

Concurrent Session: Risk Management Issues

Thursday, March 23rd

1:45pm – 3pm

La Quinta Resort & Club, La Quinta, California

Moderator:

Joann Cangelosi, Partner, Grant Thornton LLP

Panelists:

Lawrence Jones, Audit Committee Chair, Cole Credit
Property Trust

Oliver Schmidt, Chief Audit Executive, QTS Realty Trust,
Inc.

Ari Schwartz, Director-Cybersecurity Services, Venable
LLP

© Copyright 2017

National Association of Real Estate Investment Trusts ®

This material is provided by NAREIT and REITWise 2017 panelists for informational purposes only, and is not intended to provide, and should not be relied upon for, legal, tax or accounting advice.

QUESTIONS ON NON-GAAP MEASURES

A TOOL FOR AUDIT COMMITTEES

Outside the audited financial statements, company presentation of measures that do not conform to Generally Accepted Accounting Principles (GAAP) has increased in recent years. While non-GAAP measures can be useful to enhance analyst and investor understanding of a company and its performance, care must be taken to foster compliance with the regulations and guidance from the Securities and Exchange Commission (SEC). The SEC has established regulations specific to the presentation of non-GAAP measures in SEC filings and other company communications to investors, such as earnings releases.

In May 2016, the SEC staff updated its compliance and disclosure interpretations (C&DIs)¹ on these regulations.² This guidance followed public statements made by various senior SEC staff members. In May 2016, for example, SEC Deputy Chief Accountant Wesley R. Bricker noted that “company practices related to non-GAAP measures have caused concern.”³ Bricker also stated “audit committees should pay close attention to the non-GAAP measures a company presents, including the required related disclosures and processes it follows to consider both the appropriateness and reliability of the measures.”⁴

In this policy context, there is an opportunity for audit committees to take a renewed look at their company’s presentation of non-GAAP measures. The Center for Audit Quality (CAQ) has developed this publication—based on existing SEC rules and further informed by the updated C&DIs—to assist audit committees in this heightened scrutiny. The dialogue resulting from the questions in the publication will help refresh an audit committee’s

understanding of how management is following SEC regulations, and understanding management’s purpose in presenting a non-GAAP measure, why it is being used, and whether it is reasonable and consistent.

Non-GAAP financial measures are specifically defined in the SEC regulations,⁵ and it is important to note that not all non-GAAP information presented by companies will meet the definition of a non-GAAP financial measure. While this publication focuses on questions to ask that are specific to non-GAAP financial measures, the spirit of these questions could also be useful in evaluating other non-GAAP information that does not meet the SEC definition of non-GAAP financial measures, but may be relevant to the audit committee’s understanding of the overall communications to investors relative to the company’s performance.

This publication is not meant to provide an all-inclusive list of questions or be seen as a checklist. Rather, it provides examples of the types of questions audit committees may ask of management and external auditors. Non-GAAP measures and other non-GAAP information presented will vary from company to company and industry to industry, and therefore each discussion will be unique and specific to the individual company. By providing sample discussion questions regarding transparency, consistency, and comparability of non-GAAP measures, the CAQ hopes to assist audit committees in asking questions to help determine: (1) that management is complying with the SEC rules and related interpretations to non-GAAP measures, and (2) that non-GAAP measures are aiding analysts and investors in understanding the business and its performance. Where applicable, individual questions include a footnote with reference to the related C&DIs that provides more guidance or additional questions to consider related to that particular question.



**CENTER
FOR AUDIT
QUALITY**

TRANSPARENCY

Non-GAAP measures should be presented to supplement the GAAP measures, and their purpose and calculation should be clear to investors. Non-GAAP measures included in filings with the SEC (e.g., Forms 10-K, 10-Q), or furnished to the SEC (e.g., press releases) should be clearly labeled as non-GAAP and not given any more prominence

than their closest GAAP measures.⁶ Non-GAAP measures should supplement, not supplant, the GAAP measures. The following questions may help audit committees address the transparency of the company's non-GAAP disclosures or whether improvement may be needed.

1 What is the purpose of the non-GAAP measure? Would a reasonable investor be misled by the information?

2 Has the non-GAAP measure been given more prominence than the most directly comparable GAAP measure? For example, an earnings release headline or caption that may present a non-GAAP measure without the comparable GAAP measure.⁷

3 How many non-GAAP measures have been presented? Is this necessary and appropriate for investors to understand performance?

4 Why has management selected this particular non-GAAP measure to supplement GAAP measures that are already established and consistently applied within its industry or across industries?

5 Does the company's disclosure provide substantive detail on the purpose and usefulness of the non-GAAP disclosure for investors?

6 How is the non-GAAP measure calculated? Does the disclosure clearly and adequately describe the calculation, as well as the reconciling items between the GAAP and non-GAAP measure?

7 How does management use the measure, and has that been disclosed? For example, is the measure linked to executive compensation?

8 Is the non-GAAP measure sufficiently defined and clearly labeled as non-GAAP? Could the title or description of the measure be confused with a GAAP measure?

9 Are any of the "per-share" non-GAAP measures in substance per-share non-GAAP liquidity measures, which are prohibited, or could they be used as liquidity measures even if disclosed as a performance measure?⁸

10 What are the tax implications of the non-GAAP measure? Does the calculation align with the tax consequences and the nature of the measure (i.e., performance vs. liquidity)?⁹

11 Does the company have material agreements, like a debt covenant, that require compliance with a non-GAAP measure? Does the company disclose that?¹⁰

CONSISTENCY

According to a 2014 survey conducted by the University of Washington and the University of Georgia, 27 percent of companies disclosed non-GAAP earnings that excluded one-time losses but did not report adjusted figures for one-time gains.¹¹ Audit committees should consider

asking questions of management to determine whether non-GAAP measures are consistent indicators that provide accurate insight into a company's performance—and not calculations solely aimed at showing the company in a favorable light.

1 Are the non-GAAP measures presented by the company balanced? Do the measures eliminate similar items that affect both revenue and expense, or do they only eliminate one or the other?

2 Has the company presented this measure before? Has the company stopped presenting certain measures?

3 Has the method or nature of the inputs to the calculation changed since the last time presented? If so, why and have the comparable periods been revised consistently?

4 If the calculation has changed, are the changes adequately described? Is there a need to revise prior period measures for consistency and to avoid a potentially misleading presentation? Would they have been materially different such that the prior period calculations should be revised?¹²

5 Is there a correlation between what the measure presents, and the company's actual results? For example, if a non-GAAP measure presents positive growth, does that correlate with the GAAP results of the company? If not, have those differences been clearly communicated to investors?

6 Have items characterized as nonrecurring, infrequent, or unusual occurred in the past two years? Are these items not reasonably likely to recur again in the next two years?¹³

COMPARABILITY

There is no authoritative framework that defines the calculation of each non-GAAP measure. This enables the non-GAAP measure calculations to be tailored from one company to the next. The more tailored the calculation, the less comparable the measure may be across

an industry. The less comparable the measure, the more confusing it may be to investors. Audit committees could consider asking the following questions to promote comparability of the non-GAAP measures presented.

1 Do other companies present this measure or similar measures? If not, why is this measure important for this company but not its peers?

2 Is management aware of differences in their calculation compared to other companies? Why are the calculations different?

3 If there are differences from peers, is the disclosure transparent about how the measure is calculated differently than peers?

4 Have any industry groups defined standard calculations that companies within the industry could follow in order to present more comparable measures to investors?

OTHER IMPORTANT QUESTIONS

Several procedural questions apply to all three categories—transparency, consistency, and comparability—set forth above.

1 Who in management is responsible for the oversight of non-GAAP measures? Does management maintain a policy on non-GAAP measures? Does that policy address the calculation, presentation, and disclosure of these measures?

2 Has the disclosure committee reviewed the non-GAAP measures?

3 What is the source of the information used in the calculation? Are there adequate controls and oversight in place over both the calculation and disclosure of the measure?¹⁴

4 How has management involved legal counsel on presentation and usage of non-GAAP measures and their compliance with SEC regulations?

5 Has management monitored SEC speeches and comment letters regarding non-GAAP measures and considered those in making its own presentation?

6 Is management aware of any others in the industry who have received an SEC comment letter about a particular non-GAAP measure, and, if so, have they considered that in reference to their disclosures as applicable?

7 Has internal audit been involved with non-GAAP measures? What feedback have they given management?

THE AUDITOR'S ROLE

SEC rules prohibit the presentation of these measures in the audited financial statements on which the auditor provides an opinion. However, they are often included in other areas of the annual and quarterly filings, such as in Management's Discussion and Analysis. Public Company Accounting Oversight Board (PCAOB) standards require auditors to read and consider other information included in documents that contain annual or interim financial statements. The rules refer to this additional information as "other information." According to current PCAOB standards, the auditor is required to read the other information for material inconsistency with the financial statements, but is not required to perform any other procedures over this information in situations where no inconsistencies are identified. Non-GAAP information

is also presented in information not filed with SEC for which the auditor has no responsibility (e.g., press releases, earnings presentations).

The auditor's role with company performance measures, including non-GAAP measures, under current PCAOB standards was a topic of conversation at the PCAOB's Standing Advisory Group (SAG) meeting in May 2016.¹⁵ This discussion highlighted that some users may have a misunderstanding about the level of auditor involvement with non-GAAP measures. It was noted that in certain situations, at the direction of the audit committee or management, auditors may perform additional procedures over these measures.

