regulatory risk can result, of course, from a loss of sensitive or private information, especially if customer related, and they rank at three and four.

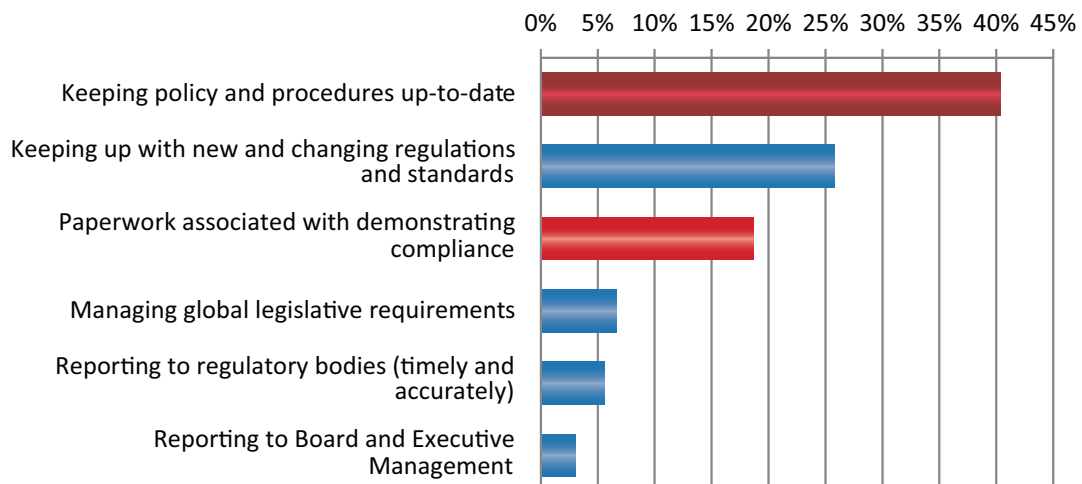
**Figure 2: Please rate your concern for each of the following types of risk and the potential impact they could have on your organization. (N=197)**



## Challenges

Given the backdrop of constantly changing regulations, one might feel that simply keeping up with the latest rulings and legislation would prove to be the biggest challenge (26%), but it turns out that updating policies, procedures and process instructions to reflect required changes ranks higher (40%). Managing the paperwork and records associated with demonstrating compliance is also a big headache (19%). Taking these two together, we can see that document-centric issues are at the core of GRC management, and are proving problematical for many organizations.

**Figure 3: What would you consider your organization's biggest challenge when it comes to regulatory compliance or risk management? (Chose only one) (N=198)**

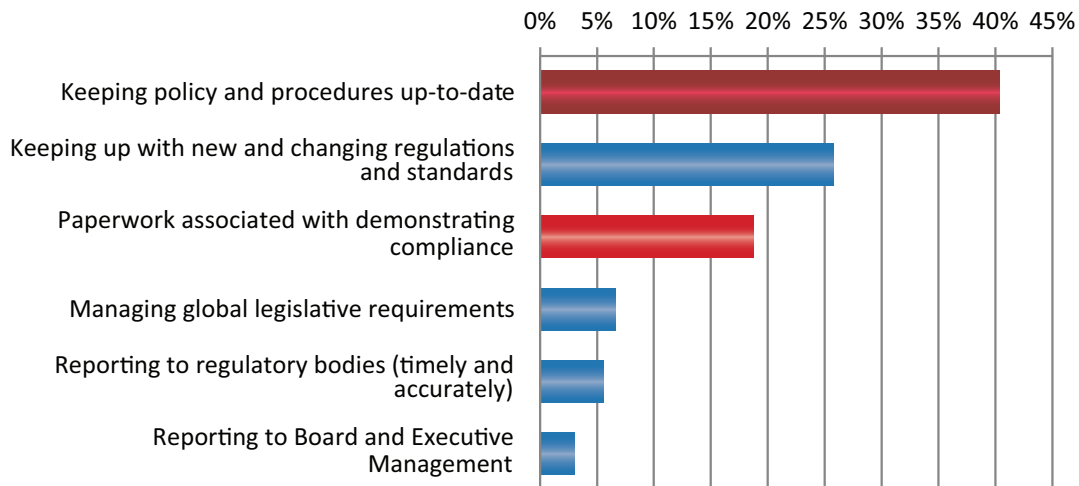


## Stakeholders

Despite the critical importance that GRC plays in the health and compliance culture of any organization, allocation of key leadership roles for strategy setting and ownership of the program is very broad, with little in the way of consensus as to where this responsibility lies. The Chief Legal Officer or General Counsel is the most likely to “own” the GRC process, but only in 14% of organizations. Or it may be run by a GRC Committee for 12% of organizations – but only 29% of organizations actually have such a committee. Interestingly, the Chief Compliance Officer takes the lead for just 10%, even though 40% of organizations answering the survey have one. 50% have a Chief Information Security Officer and 35% a Chief Risk Officer.

The CIO is likely to play a role in most businesses, particularly in the security side of things, and it is reassuring that the CEO is involved for 70%, along with the CFO (72%) and the COO (59%). What the findings seem to point to is that there are a number of different functions participating in GRC planning, not only traditional departments like Compliance, Risk and Audit, but also across the financial and operational areas, and, of course, IT. However, there is no obvious choice of leader, which can make it difficult to generate a GRC discipline where one does not exist at present.

**Figure 4: Which stakeholders play leadership roles in setting the strategy for your governance, risk and compliance (GRC) program? (N=193)**



