



The Role of Governance, Risk Management & Compliance in Organizations

Study of GRC practitioners

Sponsored by RSA, The Security Division of EMC

Independently conducted by Ponemon Institute LLC

Publication Date: May 2011

The Role of Governance, Risk Management & Compliance in Organizations

Ponemon Institute, May 2011

Part 1. Introduction

Ponemon Institute is pleased to present the results of *The Role of Governance, Risk Management & Compliance in Organizations*, sponsored by RSA, The Security Division of EMC. The focus of this research is to examine the challenges global organizations face in meeting escalating enterprise Governance, Risk and Compliance (eGRC) objectives. Respondents representing global financial services, technology, healthcare and pharmaceutical industries identified the largest barriers to achieving their GRC goals as lack of a defined GRC strategy and lack of enterprise cooperation and collaboration.

GRC stands for “Governance, Risk and Compliance”. Organizations leveraging GRC processes desire to establish a regulatory or internal framework for satisfying governance requirements, evaluate risk across their enterprise and track how the organization complies with the established governance requirements. GRC processes typically fall within one of four key domains: IT, operations, finance and legal. Domain specific needs include:

- **IT GRC:** Includes the management of IT-related controls. These may include security controls such as firewalls and or security information management system, system controls automation and vulnerability monitoring tools, identity and access management system or disaster planning and recovery systems.
- **Operations GRC:** Includes the management of core operations of the organization. For example, organizations must ensure that there is support to manage processes from manufacturing systems, HR systems, procurement, purchase order systems, power generation monitoring and many more depending on the industry.
- **Finance GRC:** Includes the management of financial controls. For example, organizations may wish to review segregation of duties to manage conflicting permissions, process-related business rules such as the signature requirements for expenses above a certain amount or auditing inspections.
- **Legal GRC:** Includes managing controls for regulatory compliance and contractual requirements including the organization’s communication with government supervisory entities. For example, an organization must assure proper management of corporate governance reporting, anti-fraud, anti-bribery and anti-corruption, and privacy and consumer protection management.

In this inaugural study, we independently surveyed 190 individuals from one of the largest eGRC practitioner communities and the results were presented at the RSA Archer eGRC Summit. The survey focused on eGRC, privacy and data protection activities and how they relate to business objectives or mission. These participants are known to be involved in their organization’s GRC initiatives. The majority of respondents are at or above the manager level, and more than half work for large-sized organizations. Our survey topics focused on the following key issues:

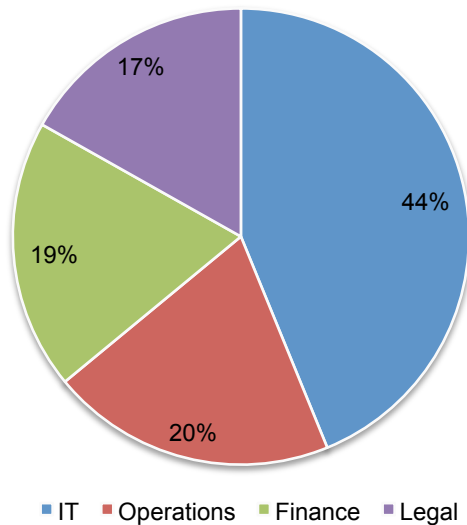
- Where most GRC activities take place in an organization
- Collaboration and cooperation across GRC functional areas
- GRC strategies in organizations
- Barriers to implementing and achieving GRC objectives
- Compliance challenges with privacy and data security regulations

Part 2. Key findings

IT represents the largest area of GRC-related activities and is where the majority of respondents say their GRC program started. Pie Chart 1 shows 44 percent of respondents who state their GRC activities are primarily contained within the IT function – followed by 20 percent in operations, 19 percentage in finance and 17 percent in legal.

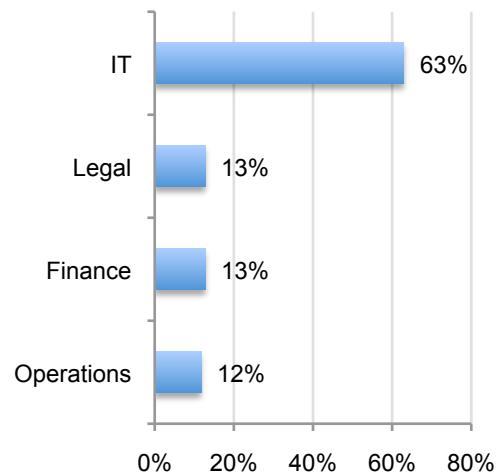
Bar Chart 1 shows the origins of GRC among respondents' organizations. An overwhelming majority of respondents (63 percent) say their organization's GRC activities started within the IT function. Only thirteen percent say GRC started in legal or finance, and 12 percent say it started in operations.

Pie Chart 1. How much of your organization's GRC activities fall into each one of four GRC domains?



Bar Chart 1. Where did your organizations GRC program or initiatives start?

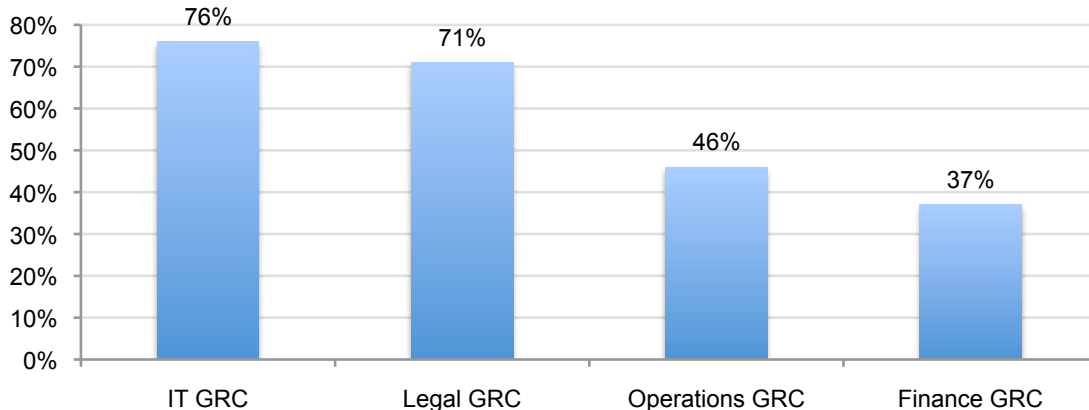
Very important response



Bar Chart 2 reports the relative importance of privacy within four GRC domains. As shown, 76 percent of respondents say privacy is a very important part of IT GRC activities and 71 percent say it is very important to legal GRC.

