Grant Thornton
An instinct for growth™

Resource-strapped in-house counsel battle regulations, cybercrime and litigation

Grant Thornton LLP 2014 Corporate General Counsel Survey

A Grant Thornton LLP online survey, conducted in early 2014 by American Lawyer Media, served to gain further insight into in-house counsels' assessment of the following three threats uncovered in the 2013 *Corporate General Counsel Survey*:

- Regulatory compliance related to corruption and bribery
- Regulatory-related litigation and investigations
- Cybersecurity and data privacy

The results show that in-house counsel are dealing with a lack of resources, which impacts their ability to proactively reduce and appropriately react to these risks.

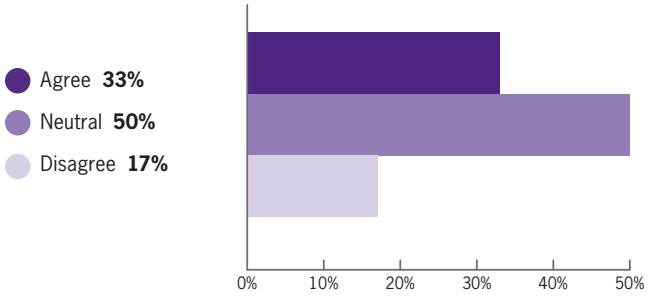
"Corporate counsel are facing a variety of new regulatory risks every day. In addition to industry-based regulation, there are concerns about fraud, ethical behavior and new threats such as data security," says Brad Preber, national managing partner of Grant Thornton's Forensic and Valuation Services practice. "At the same time — or perhaps because of these new risks — corporate counsel do not feel they have the resources to keep up, perhaps creating a vicious circle of regulatory and litigation risk."

Corporate counsel do not have the resources they need

While many respondents were neutral, about one-third claim that "the pace of new regulatory legislation/regulations is more than we can keep up with." Only 17% disagreed with that statement.

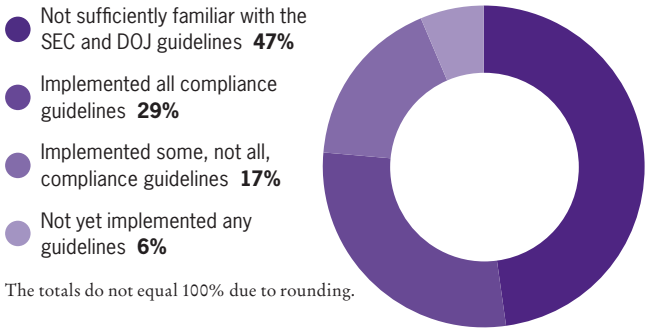
Even with the movement towards the codification of compliance plans by the Department of Justice (DOJ) and the SEC over a year ago, only 29% of survey respondents state that they have implemented all of the guidelines, while 47% are "not sufficiently familiar" with the guidelines to reply.

The pace of new regulatory legislation/regulations is more than we can keep up with



In late 2012, the DOJ and the SEC collaborated to publish *A Resource Guide to the U.S. Foreign Corrupt Practices Act.* This guide is designed to "provide the public with detailed information about our FCPA enforcement approach and priorities."[1]

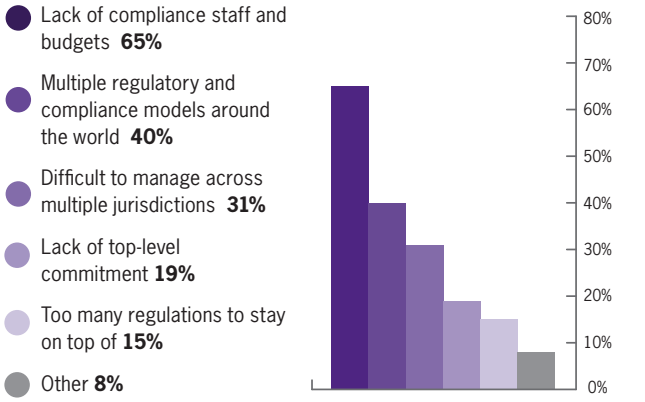
Reasons for not implementing compliance guidelines



The totals do not equal 100% due to rounding.

[1] See www.justice.gov/criminal/fraud/fcpa/guide.pdf for additional details.