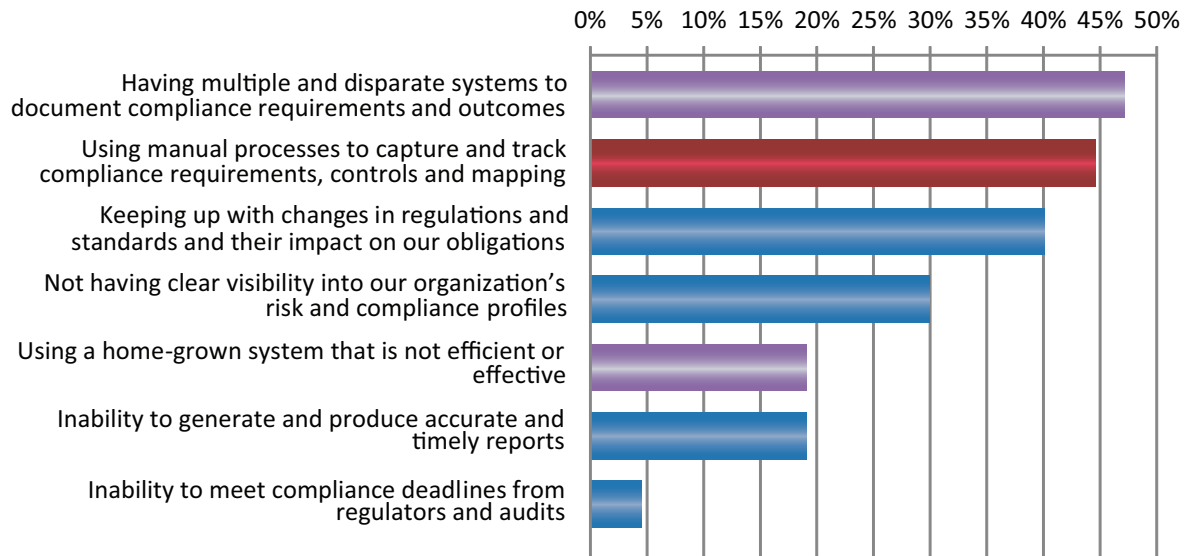
## GRC Issues

As we mentioned in the introduction, there are a number of distinct elements of a best practice GRC discipline. Monitoring changes and maintaining awareness of regulatory standards that affect the business is critical, and in order to maintain standards certification or compliance, continuous monitoring is needed. These standards and regulations are likely to be incorporated into operational policies, and these policies need to be managed through their lifecycles of introduction, revision, and retirement. Managing and containing risk in a systematic way is a core requirement, both for internal risk, and for external supply chain risk. Continuous audit and reporting to senior management and stakeholders is also important.

### Managing Regulatory and Standards Compliance

Documenting compliance requirements and outcomes across multiple disparate systems is given as the biggest issue with managing regulatory and standards compliance – more so than keeping up with the changes and their potential impact on the business. Using manual processes to capture and track compliance requirements and controls is time-consuming and error-prone. Many organizations have home-grown systems to do this which are not efficient or effective.

**Figure 5: What have been the biggest issues with managing regulatory and standards compliance (e.g. Sarbanes-Oxley, ISO 9000, ISO 27001, etc.) in your organization? (MAX 3) (N=157)**

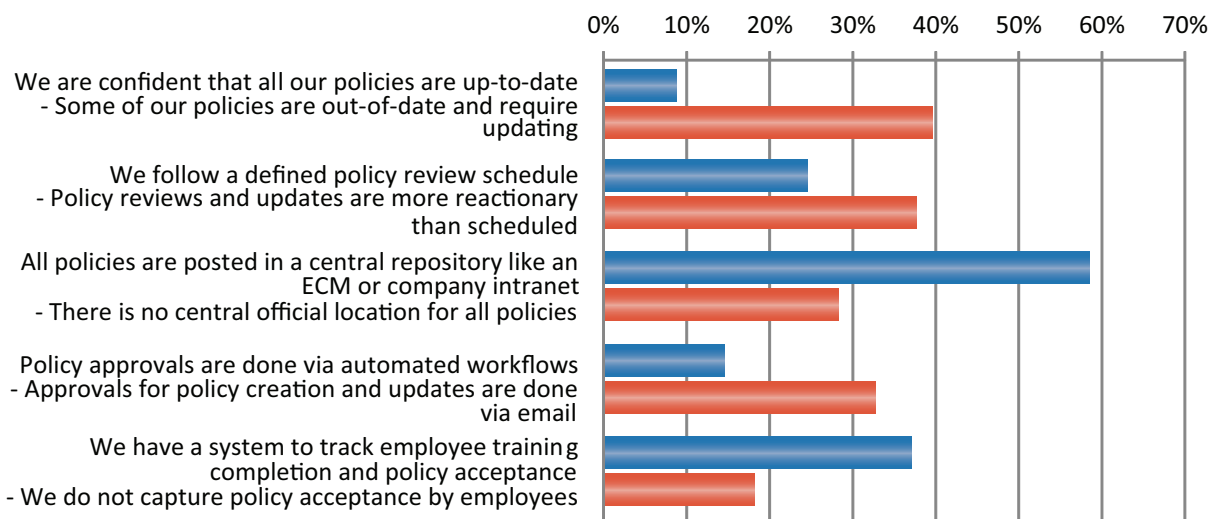


### Managing the Policy Lifecycle

Corporate policies are the direct link between an organization's vision and their day-to-day operations. Policies provide the rules to guide employee decision-making, handle issues and set overall business behavior. Managing policy changes and alerting staff to those changes is a major challenge. Policies should be kept up-to-date with a defined review schedule. Best practice would suggest that all policies be posted in a central repository and managed for versions. Management approvals are most effective and efficient when controlled by automated document workflows. Employee training and formal policy acceptance should be tracked and recorded.

Unfortunately, we can see from Figure 6 that best practice is losing out in most areas. Only 9% are confident that their policies are up-to-date and only 26% hold regular reviews. Although most do use a central repository such as ECM or a company intranet for policies, 28% have no official location for all policies, and only 15% use automated workflows for policy sign-off. 18% admit that they do not capture or record policy acceptance by employees.

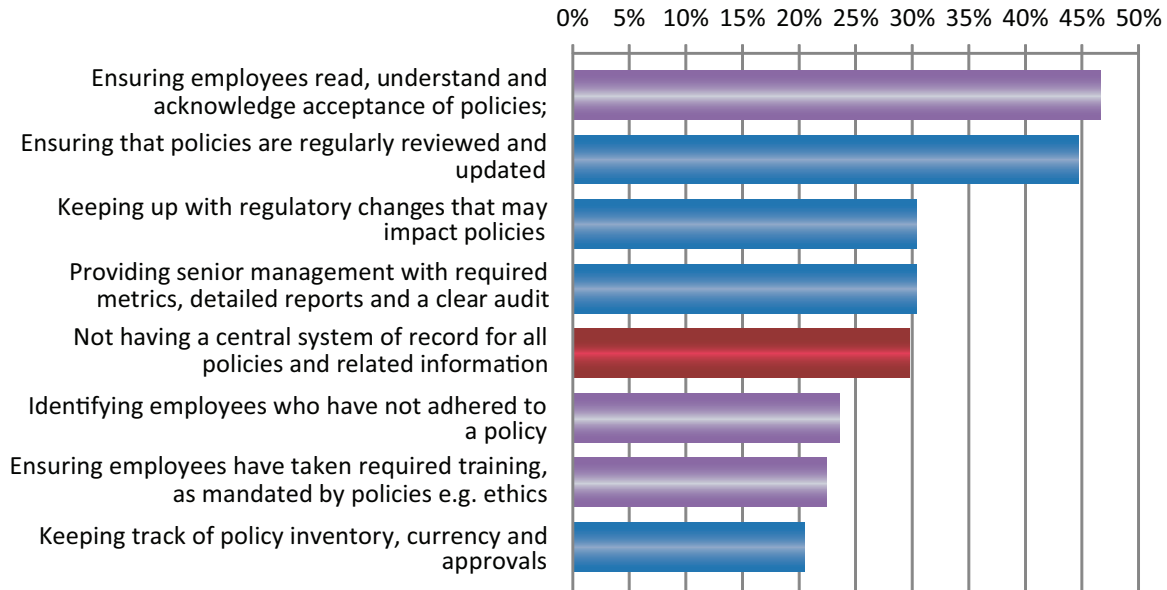
**Figure 6: How does your organization currently manage the policy lifecycle? [Select all that apply] (N=159)**



We can see these contrasting practices highlighted as issues in Figure 7 where ensuring that employees read, understand and acknowledge acceptance of policies is given as the biggest issue, along with ensuring that they take training, and, of course, identifying those who do not adhere to the policy. Not having a central system of record for all GRC related policies and assessments is also a significant issue for many.



