Risk Intelligence Quarterly

Q4 2014 Edition

Dodging Risk-Related Meteors

Latest Trends for the Compliance and Ethics Function

Top Efficiency and Budgeting Guidelines for General Counsel in 2015

The Three Biggest Barriers to Data Privacy Program Effectiveness

Setting Internal Audit Plans for 2015

CEB
WHAT THE BEST COMPANIES DO

Q4 2014 Edition

Contents

A Letter to Our Readers

Welcome to our Q4 2014 edition of the *Risk Intelligence Quarterly*, published by CEB, the world's leading member-based advisory company. We continuously provide legal, risk management, audit, and compliance executives with valuable insight on how leading organizations best manage their functional and enterprise-wide risks. This edition centers on our latest survey findings to help executives and their teams benchmark 2015 plans regarding program structure, priorities, budget, staffing, and strategy.

In addition to identifying where leading programs are headed in 2015, we also provide detailed analyses of key emerging risks and how they affect organizations around the globe, which are critical to the planning process. One of these emerging risks is data privacy, a top risk that many companies not only underestimate but also fall short of properly supporting with an effective program. We recognize the significance of data privacy in today's complex business landscape and are proud to introduce our newest leadership council program, CEB Data Privacy Leadership Council, which provides new and mature programs with best practices on valuable resourcing, impactful policies, influential training, and effective metrics.

The articles in this publication provide detailed insight on the latest trends affecting compliance departments; guidelines for general counsel to achieve top efficiency and budgeting; and recommendations for setting internal audit plans, tackling data privacy challenges, and preparing for emerging risks throughout the enterprise—all of which will prepare executives like you for a strong business approach in the coming year.

We encourage you to share this publication with your colleagues and contact us at **LRC.Support@executiveboard.com** with your feedback.

Sincerely,
CEB

Dodging Risk-Related Meteors

By Dan Herd, Director, CEB Risk Management Leadership Council

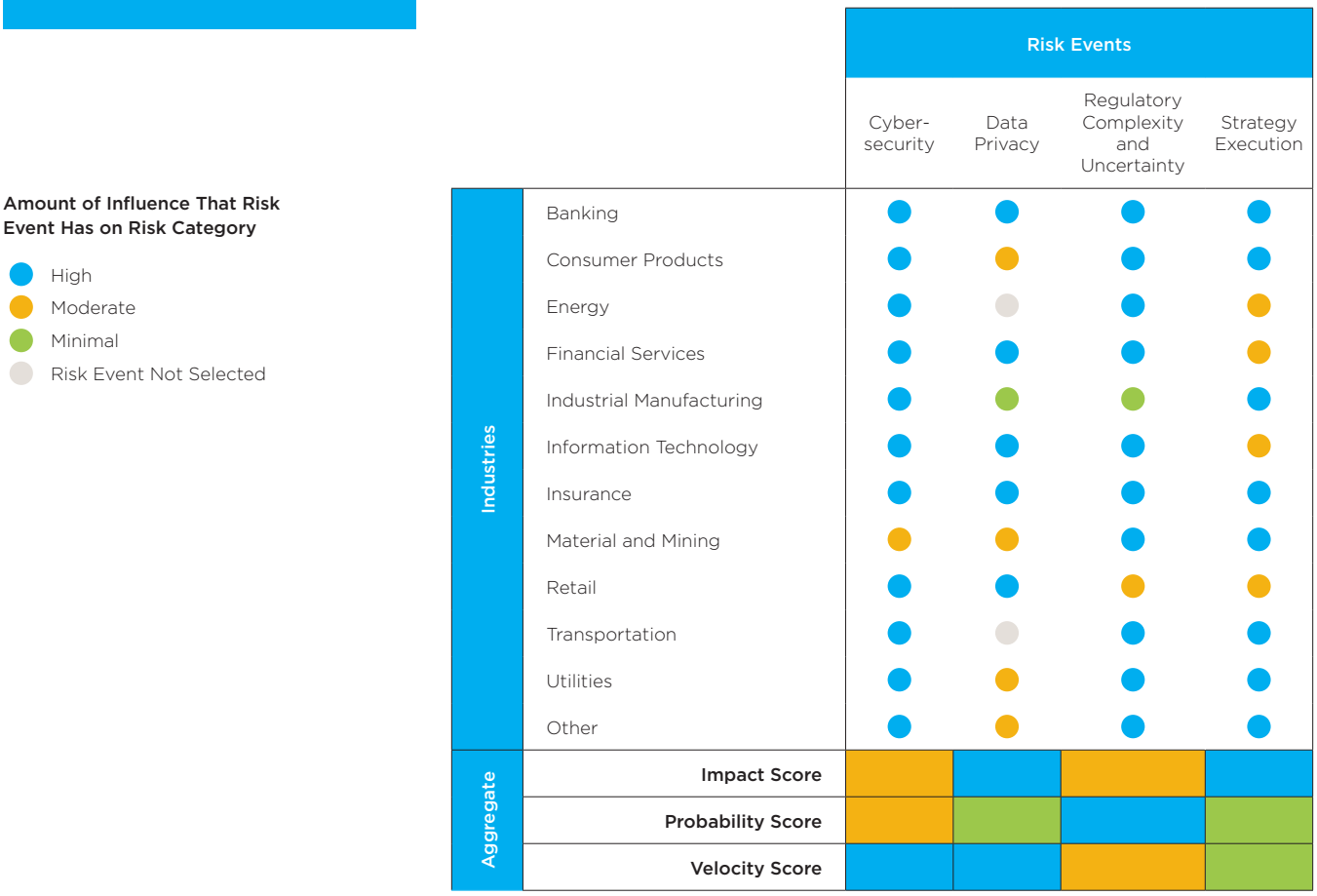
Latest Top Four Emerging Risks:

1. Regulatory Complexity and Uncertainty
2. Cybersecurity
3. Strategy Execution
4. Data Privacy

Each quarter, we survey risk management and audit executives on key emerging risks and how they affect large companies across the globe. The survey asks executives to identify the top risks affecting their companies and to provide estimates of probability, impact, and velocity for each risk.

The dashboard in Figure 1 captures the amount of influence a risk event has on various industries. The amount of influence is determined by the overall risk score relative to other risks within the industry (blue = those greater than the 75th percentile; gold = 25th–75th percentile; and green = below the 25th percentile). The bottom three rows of the dashboard encompass the aggregate score across all industries.

Figure 1: Quarterly Emerging Risk Dashboard



Source: CEB analysis.

1. Regulatory Complexity and Uncertainty

For the first time in more than a year, regulatory complexity and uncertainty has taken the top spot away from cybersecurity or information security. The heightened global regulatory atmosphere continues to affect corporate assurance departments as their scope and responsibilities to comply with new regulations require an ever-increasing amount of resources. Although most companies certainly intend to comply with the legal requirements in their operating environments, many organizations continue to rely on specific functions' regulatory knowledge of pertinent laws. However, leading companies ensure business units and assurance functions communicate with one another by creating central processes and proactively set the tone of regulatory debates.

For the first time in more than a year, **regulatory complexity and uncertainty has taken the top spot** away from cybersecurity or information security.

2. Cybersecurity

With regulatory uncertainty jumping up to the top spot, it likely comes as no surprise that cybersecurity is the number two risk our members are concerned about this quarter. Significant dependence on information technology increases susceptibility to cyber attacks and hacks. Costly information breaches not only are top of mind for information security professionals and members of the media but also are front and center for senior executive teams. When it comes to cybersecurity, the best companies develop information security policies in light of the organization's risk appetite to ensure policies support business goals. Progressive organizations also respond to cyber attacks by emphasizing detection and response over prevention and end-user awareness over technical controls.

3. Strategy Execution

Our research shows that an inability to bridge the gap between strategy and execution is the prime cause of failed growth initiatives. Two factors may contribute to this worrisome gap. The first is quick wins; with the economic climate improving, managers may choose to take a detour from long-term bets and concentrate on easier, short-term initiatives. Second, heavier workloads may be a factor. After extreme staff cuts during the recession, many employees had to pick up extra tasks, reducing their time for growth efforts. Leading companies align the strategic plan and the specific actions business partners need to take, avoiding conflicts and confusion about priorities. In addition, a two-way dialogue about strategy with influential employees helps keep them on board and engaged with achieving the company's overarching objectives. Further, holding partners accountable by monitoring key metrics allows for a timely course correction if necessary.

4. Data Privacy

With the increasing digitization of employee, health, financial, and other personal information and the advent of social media and Web 2.0 technologies, attempts to appropriately collect, secure, and dispose of personal information face far greater scrutiny from regulators, customers, and employees. Further, as the legal, financial, and reputational costs of highly publicized data breaches grow, the adequacy and robustness of data privacy efforts is increasingly becoming a top priority for companies around the world. However, many companies' data privacy efforts continue to be siloed and inconsistent throughout the organization, lacking an overarching plan or framework that considers all regulatory obligations. Leading companies are developing a comprehensive inventory of where they do business and where they collect, store, and transfer sensitive data. In addition, progressive organizations actively collaborate with their information technology and information security partners to develop appropriate technical, administrative, and physical procedures and comprehensive breach response plans.

As the legal, financial, and reputational costs of highly publicized data breaches grow, the adequacy and robustness of **data privacy efforts is increasingly becoming a top priority** for companies around the world.