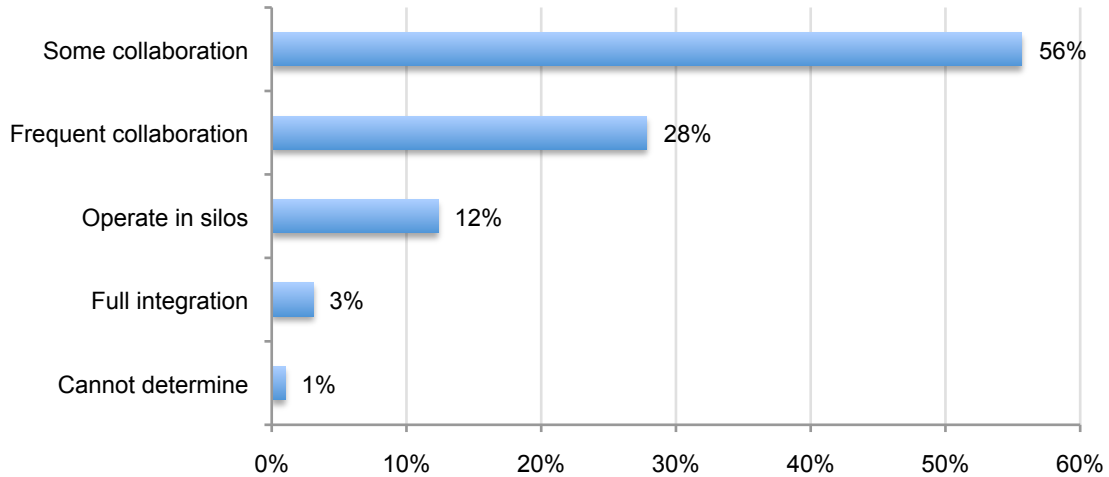
Bar Chart 2: How important are privacy-related issues for each one of the four GRC domains?

Very important response



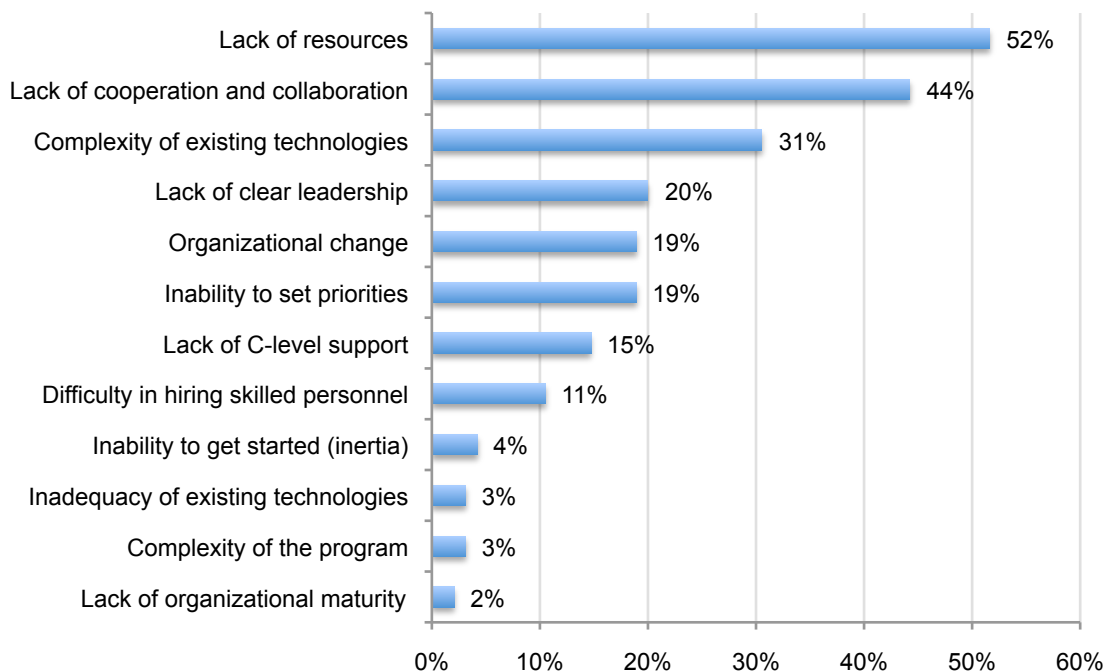
A major barrier to tackling risk and privacy challenges is a lack of enterprise collaboration. Bar Chart 3 shows 28 percent of respondents say there is frequent collaboration or cooperation among GRC areas and 56 percent say they sometimes collaborate. Finally, as an indication that silos are breaking down, only 12 percent of respondents say they operate in silos with little or no collaboration.

Bar Chart 3: What best describes the working relationships among finance, IT, operations and legal GRC functions in your organization today?



According to Bar Chart 4, the lack of resources (52 percent) and the lack of cooperation and collaboration (44 percent) are the two most salient barriers to successfully achieving GRC-related goals. The complexity of existing technologies (31 percent) and the lack of clear leadership (20 percent) are the third and fourth most salient barriers to a success according to respondents.

Bar Chart 4: What are the top two barriers to achieving your organization's GRC-related goals?

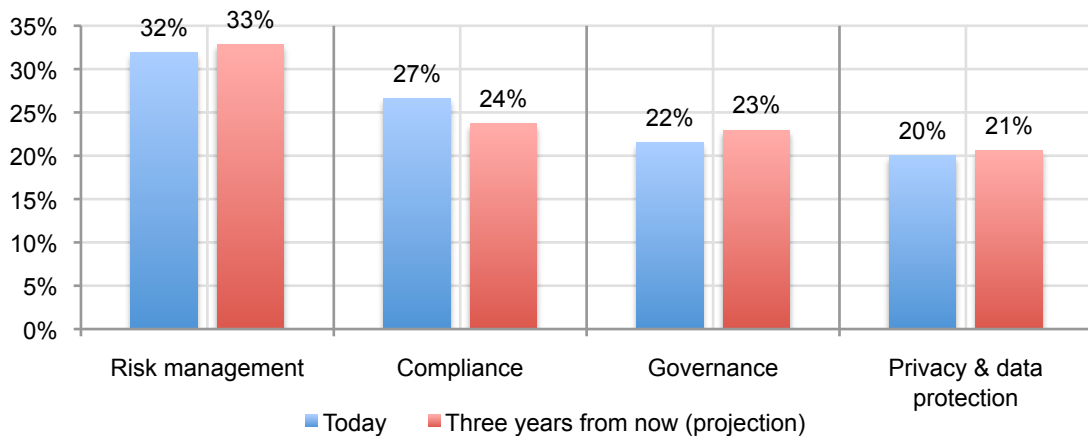


Risk management is and will continue to be the biggest focus for organizations. Risk management is top of mind for GRC professionals. Organizations are finding that the cost of complying with a myriad of regulations is very expensive. Taking a risk-based approach toward compliance requirements enables them to focus resources on the most significant regulatory or legal issues facing their organizations.

