OCEG®
Driving Principled Performance

2017 GRC Maturity Survey

How GRC Strategy & Integration Affects Confidence

OCEG®

Driving Principled Performance

About OCEG . . .

OCEG is a global, nonprofit think tank and community. We invented GRC. We inform, empower and help advance more than 50,000 members on governance, risk management, and compliance (GRC).

Independent of specific professions, we provide content, best practices, education, and certifications to drive leadership and business strategy through the application of the OCEG GRC Capability Model™ and Principled Performance®. An OCEG differentiator, Principled Performance enables the reliable achievement of objectives while addressing uncertainty and acting with integrity.

Our members include c-suite, executive, management, and other professionals from small and mid-size businesses, international corporations, nonprofits, and government agencies. We assist them and their organizations in developing and implementing GRC capabilities that enable Principled Performance by providing authoritative resources for integrating the governance, assurance and management of performance, risk and compliance.

For more information visit http://www.oceg.org or contact us at info@oceg.

The OCEG 2017 GRC Maturity Survey was designed and analyzed by GRC 20/20 Research . . .

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide independent and objective insight into leading GRC practices and processes, including market dynamics and intelligence; risk, regulatory and technology trends; competitive landscapes; market sizing; expenditure priorities; and mergers and acquisitions.

For more information go to www.GRC2020.com or contact GRC 20/20 at info@GRC2020.com.

grc2020

Preface

OCEG is the only organization that focuses on Principled Performance and integrating the governance, assurance and management of performance, risk, compliance and ethics (GRC). By integrating these areas, organizations simultaneously increase performance, address risk and reduced costs. As a non-profit that does not represent a specific profession, we are uniquely positioned to serve as a hub around which many professions can collaborate on solutions.

This OCEG 2017 GRC Maturity Survey report takes a look at how organizations are taking varying approaches to GRC from the siloed to the fully integrated and measures the satisfaction and confidence organizations have as a result.

We hope this survey report provides you with valuable insights to improve GRC strategy, processes, and architecture within your organization.

Survey data can be downloaded at: http://www.oceg.org/resources/grc-maturity-survey-data-set-2017/

Contents

INTRODUCTION: GRC Technology Strategy Impacts Maturity

Every organization does GRC whether they use the acronym or not. All have some approach to governing the organization, managing risk, and addressing compliance. It could be scattered in silos and disconnected, or it could be highly collaborated and integrated. Organizations should not be asking if they should do GRC but are to ask how mature their organization's approach to GRC is and how it can be improved.

The formal definition for GRC found in the OCEG GRC Capability Model is that "GRC is a capability to reliably achieve objectives [governance] while addressing uncertainty [risk management] and acting with integrity [compliance]."

In the ideal world there is a natural flow through to GRC. Governance sets objectives and directs and steers the organization setting the context for risk management. Risk management aims to understand and minimize uncertainty in those objectives and reduce exposure to loss while maximizing performance. Compliance assures that the organization operates with integrity to the boundaries established in organization values, policies, regulatory and legal requirements, as well as boundaries set by risk limits and thresholds.

However, within many organizations there are often many GRC functions operating in isolation producing redundancy and gaps while remaining ignorant of the interrelationship of risk across silos. This has a measurable cost to the organization in inefficiency, ineffectiveness, and lack of agility.

Other organizations have mature and structured processes and reporting on GRC that brings together an integrated and orchestrated view of GRC processes and information.

The goal of this 2017 OCEG GRC Maturity Survey report is to help organizations:

- Understand the level of integration of GRC within organizations;
- Differentiate the degree of confidence in performance with the ability to identify and manage risks and requirements;
- Examine the benefits of an integrated GRC capability and the negative effects of siloed operations.

Michael Rasmussen
OCEG Fellow & Co-Chair of OCEG GRC Solutions Council
The GRC Pundit @ GRC 20/20 Research, LLC

A Word From Our Survey Sponsor: MetricStream

The 2017 OCEG GRC Maturity Survey is made possible through the support of the entire OCEG GRC Solutions Council and the following survey sponsor members: MetricStream & Workiva

MetricStream

This landmark OCEG GRC Maturity survey spells out that the vast majority of organizations are not only realizing efficiencies through integrated GRC by sharing risk management and compliance data across audit, compliance, risk management, cybersecurity and other disciplines, but also gaining significantly greater executive confidence by addressing enterprise, operational, IT and regulatory risks that can enable better business performance.

We at MetricStream see GRC leaders increasingly striving for a higher level of maturity, since, more and more, GRC has been proven to contribute in high value ways to effective business decisions. Business drivers for GRC have shifted over the last few years from compliance and visibility to managing not only downside risk, but more importantly, providing insights on how to transform risks into opportunities.

GRC programs are delivering better oversight and insights into new and emerging risks as organizations steer toward their goals through tumultuous waters. Business leaders need to make decisions faster than ever, against a backdrop of growing geopolitical uncertainties, cyber-attacks and rapid regulatory changes – and GRC programs are helping them do it.

What we see at MetricStream is that automation contributes greatly to achieving these goals - GRC apps that support common risk frameworks, collaboration and insight through analytics are table stakes for maturing GRC in a business environment that is increasingly mobile, social, global, and virtual. In addition, it's critical to build community, best practices and methodologies in program management that support the GRC Journey itself.

Organizations throughout the globe are benefiting from MetricStream's simple and modular approach to GRC - enabling organizations to optimize GRC execution while driving business performance along their GRC Journey.

Yo Delmar, Vice president, GRC Solutions

MetricStream makes GRC simple with solutions that strengthen risk management, regulatory compliance, cybersecurity, and quality management while preserving corporate integrity, protecting brands and reputations, and ensuring exceptional business performance.

A Word From Our Survey Sponsor: Workiva

The 2017 OCEG GRC Maturity Survey is made possible through the support of the entire OCEG GRC Solutions Council and the following survey sponsor members: MetricStream & Workiva

Although GRC is not a technology initiative, technology has proven to play a critical role in the maturity of GRC processes. As GRC has matured in organizations the past ten years so to has the technology that supports it. As organizations evolve and mature their GRC programs, adoption of the most modern and collaborative technology may accelerate GRC maturity.

Convergence of GRC data, processes, and activities is by nature a collaborative process. To optimize your GRC processes, your technology solution should be simple, intuitive and require no expertise to accomplish a task. Your technology should engage people at all three lines of defense - not just automate part of a business process workflow. Your technology should support real-time collaboration within teams and across departments.

Today, there are cloud-based GRC solutions that are as simple to use as traditional office applications . These solutions connect and optimize risk, control and compliance processes by simplifying complex collaboration while keeping data in sync. Cloud-based solutions free you from the costs, complexities, and on-going maintenance and upgrades of legacy GRC platforms, enabling you to focus your time and efforts on more strategic activities and execution. With productivity-driven solutions, you can better automate business processes to drive much more efficiency—both with your team and data. These solutions propel GRC maturity by solving the problem of disparate pockets of information kept by multiple users and desktop documents. If you are looking for GRC maturity, consider looking at the new technologies that have come to market the past several years.