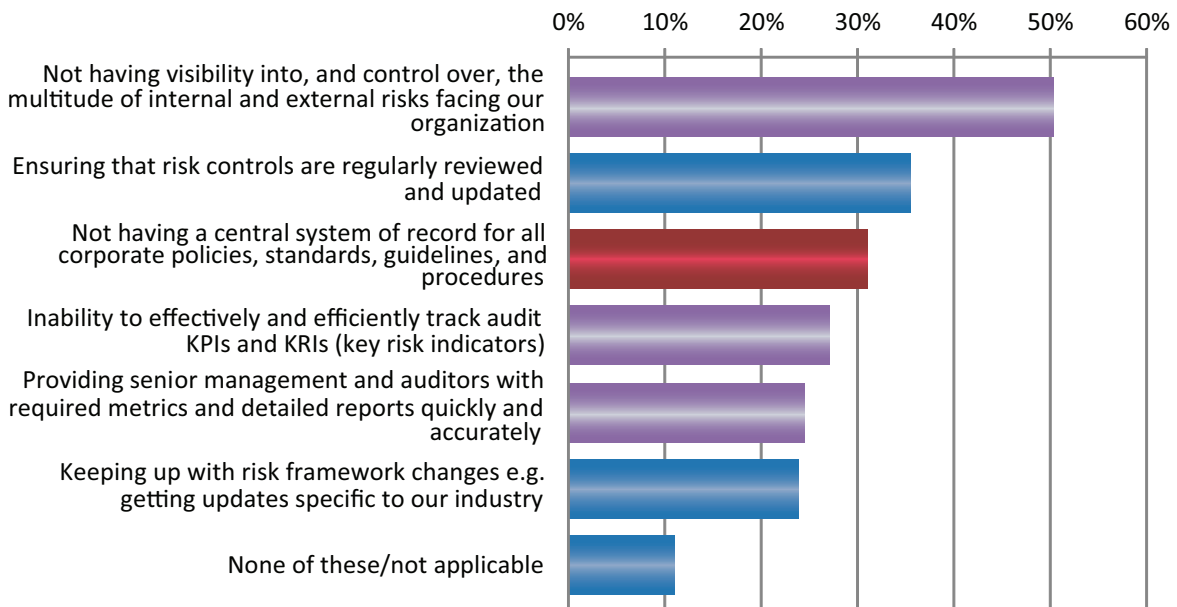
**Figure 7: What have been the biggest issues with managing the policy lifecycle in your organization? (MAX 3) (N=151, excl. N/As)**



## Managing Operational Risk

Operational risk can be described as the risk of business operations failing due to human error; and the risks will vary from industry to industry. Anyone tasked with managing and limiting operational risk would love to be able to readily identify where and what those risks are, and even better, to have personal control over them. In reality, risk officers can only strive to do their best with the tools available to them. Even where the risks are known, having an effective way to track and audit them through KPIs and KRIs (Key Risk Indicators) is vital if they are to be reported to senior management and auditors. Once again, we see in Figure 8 that a central system of record is considered to be very important.

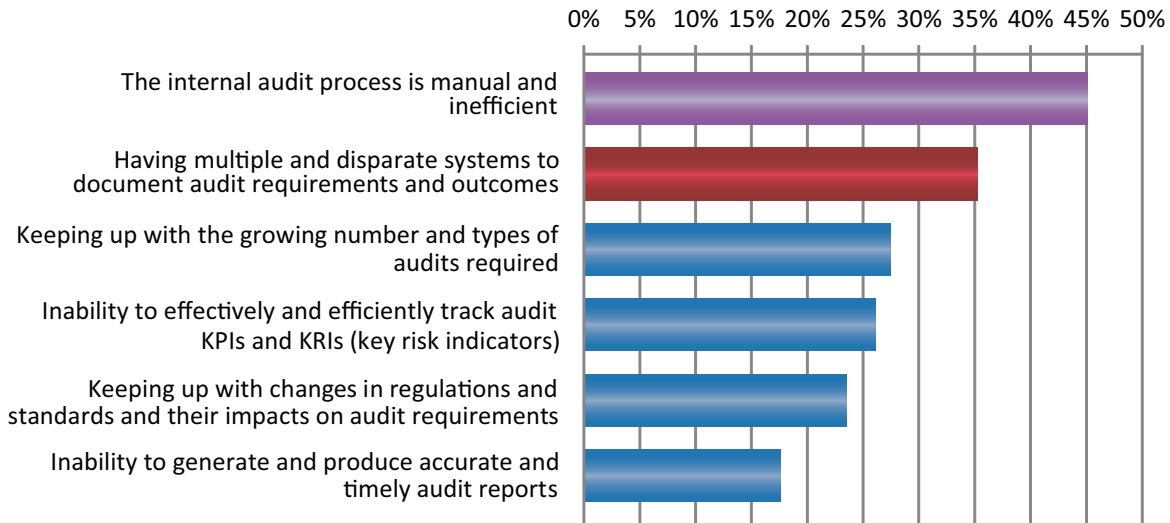
**Figure 8: What have been the biggest issues with managing operational risk in your organization? (MAX 3) (N=155)**



## Managing Audit

The role of Internal Audit is a critical but sometimes difficult one: to provide independent and objective assurance that an organization’s risk management, governance and internal control processes are operating effectively and ethically. Demonstrable confirmation of compliance can only be achieved by suitable and regular audits. The work involved in these is hugely dependent on the efficiency of the audit process, the number of systems involved, and the degree of automated tracking and verification that is in place. For nearly half of our respondents, the internal audit process is manual and inefficient, and documenting requirements and outcomes across the multiple systems and process workflows involved makes things challenging.