Today, the largest percent of respondents (32 percent) believe risk management is considered the most important element within their organization’s GRC program. When asked to forecast priorities three years into the future, 33 percent of respondents state risk management is most important. Compliance declines slightly from 27 percent to 24 percent of respondents who say it will be most important. Governance and privacy increase slightly in three years.

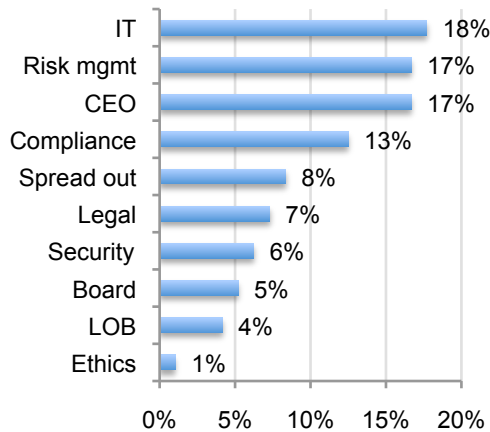
Bar Chart 5: How important are the following four GRC focus areas to your job function today and three years from now?

Response required the allocation of 100 points

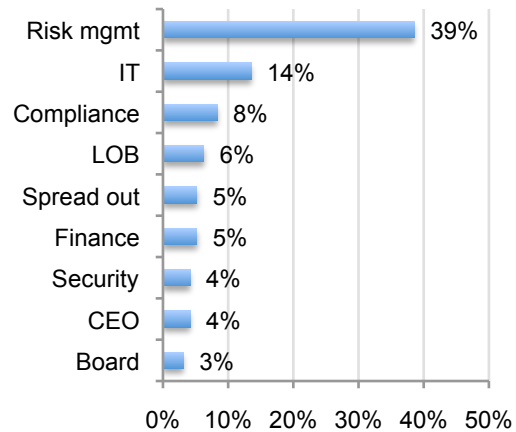


The next four charts show where GRC-related activities reside in respondents’ organizations. Bar Chart 6 suggests governance activities are mostly likely to reside within in the corporate IT function according to 18 percent of respondents, followed by 17 percent who say it resides within the enterprise risk management function. Bar Chart 7 shows risk management activities are most likely to be located within enterprise risk management according to 39 percent of respondents, and corporate IT according to 14 percent of respondents.

Bar Chart 6: Where governance GRC activities reside

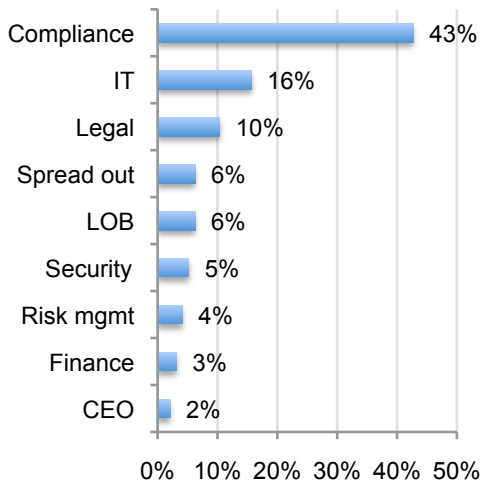


Bar Chart 7: Where risk management GRC activities reside

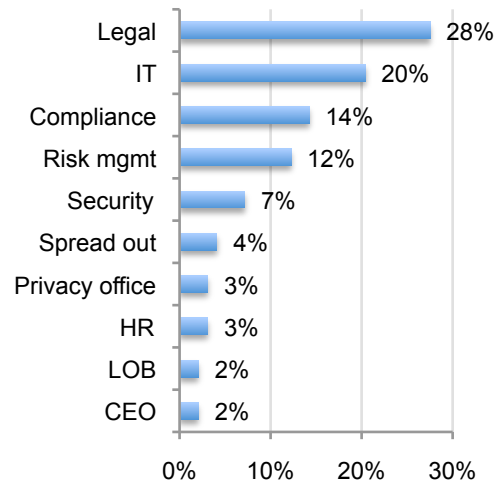


Bar Chart 8 shows compliance activities are most likely to be located in corporate compliance (43 percent) followed by corporate IT (16 percent). Privacy program management activities are located in legal, according to 28 percent of respondents followed by IT, according to 20 percent.

Bar Chart 8: Where compliance GRC activities reside



Bar Chart 9: Where privacy program management activities reside



As shown in Bar Chart 10, assessing risk (83 percent), monitoring compliance (63 percent) and developing strategies (61 percent) are considered the most essential activities in order to meet GRC objectives or goals. GRC-related activities considered less essential include advising the organization's management (40 percent), responding to incidents (42 percent) and training or raising awareness (43 percent).¹

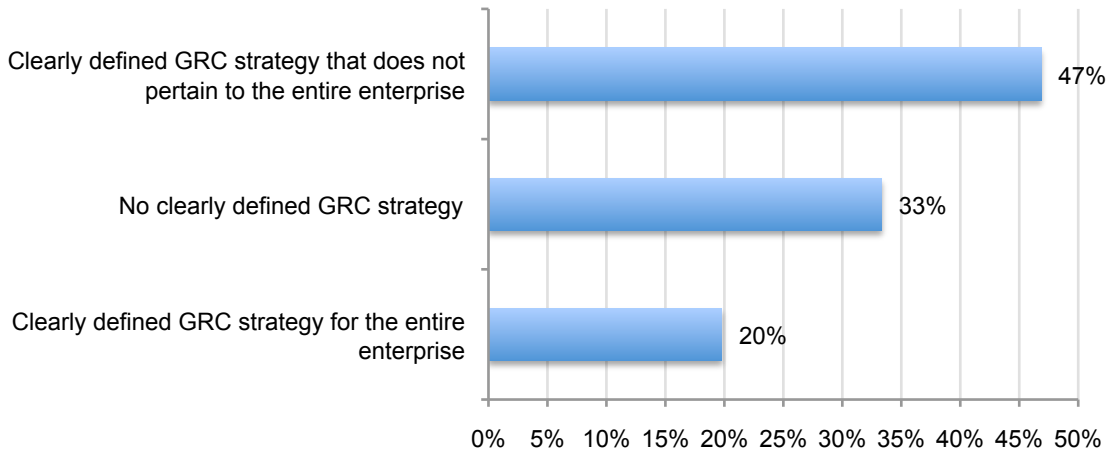
Bar Chart 10: Activities believed to be essential in order to meet GRC objectives or goals



¹ Even if an activity is considered less essential, it does not mean it is not considered important or very important to meeting GRC objectives.