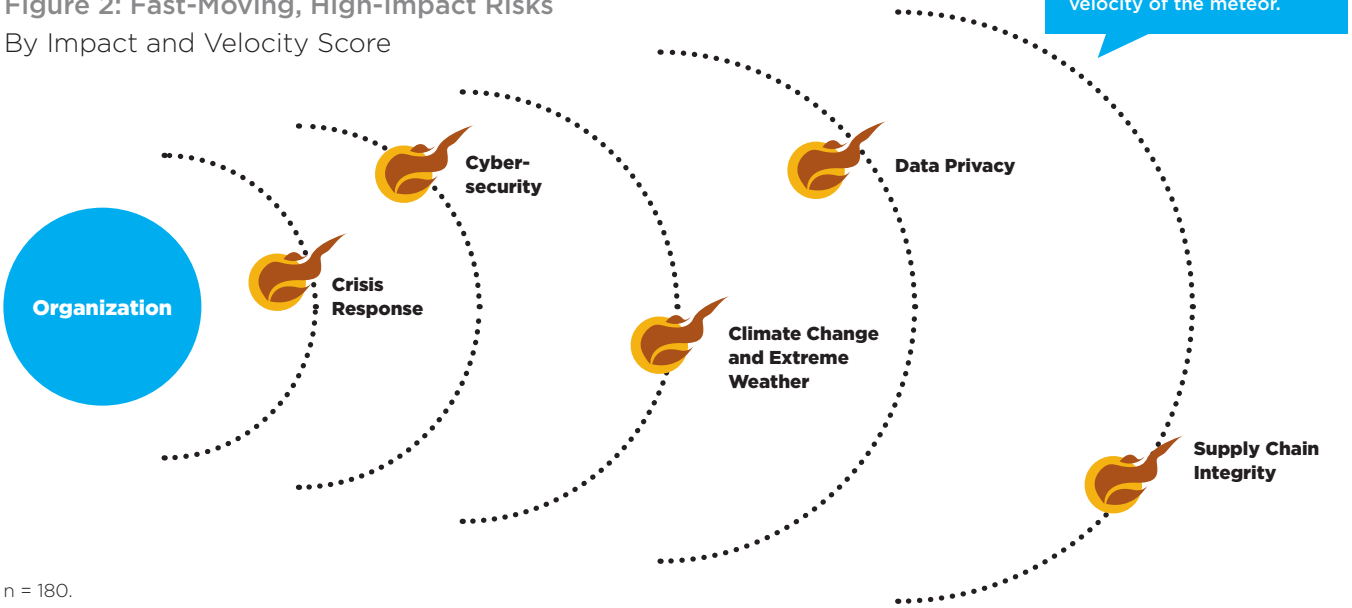
Beware of the Meteors

The top risks we just covered have high enough impact and likelihood ratings to easily show up on many companies' radar screens. But what about risks that are extremely unlikely yet fast moving and high impact, with the potential to cripple your organization? We call these risks "meteors." Some might even call these the cousins of your "black swan" risks, which are high-impact, low-probability risks that could not have been foreseen.

Figure 2 captures our most recent meteor analysis. The size of the meteor represents its impact score, and the distance between the organization and each meteor represents its velocity. In this case, five risks are considered meteors. Keep in mind that the danger with meteors is that they are not always apparent—despite having the highest meteor score, only 5% of respondents selected crisis response as one of their top risks.

Figure 2: Fast-Moving, High-Impact Risks
By Impact and Velocity Score

The size of the meteor represents its impact score. The distance between the organization and each meteor represents the **velocity of the meteor.**



n = 180.
Source: CEB Q3 2014 Emerging Risks Survey.
Note: Meteor Score = Square Root (Impact Score x Velocity Score).

Think Outside the Box to Spot Meteors

Corporate boards and risk committees are always interested in hearing about emerging risks to learn what unforeseen event may lie around the corner. In fact, our research shows that 66% of ERM teams report on emerging risks to their executive risk committees, and the emerging risks dashboard shown earlier has a tendency to make its way into many of our members' risk reports. However, where do these risks come from? Beyond our emerging risks report and other external sources, how do organizations identify new risks?

One leading CEB member holds workshops consisting of unconventional brainstorming exercises to create a list of hypothetical risk events that may force the company to cease operations. The workshops' goal is simply to find and discuss risks that could devastate the company. The likelihood of an event occurring and existing controls are not considered to uncover the risk's true effect in a catastrophic event. The following unconventional exercises are meant to get participants to think outside the box and stimulate ideas and discussion:

- **Reverse stress-testing—**Starting with an imaginary business failure, have breakout groups separately determine how it might have occurred (e.g., understanding what factors would lead to a catastrophic systems failure).
- **"Green hat" brainstorming—**Generate as many crazy ideas as possible (e.g., an ice storm destroys power lines to the data center).
- **Lateral thinking—**Take an abstract idea and work it back into the context of a business problem (e.g., when you think about a penguin, what else comes to mind?).

Following the workshop, the highest-rated inherent risks are mapped to risk events from the workshop. If a risk cannot be tagged, it is reevaluated to determine what discussions should be added for the next risk workshop. Many organizations believe their company culture won't allow for similar brainstorming exercises and focus on external research instead. However, this member reported that the brainstorming exercise resulted in a list of 31 hypothetical events. Perhaps identifying one of these events through a brainstorming exercise will help you spot the next meteor.

If a risk cannot be tagged, it is reevaluated to determine what **discussions should be added for the next risk workshop.**

Latest Trends for the Compliance and Ethics Function

By Ryan Ulbrich, Associate Director, CEB Compliance & Ethics Leadership Council

Since its inaugural launch 10 years ago, our biennial State of the Function benchmarking survey has captured the burgeoning change of corporate compliance and ethics. With over 300 respondents across 20 industries this year, the results offer a key efficiency perspective for executives and their teams to help them build confidence in their decision making and strategic focus. Three notable inflection points on structure, focus, and strategy indicate where programs will head in 2015.

The Business Case for Liaisons: A Widening Scope of Program Activities and Risk Ownership

The range of activities that compliance departments either own or participate in continues to expand across industries. In 2014, employee-facing activities such as policy development, training, helpline administration, and effectiveness reporting were obvious choices for ownership, and reviewing new business strategies and conducting initial due diligence of third parties returned to the fold. At the same time, Compliance and its legal counterparts remain the primary risk owners at companies worldwide (Figure 1).