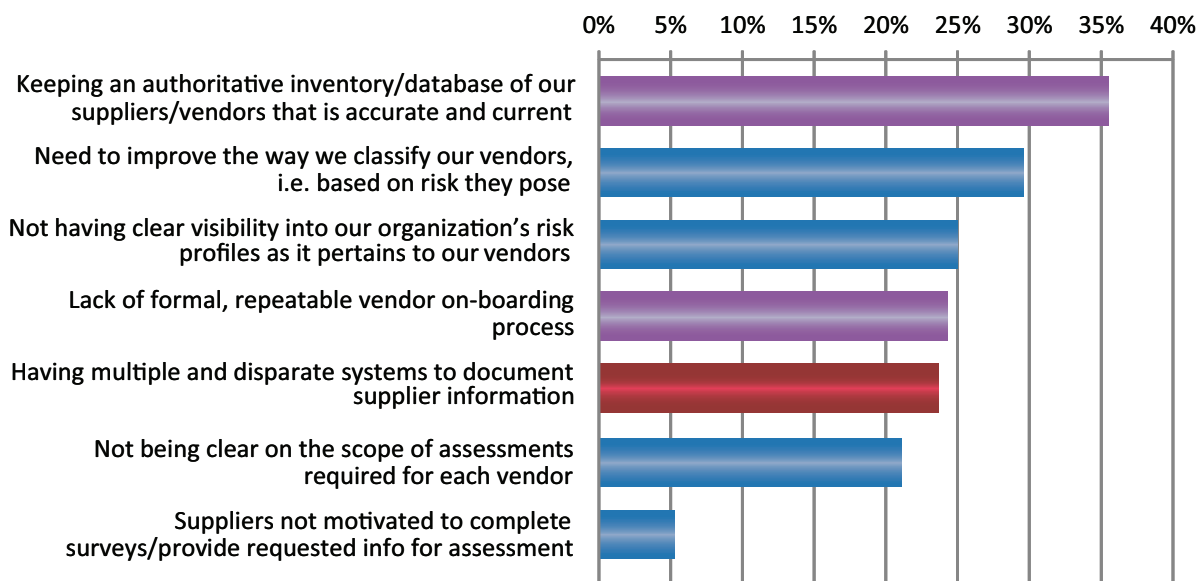
**Figure 9: What have been the biggest issues with managing the internal audit operations in your organization? (MAX 3) (N=153)**



## Managing Supply-Chain Risk

Supply chain and sub-contracted operations are becoming increasingly complex, particularly in the manufacturing sector. Extending internal control and visibility into the supply-chain may involve a wide range of contractors, suppliers, partners, vendors, and other third parties. Generally, findings below show that vendor information is not in one place and is not up-to-date. Many organizations are struggling to keep an inventory of their suppliers, and to classify them by risk profile. It is also apparent that many do not carry out formal vendor on-boarding or conduct reliable assessments to ensure the third parties they work with are compliant.

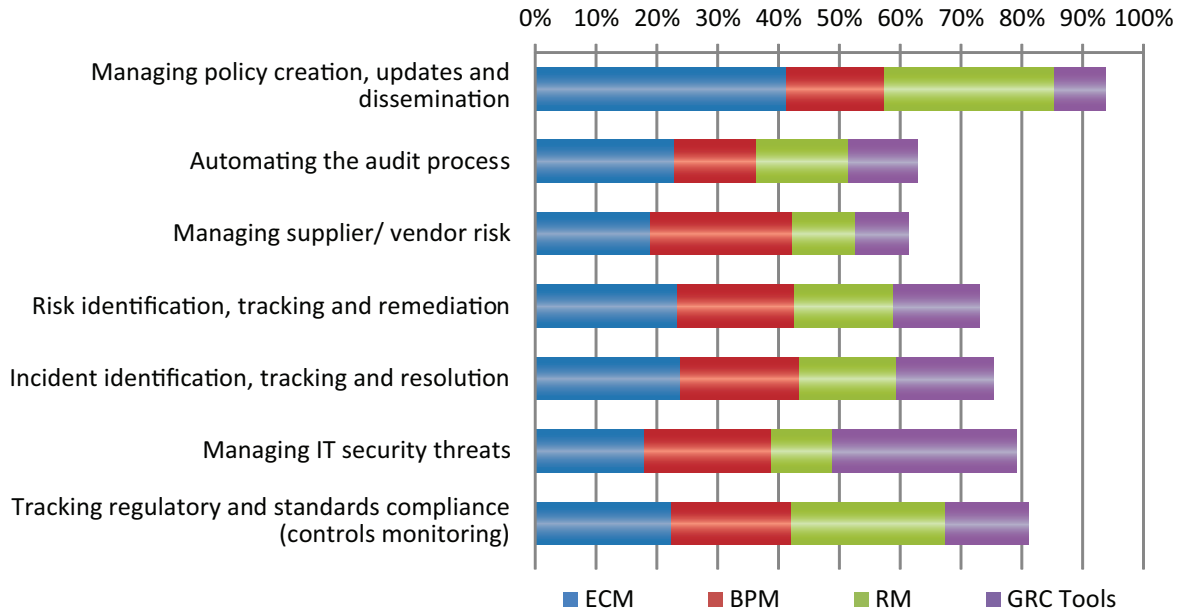
**Figure 10: What have been the biggest issues with managing supply-chain risk - vendors you do business with such as contractors, suppliers, partners and other 3rd parties? (MAX 3) (N=152)**



## Use of ECM/RM/BPM

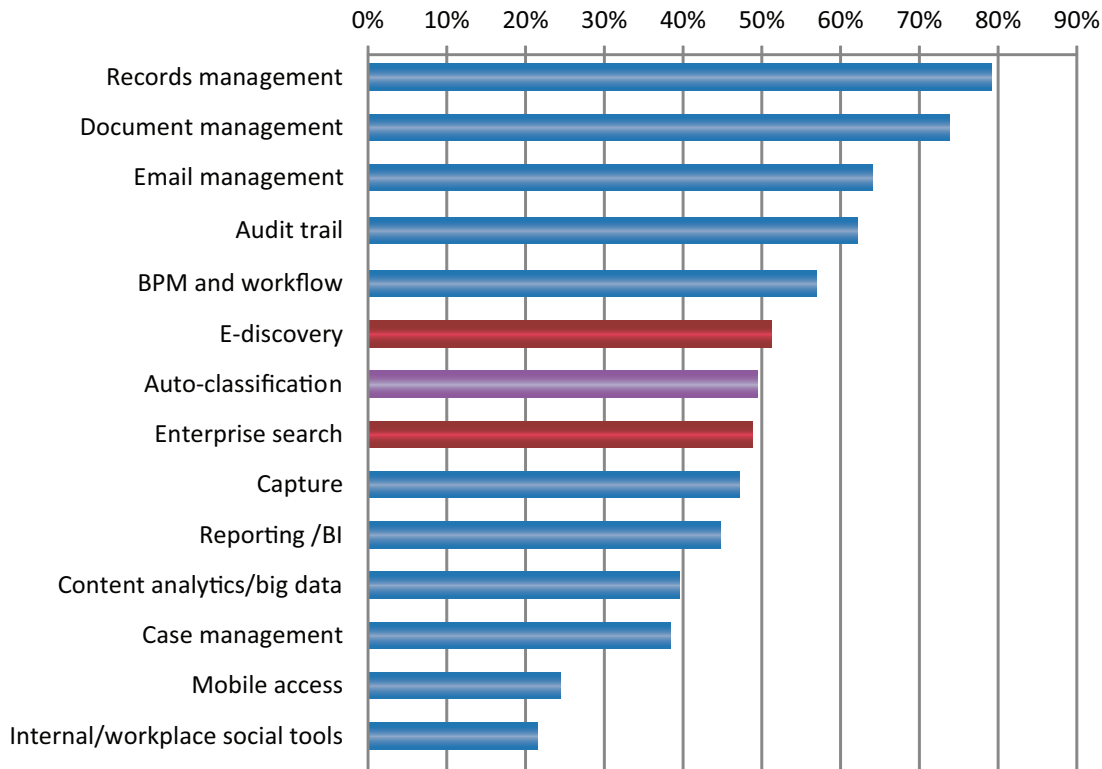
Given that many of the GRC challenges we saw earlier are centred on documents and document processes, we would expect that traditional document handling and records management tools would play a strong part in solving GRC problems. ECM and RM are particularly important for managing policy creation, updates and dissemination, given that collaboration, versioning, audit trails, publication and record-keeping are involved. They also figure strongly in other aspects of the GRC process such as an internal audit workflow or as the central repository for vendor information. Respondents indicate that BPM also has a large role to play in GRC, particularly within supply chain/vendor risk management, and in tracking compliance and incident management. Dedicated GRC toolsets are part of the mix for many organizations, particularly for IT security threats.