At Workiva, our customers have proven that when you collaborate in the same intuitive cloud platform, you save a lot of time. When you trust your data from beginning to end, you reduce risk. When you have peace of mind, you make better decisions. With the most modern of technology, you can drive GRC maturity.

Mike Rost, Vice President

Workiva Wdesk gives organizations the flexibility to identify and adapt to changing internal control, risk, and compliance management needs

MEASURING GRC MATURITY

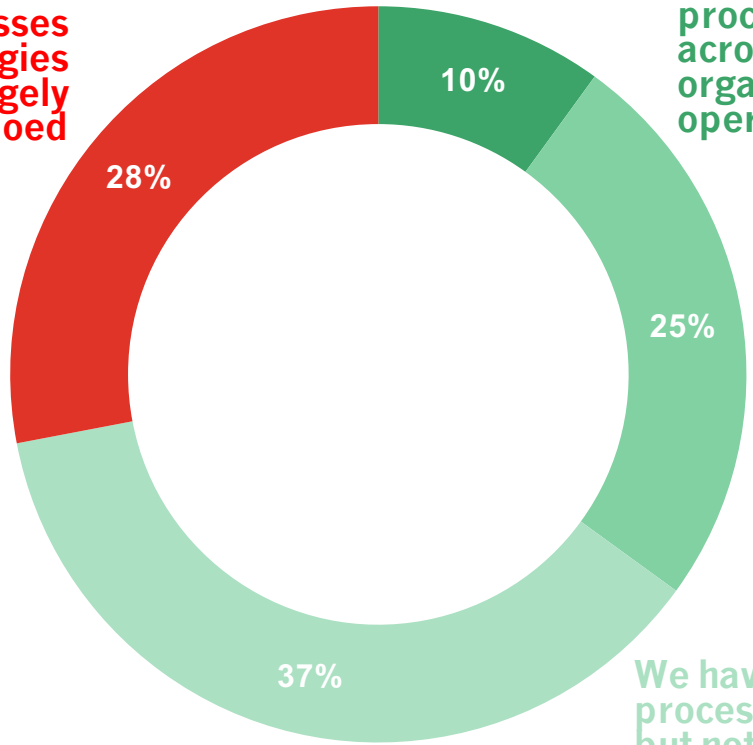
From Silos to Integrated GRC

Level of GRC Integration Within Organizations

The critical pivot of the survey results stems from the question on GRC integration. Twenty-eight percent of organizations responding state that their GRC processes largely remain in silos of processes and technologies. On the flip-side of this, seventy-two percent of organizations indicate some level of GRC integration. This includes ten percent that report the majority of their processes and technology are integrated, with twenty-five percent reporting significant progress in GRC integration, and thirty-seven percent stating they have standardized in some areas of GRC but not all of them.

This question is critical to the results of the rest of the survey as we pivot the siloed responses (28%) and contrast them to the varied stages of integration responses (72%) to measure the impact of GRC integration.

Pick the statement that best describes your organization's state of integration of GRC capabilities. (The more integrated you are, the more you share information and use standardized approaches to how you manage and provide assurance about performance, risk and compliance.)

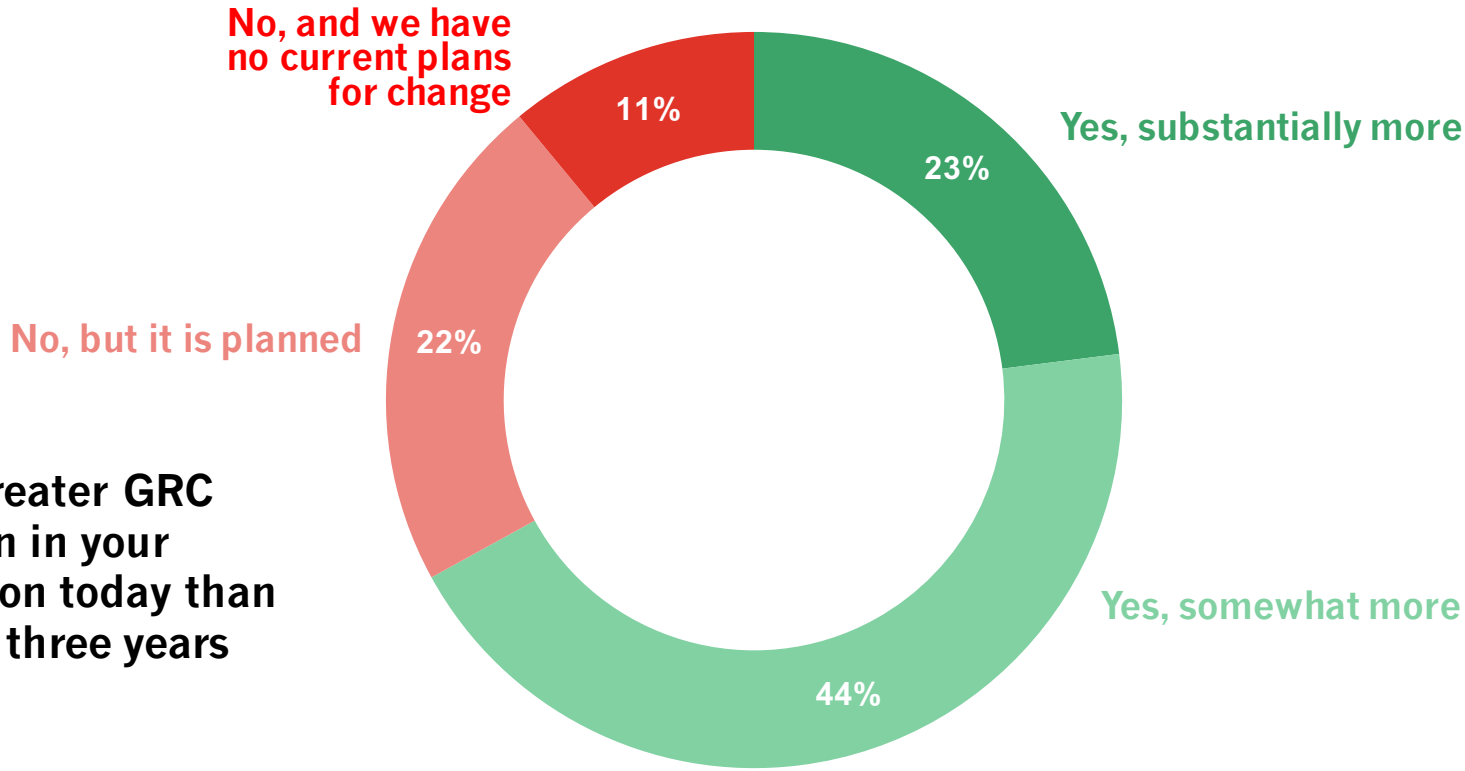


Level of GRC Integration Compared to 3 Years Back

When asked about the current state of GRC integration now compared to three years back the survey reveals that sixty-seven percent of respondents indicate they are more integrated (23% substantially more, and 44% somewhat more). Only eleven percent indicate they have no change in level of GRC integration over past three years and have no plans to change, while another 22% who have not yet changed have plans to do so.