As such, audit committees should ask the following: What level of involvement do the auditors have with the company's non-GAAP measures? What feedback have they given management?

CONCLUSION

These questions are meant to spark a dialogue among audit committees, management, and auditors on the non-GAAP measures presented by companies. While no one question is a silver bullet, collectively they can assist audit committees in assessing whether the information presented to investors is meaningful and not confusing or misleading.

APPENDIX: DEFINITIONS

COMPANY PERFORMANCE METRICS

These metrics consist of non-GAAP financial and other metrics and information presented by companies in their SEC filings, press releases, conference calls, and other information distributed by the company.

NON-GAAP FINANCIAL MEASURES

The SEC defines a non-GAAP financial measure, often referred to as a non-GAAP measure, as a numerical measure of a registrant's historical or future financial performance, financial position, or cash flow that (i) excludes amounts, or is subject to adjustments that have the effect of excluding amounts, that are included in the most directly comparable measure calculated and presented in accordance with GAAP in the statement of income, balance sheet, or statement of cash flows (or equivalent statements) of the issuer; or (ii) includes amounts, or is subject to adjustments that have the effect of including amounts, that are excluded from the most directly comparable measure so calculated and presented.¹⁶ A common example might be earnings before interest, taxes, depreciation and amortization (EBITDA).

As previously noted, the SEC recognizes that the use of non-GAAP financial measures may be useful to investors and has established regulations specific to the presentation of non-GAAP financial measures in SEC filings and other company communications to investors, such as earnings releases. The spirit of these regulations is that the non-GAAP measure should be a relevant and meaningful measure that does not mislead investors. A non-GAAP financial measure should supplement, not supplant, the GAAP measures presented. These rules require that non-GAAP financial measures be clearly labeled as non-GAAP and not be presented more prominently than the GAAP measure.

OTHER NON-GAAP INFORMATION

Companies could choose to present other information to investors that is not defined or directly determined under GAAP related to the strategic focus and future orientation of the company. Some of this information may be measures or metrics that do not meet the definition of a non-GAAP financial measure. These measures could include performance metrics, key performance indicators (KPIs), and other financial measures. Examples of these metrics include unit sales, number of subscribers, and number of advertisers. Other examples include metrics that are calculated using amounts partially derived from GAAP numbers (e.g., same store sales, revenue per subscriber). However, some of this non-GAAP information, such as integrated reporting or sustainability reporting, may not be a metric.

NOTES

- ¹ See the C&DIs released by the SEC on May 17, 2016 <http://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ² The SEC rules applicable to non-GAAP disclosures are Regulation G and Item 10(e) of Regulation S-K. Regulation G is applicable to all non-GAAP financial measures included in public disclosures made by registrants with any shares registered under the Securities Exchange Act of 1934 (Exchange Act) or is required to file reports pursuant to the Exchange Act. Item 10(e) is applicable to any filing with the SEC under the Securities Act of 1933 (Securities Act) and/or the Exchange Act. Additionally, item 2.02 of Form 8K also has non-GAAP requirements.
- ³ Wesley R. Bricker, "Remarks Before the 2016 Baruch College Financial Reporting Conference" (speech, New York, New York), Securities and Exchange Commission, <https://www.sec.gov/news/speech/speech-bricker-05-05-16.html>.
- ⁴ Ibid 3.
- ⁵ See appendix for definition per the SEC regulations.
- ⁶ See question 102.10 of the C&DIs for 1) Guidance on information "furnished" to the SEC and 2) examples of non-GAAP disclosures that the staff would consider to be more prominent <https://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ⁷ Ibid.
- ⁸ Non-GAAP liquidity measures are prohibited from being presented on a per-share basis; See question 102.05 of the SEC's C&DIs: <https://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ⁹ Adjustments to arrive at non-GAAP should not be shown net of tax, but as separate components. See C&DI question 102.11 <https://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ¹⁰ See question 102.09 of the C&DIs <https://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ¹¹ Dave Michaels. "SEC Cracks Down on Novel Earnings Measures That Boost Profits," *Wall Street Journal*, April 26, 2016. Accessed May 24, 2016. <http://www.wsj.com/articles/sec-cracks-down-on-novel-earnings-measures-that-boost-profits-1461870107>.
- ¹² See question 100.02 of the C&DIs <https://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ¹³ See question 102.03 of the C&DIs <https://www.sec.gov/divisions/corpfin/guidance/nongaapinterp.htm>.
- ¹⁴ Note that a benefit of the Committee of Sponsoring Organizations (COSO) 2013 *Internal Control — Integrated Framework* is the ability to expand the application internal control beyond financial statement reporting. http://www.coso.org/documents/990025p_executive_summary_final_may20_e.pdf.
- ¹⁵ See link to materials from PCAOB SAG meeting May 18-19, 2016: <https://pcaobus.org/News/Events/Pages/SAG-meeting-May-2016.aspx>.
- ¹⁶ See Item 10(e)(2) of Regulation S-K, 17 CFR 229.10(e)(2) and Item 101 of Regulation G, 17 CFR 244.101.

ABOUT THE CENTER FOR AUDIT QUALITY

The CAQ is an autonomous public policy organization dedicated to enhancing investor confidence and public trust in the global capital markets. The CAQ fosters high quality performance by public company auditors, convenes and collaborates with other stakeholders to advance the discussion of critical issues requiring action and intervention, and advocates policies and standards that promote public company auditors' objectivity, effectiveness and responsiveness to dynamic market conditions. Based in Washington, DC, the CAQ is affiliated with the American Institute of CPAs.

Cybersecurity: How CPAs and their Firms Are Addressing a Dynamic and Complex Risk



CPAs and their public accounting firms are fostering a conversation to drive a market-based solution to evaluating cybersecurity risk management programs. This solution is intended to enhance public trust in the effectiveness of a company's cybersecurity risk management program.

Evolving Cybersecurity Risks

Awareness continues to grow around the evolving cybersecurity threats to companies. Given the immense scale and complexity of the cybersecurity challenge, every sector of the global economy must do their part to promote cybersecurity resilience.

The public accounting profession is in a strong position to play an important role in fostering instructive conversations about cybersecurity risk management, bringing to bear the CPA's core values—including independence, objectivity, and skepticism—as well as the profession's deep expertise and skills in providing independent evaluations in a variety of contexts.

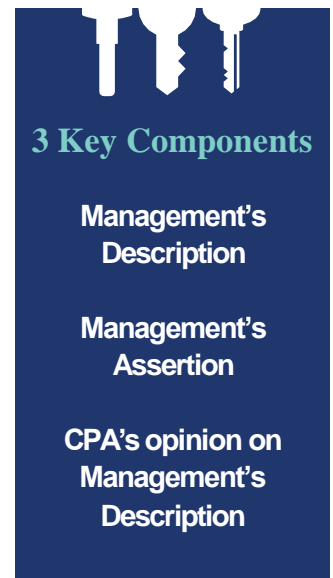
A Comprehensive Approach to Addressing Cybersecurity Risk Management Programs

Entity-Level Cybersecurity Reporting Framework

In response to growing challenges related to cybersecurity risk management, the American Institute of CPAs (AICPA)¹ is developing a reporting framework that organizations can use to communicate useful information about their cybersecurity risk management program to a broad range of stakeholders. The entity-level reporting framework has three key components that can be used to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of their organization's cybersecurity risk management program. The development of a reporting framework springs from the public accounting profession's commitment to continuous improvement, public service, and increasing investor confidence. The profession is working to provide a common approach for evaluating cybersecurity risk management that could enhance public trust in the effectiveness of a company's cybersecurity risk management program. The approach will be voluntary, flexible, and comprehensive.

There are three key components of the reporting framework that can assist stakeholders in understanding an entity's cybersecurity risk management program.

- ▶ **Management's Description** of the entity's cybersecurity risk management program. This management prepared narrative description is designed to provide potential users with information about the entity's operations, how the entity identifies its sensitive information and systems, the ways in which the entity manages the cybersecurity risks that threaten it, and a summary of controls implemented and operated to protect the information and systems against those risks. Management's Description is intended to provide the context needed to understand the conclusions expressed by management in its assertion, and by the auditor in its report, about the effectiveness of the controls included in the entity's cybersecurity risk management program.



Cybersecurity: How CPAs and their Firms Are Addressing a Dynamic and Complex Risk

- ▶ **Management’s Assertion** Management will also assert to the presentation of their management description, and that the controls implemented as part of the cybersecurity risk management program are effective to achieve the entity’s cybersecurity objectives.
- ▶ **CPA’s opinion** on the description of the entity’s cybersecurity risk management program (i.e. completeness and accuracy) and the effectiveness of the controls within the program to achieve the entity’s cybersecurity objectives.

Independent Examination

The public accounting profession believes that when an entity provides information to stakeholders—such as the board of directors or audit committees—to enable decision making, it is not enough to provide them merely with information. Decision makers need confidence that the information they have been provided is fairly presented. The third component described above in the AICPA’s approach to a cybersecurity risk management program framework, the CPA’s opinion, is the component that can enhance confidence that Management’s Description is fairly presented. CPAs will perform a cybersecurity risk management program examination (“examination”) in order to provide an opinion on Management’s Description and on the effectiveness of the controls implemented as part of the cybersecurity risk management program.