**Figure 11: To what extent are you using ECM, BPM, RM and GRC tools to solve the following GRC business problems? (N=143, line-length indicates “None of these”)**



Looking in more detail, we asked about specific ECM/RM functionalities that would be important to solving GRC problems. All of the classic capabilities of an ECM or EIM suite come into play, headed up by records management and document management, but also email management, and more on the BPM side, audit trails and workflow. E-discovery appears above Enterprise Search, although both will be involved in routine checks, and any investigations or incidents. Auto-classification is deemed important by half the respondents, not surprising given that a leading driver to implement ECM/RM is to meet regulatory records retention requirements. The finding is also a strong endorsement of the need to move away from reliance on staff to do the right things - filing content in the right places and securing or redacting sensitive information - towards computer analytics where, once set, the rules will be followed every time. We found it interesting that only 24% of respondents cited mobile access as important for GRC, although this is in line with mobile access across other areas of content management. Many of those involved with GRC would probably balance the benefits for their own role against the considerable threat to compliance that general data access on mobile presents.

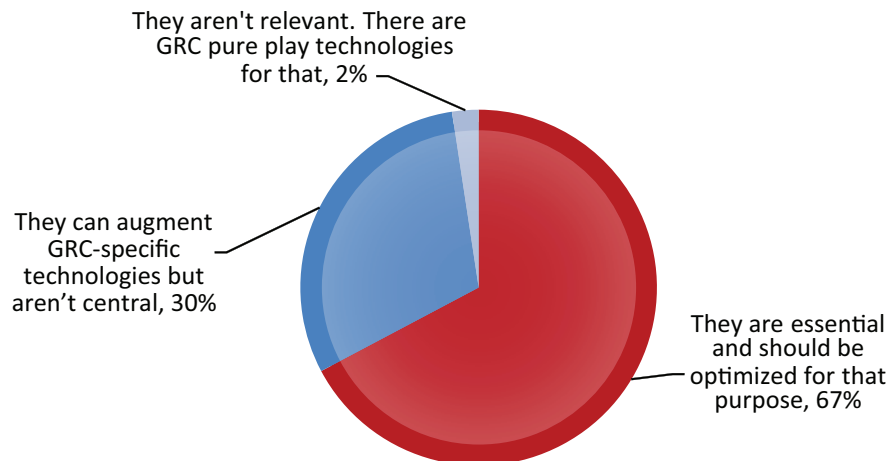
**Figure 12: Which of the following ECM/RM functionalities are, or would be important for solving your GRC problems? (N=172)**



### Role of ECM/RM/BPM in GRC

Based on previous AIIM surveys, many organizations have incomplete ECM and RM implementations; they are struggling to achieve universal adoption, not enabling records management capability or using it poorly. Sometimes organizations can also struggle with BPM or workflow, understanding the value these technologies bring but unable to capitalize on them. So it is reassuring to see that 67% consider these systems to be essential to GRC, and that they need to be optimized for this purpose. We believe that most of the respondents have an understanding that the core components of a GRC platform include a central repository with audit trails, workflow, and reporting capabilities, all inherent in ECM and BPM suites.

**Figure 13: How do you feel generally about the use of ECM, BPM and RM to solve GRC business problems? (N=168)**



## Current Usage

When we look at current use of ECM, RM and BPM for GRC, they are either acknowledged as a core part of the GRC program (14%) or they constitute the main play for governance and compliance, even though there is no official GRC discipline as such (29%). A further 27% feel that they should be a core part of the program, although right now their systems are not optimized to do so, or as an organization, they have insufficient knowledge in this area.

**Figure 14: How would you best describe the use of ECM, BPM and RM to solve GRC business problems in your organization today? (N=171)**

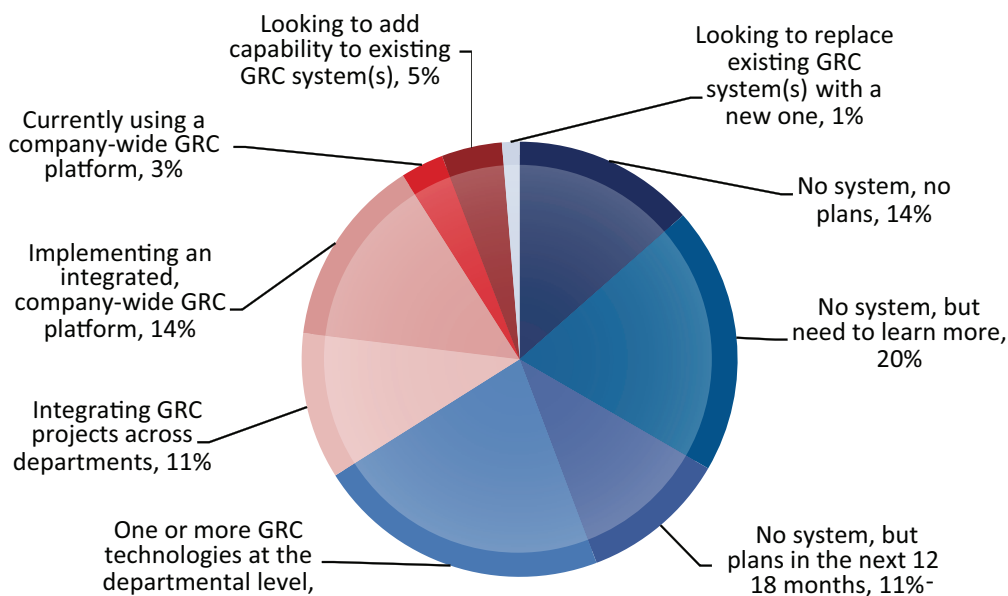


## GRC Solutions

We have seen that for many organizations, ECM, BPM and RM systems cover or could cover the bulk of their GRC needs, but that a degree of optimization and supplemental tools would improve their capability. From Figure 14 we can see that only 8% of our respondents have successfully implemented an enterprise-wide GRC platform, although 25% are in the process of implementing one. 45% have no GRC solution in place.

22% are using in-house developed systems, and a similar number are reliant on their ERP/finance system, albeit that these are not generally optimized for records management nor document generation, circulation and approval processes.