Reasons for not implementing compliance guidelines



Respondents were able to select more than one answer.

Among organizations that have not fully implemented the DOJ and SEC guidelines, 65% responded that a "lack of compliance staff and budgets" was the primary reason. The second-most common response from in-house counsel was that there are "multiple regulatory and compliance models around the world." The next most common answer was that it is "difficult to manage across multiple jurisdictions." These responses reflect the challenges of implementing and sustaining global compliance programs.

It's not only the new DOJ and SEC guidelines that are tripping up in-house counsel: Only 62% of respondents say their organization is "designing and operating robust internal compliance programs."

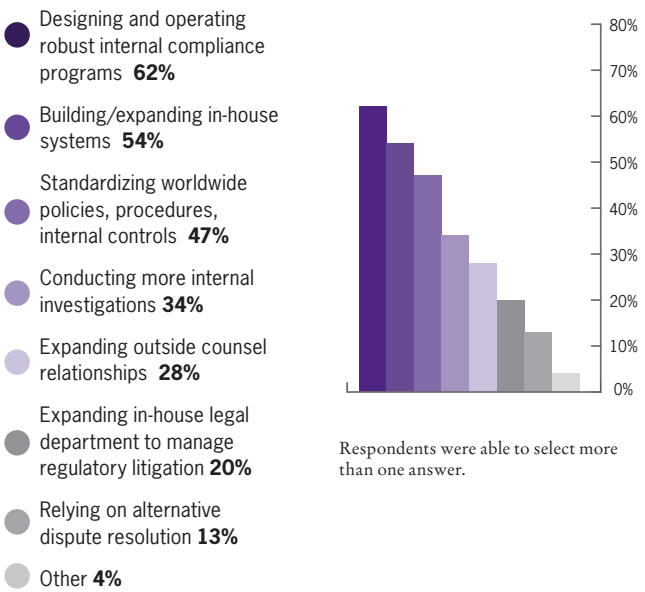
That means that more than one-third of organizations acknowledge that they do not have a robust program, and that they are not building one. "The absence of a robust regulatory compliance program presents potentially great risks to enterprises," Preber says. "However, these risks can be successfully managed by taking a few basic steps towards designing, implementing and operating a program consistent with the federal government's guidelines."

> "It is hard to imagine a government investigator —or a jury— accepting 'lack of resources' as the primary reason for failure to comply."
>
> — Bill Olsen, Principal and Global Investigations and Anti-Corruption Services leader at Grant Thornton

Furthermore, in a time of increasing regulatory risk, less than half of the in-house counsel surveyed believe that their organization is conducting more internal investigations, expanding outside counsel relationships, or developing the in-house legal department to manage regulatory investigations and litigation.

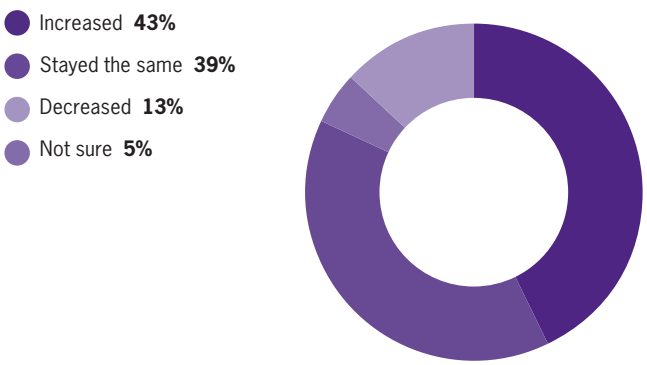
"I can't overstate how risky this is," says Bill Olsen, principal and Global Investigations and Anti-Corruption Services leader at Grant Thornton. "Organizations are expected to have a robust compliance program, and the SEC and DOJ have drawn a roadmap. "It is hard to imagine a government investigator — or a jury — accepting 'lack of resources' as the primary reason for failure to comply."

Responses to regulatory-related and investigation risk



Respondents were able to select more than one answer.

Change in cybersecurity and data privacy risk



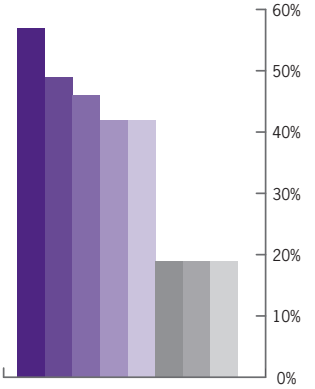
Grant Thornton's survey results show other areas — both old and new risks — where a lack of resources creates a threat to the organization.