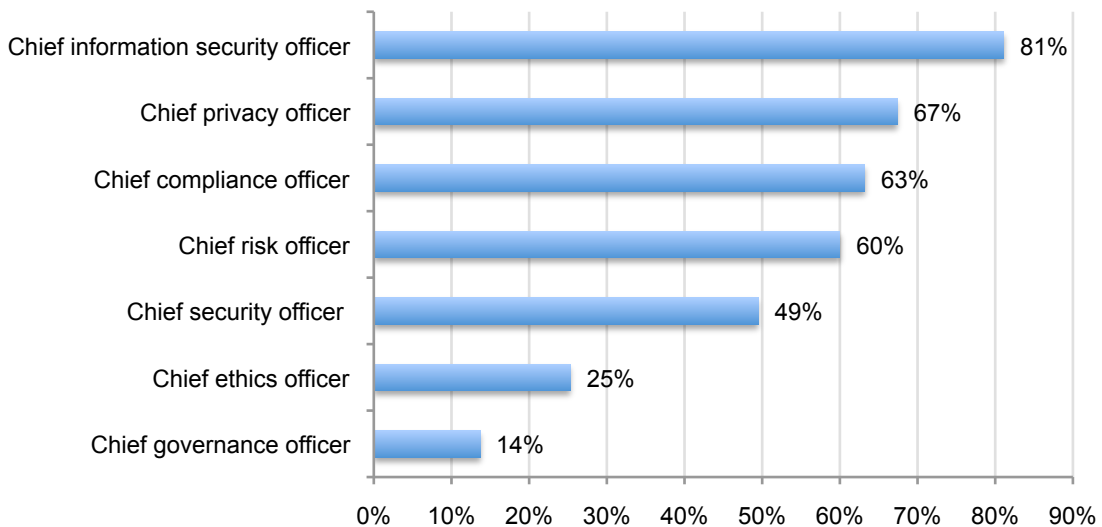
Bar Chart 11 shows only 20 percent of respondents say their organizations have a clearly defined GRC strategy that pertains to the entire enterprise. Forty-seven percent say their organizations have a clearly defined GRC strategy, but it does not pertain to entire enterprise. Third-three percent admit their organizations do not have a GRC strategy.²

Bar Chart 11: What best describes the respondent organization's GRC strategy



To help achieve and support their GRC strategy, according to Bar Chart 12, many respondents' organizations have a Chief Information Security Officer (81 percent) followed by a Chief Privacy Officer (67 percent). Sixty-three percent of respondents say their organizations have a Chief Compliance Officer and 60 percent have a Chief Risk Officer.

Bar Chart 12: Does your organization have the following leaders (or approximate titles)?

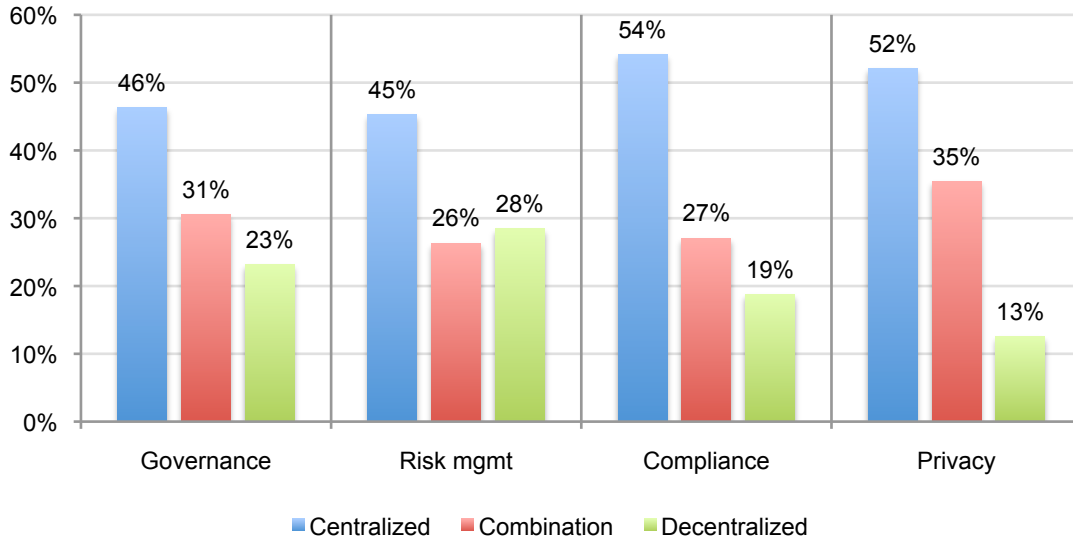


²While not tested in our survey, it is possible that respondents' companies that do not have a clearly defined GRC strategy do have an informal strategy or tactical plan in place.

Bar Chart 13 shows the degree to which GRC activities are centralized or decentralized. As can be seen, all four GRC activities are more likely to be centralized than decentralized. GRC activities relating to governance and privacy tend to be more centralized than activities relating to compliance and risk management tend to be decentralized.

Bar Chart 13: Are GRC activities centralized or decentralized?

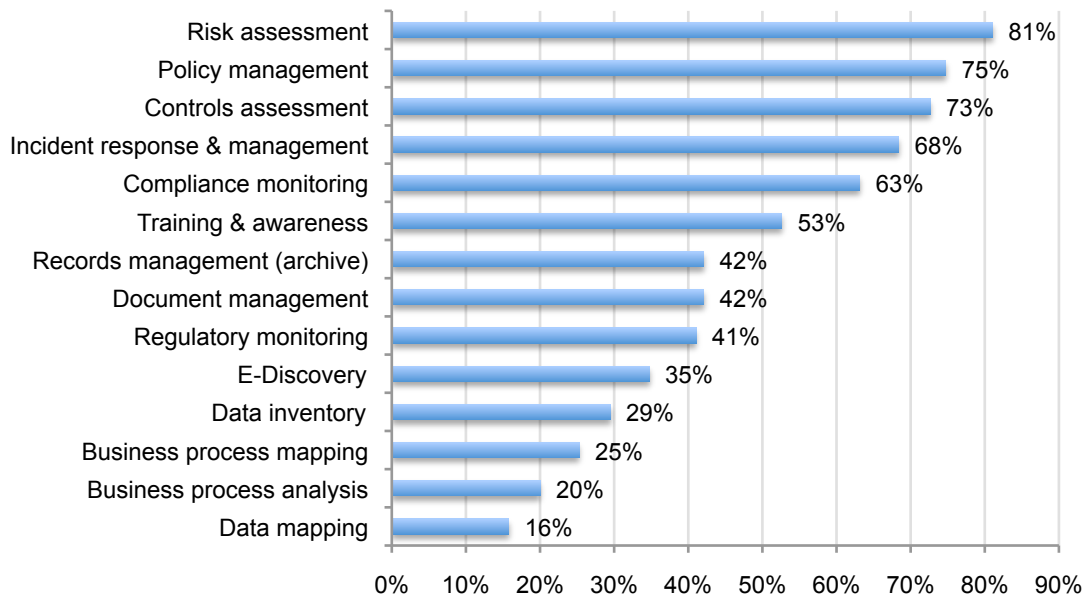
Response measured using a five-point scale from 1+2 = centralized to 4+5 = decentralized



Technology is important for GRC-related activities. As shown in Bar Chart 14, the primary technology solutions used to support GRC-related activities are risk assessment (81 percent), policy management (75 percent) and controls assessment (73 percent).