Figure 1: Compliance and Legal Still Primary Risks Owners
Percentage of Respondents, 2014

Risk Topic	Compliance and Ethics	Legal	Business Unit	Independent Function	Internal Audit	Human Resources	Other	Not Applicable	n
Anti-Corruption	71.7%	20.8%	2.7%	0.3%	2.7%	0.0%	0.7%	1.0%	293
Anti-Money Laundering	39.9%	21.3%	5.6%	2.4%	6.6%	0.0%	10.8%	13.3%	286
Antitrust/ Competition Law	22.1%	75.1%	1.8%	0.0%	0.0%	0.0%	0.0%	1.1%	285
Conflicts of Interest	72.9%	16.8%	1.0%	0.7%	2.1%	5.1%	0.7%	0.7%	292
Corporate Security	10.8%	15.0%	10.8%	31.0%	1.7%	5.6%	21.6%	3.5%	287
Data Privacy	34.4%	29.5%	9.8%	7.7%	0.7%	3.5%	13.7%	0.7%	285
Environmental, Health, and Safety	5.2%	7.3%	20.4%	32.5%	0.0%	12.5%	20.1%	2.1%	289
Government Contracting	4.3%	36.7%	27.8%	5.3%	0.0%	1.8%	9.3%	14.9%	281
Records Management	22.5%	36.5%	12.6%	11.9%	0.4%	2.1%	11.9%	2.1%	285
Sales and Marketing	25.3%	14.2%	41.7%	5.6%	0.0%	0.0%	6.3%	6.9%	288
Securities and Insider Trading	20.5%	64.6%	3.1%	1.4%	0.3%	0.0%	3.5%	6.6%	288
Third-Party Compliance	42.7%	12.2%	26.9%	3.5%	0.3%	0.0%	12.6%	1.7%	286
Trade Compliance	26.7%	23.5%	18.2%	11.6%	0.0%	0.0%	6.7%	13.3%	285

Source: CEB 2014 State of the Compliance and Ethics Function Survey.
Note: Shading indicates corporate function with largest share of risk ownership by category.

Despite regulatory intensity's proven effect on program location, budget size, and staff head count, the average budget showed a modest uptick in the past two years—and with a 0% growth projection to boot. On the other hand, staffing levels have held steady across the board at roughly 0.55 full-time staff for every 1,000 employees. Although not the norm, industries such as insurance saw a drastic 21% staffing cut since 2012.

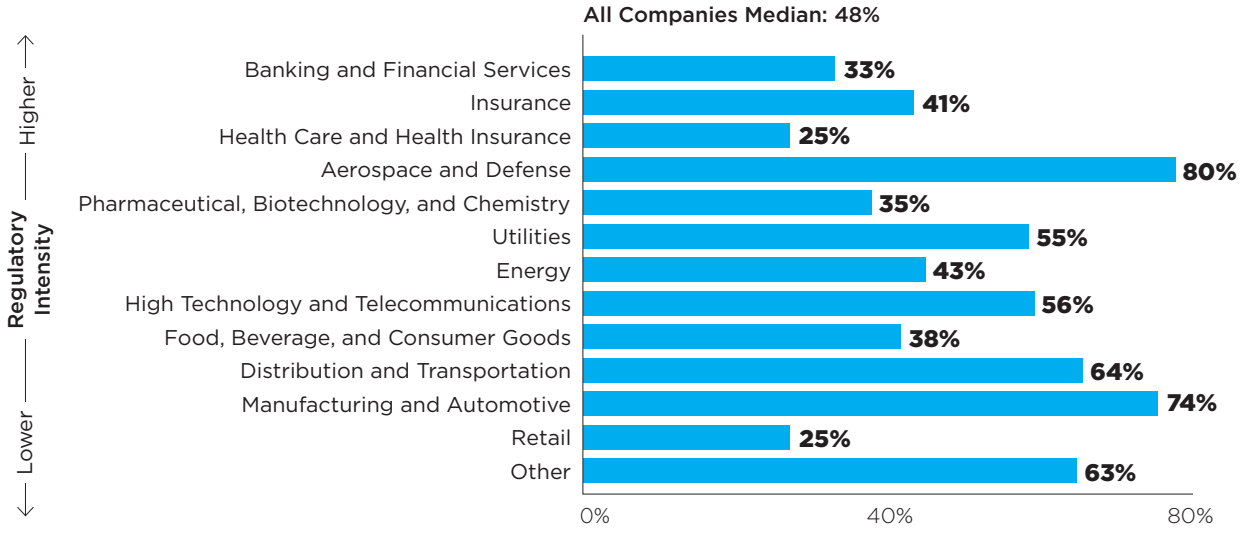
To compensate for these trends, compliance and ethics executives are turning to program liaisons—defined as staff outside the function spending 5%–10% of their time supporting compliance and ethics initiatives—to increase their enterprise influence. In fact, the median number of liaisons at respondent companies from all industries grew from 0.5 in 2010 to an incredible 15 in 2013 (Figure 2). Common support areas for liaisons include training and communication, ethical leadership, risk management, and investigations.