New risk: Data privacy and cybersecurity risks are increasing at an alarming speed

Privacy and data breaches have gotten a lot of press in the past few years; almost 60% of in-house counsel respondents see privacy as one of the top three concerns. Perhaps even more surprising is the rate at which this concern is growing. More than 40% claim that the risk of a cybersecurity/data privacy breach has increased in the past year, and that risk was at record-high levels last year.

Top 3 cybersecurity and data privacy concerns

- Customer/client data privacy **57%**
- Unknown and unidentified risks **49%**
- Legal compliance with data security laws **46%**
- Potential for undetected breaches **42%**
- Employee and workplace data privacy **42%**
- Payment card protection **19%**
- Health care privacy **19%**
- Cross-border data transfers **19%**



Respondents selected three concerns.

According to in-house counsel, the areas of greatest concern are the security and privacy of customer and client data (57%). Fear of the unknown also ranked high (49%), alongside legal compliance (46%), the potential for undetected breaches (42%), and employee and workplace privacy (42%).

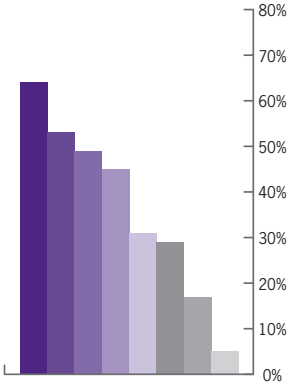
"The problem with cybercrime is that it can go undetected and cause massive amounts of damage in very short amounts of time," says Skip Westfall, managing director and Forensic Technology Services leader at Grant Thornton. "Combine this with the ever-increasing amount of sensitive data sources, and you have a recipe for potential disaster."

> "Cybercrime and data security risks are clear and present dangers."
>
> — Skip Westfall, Managing Director and Forensic Technology Services leader at Grant Thornton

Survey data about how organizations are responding to cybersecurity and data privacy risks reflects a focus on monitoring, policies and the identification of sensitive data. However, there is room for improvement. Only 45% claim their organizations are performing vulnerability assessments and penetration testing, and just 31% have developed and tested an incident response plan in case of a data security breach. Seventeen percent of respondents were unsure about

Responses to cybersecurity and data privacy risks

- Monitor cybersecurity/data privacy internal controls **64%**
- Prepare cybersecurity/data privacy policies and procesures **53%**
- Determine locations of sensitive/ private data **49%**
- Perform vulnerability assessments and penetration testing **45%**
- Develop and test incident response plan **31%**
- Evaluate cybersecurity and data privacy insurance coverage **29%**
- I'm not sure **17%**
- Other **5%**

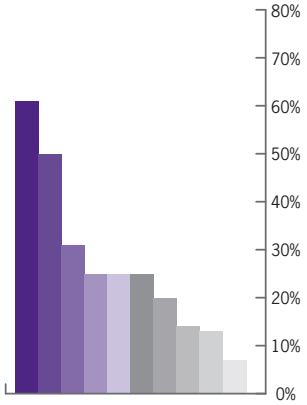


Respondents were able to select more than one answer.

Organizations can take a few simple steps to help reduce the risk of potential data breaches. Proper training on data security policies and procedures, together with regular risk assessments, can help create a solid foundation for a data security program. Protecting your data through the use of policies, passwords, secure logins, data encryption, firewalls and the logging of security events should also be part of your basic program. In addition, penetration testing and anti-viral and malware programs are essential. Every organization should have a comprehensive incident response plan in place for a rapid and strategic response.

Regulatory issues presenting the greatest risk

- Data privacy law **61%**
- Industry-specific regulation **50%**
- Anti-corruption laws **31%**
- Affordable Care Act **25%**
- Labor laws **25%**
- Dodd-Frank Wall Street Reform and Consumer Protection Act **25%**
- Environmental laws **20%**
- Antitrust laws **14%**
- SEC Conflict Minerals Disclosure Rules Act **13%**
- Other **7%**



Respondents were able to select more than one answer.

what was being done to deal with cybersecurity and data privacy risks within their organizations.