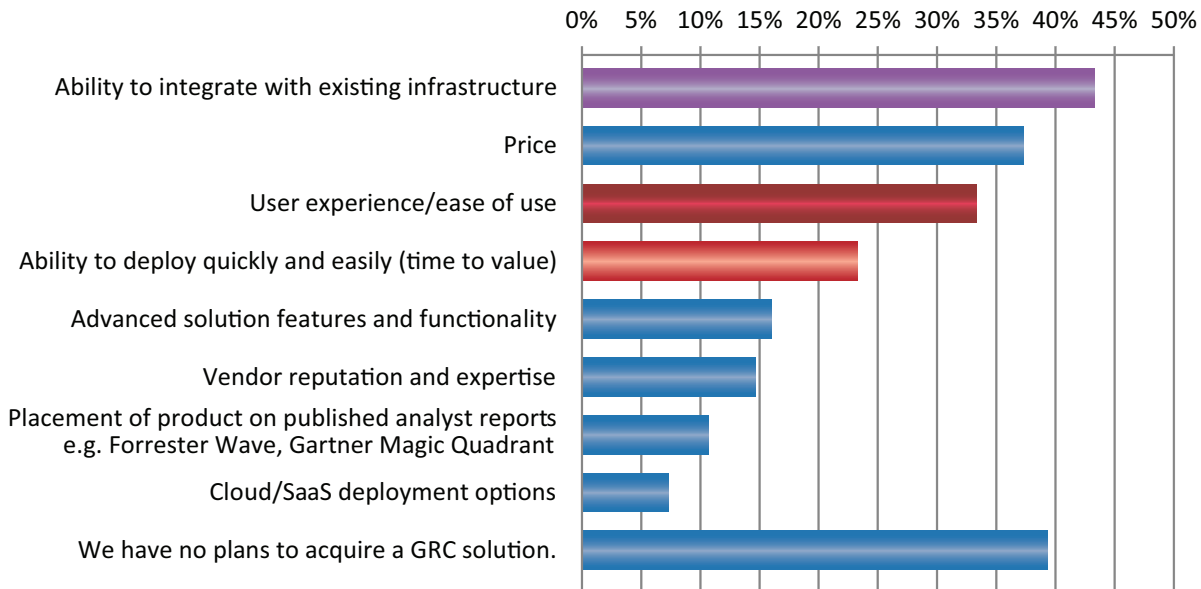
**Figure 15: How would you best characterize your organization's experience with governance, risk and compliance (GRC) solutions? (N=171)**



## Solution Selection

GRC solutions are offered as an integrated platform as well as discrete applications to solve specific use cases. They are offered in the traditional perpetual license model as well as cloud and subscription-based deployments. A key factor for our respondents in GRC solution selection is the ability to integrate with existing infrastructure – more so than features, vendor reputation and formal solution evaluations. The importance of integration is likely based on the need for GRC to pull important data and information from other source applications such as ERP and other disparate central repositories. Price is the next most important factor, followed by ease of use and the ability to deploy quickly and easily – both becoming key requirements for any IT solution these days.

**Figure 16: What are/would be the most important factors influencing your GRC solution selection? (MAX 3) (N=86, excl. 97 Don't Know)**



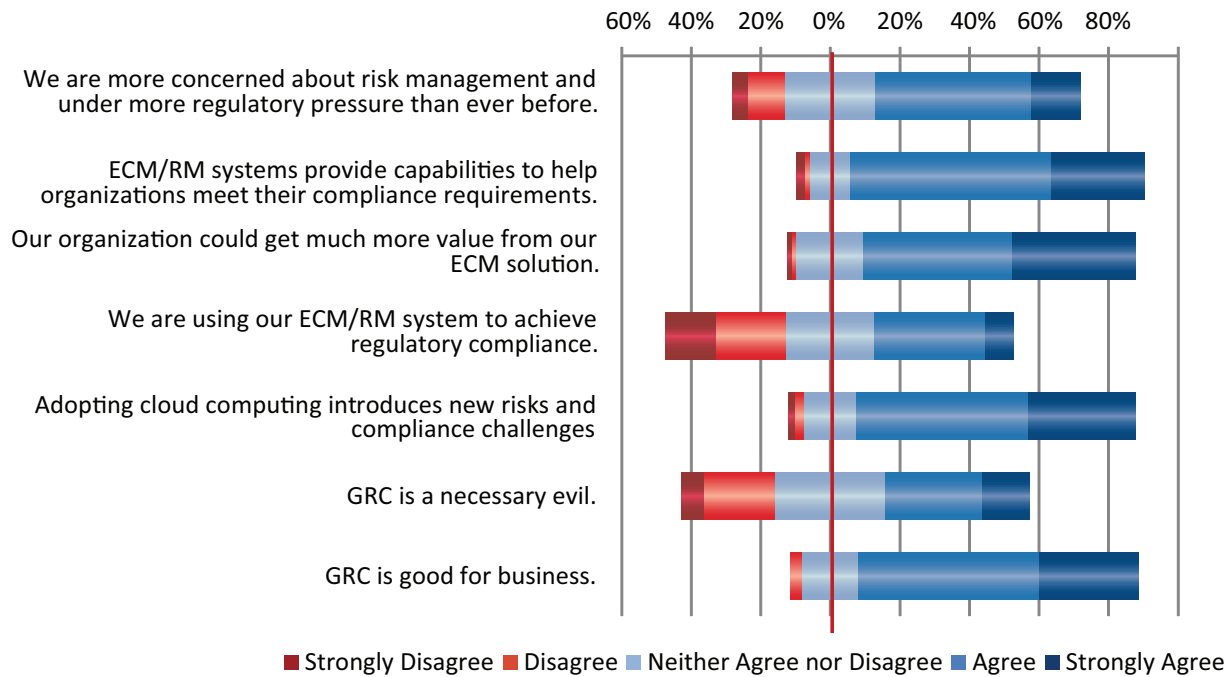
## Opinions and Spend

There is full support of the view that risk management and regulatory pressure are increasing, and that ECM/RM solutions provide capabilities to help meet these needs (85%). In fact 50% are using ECM/RM to achieve regulatory compliance today. A significant number of respondents (78%) feel that their ECM/RM system could provide much more value, indicating perhaps that they have yet to use it to solve GRC problems.

Inevitably, 80% feel that cloud is increasing risk, particularly across data privacy and data security, although the benefits need to be weighed against this.

As a positive note, 81% would agree that GRC is good for business, although 42% consider it to be a necessary evil, so there must be some overlap here.