On average, 48% of compliance and ethics programs use liaison networks to better distribute and localize communications, improve risk detection on the ground, and increase employees' comfort levels in speaking up. Given flat staffing trends and an outsized scope of activity and risk ownership levels, these ambassadors have saved compliance officers time and money while expanding the program's impact in business units and dispersed geographies.

On average, 48% of compliance and ethics programs use liaison networks **to better distribute and localize communications, improve risk detection on the ground, and increase employees' comfort levels in speaking up.**

Figure 2: The Use of Compliance and Ethics Liasons

Percentage of Respondents, 2013



n = 230.
Source: CEB analysis.

The New Compliance Priority: Third-Party Risk and Related Activities

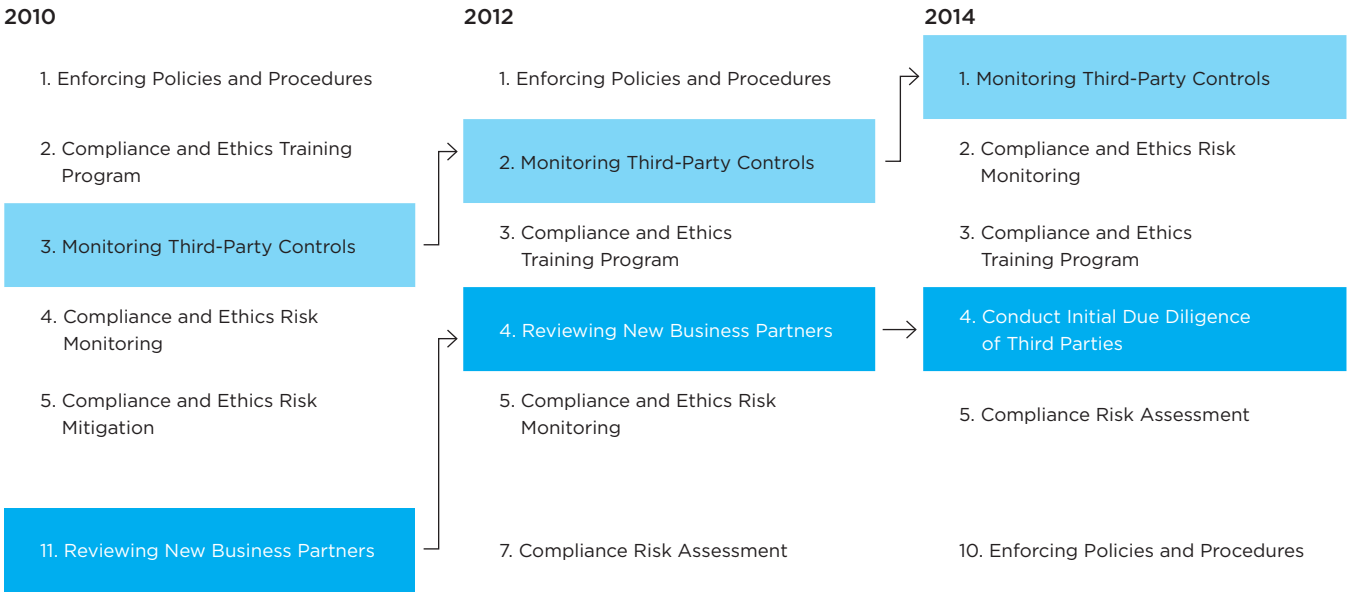
As companies expand their presence in new and riskier markets, supply chains become more interconnected, regulations fragment, and exposure to anticorruption risk—and its ancillary risk of third parties—increases significantly. Enforcement trends focused on third-party activities have led to a new paradigm in compliance risk management.

In 2014, nearly half of all survey respondents indicated they **work with over 10,000 third parties** or were **unsure of the volume altogether.**

In 2014, nearly half of all survey respondents indicated they work with over 10,000 third parties or were unsure of the volume altogether. At the same time, the average compliance program classifies up to 25% of its third-party network as high risk. Combined, these factors have intensified third-party risk and shifted the priority landscape for compliance teams, wherein monitoring third-party controls and conducting due diligence on new business partners have become areas of increased functional emphasis (Figure 3).

Figure 3: Top Five Priority Areas for Compliance Departments

Average Priority Scores[a] for 2010, 2012, and 2014



Source: CEB analysis.

[a] Priority Score = (Mean Importance – Mean Effectiveness) x Mean Importance.

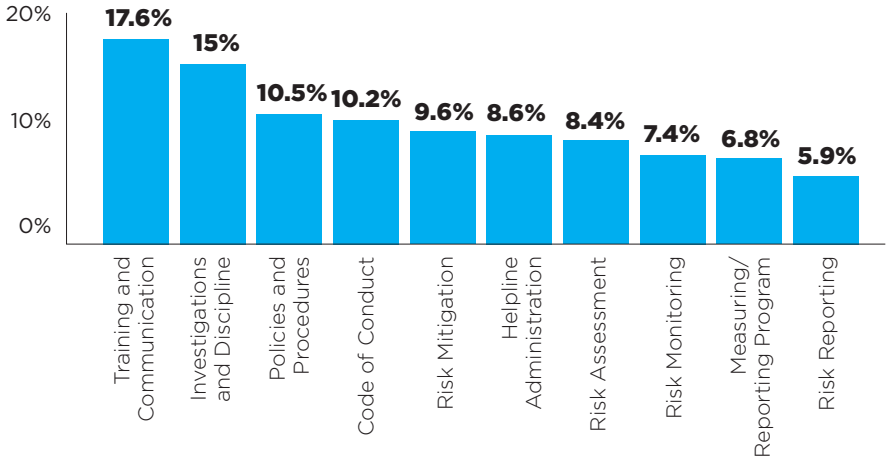
Placing the Big Bets: Compliance and Ethics Training and Communications

Year after year, compliance departments spend considerable time and money on their training and communication programs. After staff salaries, bonuses, and benefits, training and communication line items have received the most allocated dollars each year since 2008. In 2014, more total time was spent on this activity than on risk assessments and program effectiveness activities combined, with 41% of respondents spending the most time on training and communication (Figure 4).