The CPA Firm’s Role in Cybersecurity Risk Management

Today, four of the leading 10 information security and cybersecurity consultancies are CPA firms. Many CPA firms have built substantial cybersecurity practices and capabilities that enable them to advise companies in all aspects of cybersecurity risk management. If CPA firms choose to perform the examination for companies, CPAs will work in collaboration with individuals at their firms who also have credentials related to information technology and security, often in addition to their CPA. These include: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), and Certified Information Technology Professional (CITP). Cybersecurity expertise and an understanding of controls will be required to complete the examination, and both are present in CPA firms. As multidisciplinary firms, CPA firms routinely provide a diverse range of services, beyond the financial statement audit.

CPA firms also have quality control systems in place to monitor their engagement teams’ adherence to professional standards, and are subject to oversight by the profession through peer reviews, further ensuring that quality of the services delivered.

Potential Benefits of the Proposed Cybersecurity Risk Management Framework

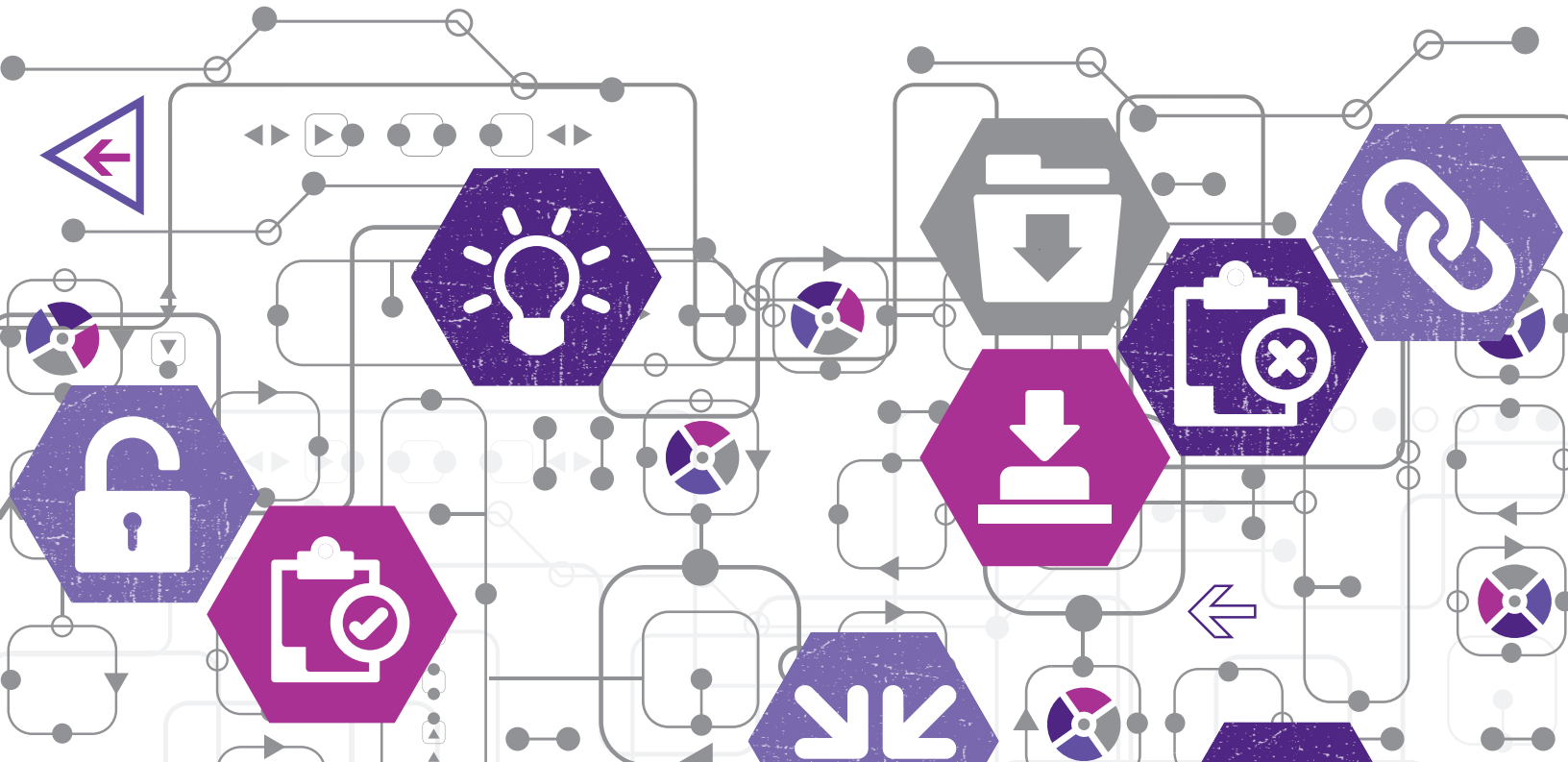
There are a number of potential benefits to a market-based solution to evaluating a company’s cybersecurity risk management program. They include:

- ▶ **Flexibility**—Companies, even within the same industry, are not identical. As designed, the proposed examination will be voluntary and principles-based. This flexible approach will provide companies and stakeholders with an evaluation of their cybersecurity risk management program in a manner tailored to their particular situation, and the evolving cybersecurity threats they face.
- ▶ **Common approach**—A common and consistent approach, once established and accepted in the market, could potentially reduce industry and other regulatory compliance requirements that can (1) distract company resources away from cybersecurity risk management and (2) burden companies with checklist compliance exercises that are typically ineffective responses to advancing data security threats. Widespread market acceptance of the examination could aid in establishing a uniform, cross-industry approach to evaluating a company’s cybersecurity risk management program
- ▶ **Innovative and sustainable solution**—The AICPA plans to adapt and advance the examination according to feedback from users in the marketplace, with an emphasis on identifying opportunities to enhance efficiency and reduce compliance burdens.

¹ The AICPA’s mission is to power the success of global business, CPAs, CGMAs and specialty credentials by providing the most relevant knowledge, resources and advocacy, and protecting the evolving public interest. The AICPA develops standards for audits of private companies and other services performed by CPAs.

Balancing risk with opportunity in challenging times

Governance, Risk and Compliance Survey 2016





Contents

- 3** Executive summary
- 4** GRC awareness and management trends
- 6** Risk capabilities and effectiveness
- 9** Application of data analytics and technology to GRC activities
- 12** Use of third parties
- 14** GRC roles and skills
- 17** Call to action: Opportunities for GRC leaders to add value
- 18** About the survey

Executive summary

Leaders everywhere face increasing risks for their organizations. These risks come from all directions — regulatory, cybersecurity, financial, global competition, litigation, etc. — and put every leadership position on the front lines of risk management. But not all risks are created equal. And not all organizations or executives have the same appetite — or tolerance — for these risks.

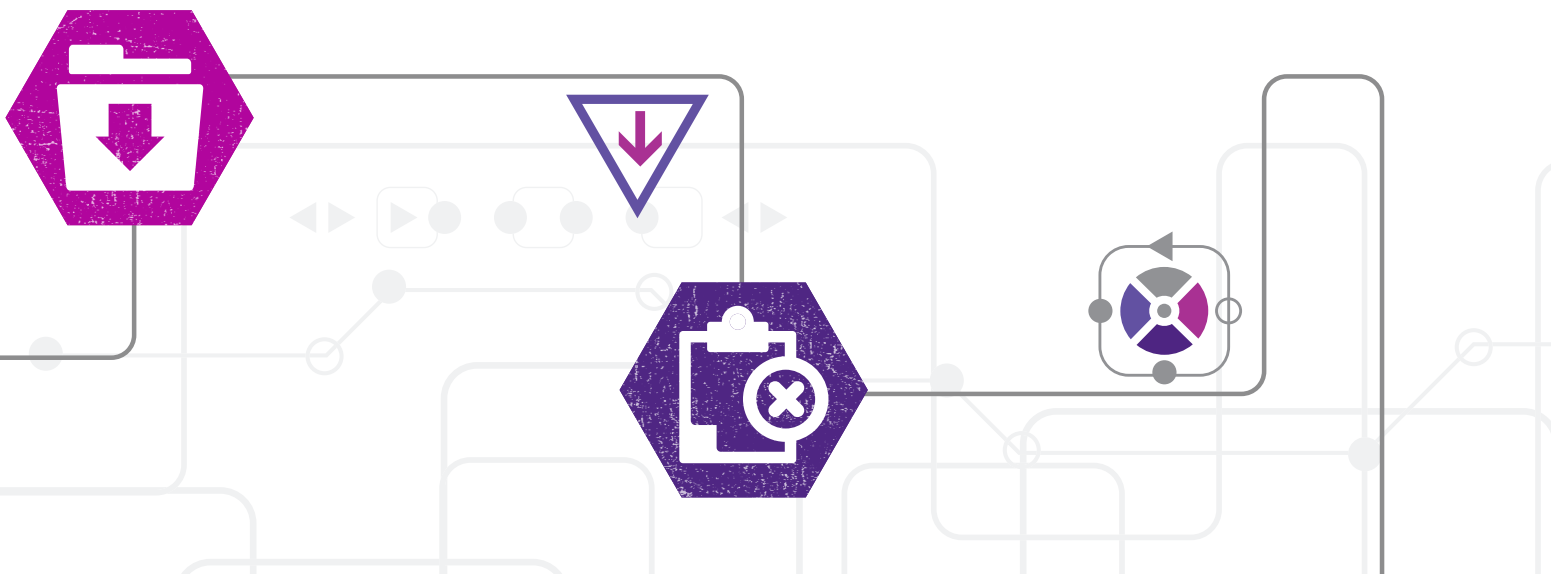
Balancing risks versus opportunities, or proactively viewing risk as a driver of opportunity, is a key component of 21st-century strategic planning. Successful leaders will evaluate and implement risk management approaches that add strategic value to their organizations while prudently managing risks, thereby maintaining and enhancing competitive advantage.