This is an indicator on increased awareness and collaboration on GRC even when GRC responsibilities still remain siloed and uncoordinated.

Is there greater GRC integration in your organization today than there was three years ago?

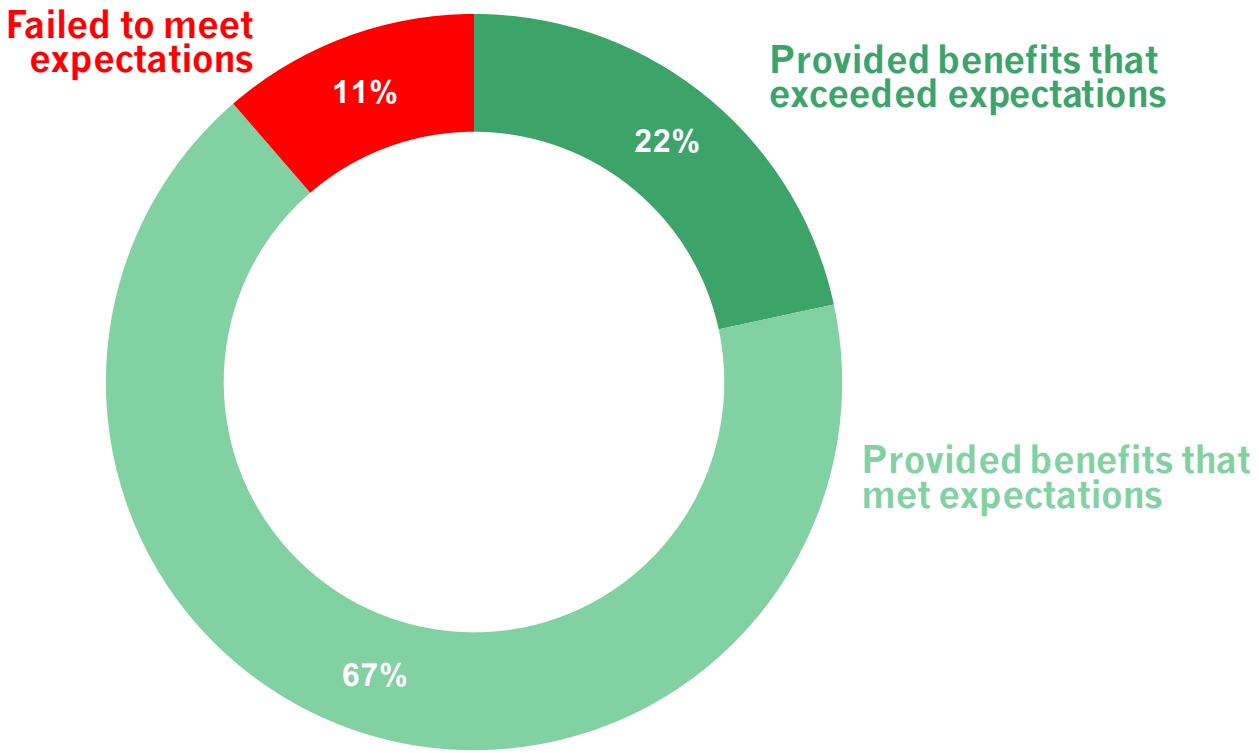


Satisfaction of GRC Integration from those Who Integrated

Of the 578 total respondents, 416 (72%) indicate they have some level of GRC standardization and integration across their organization.

Of these 416 respondents with integrated GRC strategies, sixty-seven percent state that integration provided benefits that met expectations, while twenty-two percent indicate integration exceeded expectations, and only ten percent say that they failed.

Where your organization has integrated processes for governance, assurance and/or management of performance, risk and compliance (GRC), the results have:

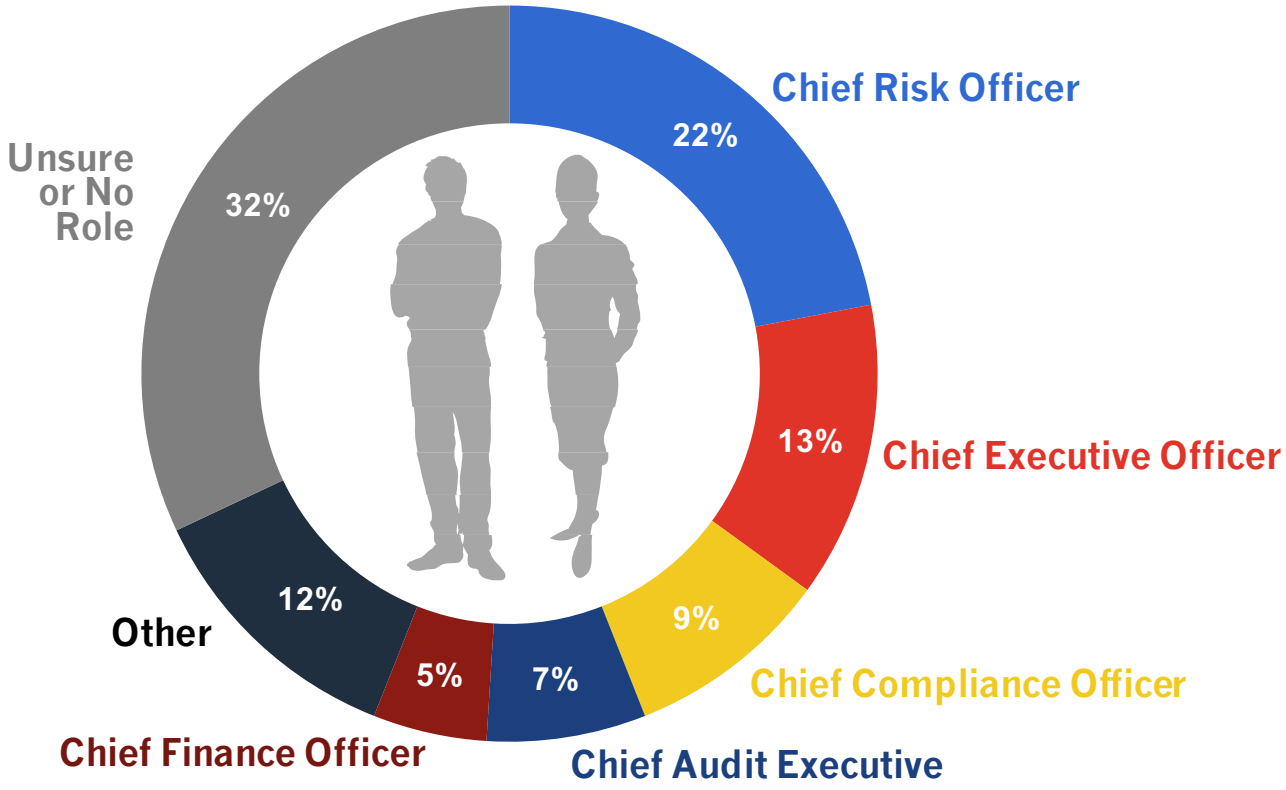


Who Leads the GRC Strategy?