After staff salaries, bonuses, and benefits, **training and communication line items have received the most allocated dollars** each year since 2008.

Figure 4: Compliance and Ethics Program Time Allocation

Percentage of Respondents



n = 260.

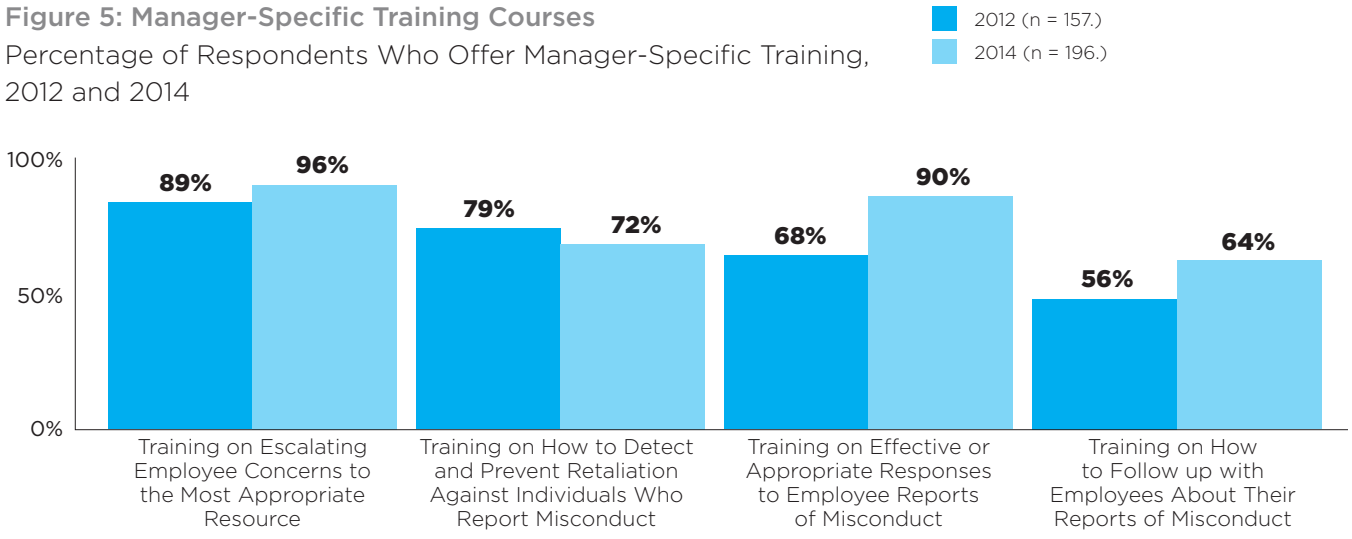
Source: CEB analysis.

However, much to the dismay of compliance executives, employee feedback and behaviors suggest fundamental gaps in current training that limit its influence and effectiveness. Overall, employees hold fairly negative reactions to compliance training—only one-third find it relevant or helpful. To reverse this trend, compliance teams are discovering the key drivers of effective programs, using application as the primary focus, keeping timing top of mind, and reinforcing concepts between sessions to drive stronger retention outcomes.

Manager training has also permeated the common curriculum, and more companies are rolling out courses on escalating concerns to the appropriate contact, responding to employee reports, and using effective follow-up procedures (Figure 5). In particular, the number of programs training managers on the effective handling of employee reports increased by 32% since 2012. This surge is crucial, given that 66% of employees choose to report concerns directly to their managers.

Figure 5: Manager-Specific Training Courses

Percentage of Respondents Who Offer Manager-Specific Training, 2012 and 2014



Source: CEB analysis.

Top Efficiency and Budgeting Guidelines for General Counsel in 2015

By Sampriti Ganguli, Executive Director, CEB's Legal, Risk & Compliance Practice

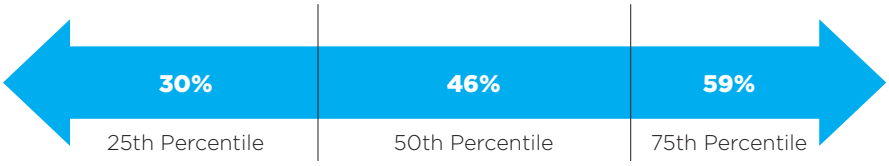
Statistical analysis of what drives lower costs in legal departments will **shape longer-term strategic priorities.**

Seventy percent of business executives expect revenue growth pressures to increase in 2015, and 68% expect cost pressures to increase as well. This broader business context also drives Legal's budget conversations; after all, if growth comes from more risks (presumably across more products and geographies), the demand for legal services will increase. However, if general counsel (GCs) need to maintain budgets in line with corporate cost measures and keep pace with inflation, how can GCs ensure they have the right resources for the amount of work that needs to be done?