"Stakeholders ranging from regulators to customers and shareholders are concerned about these matters. It is a business imperative for organizations to effectively deal with these risks," Westfall says.

Old risk: Concerns about industry-specific regulation

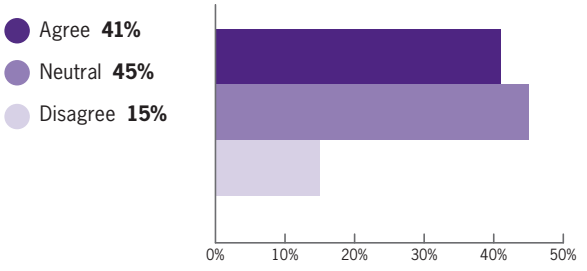
Consistent with the responses on cybersecurity, data privacy regulation was cited as the No. 1 risk facing organizations, with 61% of in-house counsel selecting it in the survey. However, respondents cited "industry-specific regulation" as the second-biggest concern (50%) ahead of anti-corruption laws; labor laws; the Affordable Care Act; Dodd-Frank; and a number of new laws, policies and enforcement priorities [2].

Regulatory-induced litigation is an incentive for action

More than 40% of in-house counsel agree that regulatory-related litigation is driving organizational compliance more than legislation and regulation; only 15% disagreed. This illustrates that corporate counsel may be more concerned about shareholders' lawsuits, for example, than the potential for penalties imposed from an investigation itself.

"This is a case of an ounce of prevention being worth a pound of cure," says Craig Casey, partner and Litigation and Dispute Services leader at Grant Thornton. "There are still a large number of organizations ignoring the warning signs of regulatory compliance enforcement, instead preferring to wait until litigation arises to handle the problem. This is not a sustainable position in the long run."

Regulatory-related litigation is driving corporate compliance more than new legislation/regulations



The totals do not equal 100% due to rounding.

About Grant Thornton Advisory Services

Grant Thornton consultants can help your organization design and implement a regulatory compliance program, protect your data from unauthorized access, handle investigations of potential regulatory violations, and prevent many significant risks related to regulatory compliance. Our specialists combine insight and innovation to assist dynamic organizations, using a multidisciplined approach from a wide range of business and industry knowledge. Visit grantthornton.com/advisory to learn more.

About Grant Thornton LLP

The people in the independent firms of Grant Thornton International Ltd provide personalized attention and the highest-quality service to public and private clients in more than 120 countries. Grant Thornton LLP 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. Grant Thornton International Ltd and its member firms are not a worldwide partnership, as each member firm is a separate and distinct legal entity.

In the United States, visit grantthornton.com for details.

Demographics

The Grant Thornton LLP Corporate General Counsel Survey was conducted online between Jan. 28 and Feb. 12, 2014, by ALM Marketing Services. There were 256 respondents: All were in-house counsel, 29% were general counsel, and 28% held the title of deputy/assistant general counsel or senior counsel/practice head. The respondents were from both publicly traded (37%) and privately held (50%) companies, as well as some government entities and not-for-profits. Respondents' organizations represented a broad range of sizes, with 31% falling in the less than $100 million in annual revenue range and 18% falling in the greater than $5 billion range. Organizations were distributed across industry sectors.

For more information, contact one of Grant Thornton's Forensic and Valuation Services leaders:

Brad Preber
National Managing Partner, Forensic and Valuation Services
602.474.3440 | brad.preber@us.gt.com

Mark Sullivan
Principal, Fraud and Investigation Services Leader
312.602.8110 | mark.sullivan@us.gt.com

Craig Casey
Partner, Litigation and Dispute Services Leader
212.542.9810 | craig.casey@us.gt.com

Bill Olsen
Principal, Global Investigations and Anti-Corruption Services Leader
703.847.7519 | william.olsen@us.gt.com

Skip Westfall
Managing Director, Forensic Technology Services Leader
832.476.5000 | skip.westfall@us.gt.com

John Ferro
Partner, Valuation Services Leader
212.542.9574 | john.ferro@us.gt.com

[2] Respondents came from a wide array of industries, only some of which are highly regulated. Finance and insurance, and professional, scientific and technical services combined to make up 42% of respondents, with the remainder spread among eight other categories.