When asked who is responsible for leading an integrated GRC strategy, the most common answer is the Chief Risk Officer in organizations. This makes since as the Chief Risk Officer is the point of view that aggregates to range of risks across the organization that impacts strategy and objectives.

Surprisingly, the second most common role to lead a GRC strategy is the Chief Executive Officer. This role is ideal to ensure cross organization cooperation and alignment of risk and compliance with organization strategy and objectives.

Who in your organization is responsible for leading strategy around integrating GRC processes?

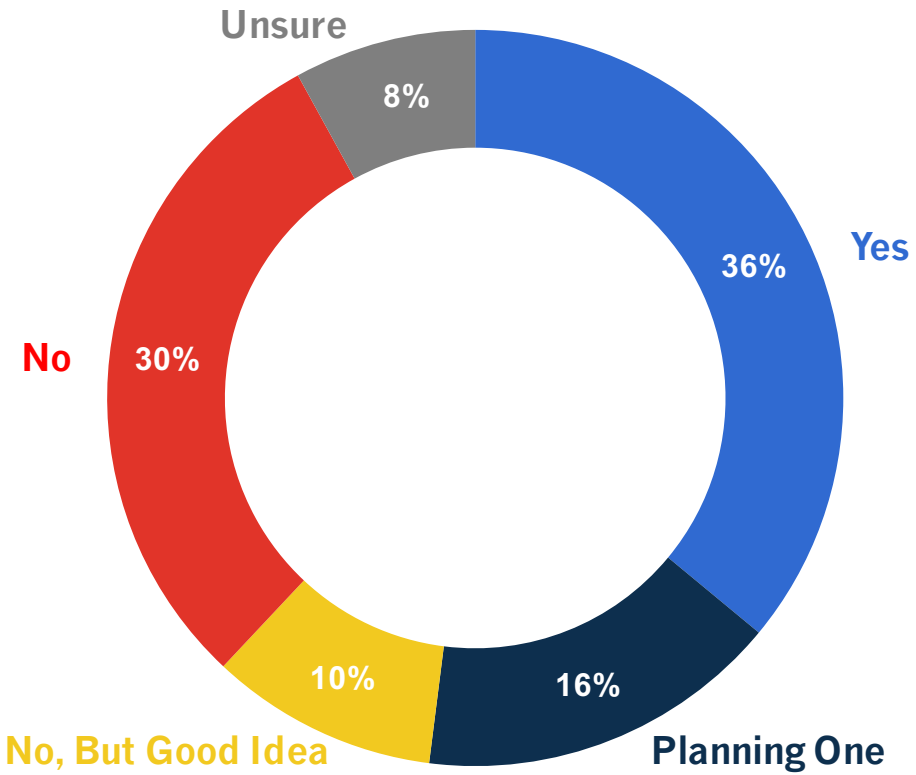


Management Level GRC Committee: Those with GRC Integration

Of the organizations that have an integrated GRC strategy, over a third (36%) state they have a management level committee to address GRC integration enterprise-wide. This committee oversees the sharing of information and collaboration of GRC related roles, processes, activities, and information.

Sixteen-percent state they are planning a management level committee to address GRC integration, while ten-percent state that they do not have one but like the idea.

Does your organization have a management level committee to address integration of GRC enterprise-wide?

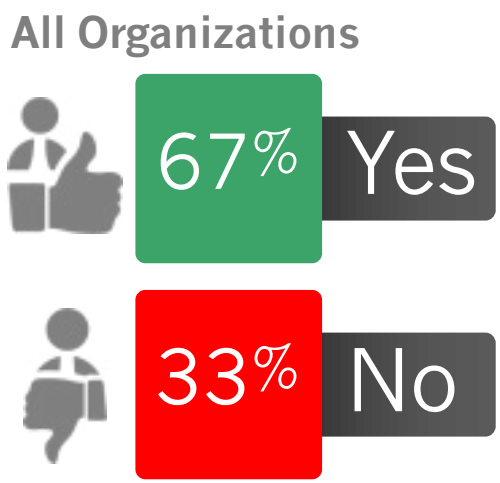


Chief Compliance & Risk Officer Roles in Organizations

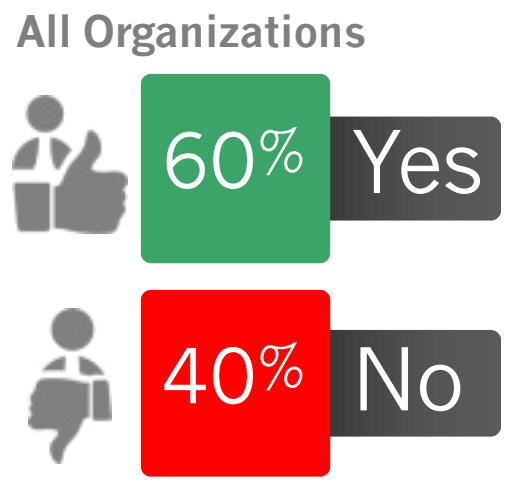
Across all respondents, over two-thirds (67%) of organizations responding to the survey state they have a Chief Compliance Officer, and slightly less (60%) report that they have a Chief Risk Officer in the organization.

Both of these roles have seen growth with a greater number of organizations establishing both of these roles. It is not surprising that the compliance role has a slight lead in penetration of organizations over the risk role given the breadth of regulations organizations have to respond to.

Does your organization have an enterprise-wide Chief Compliance Officer?



Does your organization have an enterprise-wide Chief Risk Officer?



Chief Compliance & Risk Officer Roles: Geographic Perspectives

What is very interesting is the differentiation of risk and compliance executives when contrasted between North America and Europe. North America (68%) has a slightly stronger penetration of the Chief Compliance Officer role over Europe (65%). This is to be expected given the more prescriptive nature of regulatory enforcement and the litigious legal culture of North America.

However, there is a stronger discrepancy of Europe having the higher penetration of Chief Risk Officers (63%) in contrast to North America (50%). This too is partly due to the regulatory cultures between the two continents. Europe has a principle-based approach that is not prescriptive which requires a risk-based approach to compliance. Europe also tends to be more mature than North America in integrating risk into business strategy, objectives, and processes.