Benchmarking budgets can help provide a solid business case for Legal and garner additional point-in-time resources, but statistical analysis of what drives lower costs in legal departments will shape longer-term strategic priorities. As we analyzed legal departments with lower expenses than peers (which we use as a proxy for efficiency), we found the following top insights for efficiency as a priority in 2015:

1. Perform More Legal Work in House—It's no secret that having in-house staff handle the work outside counsel often manages is more cost-effective. We've been advising clients to do this for a decade, in part because budget data consistently show it to be true. Unless there's major litigation involved, the ideal spend ratio is considered to be 40% outside and 60% inside. However, many departments employ the reverse. Plenty of good reasons exist, of course, to rely predominantly on outside counsel for specialized matters, but if your CFO is questioning department costs, systematically bringing work in house is a good place to start. A deeper analysis indicates that leading departments are often more cost-effective because they invest heavily in workload allocation, develop in-house lawyer capabilities, and pay close attention to the right mix of specialist and generalist lawyers, given their business needs.

Figure 1: Percentage of Legal Expenses Allocated In House, 2013



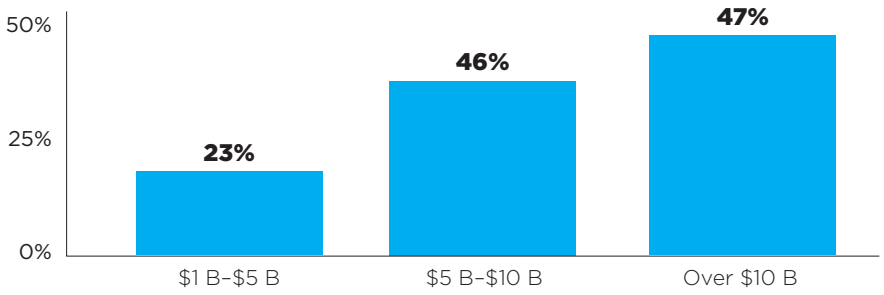
n = 125.
Source: CEB analysis.

2. Use Non-Lawyer Professionals More Often—Forty-two percent of companies employ at least one non-lawyer (e.g., paralegal, administrative professional) for every two lawyers within the department. This structure gives legal departments more flexibility to delegate urgent but lower-impact tasks (e.g., organizing contracts, reviewing documents, preparing filings) downward to less-costly paralegals, as opposed to delegating tasks to outside counsel who are often significantly more expensive. This strategy has other payoffs, too: companies with this higher ratio bring more complex regulatory work and more routine intellectual property (IP) work in house, suggesting that the freed-up time is well spent on higher-value activities. Before assuming your next hire should be an experienced attorney, revisit workloads to streamline certain processes (e.g., contracts) and consider whether a non-lawyer professional can provide greater value.

3. Invest in Legal Operations Capabilities—The legal operations manager is an ascendant function in Legal; 80% of large legal departments use the role. Legal operations managers can play a critical role in creating efficiency (particularly with larger legal departments), often through providing law firm and budget oversight. In addition, regardless of size, departments with a legal operations manager allocate a higher percentage of total legal expenses in house (typically the less expensive option) than those that don't. Legal operations managers help with department budgeting, managing law firm relationships and invoices, technology oversight, and department training. In the absence of dedicated operations staff, these activities must be delegated and performed by other in-house lawyers and staff, reducing efficiency and employee engagement.

Forty-two percent of companies **employ at least one non-lawyer for every two lawyers** within the department.

Figure 2: Percentage of Departments Employing a Legal Operations Manager by Company Revenue (USD), 2013

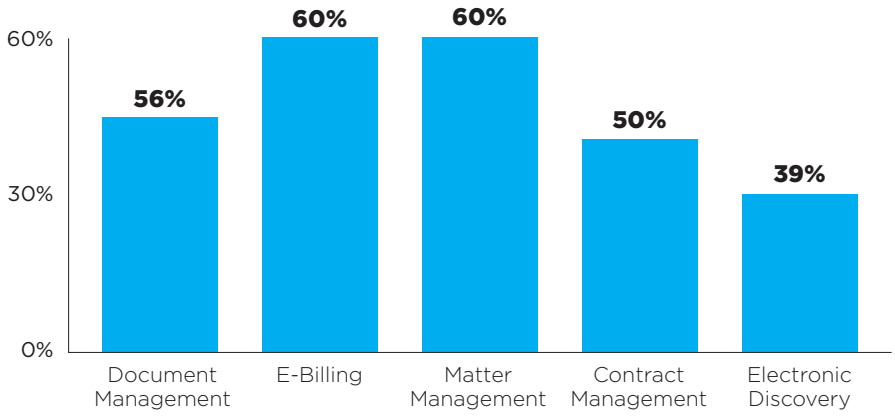


n = 140.
Source: CEB analysis.