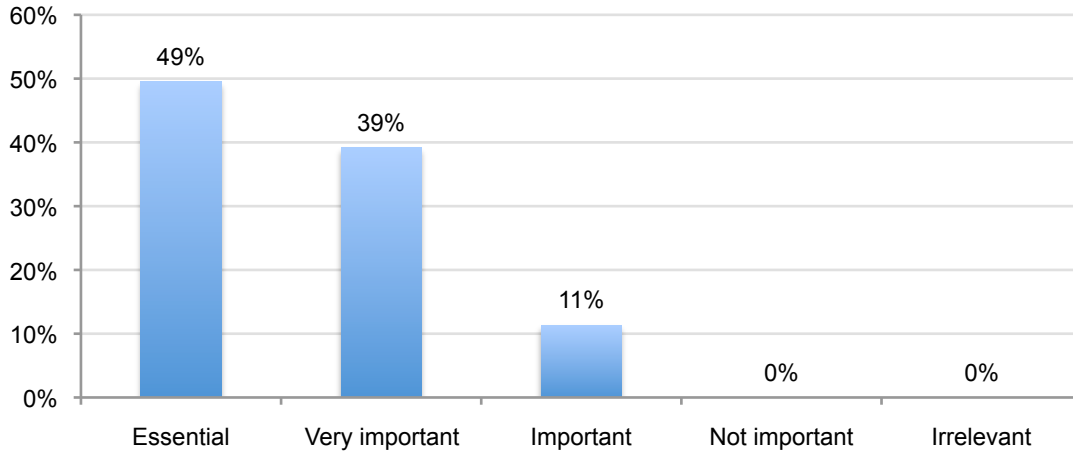
Bar Chart 14: Has your organization implemented technology solutions to accomplish GRC-related activities?

The percentage rate of technology deployment



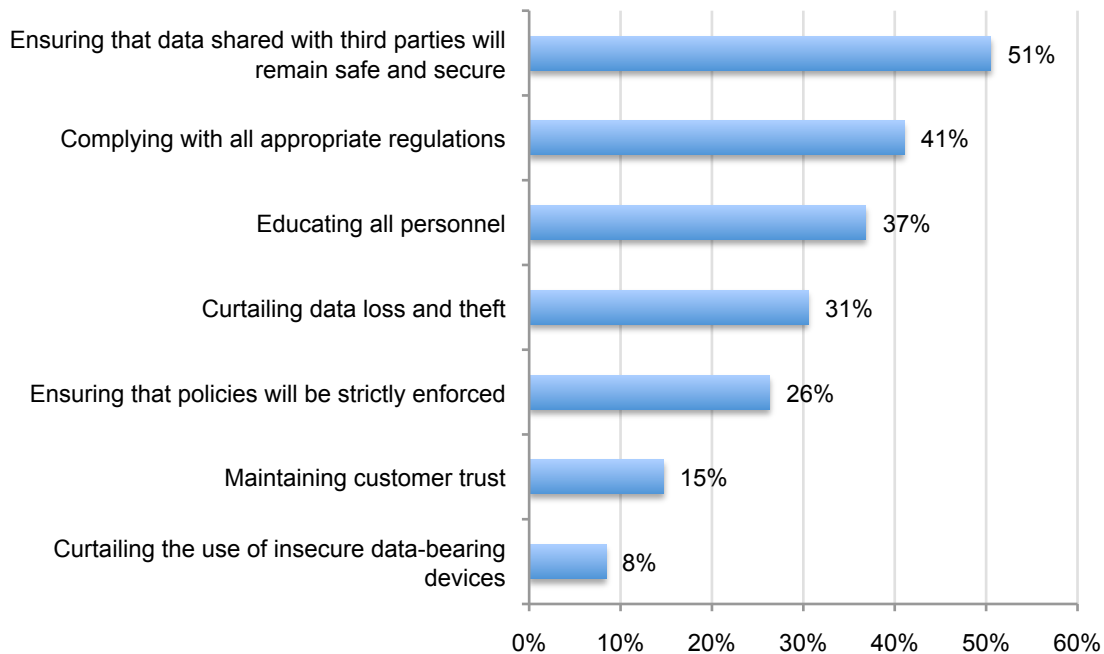
With respect to the GRC technology solutions shown above, Bar Chart 15 reports that 88 percent of respondents believe these solutions are essential (49 percent) or very important (39 percent). No respondent believes these technology solutions are not important or are irrelevant.

Bar Chart 15: How important are the above-mentioned technologies for achieving GRC-related objectives and goals in your organization?



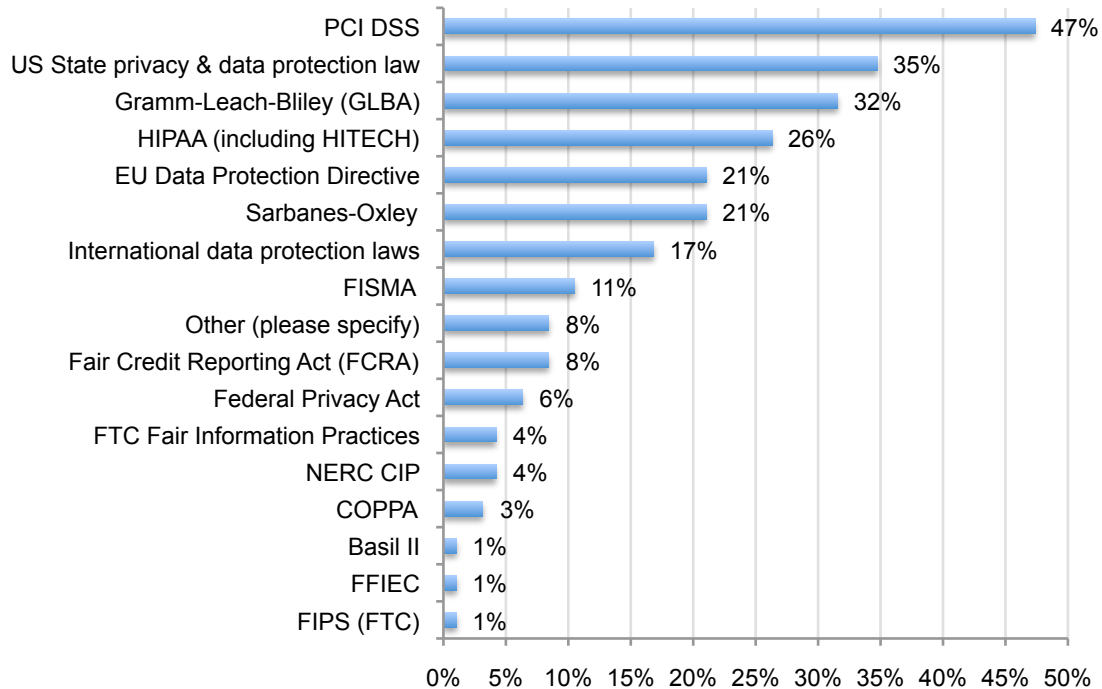
Organizations are struggling to manage privacy regulations and ensure data sharing practices are secure. According to Bar Chart 16, the top two privacy-related challenges or issues facing respondents are ensuring that data shared with third parties (including cloud providers) will remain safe and secure (51 percent) followed by complying with all appropriate regulations (41 percent). Thirty-seven percent of respondents say education is most important, while 31 percent say curtailing data loss is the most salient challenge to privacy.