To help executives plan for 2017 and beyond, Grant Thornton LLP deployed the *Governance, Risk and Compliance (GRC) Survey* earlier this year. It's important to note that GRC typically isn't a specific organizational department, but instead is a collaboration among many roles and functions (e.g., legal, internal audit, audit committee, finance, compliance). The *GRC Survey* assessed the management of GRC activities and processes across these roles and functions. This required input from a range of titles and builds upon the research we conducted on internal audit and general counsel roles in recent years.

Major findings include:

- Strategic risks are rated as highly significant, yet GRC leaders are not focusing time and budgets on them in order to measure and mitigate these risks.
- Many organizations say their GRC maturity levels are ad hoc or fragmented; these organizations have great opportunity to make changes to improve their levels.
- GRC leaders have not embraced the application of data analytics and technologies to GRC activities despite the benefits of these tools.
- Third-party risks are still a threat, but other priorities have taken precedence over risk management activities.

Grant Thornton LLP is committed to helping executives and their organizations identify, prioritize, manage and monitor risks. Leaders can leverage this survey to optimize GRC activities and investments, and prepare for events commensurate with their organizations' appetites for risk.



GRC awareness and management trends

A majority of executives are concerned about general (e.g., compliance, financial) and business-specific risks, including regulatory, cybersecurity, IT, market and competitive threats. Yet despite executives' concerns, their ability to monitor, measure and mitigate these risks falls short (Figure 1). For example, although 60% of executives report that cybersecurity risk is significant, only 43% measure and monitor it effectively — and just 46% are effective at mitigation.

Oddly enough, many risks that don't particularly worry executives (e.g., tax, litigation) receive substantial management attention. Leaders may want to review how GRC resources are deployed, to:

- Balance investment versus threat levels
- Share practices and resources from areas that are currently effective with those in need of assistance
- Coordinate risk perspectives throughout the organization (i.e., minimize siloed application of risk management)

- Confirm that risks are rated appropriately, and receive corresponding levels of monitoring and awareness
- Compare risk practices and performance metrics versus industry benchmarks

Strategic risk was rated the highest in significance of the general risks, yet executives rated effective measurement, monitoring and mitigation of strategic risk as the lowest. This suggests that GRC resources can do more to assist management and the board in assessing the appropriateness of the organization's strategy and the risks to achieving its underlying strategic objectives.

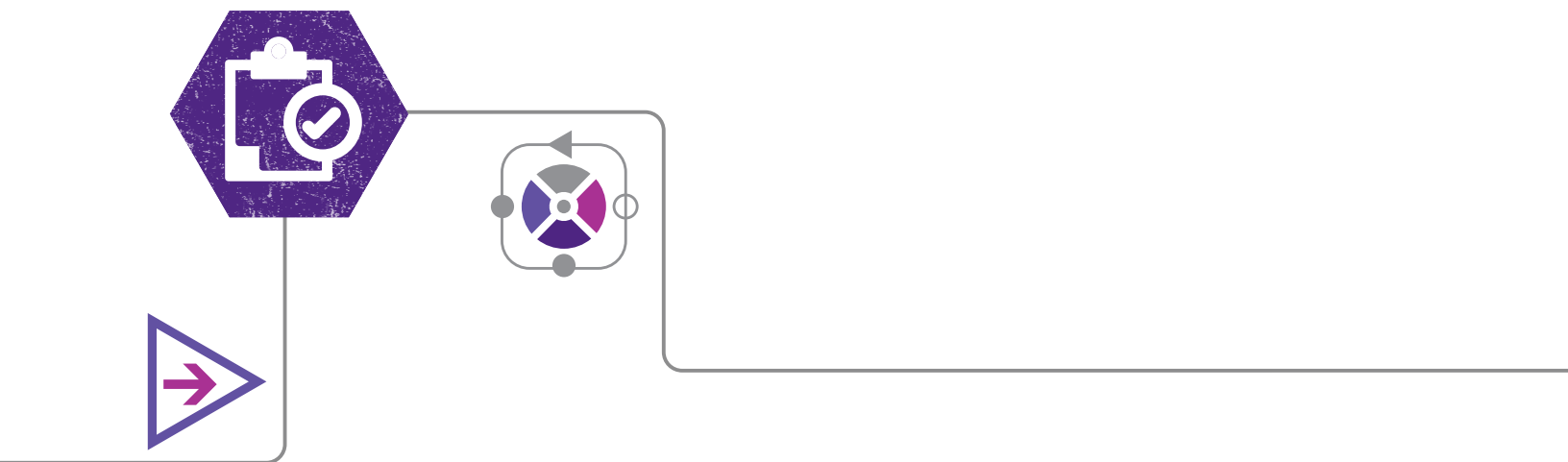
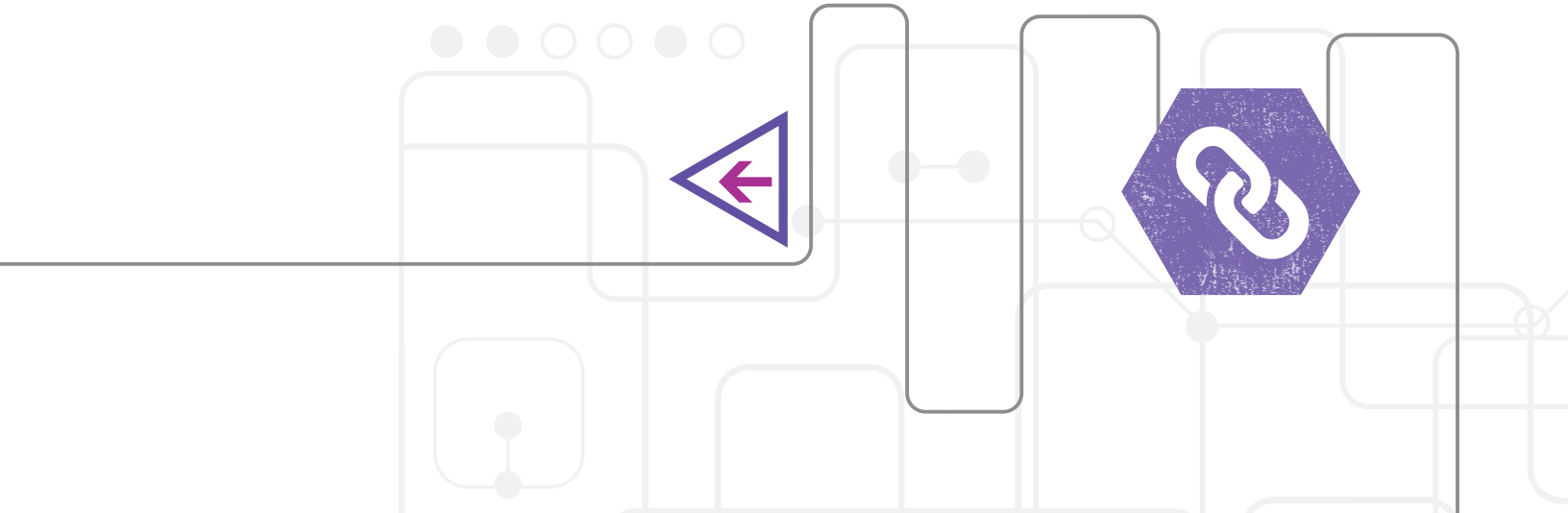


Figure 1
Risk concerns, measurements and mitigation

General risks	Significant risk level*	Effective measurement and monitoring**	Effective mitigation***
Strategic	64%	43%	50%
Compliance	59%	56%	65%
Operational	59%	50%	53%
Financial	55%	71%	71%

Business-specific risks	Risk	Measure and monitor	Mitigate
Regulatory	63%	60%	64%
Cybersecurity	60%	43%	46%
Market	52%	46%	42%
Competitive	50%	44%	41%
IT	50%	44%	47%
Liquidity/credit	30%	58%	60%
Third-party	28%	35%	38%
Fraud/anti-corruption	27%	45%	53%
Litigation	19%	43%	49%
Supply chain	18%	38%	40%
Global expansion	17%	27%	31%
Environmental	15%	36%	40%
Tax	13%	44%	52%

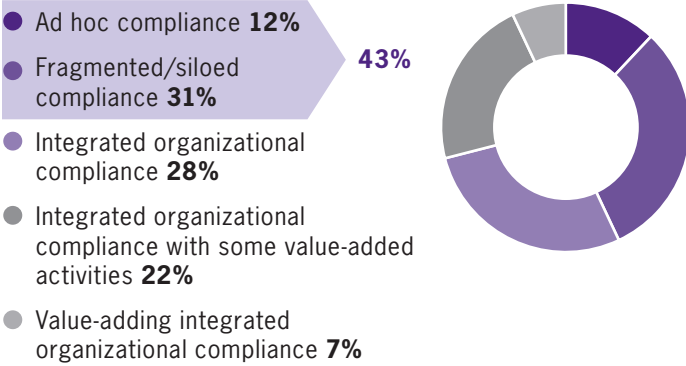
*Rate 4 or 5 on a scale of 1–5 where 5 = significant risk.
 **Rate 4 or 5 on a scale of 1–5 where 5 = highly effective at measuring and monitoring key risk indicators.
 ***Rate 4 or 5 on a scale of 1–5 where 5 = highly effective at mitigating risk.