COMPARISON & ANALYSIS

GRC Integration Improves Alignment & Confidence

COMPARISON: GRC Confidence

A revealing finding is the significant disparity between silos and integrated GRC strategies in the context of confidence. Organizations with standardized to integrated GRC show significantly increased confidence in mapping risks and controls, GRC activities, and the ability to identify changing threats and requirements in a dynamic environment.

Organizations with silos of GRC report a general lack of confidence in these respective areas.

How confident are you in your organization's ability to map risks to the drivers of each risk across all risk functions?

How confident are you in your organization's ability to map ownership of each risk, requirement and control to specific individuals/roles, thus ensuring oversight of operation and consideration of need for design or application changes?

How confident are you in your organization's ability to map each control it has to a given risk (or risks) or requirement(s) and track changes that would trigger need for change in the control?

COMPARISON: GRC Confidence

Further, organizations with GRC integration show greater confidence that they are effectively implementing the right management activities and controls to address risks as well as regulatory requirements.

They also indicate that they have greater confidence in the identification of threats to their objectives and organization, as well as identification of regulatory and other requirements they need to comply with.

How confident are you that your organization has selected and is effectively implementing the right management activities and controls to address your risks and requirements?

How confident are you in your organization's ability to identify threats and requirements that give rise to risks and compliance needs?

COMPARISON: GRC Confidence

Two of the greatest challenges organization face in 2017 is the management of third party risks (e.g., vendor, supplier, contractor) and securing IT and information infrastructures.

Organizations with integrated GRC strategies show significantly greater confidence in addressing both third party risks as well as IT security within their organizations than those with siloed approaches that do not integrate.

How confident are you in your organization's ability to identify vendor and other third party risks and compliance requirements?

How confident are you in your organization's ability to identify IT security vulnerabilities, threats and requirements that give rise to risks and compliance needs?

COMPARISON: GRC Confidence

The impact of integrated GRC is also apparent on the governance of the organization.

Organizations with integrated GRC strategies show greater confidence that their governing bodies (e.g., board of directors) are receiving the right level of risk and compliance detail to aid in the establishment and achievement of objectives of the organization.

How confident are you that your governing authority (board or other oversight committees) get adequate information about risk and compliance to use in establishing objectives?

How confident are you that your governing authority (board or other oversight committees) get adequate information about risk and compliance to use in determining success in achieving objectives?

COMPARISON & ANALYSIS

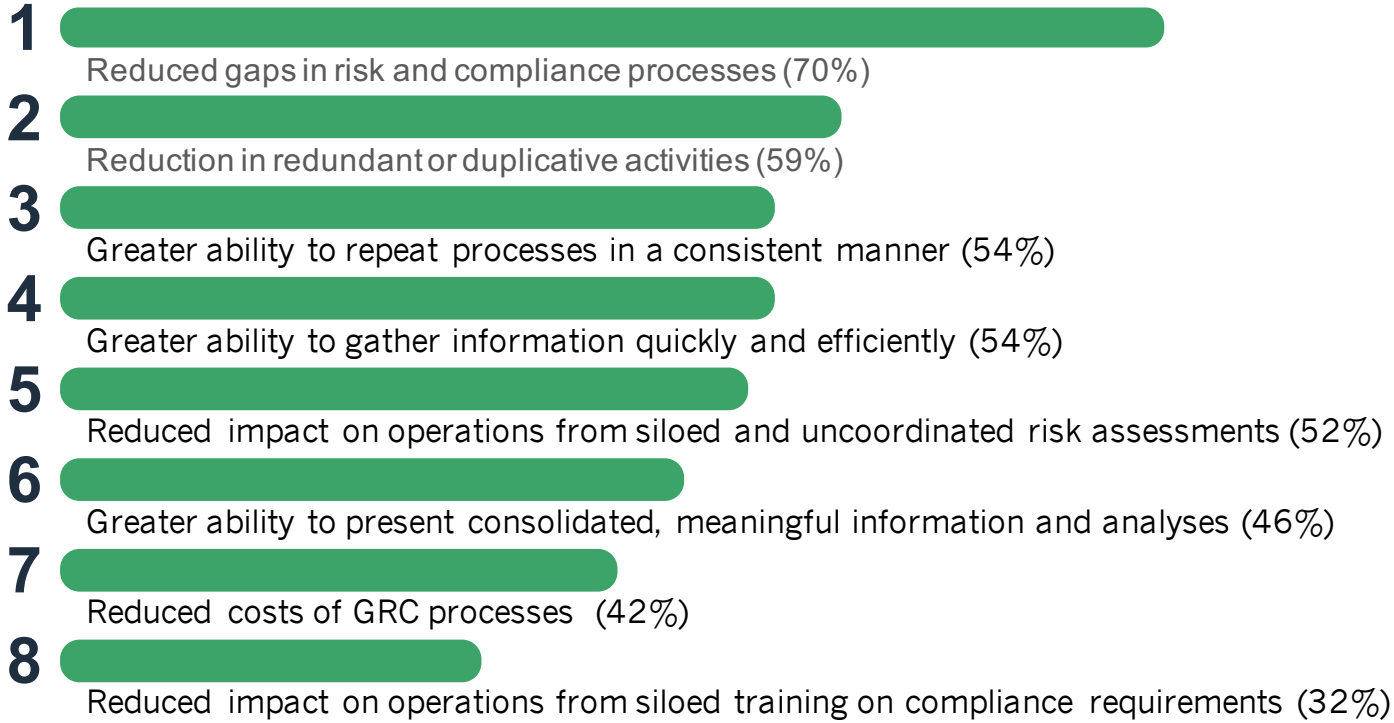
GRC Integration Improves Alignment & Confidence

Beneficial Outcomes From Those Who Have Integrated GRC processes

Organizations indicating they have standardized to integrated GRC processes report a range of value and specific benefits this has brought to their organization. The most significant benefits are reduced gaps in GRC processes as well as reduction in redundancy of duplicated activities and processes. This indicates increased effectiveness in GRC capabilities in organizations with integrated GRC.

These organizations also report increased ability to gather and report on GRC information, present GRC information to stakeholders, and to repeat processes consistently. This illustrates that integrated GRC brings greater agility to the organization.

Organizations with integrated GRC also report reduced impact on operations and costs of GRC processes which means that integrated GRC brings greater human and financial capital efficiency to the organization.



Greatest Barriers to Integrated GRC in Siloed Organizations

Organizations that lack an integrated GRC strategy clearly indicate that their number one barrier to an integrated GRC strategy is the lack of an established strategy for integration.