Bar Chart 16: What are your organization’s most salient privacy-related challenges or issues?
Top two choices



Bar Chart 17 lists the regulations that respondents perceive as most difficult to implement effectively. According to respondents, the most difficult regulations to comply with are PCI DSS, various US state privacy and data protection laws, GLBA, and HIPAA.³

Bar Chart 17: What privacy or data protection regulations are most difficult to comply with?
Top three choices



³Please note that our final sample of GRC practitioners was heavily skewed to individuals in the financial services industry (51 percent). This may explain why GLBA was rated more frequently than other sector regulations.

Part 3. Methods

Table 1 reports the sample response realized in this study. Our sampling frame consisted of a known community of 1,240 GRC practitioners invited to attend an annual conference on eGRC sponsored by RSA Archer. All individuals were invited to participate in a web-based survey. Of these individuals, 206 returned survey responses. Sixteen surveys were rejected because of reliability issues, resulting in a final sample of 190 respondents (15 percent response rate).

Table 1: Sample response	Freq.	Pct%
Total sample frame	1,240	100%
Total returns	206	17%
Rejected surveys	16	1%
Final sample	190	15%

Pie Chart 2 provides the percentage frequency of respondents according to the organization's primary industry sector. As can be seen, more than half of respondents are employed by financial service organizations (including retail banks, insurance, investment management, brokerage, and payment processing (credit card)).

Pie Chart 2: Industry distribution of respondents

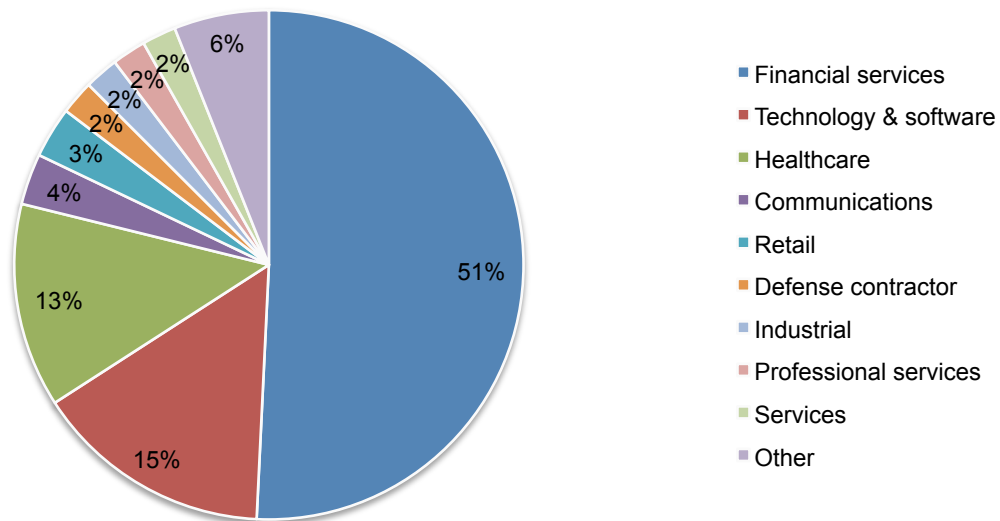


Table 2 reports the approximate position level of respondents. As reported, more than 62 percent of respondents state they are at or above the manager level within their organizations.

Table 2: Respondents' approximate position levels	Pct%
Senior Executive	3%
Vice President	12%
Director	19%
Manager	28%
Associate/Staff	26%
Technician	4%
Consultant	2%
Other (please specify)	6%
Total	100%

Table 3 lists the primary reporting channel of respondents. The most frequently cited reporting channels include the CRO (20 percent), CISO (19 percent) and CIO (14 percent).

Table 3: Respondents' reporting channel within their organization	Pct%
Chief Risk Officer (CRO)	20%
Chief Information Security Officer (CISO)	19%
Chief Information Officer (CIO)	14%
Chief Security Officer (CSO)	13%
Compliance/Ethics Officer	9%
Director, Internal Audit	6%
All other titles	6%
Chief Technology Officer (CTO)	5%
Chief Financial Officer (CFO)	3%
General Counsel (GC)	2%
GRC Leader	2%
Chief Privacy Officer (CPO)	1%
Total	100%

Table 4 lists the worldwide headcount of organizations represented by respondents. As can be seen, the majority of organizations (57 percent) are larger-sized entities with more than 25,000 full time equivalent employees.

Table 4: The worldwide headcount of respondents' organizations	Pct%
Less than 500 people	4%
500 to 1,000 people	1%
1,001 to 5,000 people	12%
5,001 to 25,000 people	26%
25,001 to 75,000 people	34%
More than 75,000 people	23%
Total	100%

Table 5 provides the global footprint of respondents' organizations. As shown, the vast majority of respondents work for organizations that are located in the United States. Many organizations have operations in Europe (55 percent), Canada (42 percent), the Asia-Pacific region (46 percent) and Latin America (37 percent).

Table 5. The global footprint of participating organizations	Pct%
United States	97%
Canada	42%
Europe	55%
Middle East & Africa	31%
Asia-Pacific	46%
Latin America (including Mexico)	37%

Part 4. Conclusion

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of GRC practitioners in various business organizations, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that auditors who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are members of the emerging GRC community. We also acknowledge that responses from paper, interviews or by telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

Concluding Thoughts

We believe this study reveals the importance of an enterprise-wide strategy and increased collaboration among domains to meeting eGRC objectives. Currently, only 20 percent have an enterprise-wide strategy and collaboration among GRC areas is far from perfect. Only 28 percent of respondents say their organizations enjoy frequent collaboration or cooperation among GRC areas. However, the good news is that only 12 percent say GRC areas operate in silos in their organizations.

The study also demonstrates that privacy is an eGRC collaboration flashpoint. Regardless of their industry, all organizations are struggling to manage privacy regulations that must be addressed by geography and in accordance with country or state laws. Today privacy management responsibilities are typically split between the legal and IT functions. While the legal department plays a dominant privacy role overall, IT still holds accountability for implementing controls to address privacy regulations. Respondents identified their top two privacy challenges as ensuring data shared with third parties will remain safe and secure and complying with all appropriate regulations.