Risk capabilities and effectiveness

The survey results show that 43% of respondents are operating compliance efforts at an ad hoc or fragmented/siloed maturity level (Figure 2). This group of respondents has the largest challenge to move along the maturity model curve to become a higher-functioning unit. It is important that organizations work toward a higher maturity of GRC activities, including compliance, by striving for more integration with various compliance and GRC functions in the organization, greater communication, data sharing, and knowledge sharing that is unified in a plan, with measurable and repeatable results over time.

Figure 2
Maturity level of governance, risk and compliance (GRC) activities



Some suggestions to improve maturity levels:

- Understand some of the limitations that are holding the organization in the lower levels of maturity.
- Create a plan about how the organization’s groups will focus on compliance and GRC, as well as how the organization taken as a whole will strive to coordinate and collaborate across functions.
- Measure progress against the plan and continuously make improvements.
- Benchmark against higher-performing organizations and learn from what works well elsewhere.
- Understand the appetite of management and the audit committee for greater collaboration, and sell the benefit of greater collaboration as foundational for greater risk coverage.
- Utilize technology more effectively to create broader views and data sharing.

48% spend just **5%** of total revenues or less on GRC activities

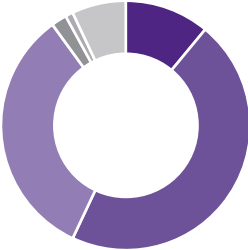
Organizations spend 12% of total revenue (average) on GRC activities. Spending levels vary widely across organizations: 48% spend just 5% of total revenues **or less** on GRC activities. Organizations generally increased their investments in GRC activities in 2015 versus 2014 (Figure 3).

GRC costs (by average percentage of GRC spending¹) are allocated to the following risks:

- Financial risks — 28%
- Compliance risks — 27%
- Operational risks — 20%
- Strategic risks — 13%

Figure 3
GRC investments — 2015 vs. 2014

- Increased significantly **11%**
- Increased somewhat **46%**
- Stayed the same **33%**
- Decreased somewhat **2%**
- Decreased significantly **1%**
- Not sure **7%**



These allocations generally correspond with organizational objectives for GRC activities (Figure 5). Yet operational risks seem to require investments that outweigh the level of worry they cause most executives. Looking again at strategic risk, the historically low percentage of GRC spending and low focus on strategic GRC activities (Figure 4) is concerning, as GRC organizations are trying to provide for strategic insight and value. There is a disconnection between wanting to provide more strategic insight and value regarding risk topics, and actually doing it. We saw in Figure 1 that strategic risk was rated the highest in significance of the general risks, yet executives rated effective measurement, monitoring and mitigation of strategic risk as the lowest. In addition, they aren't investing or focusing heavily on the area. GRC teams have an opportunity to become more strategic and add value. They need to focus, prioritize and invest to improve the results. Where investment is not possible, GRC leaders need to look at ways to streamline and reduce existing costs, thereby finding efficient and effective ways to maintain existing coverage and increase coverages that add value to the organization.

Figure 4
Focus of GRC activities

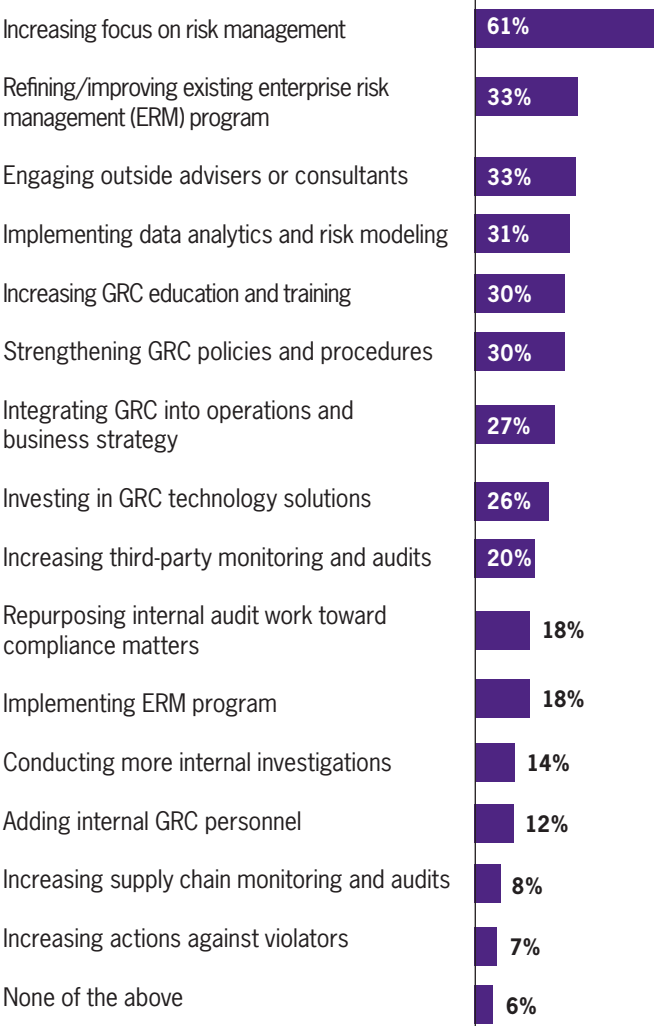
	2016	2015	2014	2013	2012	2011
Financial risks	3	2	3	3	4	4
Compliance risks	4	4	4	4	3	3
Strategic risks	1	1	1	1	1	1
Operational risks	2	3	2	2	2	2

Rated by importance with 4 = Most important, 1 = Least important.

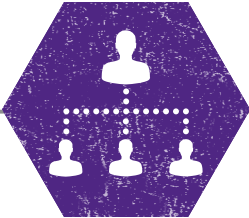
¹ Averages will not sum to 100% because some survey participants answered 0% for all risk categories.

Figure 5 provides those charged with managing and overseeing GRC prioritized activities to drive enhancement in GRC activities. While 61% say increasing focus on risk management is at the top, this can be viewed as a catch-all topic. Further down the list, greater levels of granularity become apparent. The additional top ways that organizations enhance GRC activities are refinement/improvement of enterprise risk management (ERM) programs, use of outside advisers or consultants, and use of data analytics, which will be discussed in the next section.

Figure 5
Steps to enhance GRC activities*



*Respondents were able to select more than one answer.



Application of data analytics and technology to GRC activities

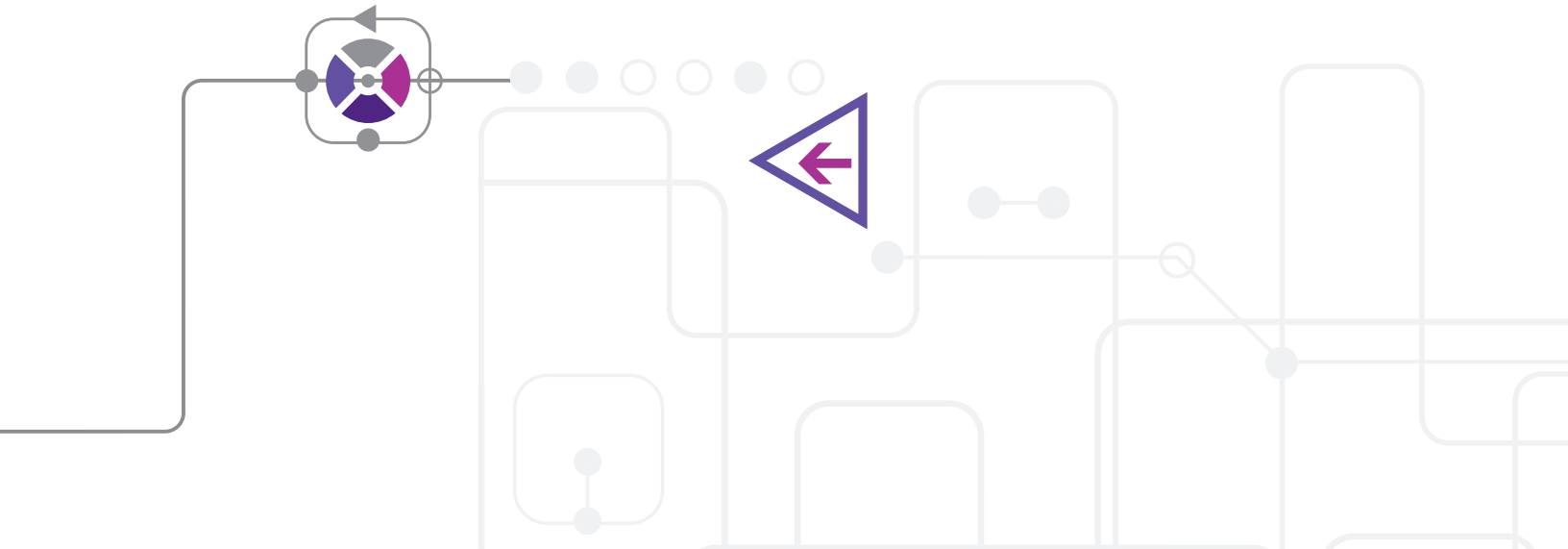
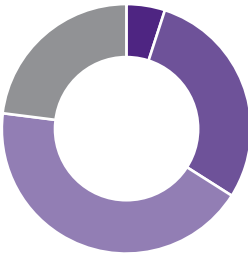
About one-third of organizations are implementing data analytics and risk modeling to enhance GRC activities. But the use of data analytics/business intelligence for GRC activities remains modest, and organizations have opportunities to do far more (Figure 6). Surprisingly, reliance on data analytics did not vary based on the size of the organization:

- Less than \$100 million revenue — 35% moderate or extensive use
- \$100 million to \$1 billion revenue — 35% moderate or extensive use
- \$1 billion or more revenue — 34% moderate or extensive use

The adoption of data analytics by GRC leaders is low, and recent research specific to internal auditors also shows its use has largely been limited. With benefits such as streamlining the audit process and reducing fieldwork time, data analytics has the ability to transform GRC activities. Grant Thornton partnered with The Institute of Internal Auditors Research Foundation to help audit executives learn how to develop a plan to capitalize on data analytics technology and resources. People, process and technology are discussed, in that order, along with supporting maturity models, to provide useful targets for improvement in the use of data analytics. Visit www.gt.com/data-analytics to learn more.

Figure 6
Reliance on data analytics/business intelligence for GRC activities

- Extensive use **5%**
- Moderate use **29%**
- Some use **43%**
- No use **23%**



Data analytics is most beneficial for mitigating common risks — financial, operational, and compliance/regulatory — but one in five organizations also uses it to seek business insights and identify GRC weaknesses (Figure 7). Unfortunately, many organizations fail to recognize the value of data analytics for improving GRC activities — improving efficiency or effectiveness — or are unaware of the strategic value of analytic insights. For example, few executives see benefit in using business intelligence to monitor third parties or suppliers, despite the dangers these risks pose to an organization’s operations, reputation and brand. GRC leaders must educate their executives to show the true value in utilizing technology for efficiencies in the process and the ability to be able to expand coverage to areas that are critical to the organization.

Fifty-seven percent of organizations use data analytics for performance measurement, up from 45% in 2015; 26% use it for predictive analytics; and 17% for forensic analysis, which is down from 2015 (Figure 8). Overall use of data analytics has improved as the response of *None* decreased from 37% to 28%. The data trend shows that higher-level uses of data analytics, such as measuring performance and predicting a future outcome, is becoming more popular. These are the data analytics applications that excite senior executives as well, because they can derive benefits from the extensive data within the company in a forward-looking way. Executives are seeing that data analytics will help organizations improve performance as a key driver. They are also utilizing data analytics in a preventive way, as opposed to using forensic analysis as an after-the-fact detection method.

Figure 7
Beneficial applications of data analytics*



*Respondents were able to select more than one answer.

Figure 8
Functions for which data analytics is used*

Function	2016	2015
Performance measurement	57%	45%
Predictive analytics	26%	22%
Forensic analysis	17%	25%
Other	3%	5%
None	28%	37%

*Respondents were able to select more than one answer.

Figure 9

Leverage of technology to mitigate risks

General risks	1 = no use of technology	2	3	4	5 = significant use of technology
Financial	5%	17%	33%	31%	14%
Operational	10%	16%	42%	23%	10%
Compliance	9%	25%	37%	23%	6%
Strategic	20%	29%	33%	15%	3%
Business-specific risks	1 = no use of technology	2	3	4	5 = significant use of technology
Cybersecurity	6%	13%	29%	33%	19%
IT	6%	13%	30%	34%	17%
Fraud/anti-corruption	14%	26%	37%	17%	6%
Regulatory	12%	19%	37%	27%	5%
Liquidity/credit	18%	23%	34%	20%	5%
Tax	21%	27%	34%	15%	3%
Market	17%	26%	36%	18%	3%
Competitive	21%	30%	33%	14%	2%
Third-party	24%	27%	36%	11%	2%
Litigation	27%	31%	33%	8%	2%
Supply chain	27%	26%	37%	8%	2%
Environmental	34%	29%	29%	7%	1%
Global expansion	38%	25%	28%	8%	1%

Almost half of companies are making good use of technologies for financial risk, the top target among general risks. Given the significance of strategic risk (Figure 1), there is opportunity to use technology to better manage strategic objectives. For business-specific risks, cybersecurity and IT risks get high attention via technology. Yet many other threats receive little technological attention (Figure 9).

Leveraging technologies to address business-specific risks correlates with the size of the organization. For example, larger organizations significantly deploy technologies to manage specific risks over their smaller counterparts:

- **Tax risk:** 25% of organizations with revenues of \$1 billion or more versus 11% of organizations with less than \$100 million in revenue
- **Third-party risk:** 20% versus 11%
- **Litigation risk:** 16% versus 4%
- **Supply chain risk:** 15% versus 9%

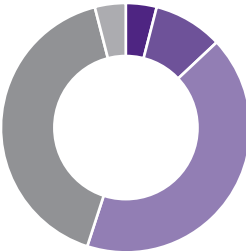
Use of third parties

Nearly all organizations participating in the *GRC Survey* conduct business with a third party (i.e., an individual or organization that is not a principal party to a legal transaction, unlike the role of a customer, supplier or contractor). A majority (60%) of these organizations maintain a comprehensive catalog/list of all third parties with which they conduct business, but 37% **don't** have a full roster of third parties.

Awareness of third-party risk is important, but proactive management is even more critical. Unfortunately, many organizations fail at this: 21% don't rate third parties by the risks they pose, and nearly half (41%) don't audit **any** of their third parties (Figure 10).

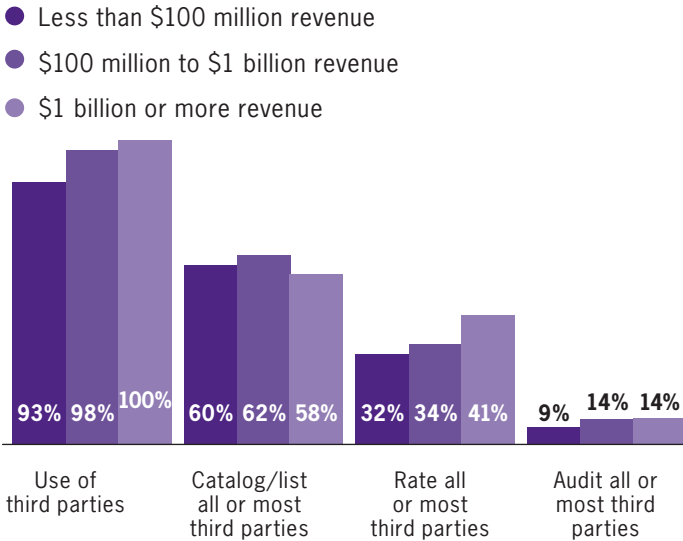
Figure 10
Third parties audited by the organization

- All third parties **4%**
- Most third parties **9%**
- Some third parties **42%**
- No third parties **41%**
- We do not conduct business with third parties **4%**



Rating and auditing of third parties gets a bit more attention among larger organizations, but even those firms — which also are more likely to be using third parties — still could be doing far more to protect themselves (Figure 11).

Figure 11
Third-party practices by organization size



Due diligence prior to a business relationship with a third party is the top way to manage third-party risk; yet one in 10 organizations takes **no steps** to manage third-party risk (Figure 12). Furthermore, the focus on third-party risk has decreased as the year-over-year data shows that overall efforts to manage these risks have dropped. GRC leaders are facing more pressing issues like cybersecurity, compliance costs, data analytics and others, with the result that third-party risk is perceived as having diminished significance.

Figure 12
Efforts to manage third-party risk*

- 2016
- 2015



*Respondents were able to select more than one answer.



Awareness of third-party risk is important, but proactive management is even more critical.

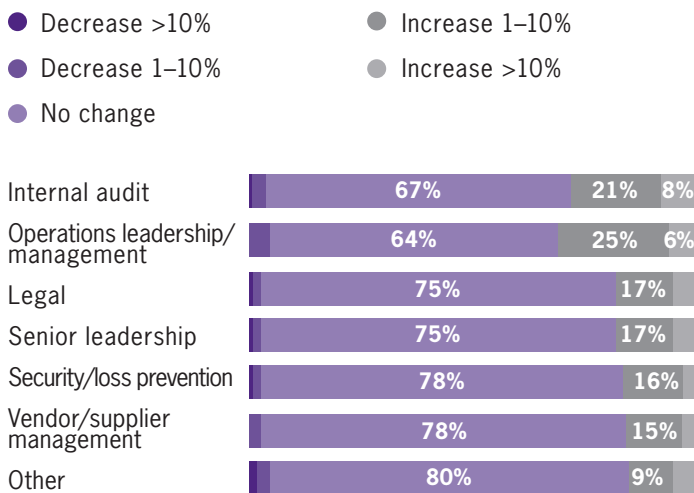
GRC roles and skills

Organizations have full-time employees (FTEs) in a variety of roles dedicated to GRC activities:

- Internal audit FTEs — 10 average
- Operational FTEs — 11 average
- Legal FTEs — 5 average
- Other FTEs — 8 average

Most GRC staff levels are likely to stay the same or increase in the next 12 months, with internal audit and operations leadership/management most likely to increase (Figure 13).