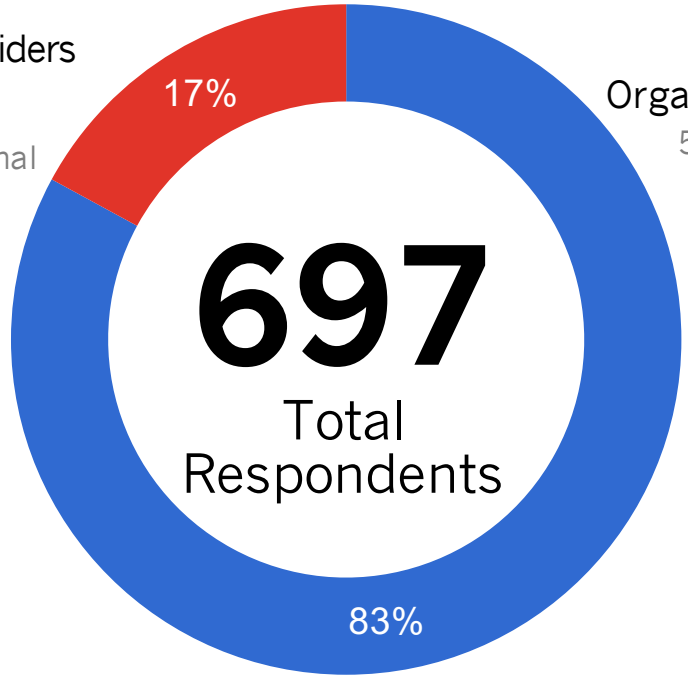
The rest of the barriers to GRC integration can all be mapped back to the lack of an established strategy to facilitate GRC collaboration and integration. These include challenges in getting departments to work together, champions, and defining a business case for GRC integration.

Survey Demographics
&
OCEG Resources

Survey Respondents by Breakout of GRC Buyers vs. Providers

GRC Solutions Providers

119 respondents were from GRC Solution Providers or Professional Service Firms in client facing roles.



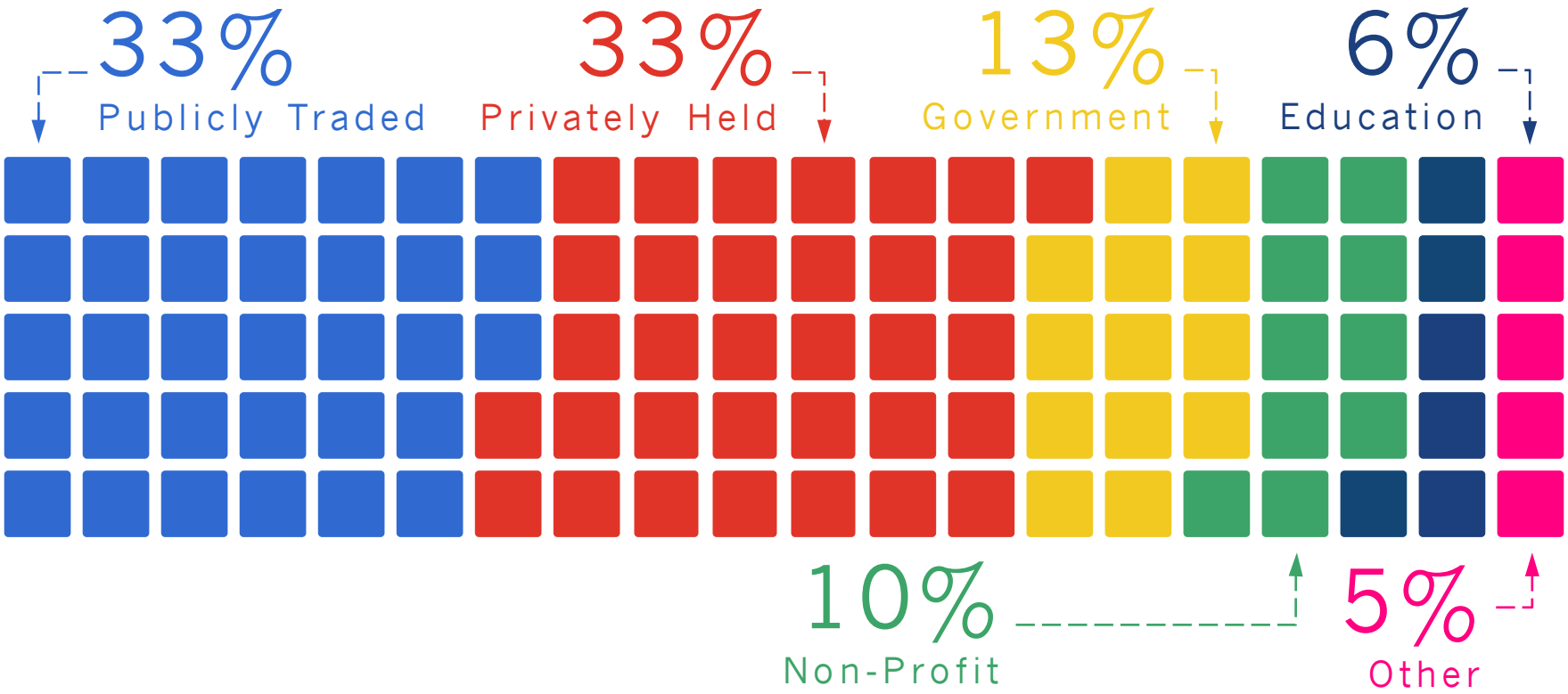
Organizations Using/Considering GRC Solutions

578 respondents were from organization using or considering GRC solutions/technology.

Our Focus Today

Today we are looking at the 578 respondents from organizations using or considering GRC solutions/technology to use within their organization.

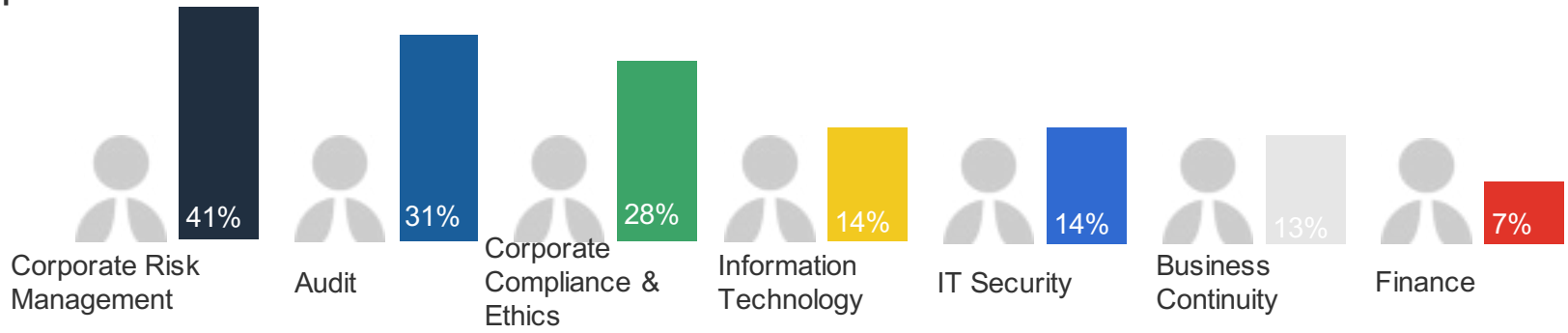
Survey Respondents by Type of Organization