In order to address the barriers related to collaboration, it has been recommended that organizations make it a priority to encourage people from the various lines of business to talk together and establish “risk ambassadors”. The need to gain visibility and control through effective cross-enterprise eGRC collaboration is important to reducing gaps in how risk is assessed and managed.

Finally, according to respondents, managing risk is and will continue to be the biggest eGRC focus for their organizations. This is understandable because organizations are finding that the cost of complying with the plethora of regulations can be daunting. Taking a risk-based approach toward compliance requirements enables them to focus their resources on the most at-risk areas of their business and achieve real value from their eGRC activities.

Appendix: Detailed Survey Findings

The following tables provide the percentage frequency of responses to all survey responses completed on March 30, 2011.

Sample response	Freq.
Total sample frame	1240
Total returns	206
Rejected surveys	16
Final sample	190
Response rate	15.3%

Q1. How much of your organization's GRC activities fall into each one of the four GRC domains? Please allocate 100 points to estimate the effort extended to each GRC domain.	Pct%
Finance GRC	19%
IT GRC	44%
Operations GRC	20%
Legal GRC	17%
Total	100%

Q2. How important are privacy-related issues for each one of the four GRC domains?	
Finance GRC	Pct%
Very important	37%
Important	41%
Not important	18%
Irrelevant	4%
Total	100%

IT GRC	Pct%
Very important	76%
Important	23%
Not important	1%
Irrelevant	0%
Total	100%

Operations GRC	Pct%
Very important	46%
Important	46%
Not important	4%
Irrelevant	4%
Total	100%

Legal GRC	Pct%
Very important	71%
Important	23%
Not important	2%
Irrelevant	4%
Total	100%

Q3. What statement best describes the working relationships among finance, IT, operations and legal GRC functions in your organization today?	Pct%
They operate in silos (little collaboration)	12%
They sometimes collaborate	56%
They frequently collaborate	28%
They are fully integrated	3%
Cannot determine	1%
Total	100%

Q4. Please answer the following four statements using the scale provided next to each item.	
Q4a. My job is primarily focused on finance.	Pct%
Strongly agree	5%
Agree	14%
Unsure	4%
Disagree	35%
Strongly disagree	41%
Total	100%

Q4b. My job is primarily focused on IT.	Pct%
Strongly agree	57%
Agree	20%
Unsure	1%
Disagree	16%
Strongly disagree	5%
Total	100%

Q4c. My job is primarily focused on operations.	Pct%
Strongly agree	11%
Agree	41%
Unsure	9%
Disagree	22%
Strongly disagree	17%
Total	100%

Q4d. My job is primarily focused on legal and compliance issues.	Pct%
Strongly agree	20%
Agree	47%
Unsure	7%
Disagree	12%
Strongly disagree	14%
Total	100%

Q4e. My job is primarily focused on privacy issues.	Pct%
Strongly agree	13%
Agree	47%
Unsure	13%
Disagree	21%
Strongly disagree	7%
Total	100%

Q5a. How important are the following four focus areas to your job function? Please allocate 100 points to estimate the importance of focus areas to the fulfillment of your job function today.	Pct%
Governance	22%
Risk management	32%
Compliance	27%
Privacy & data protection	20%
Total	100%

Q5b. How important are the following four focus areas to your job function? Please allocate 100 points to estimate the importance of focus areas to the fulfillment of your job function three years into the future.	Pct%
Governance	23%
Risk management	33%
Compliance	24%
Privacy & data protection	21%
Total	100%

Q6. What job functions do you perform in your organization? Please check all that apply.	Total%
Corporate ethics	8%
Corporate communications	5%
Corporate marketing	2%
E-Discovery	6%
General consulting	23%
General management	17%
Government affairs	3%
Human resources	3%
Information security	71%
Information technology	52%
Internal audit	17%
Legal department	6%
Public relations	2%
Privacy management	27%
Risk management	77%
Regulatory compliance	46%
Records management	11%
Total	377%

Q7a. Where are governance activities located within your organization?	Pct%
Board of directors	5%
CEO/Executive committee	17%
Finance	0%
Legal	7%
Corporate compliance	13%
Information technology (IT)	18%
Public relations	0%
Security & information security	6%
Ethics & compliance	1%
Enterprise risk management	17%
Operational risk management	2%
Business units	4%
Human resources	0%
Spread among several units	8%
Other (please specify)	2%
Total	100%

Q7b. Where are risk management activities located within your organization?	Pct%
Board of directors	3%
CEO/Executive committee	4%
Finance	5%
Legal	0%
Corporate compliance	8%
Information technology (IT)	14%
Public relations	0%
Security & information security	4%
Insurance	0%
Enterprise risk management	39%
Operational risk management	6%
Business units	6%
Human resources	0%
Spread among several units	5%
Other (please specify)	5%
Total	100%

Q7c. Where are compliance activities located within your organization?	Pct%
Board of directors	0%
CEO/Executive committee	2%
Finance	3%
Legal	10%
Corporate compliance	43%
Information technology (IT)	16%
Public relations	0%
Security & information security	5%
Insurance	0%
Enterprise risk management	4%
Operational risk management	2%
Business units	6%
Human resources	0%
Spread among several units	6%
Other (please specify)	2%
Total	100%

Q7d. Where are privacy management activities located within your organization?	Pct%
Board of directors	0%
CEO/Executive committee	2%
Finance	0%
Legal	28%
Corporate compliance	14%
Information technology (IT)	20%
Public relations	0%
Security & information security	7%
Insurance	0%
Enterprise risk management	12%
Operational risk management	3%
Business units	2%
Human resources	3%
Spread among several units	4%
Other (please specify)	1%
Privacy office	3%
Total	100%

Q8. Please rate all the activities that you pursue in order to meet GRC objectives or goals according to the three-point scale: (1) essential, (2) important or (3) not important.	
Q8a. Developing strategies	Pct%
Essential to GRC objectives	61%
Important to GRC objectives	36%
Not important to GRC objectives	3%
Total	100%
Q8b. Analyzing regulations	Pct%
Essential to GRC objectives	45%
Important to GRC objectives	51%
Not important to GRC objectives	4%
Total	100%
Q8c. Assessing risk	Pct%
Essential to GRC objectives	83%
Important to GRC objectives	16%
Not important to GRC objectives	1%
Total	100%
Q8d. Creating and implementing policies	Pct%
Essential to GRC objectives	50%
Important to GRC objectives	47%
Not important to GRC objectives	3%
Total	100%
Q8e. Training and awareness	Pct%
Essential to GRC objectives	43%
Important to GRC objectives	49%
Not important to GRC objectives	7%
Total	100%
Q8f. Monitoring compliance	Pct%
Essential to GRC objectives	63%
Important to GRC objectives	38%
Not important to GRC objectives	0%
Total	100%
Q8g. Reporting to senior management	Pct%
Essential to GRC objectives	60%
Important to GRC objectives	36%
Not important to GRC objectives	4%
Total	100%
Q8h. Administering program	Pct%
Essential to GRC objectives	44%
Important to GRC objectives	52%
Not important to GRC objectives	4%
Total	100%
Q8j. Advising or consulting within the organization	Pct%
Essential to GRC objectives	40%
Important to GRC objectives	55%
Not important to GRC objectives	5%
Total	100%