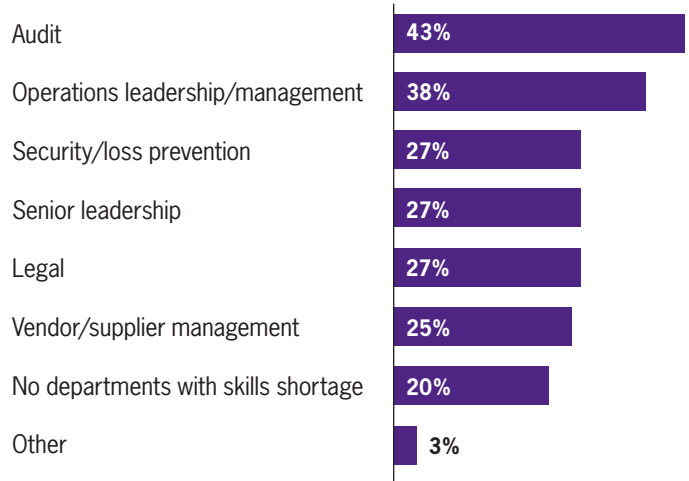
Figure 13
GRC staff level changes in next 12 months



Many executives cite skills shortages in their organizations for departments involved with GRC activities. Audit (43%) and operations leadership/management (38%) departments are most likely to experience skills shortages (Figure 14).

GRC leadership roles – chief compliance officer (CCO), chief audit executive (CAE), general counsel, chief risk officer, and similar – require unique skills and experiences; senior financial expertise, operations experience, audit experience and senior leadership experience are the top attributes for these roles (Figure 15).

Figure 14
Departments with skills shortages*



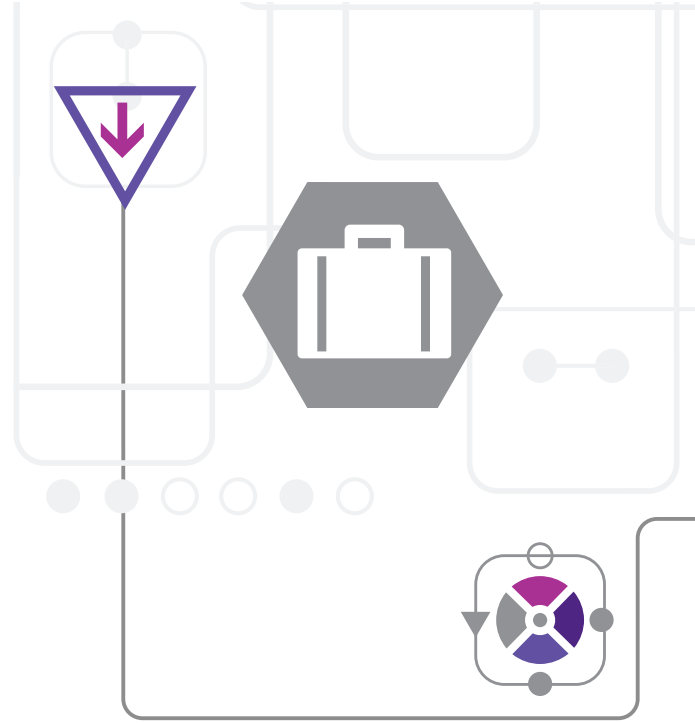
*Respondents were able to select more than one answer.

Figure 15

Skills and experiences critical for GRC leadership roles*



*Respondents were able to select more than one answer.



A majority of organizations have GRC leadership with extensive experience in addressing general risks (Figure 16). The challenge for GRC leadership will be to address the lack of experience in addressing strategic risk since it was rated high in significance. Also, many lack experience in managing business-specific risks, such as third-party, supply chain and environmental issues.

Figure 16

Organization's GRC leadership experience

General risks	1 = no experience	2	3	4	5 = significant experience
Financial	2%	7%	23%	36%	32%
Compliance	3%	6%	33%	33%	25%
Operational	4%	8%	33%	36%	19%
Strategic	4%	13%	37%	28%	18%
Business-specific risks	1 = no experience	2	3	4	5 = significant experience
Regulatory	3%	6%	28%	36%	26%
Liquidity/credit	7%	10%	31%	32%	20%
Litigation	7%	13%	35%	30%	15%
IT	5%	10%	37%	32%	15%
Market	6%	12%	40%	29%	13%
Cybersecurity	7%	12%	37%	32%	12%
Competitive	8%	13%	40%	29%	11%
Fraud/anti-corruption	6%	17%	41%	26%	10%
Tax	9%	17%	38%	26%	10%
Third-party	10%	18%	42%	24%	6%
Supply chain	17%	19%	37%	22%	5%
Environmental	20%	22%	37%	18%	4%
Global expansion	27%	18%	35%	17%	3%

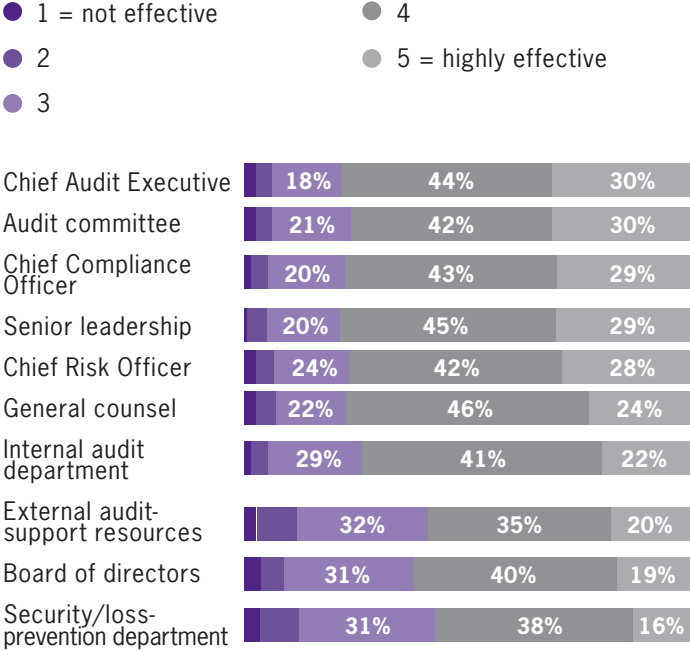
CAEs, the audit committee, the CCO, and senior leadership are most effective in mitigating risks. (Figure 17).

The roles and functions most likely to add value to GRC activities are:

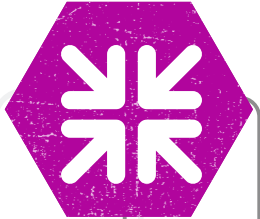
- Senior leadership — 69% of *GRC Survey* participants
- Audit committee — 51%
- Internal audit department — 47%
- CCO — 41%
- Board of directors — 37%
- General counsel — 37%
- CAE — 36%

Senior leaders and the audit committee rank high for both risk mitigation and their role in value-adding GRC activities. Other roles and functions, such as CAE and general counsel, are traditionally focused on monitoring and mitigation of risks, and may be viewed as less responsible for strategic, value-added activities.

Figure 17
Roles and functions that mitigate risks*



*Responses may not total 100% due to rounding.




Call to action: Opportunities for GRC leaders to add value

Today's corporate leaders are in business environments that are highly complex, increasingly competitive and ever-changing. They are faced with a broad array of risks that affect their businesses every day. It's an ongoing challenge for every organization to balance risk versus opportunity, one unique to every entity based on size, industry, location, experience, etc. But regardless of risk tolerance (or aversion), every organization should **add value** to its GRC activities.

Align risk management and strategic planning

The survey shows that the GRC costs (by average percentage of GRC spending) are allocated over 50% to financial and compliance risks and only 33% to strategic and operational risks. There needs to be a more balanced alignment where strategic and operational risk is getting the attention it needs to support its corporate leaders and the goals of their business. Senior leadership needs to better align risk management and the strategic-planning process. This allows better understanding of the business risks and for heavy risk management functions like internal audit to get a seat at the table. They will be able to exert more influence within the organization and monitor strategic risk as it relates to the ability to meet the organization's objectives.



There needs to be a more balanced alignment where strategic and operational risk is getting the attention it needs

Increase risk coverage efficiently

As businesses continue to be challenged, GRC professionals must find ways to not only cover their existing financial and compliance risks, but they must be able to increase their risk coverage across all facets of their organizations. They must consider how to reduce the overall costs of compliance in order to provide value on the strategic and operational side of their businesses. More organizations are moving toward an integrated approach to GRC (that is, looking for redundancies across the organizational platform in the GRC process, and aligning to a centralized or convergence approach to the overall GRC apparatus).

Use technology

Many GRC functions, such as internal audit, are moving to a digital technology-based strategy. This will only increase due to the varied use of technology, and the availability of more and more data captured and used by the organization. GRC leaders will take advantage of data analytics and data visualization to reduce time and costs, and mitigate common risks — financial, operational, and compliance/regulatory. A well-defined data analytics program could allow more time to be spent on strategic and operational risks. Organizations may struggle to initially implement data analytics or find qualified professionals. But the outcome of efficiency and effectiveness overall is clearly worth the upfront challenges.