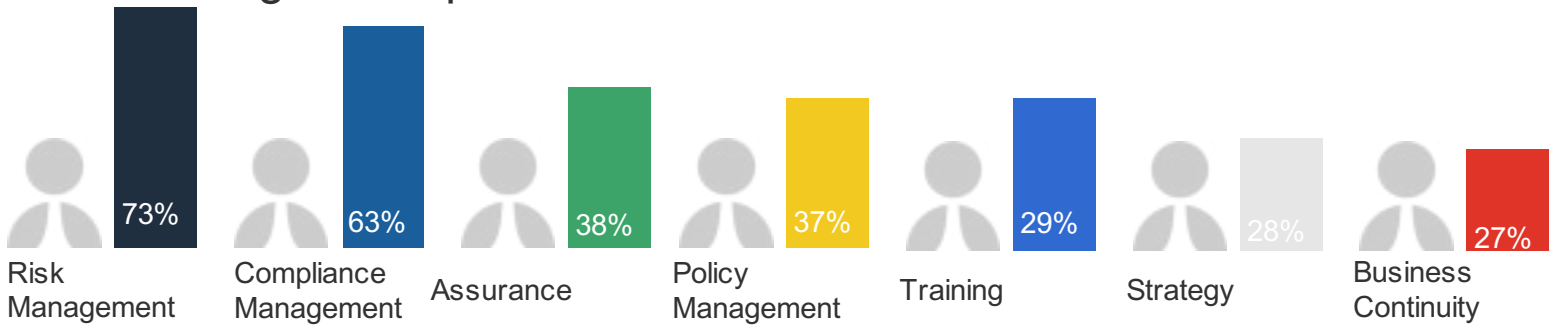
571 respondents from organization using or considering GRC solutions/technology

Survey Respondents by GRC Role in Organization

Respondents are from these business functions . . .



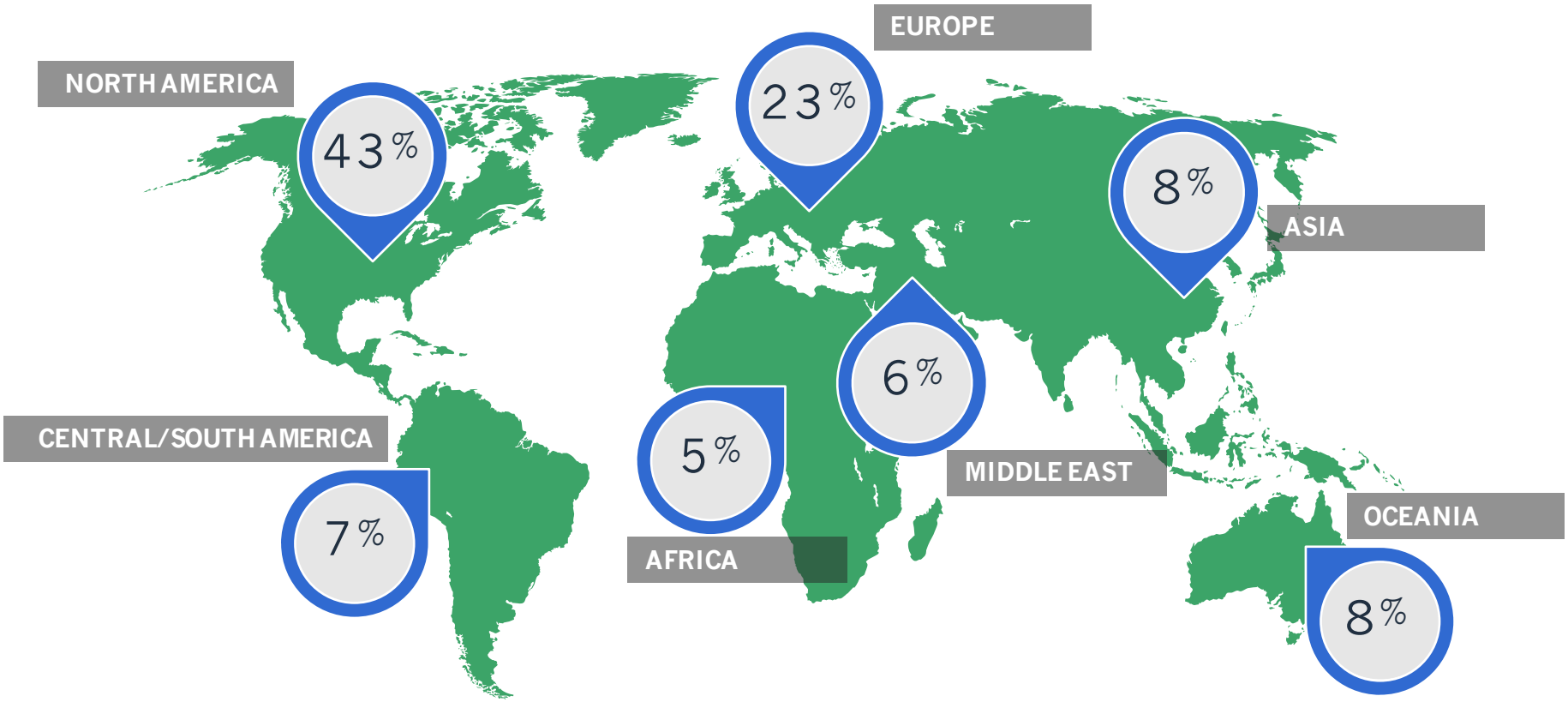
But also have a range of responsibilities . . .