Q8k. Responding to incidents	Pct%
Essential to GRC objectives	42%
Important to GRC objectives	47%
Not important to GRC objectives	11%
Total	100%

Q9. What statement best describes your organization's GRC strategy?	Pct%
Our organization has a clearly defined GRC strategy and pertains to the entire enterprise.	20%
Our organization has a clearly defined GRC strategy, but it is not applicable to the entire enterprise.	47%
Our organization does not have a clearly defined GRC strategy.	33%
Total	100%

Q10. Does your organization have the following leaders (or approximate job titles)? Please check all that apply.	Pct%
Chief privacy officer	67%
Chief compliance officer	63%
Chief ethics officer	25%
Chief governance officer	14%
Chief risk officer	60%
Chief information security officer	81%
Chief security officer	49%
Total	360%

Q11. Has your organization implemented technology solutions for the following GRC-related activities? Please check all that apply.	Pct%
Policy management	75%
Risk assessment	81%
Controls assessment	73%
Business process mapping	25%
Business process analysis	20%
Data mapping	16%
Document management	42%
Data inventory	29%
Regulatory monitoring	41%
Compliance monitoring	63%
Incident response & management	68%
Training & awareness	53%
Records management (archive)	42%
E-Discovery	35%
Total	663%

Q12. In your opinion, how important are the above-mentioned technologies for achieving GRC-related objectives and goals in your organization?	Pct%
Essential	49%
Very important	39%
Important	11%
Not important	0%
Irrelevant	0%
Total	100%

Q13. Are your organization's governance, risk management, compliance and privacy/data protection functions centralized or decentralized? Please use the five-point scale provided next to each focus area:	
Centralized – the activities or function are managed by one central authority within the enterprise.	
Decentralized – the activities or function are managed across units or spread among business segments.	
Q13a. Activities relating to governance	Pct%
Centralized=1	20%
2	26%
3	31%
4	13%
Decentralized=5	11%
Total	100%

Q13b. Activities relating to risk management	Pct%
Centralized=1	14%
2	32%
3	26%
4	20%
Decentralized=5	8%
Total	100%

Q13c. Activities relating to compliance	Pct%
Centralized=1	18%
2	36%
3	27%
4	11%
Decentralized=5	7%
Total	100%

Q13d. Activities relating to privacy	Pct%
Centralized=1	22%
2	30%
3	35%
4	8%
Decentralized=5	4%
Total	100%

Q14. What are the top two barriers to achieving your organization's GRC-related goals?	Pct%
Lack of resources	52%
Lack of C-level support	15%
Lack of clear leadership	20%
Difficulty in hiring skilled personnel	11%
Inability to set priorities	19%
Inability to get started (inertia)	4%
Lack of cooperation and collaboration among the various departments involved in GRC	44%
Major organizational changes such as mergers, downsizing, financial turmoil and others	19%
Complexity of the program	3%
Complexity of existing technologies	31%
Inadequacy of existing technologies	3%
Lack of organizational maturity	2%
Other (please specify)	2%
Total	224%

Q15. What are your organization's top two privacy-related challenges or issues?	Pct%
Curtailing data loss and theft	31%
Curtailing the use of insecure data-bearing devices including smartphones and USB sticks	8%
Complying with all appropriate regulations	41%
Educating all personnel	37%
Maintaining customer trust	15%
Ensuring that data shared with third parties (including cloud providers) will remain safe and secure	51%
Ensuring that policies will be strictly enforced	26%
Total	208%

Q16. What top three privacy or data protection regulations are most difficult to comply with?	Pct%
PCI DSS	47%
HIPAA (including HITECH)	26%
Sarbanes-Oxley	21%
Gramm-Leach-Bliley (GLBA)	32%
Child Online Privacy Protection Act (COPPA)	3%
NERC CIP	4%
Fair Information Practices (FTC)	1%
Fair Credit Reporting Act (FCRA)	8%
Federal Privacy Act	6%
FTC Fair Information Practices	4%
FISMA	11%
FFIEC	1%
Basil II	1%
EU Data Protection Directive (including Safe Harbor)	21%
Various US state privacy and data protection laws	35%
Various international privacy and data protection laws	17%
Other (please specify)	8%
Total	247%

Q17. Where did your organizations GRC program or initiatives start?	Pct%
Information technology	63%
Operations	12%
Finance	13%
Legal	13%
Total	100%

Demographics & organizational characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	3%
Vice President	12%
Director	19%
Manager	28%
Associate/Staff	26%
Technician	4%
Consultant	2%
Other (please specify)	6%
Total	100%

D2. Select the primary person you report to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	2%
Chief Information Officer	14%
Compliance/Ethics Officer	9%
Chief Technology Officer	5%
CSO	13%
Chief Risk Officer	20%
CISO	19%
Chief Privacy Officer	1%
Director, Internal Audit	6%
GRC Leader	2%
Other (please specify)	6%
Total	100%

D3. Select the secondary person you report to within the organization (or leave blank if you do not have a secondary or dotted line reporting relationship).	Pct%
CEO/Executive Committee	3%
Chief Financial Officer	2%
General Counsel	3%
Chief Information Officer	11%
Compliance/Ethics Officer	3%
Chief Technology Officer	3%
CSO	8%
Chief Risk Officer	7%
CISO	8%
Chief Privacy Officer	2%
Director, Internal Audit	2%
Other (please specify)	3%
Blank	43%
Total	100%

D4. Gender:	Pct%
Male	70%
Female	30%
Total	100%

D5. What industry best describes your organization's primary industry?	Pct%
Communications	3%
Defense contractor	2%
Education & research	0%
Financial services	51%
Healthcare	13%
Hospitality	0%
Industrial	2%
Pharmaceuticals	1%
Professional services	2%
Public sector	1%
Retail	3%
Services	2%
Technology & software	15%
Transportation	1%
Utilities & energy	1%
Media	1%
Other (please specify)	1%
Total	100%

D6. Where are your employees located? Please check all regions that apply.	Pct%
United States	97%
Canada	42%
Europe	55%
Middle East & Africa	31%
Asia-Pacific	46%
Latin America (including Mexico)	37%
Total	308%

D7. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	4%
500 to 1,000 people	1%
1,001 to 5,000 people	12%
5,001 to 25,000 people	26%
25,001 to 75,000 people	34%
More than 75,000 people	23%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.