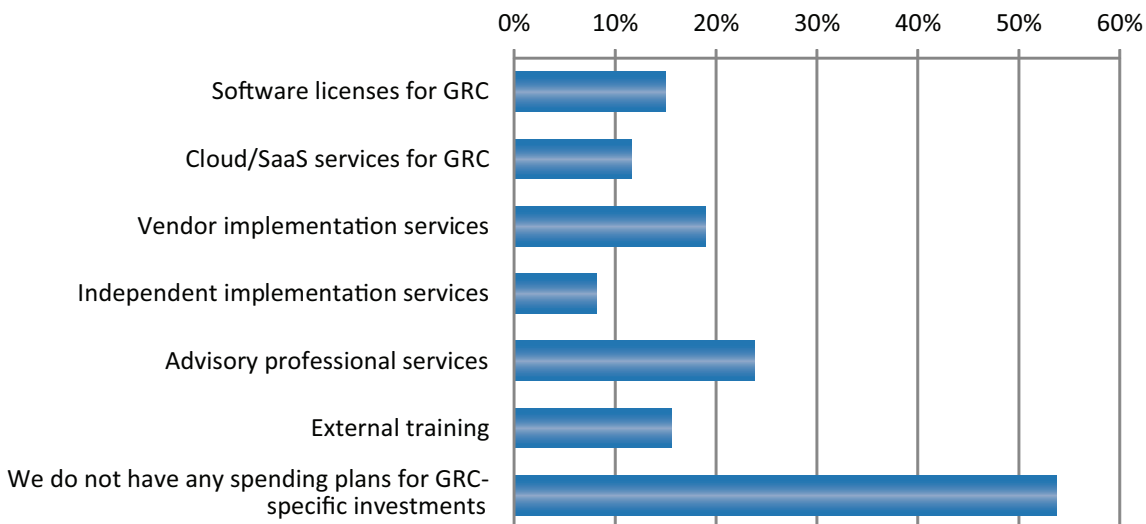
**Figure 17: How do you feel about the following statements? (N=154)**



## Spend

46% of the organizations surveyed plan to spend on GRC software or services in the next twelve months including 15% on licenses and 12% on cloud/SaaS services. As might be expected for such a crucial function, but where little expertise resides in-house, 24% are looking for help from advisory professional services.

**Figure 18: Do you plan to spend anything in the following areas in the next 12 months - for governance, risk management and compliance only? (Choose all that apply) (N=147)**



## Conclusion and Recommendations

GRC is growing in usage as a term to describe the discipline of having executive oversight and management, meeting designated standards, complying with laws and regulations, and assessing and mitigating risk to the organization. Among our survey respondents, only 15% of individuals were not aware of it as a domain, but 29% feel that their organization in general is not aware of the term.

Good GRC and ECM/BPM intersect when organizations have sound record keeping practices, a secure central content repository for key records, and business processes are consistent, auditable, and tracked.

Many of the elements involved in meeting compliance and regulatory requirements are best managed by content and records management systems, particularly where core business processes are document-centric. ECM and RM also come into their own for the management of policy records, internal audit evidence, or documents related to an incident. BPM and workflow systems can provide automated scheduling and approvals, management dashboard and reporting, and risk and compliance monitoring.

We have highlighted many specific issues related to policy lifecycle management, operational risk control, internal audit, and supply chain management, but a common thread we have found is that key documentation is not stored in one place, processes are inefficient and manual, and systems are home-grown. ECM, BPM and RM have important roles to play in solving the GRC challenge and organizations that understand this are often on the higher end of the GRC maturity scale.

### Recommendations

- Consider bringing together your multiple compliance, security and risk management groups under a single GRC regime, headed up by a GRC Committee, or a designated Chief Compliance Officer.
- Involve Legal, IT, HR, Finance and Line of Business departments, and seek endorsement of GRC authority from the highest level.
- Look to standardize procedures for regulatory awareness and training, policy generation and approval, policy dissemination, staff agreement, operational monitoring and audit.
- Bring the power of ECM, BPM and RM to your GRC program, defining review, update and approval processes, and where possible, automating collection of important compliance audit trails and reports.
- “Bake compliance into the process” by making full use of ECM and BPM, and where possible, using automated analytics to enforce consistent rules and metadata.
- Establish KPIs and KRIs, and use these to provide senior management with visibility of current performance against GRC objectives, and any related risk exposure.



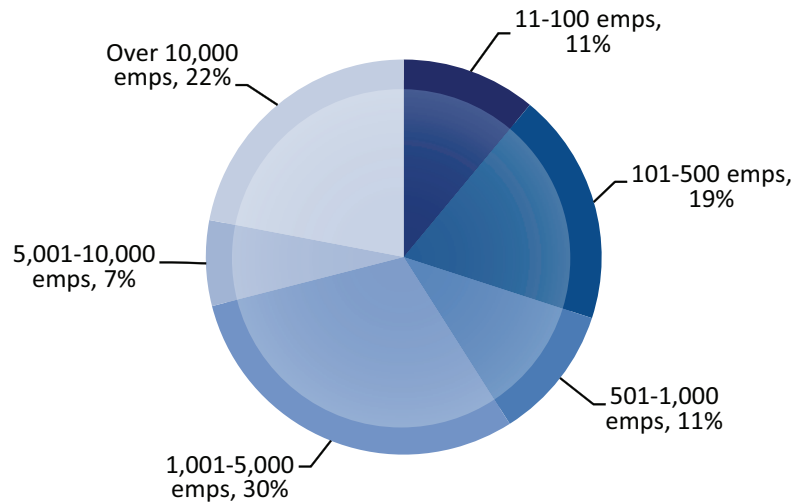
# Appendix 1: Survey Demographics

## Survey Background

The survey was taken by 211 individual members of the AIIM community between 13 March and 06 April 2015, using a web-based tool. Invitations to take the survey were sent via email to a selection of the 80,000+ AIIM community members

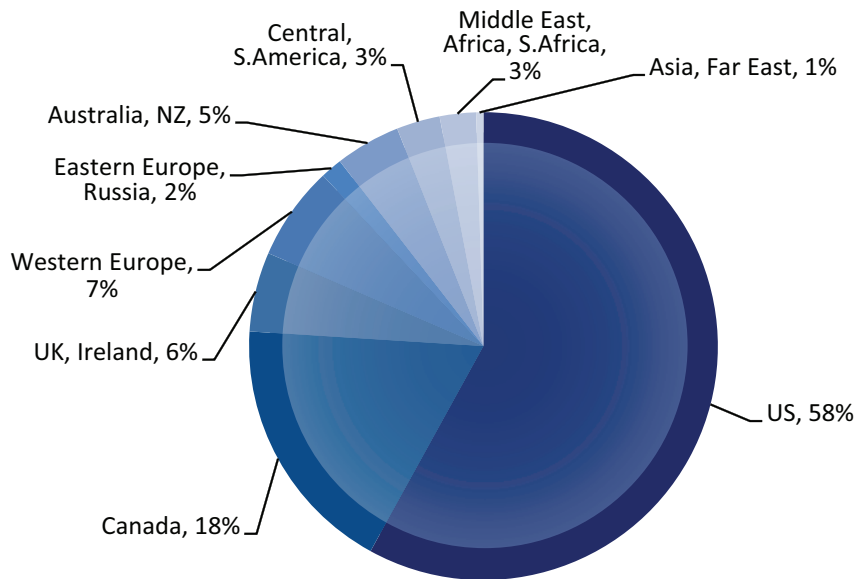
## Organizational Size

Organizations of 10 employees or less and suppliers of ECM products or services are excluded from all of the results in this report. On this basis, larger organizations (over 5,000 employees) represent 29%, with mid-sized organizations (500 to 5,000 employees) at 41%. Small-to-mid sized organizations (10 to 500 employees) represent 30%.