A unified, proactive and consistent approach can build stronger risk management programs while improving the bottom line. Successful leaders will evaluate GRC approaches that add strategic value while managing risks, thereby improving competitive advantage.

About the survey

The Grant Thornton *Governance, Risk and Compliance Survey* was administered online in January and February 2016. The survey received 535 valid submissions from a mix of executive titles and roles familiar with GRC activities. Participants in the *GRC Survey* represented a range of organization types, sizes and industries in the United States.

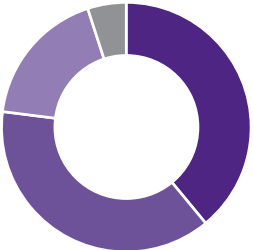
Revenue*

- Less than \$100 million **34%**
- Between \$100 million and \$500 million **23%**
- Between \$500 million and \$1 billion **14%**
- Between \$1 billion and \$5 billion **21%**
- More than \$5 billion **9%**



Organization type*

- Private **39%**
- Public/listed **38%**
- Not-for-profit **18%**
- Government **4%**



Title*

- CFO **18%**
- Chief Audit Executive or lead internal auditor **16%**
- Other internal audit title **13%**
- Board member, including audit committee and chairman **13%**
- Senior leadership title not listed **8%**
- President or CEO **5%**
- Chief Legal Officer, General counsel and in-house counsel **5%**
- Chief Compliance Officer **4%**
- Chief Risk Officer **3%**
- Other **14%**



Industry*

- Banking/financial institutions **32%**
- Technology **10%**
- Manufacturing **9%**
- Health care **9%**
- Not-for-profit **6%**
- Professional services **6%**
- Higher education **5%**
- Energy **3%**
- Real estate **3%**
- Retail **3%**
- Other **13%**



*Responses do not equal 100% due to rounding.

Offices of Grant Thornton LLP

National Office

Grant Thornton Tower
171 N. Clark St., Suite 200
Chicago, IL 60601
+1 312 856 0200

Alaska

Anchorage
+1 907 754 9200

Arizona

Phoenix
+1 602 474 3400

California

Irvine
+1 949 553 1600

Los Angeles
+1 213 627 1717

Sacramento
+1 916 449 3991

San Diego
+1 858 704 8000

San Francisco
+1 415 986 3900

San Jose
+1 408 275 9000

Colorado

Denver
+1 303 813 4000

Connecticut

Hartford
+1 860 781 6700

Stamford
+1 203 327 8300

Florida

Fort Lauderdale
+1 954 768 9900

Jacksonville
+1 904 446 4550

Miami
+1 305 341 8040

Orlando
+1 407 481 5100

Tallahassee
+1 850 201 7288

Tampa
+1 813 229 7201

Georgia

Atlanta
+1 404 330 2000

Illinois

Chicago
+1 312 856 0200

Oakbrook Terrace
+1 630 873 2500

Schaumburg
+1 847 884 0123

Kansas

Overland Park
+1 913 272 2700

Wichita
+1 316 265 3231

Maryland

Baltimore
+1 410 685 4000

Massachusetts

Boston
+1 617 723 7900

Westborough
+1 508 926 2200

Michigan

Detroit
+1 248 262 1950

Minnesota

Minneapolis
+1 612 332 0001

Missouri

Kansas City
+1 816 412 2400

St. Louis
+1 314 735 2200

Nebraska

Omaha
+1 402 513 5909

Nevada

Reno
+1 775 786 1520

Washington National Tax Office

1250 Connecticut Ave. NW, Suite 400
Washington, DC 20036
+1 202 296 7800

New Jersey

MetroPark
+1 732 516 5500

New York

Albany
+1 518 427 7762

Long Island
+1 631 249 6001

Manhattan
+1 212 599 0100

North Carolina

Charlotte
+1 704 632 3500

Raleigh
+1 919 881 2700

Ohio

Cincinnati
+1 513 762 5000

Cleveland
+1 216 771 1400

Oklahoma

Oklahoma City
+1 405 218 2800

Tulsa
+1 918 877 0800

Oregon

Portland
+1 503 222 3562

Pennsylvania

Philadelphia
+1 215 561 4200

Pittsburgh
+1 412 586 3800

Rhode Island

Providence
+1 401 214 4242

South Carolina

Columbia
+1 803 231 3100

Texas

Austin
+1 512 692 1200

Dallas
+1 214 561 2300

Houston
+1 832 476 3600

San Antonio
+1 210 881 1800

Utah

Salt Lake City
+1 801 415 1000

Virginia

Alexandria
+1 703 837 4400

McLean
+1 703 847 7500

Washington

Bellevue
+1 425 284 4454

Seattle
+1 206 623 1121

Washington, D.C.

Washington, D.C.
+1 202 296 7800

Wisconsin

Appleton
+1 920 968 6700

Madison
+1 608 257 6761

Milwaukee
+1 414 289 8200

Contacts

Warren Stippich

T +1 312 602 8499
E warren.stippich@us.gt.com

Michael Rose

T +1 215 376 6020
E michael.rose@us.gt.com

Bailey Jordan

T +1 919 881 2790
E bailey.jordan@us.gt.com

Priya Sarjoo

T +1 214 283 8166
E priya.sarjoo@us.gt.com

Shawn Stewart

T +1 949 608 5220
E shawn.stewart@us.gt.com

For more information, visit
grantthornton.com/grcsurvey

About Grant Thornton LLP

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world's leading organizations of independent audit, tax and advisory firms. In the United States, Grant Thornton has revenue in excess of \$1.3 billion and operates 58 offices with more than 500 partners and 6,000 employees. Grant Thornton works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations.

This content is not intended to answer specific questions or suggest suitability of action in a particular case. For additional information about the issues discussed, contact a Grant Thornton LLP professional.



Connect with us

 grantthornton.com

 [@granthorntonus](https://twitter.com/granthorntonus)

 [linkd.in/granthorntonus](https://www.linkedin.com/company/granthorntonus)

"Grant Thornton" refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the GTIL member firms provide audit, tax and advisory services to their clients, as the context requires. GTIL and each of its member firms are separate legal entities and are not a worldwide partnership. GTIL does not provide services to clients. Services are delivered by the member firms in their respective countries. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions. In the United States, visit grantthornton.com for details.



Cybersecurity Alert

February 27, 2017

AUTHORS

Ari Schwartz
Jami Mills Vibbert

New York's Department of Financial Services Finalizes Cybersecurity Requirements for Financial Institutions

RELATED PRACTICES

Privacy and Data Security
Banking and Financial Services Regulatory Risk and Compliance (RCOM)

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory **cybersecurity requirements** for financial services entities will become effective, with implementation to occur within 180 days (or by September 1, 2017). The requirements broadly cover all entities operating under or required to operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities. This not only includes state-chartered banks, licensed lenders, private bankers, service contract providers, trust companies, and mortgage companies, but also foreign banks licensed to operate in New York and any insurance company doing business in New York. It does exempt small companies, though, including those with fewer than 10 employees, less than \$5 million in gross annual revenue for three years, or less than \$10 million in year-end total assets.

RELATED INDUSTRIES

Cybersecurity Risk Management Services
Financial Services

The regulation delineates various minimum standards and requires a risk-based cybersecurity program tailored to each company's specific risk profile. Significantly, the regulation requires covered entities to file an annual certification of compliance with the regulation; Certifications of Compliance will commence February 15, 2018.

ARCHIVES

2017 2013 2009
2016 2012 2008
2015 2011 2007
2014 2010

As discussed in a **prior alert**, DFS proposed similar regulations on September 13 of last year, but that set of regulations elicited significant feedback. Still, the regulations require potentially significant changes and focus on cybersecurity for many institutions.

Requirements

Generally, the regulation's requirements are focused on steps to increase security awareness and to encourage a risk-based, holistic, and robust security program at covered entities. To ensure compliance, covered entities must implement the following:

1. **Risk Assessments:** Periodic risk assessments that consider threats, particular risks to the entity, and an examination of existing controls in the context of identified risk.
2. **Cybersecurity Program:** The creation of a cybersecurity program based on the periodic risk assessments and designed to identify and assess risks; protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations. The program must include annual penetration testing and biannual vulnerability assessments. The cybersecurity program referenced here follows the general mandates of those delineated in the NIST Cybersecurity Framework.
3. **Cybersecurity Policies:** The creation and maintenance of written policies and procedures for the protection of information systems and nonpublic information and based on the risk assessment. These must include a written incident response plan.
4. **CISO:** The designation of a chief information security officer to oversee the cybersecurity program.
5. **Minimum Standards:** Implementation of minimum cybersecurity standards, including systems designed to recover material financial transactions following an event and audit trails to detect events, the institution of appropriate access privileges, procedures for evaluating and testing the security of applications, multifactor authentication, data disposal, mandatory cybersecurity awareness training, and encryption measures.

6. *Third-Party Risk Management*: Implementation of a third-party risk management program, including a review of the cybersecurity practices of those providers and periodic assessment and audit thereof.

These new requirements, which are the first of their kind, signal an increased focus on risk-prioritized and managed cybersecurity.

Save the Date: On March 14, the article's authors will lead a discussion in [Venable's New York City office](#) concerning conducting cybersecurity due diligence in M&A deals. Sellers and purchasers subject to this regulation should consider such due diligence an important aspect of maintaining an appropriate cybersecurity program. Please email tfacey@Venable.com for more information on the program.