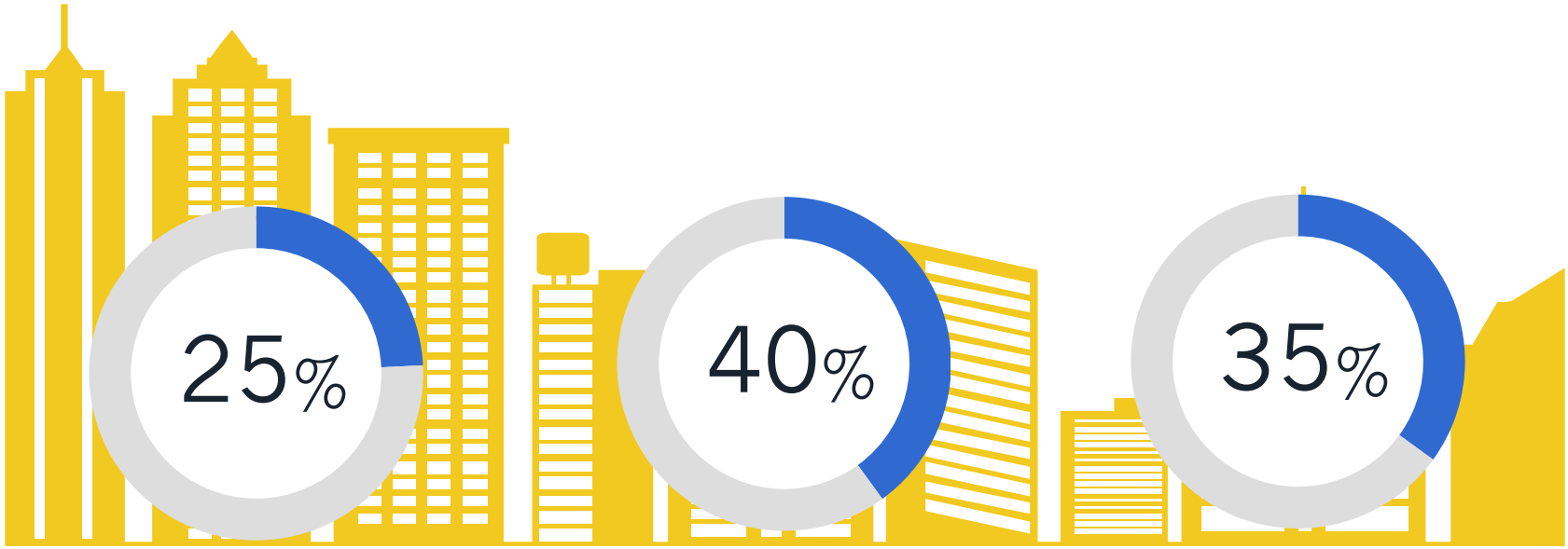
Survey Respondents, Top Industries Responding

1. Financial Services
2. Manufacturing
3. Government
4. Education
5. Healthcare

Survey Respondents by Geographic Presence



Survey Respondents by Size of Organization



Large Enterprise

10,001+ Employees

Medium Enterprise

1,001 to 10,000 Employees

Small Enterprise

1 to 1,000 Employees

OCEG's GRC Standards Library

OCEG's GRC Standards Library helps to jump-start and improve your approach to achieving Principled Performance.

Standards

GRC Assessment Tools (Burgundy Book) 3.0

Assurance

Standards

GRC Capability Model 3.0 (Red Book)

Capability Model, Compliance, Governance, Principled Performance, Risk, Strategy

Standards

Modelo de Capacidad de GRC Versión 3 (Red Book)

Capability Model, Compliance, Governance, Principled Performance, Risk, Spanish, Strategy

Guides, Standards

GRC-XML Spec and Schema

Compliance, Governance, Information Technology, Risk

OCEG's GRC Certification, Surveys & Illustrations

OCEG has a range of resources that help organizations understand, apply, and communicate Principled Performance and GRC.

Certifications

GRC CERTIFY PROFESSIONAL — GRCP CERTIFICATION

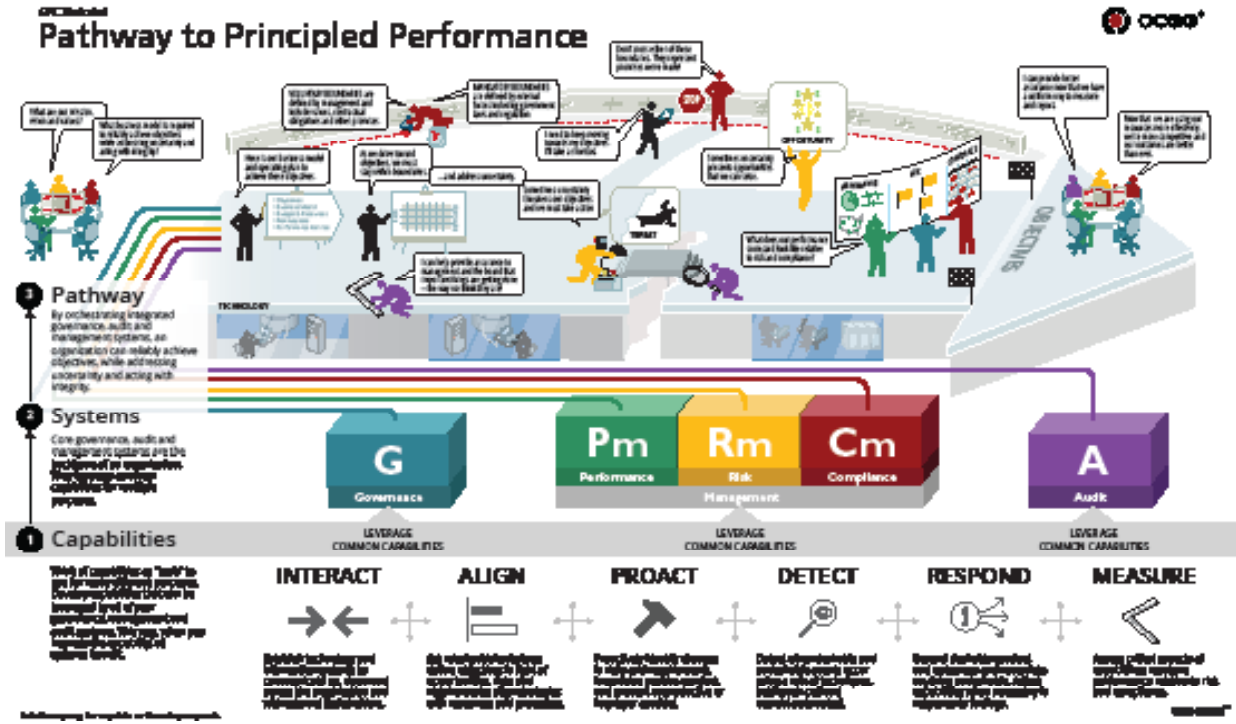
GRC CERTIFY AUDITOR — GRCA CERTIFICATION

Surveys

- OCEG One-Minute Polls
- GRC Maturity
- GRC Metrics & Measurement
- GRC Technology Strategy

GRC Illustrated

OCEG has developed over 60 GRC illustrations that are info-graphics to help organizations understand and communicate Principled Performance and GRC.



OCEG's GRC Solutions Council and Executive Council Members

Members of OCEG's GRC Solutions and Executive Council collaborate to develop educational materials on the benefits of advancing GRC processes and technologies, as well as key resources to assist companies in maturing GRC strategy.

EXECUTIVE & SOLUTIONS COUNCIL MEMBERS

Contact us

www.OCEG.org

4835 E. Cactus Road, Suite 225
Scottsdale, Arizona 85254
United States of America

info@OCEG.org
@OCEG
+1 (602) 234-9278