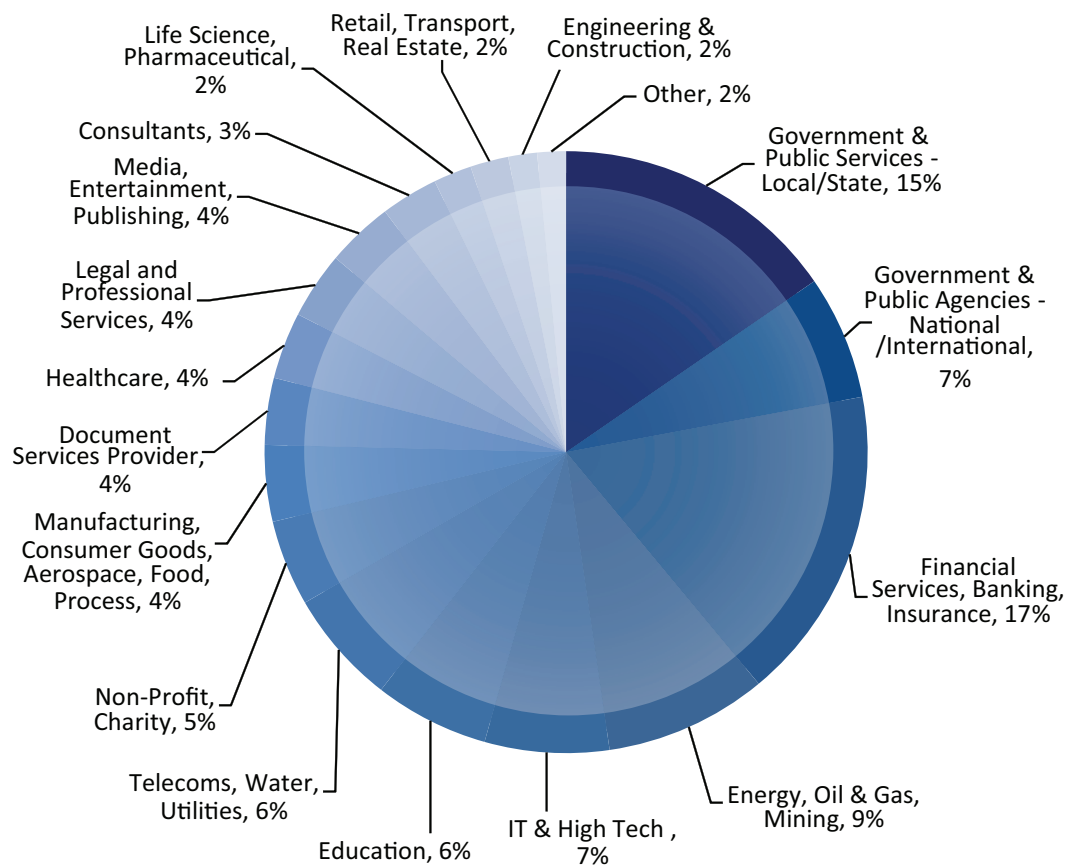
## Geography

US and Canada make up 76% of respondents, with 14% from Europe and 10% elsewhere.



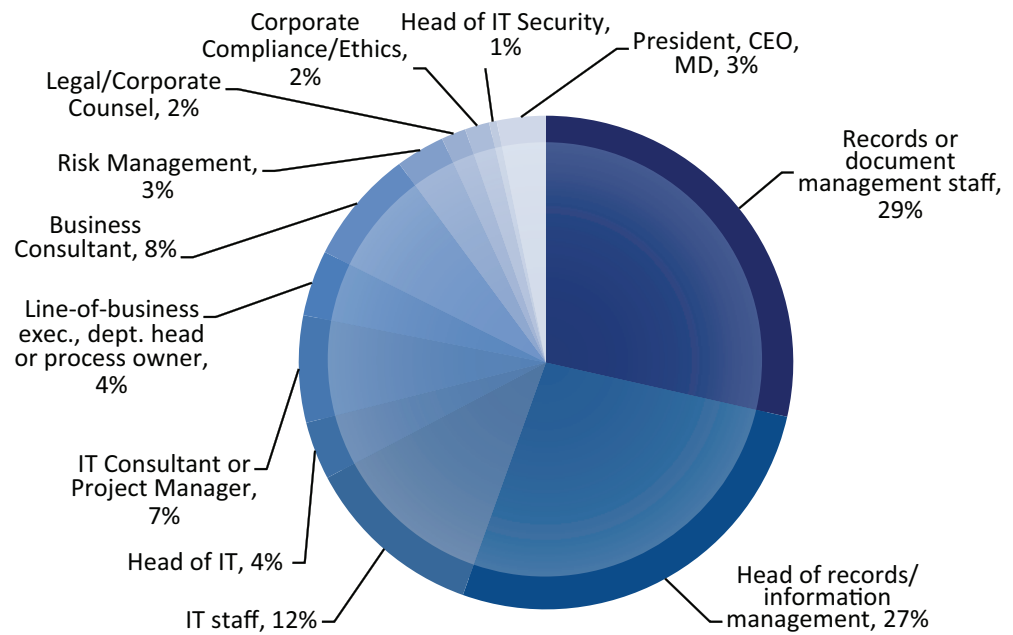
## Industry Sector

National and local government, and public services, represent 22%. Finance, banking and insurance represent 17%. Energy 9%. The remaining sectors are evenly split.



## Job Roles

56% of respondents are from records or information management, 23% are from IT, 15% general business and 8% compliance or legal.



## UNDERWRITTEN BY

# OPENTEXT

OpenText is the leader in Enterprise Information Management, helping customers to create a Digital-First World by simplifying, transforming, and accelerating their information needs. Over 100,000 customers already use OpenText solutions, either on premises or in our cloud.

For more information about OpenText (NASDAQ: OTEX; TSX: OTC), please visit: [www.opentext.com](http://www.opentext.com).



AIIM ([www.aiim.org](http://www.aiim.org)) is the global community of information professionals. We provide the education, research and certification that information professionals need to manage and share information assets in an era of mobile, social, cloud and big data

Founded in 1943, AIIM builds on a strong heritage of research and member service. Today, AIIM is a global, non-profit organization that provides independent research, education and certification programs to information professionals. AIIM represents the entire information management community, with programs and content for practitioners, technology suppliers, integrators and consultants.

© 2015

AIIM  
1100 Wayne Avenue, Suite 1100  
Silver Spring, MD 20910  
301.587.8202  
[www.aiim.org](http://www.aiim.org)

AIIM Europe  
The IT Centre, Lowesmoor Wharf  
Worcester, WR1 2RR, UK  
+44 (0)1905.727.600  
[www.aiim.eu](http://www.aiim.eu)