4. Invest Selectively in Legal Technologies—It's official, technology has become mainstream in most legal departments, as measured by adoption rates. Matter management and e-billing technologies are becoming more commonplace in large legal departments (60% of large legal departments use them), and members express relatively high satisfaction levels with those solutions. Document management solutions—more prevalent across departments of all sizes—have lower levels of satisfaction, but that may be from reluctance to change habits, not because the technology is poor. The moral of the story?

Push forward with technology initiatives, but demand more from providers and don't underestimate the workflow and change management requirements. The key is to get the capabilities right and fret less about the bells and whistles that vendors show you.

Figure 3: Percentage of Departments Using Legal Technologies, 2013



n = 135.
Source: CEB analysis.

5. Unbundle Legal Services—Leading departments continue to pick apart the law firm service bundle, taking administrative or information-intensive activities away from law firms and, as a result, reducing their outside legal expenses over a three-year period more than peers. We see this most in the area of litigation (even in small departments.) There's a tipping point here—cost efficiencies don't kick in until litigation spend exceeds 15% of the total legal budget. Innovations abound in this area, with some companies going as far as having a non–law firm third-party provider teach itself the company's negotiation tactics by creating a playbook based on a review of draft and executed agreements.

Leading departments continue to pick apart the law firm service bundle, **reducing their outside legal expenses over a three-year period more than peers.**

6. Use Analytics to Reduce Law Firm Rates—GCs believe that direct negotiation of law firm rates is a more effective cost reduction strategy than billing guidelines, project managers, or other more creative strategies. They're right—average differences upward of 15% exist in the rates charged to major clients for similar matters and comparably sized firms. Historically, those differences were related to buying power; GCs were offered the best rates only when they had millions to spend. But the power of analytics from e-billing systems and external benchmarking data is changing rate negotiation in all areas of spend. Instead, consider looking at rate volatility, a measure of the negotiation potential with law firms, which varies significantly by type of work.

The power of analytics from e-billing systems and external benchmarking data is **changing rate negotiation in all areas of spend.**

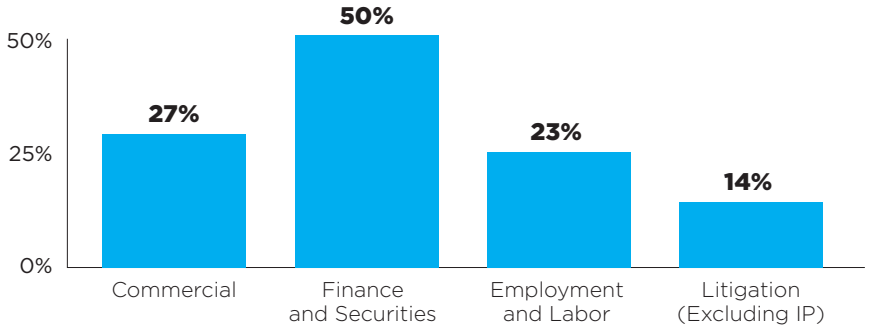
Figure 4: Litigation Partner Rate Volatility
Average Difference in Rates Outside DC/NY, 2013

Source: CEB and Datacert | Tymetrix analysis.

7. Concentrate Spend in Fewer Firms—Cost and quality benefits grow until a single law firm consumes more than 20% of a company's external legal spending. On average, the most efficient legal departments use 40–45 law firms; that's three times fewer law firms than legal departments with higher outside legal expenses. Companies with lower outside legal expenses will often consolidate a higher percentage of their outside expenses with their top 10 law firms than their peers. Leading departments use a variety of tools to narrow or expand their provider list and identify firms that serve the company's needs while valuing the business enough to provide competitive pricing and other benefits.

8. Be Judicious with Alternative Fee Arrangements—Although alternative fee arrangements are useful in reducing costs, the way in which legal departments administer and monitor fee arrangements is far more important than simply having them. In fact, departments with lower outside expenses use notably fewer fee arrangements than departments with higher outside expenses.

Figure 5: Median Percentage of Spending on Alternative Fee Arrangements, Selected Practice Areas, 2013



n = 17–37, depending on practice area.
Source: CEB analysis.

9. Use Smaller Law Firms More Often—Leading companies use smaller law firms to save as much as 45%–50% on their legal fees and achieve greater overall satisfaction as they build relationships with those firms. Outsourcing legal work to smaller law firms results in lower partner and associate rates, as the median non-litigation hourly rate in 2013 at firms with fewer than 50 lawyers was $280 for partners and $210 for associates compared to $670 for partners and $426 for associates at firms with 500–1,000 lawyers.

10. With Alternative Fees, Remember That the Matter Matters—The departments readily using fee arrangements are most likely to create them for litigation, IP, and labor and employment work. Contingency fee arrangements are common for litigation and M&A matters but are otherwise rarely used. Flat or fixed fee arrangements are most common for labor and employment work. GCs report that fee arrangements tied to a specific amount are most effective at controlling costs, whether on a specific project or for a period of time.

11. Consider Legal Budgets Relative to Other Corporate Budgets (And Where the Spend Is Going)—Although GCs would prefer to think about legal budgets in isolation, CFOs rarely do, so knowing what some of your corporate counterparts' budget growth looks like is helpful. For example, the median IT budget is increasing about 3.3% in 2015, but much of the budget is being allocated to improving the end-user experience, collaboration technologies, and analytics—all relatively new areas of spend. In contrast, the in-house legal budget is mostly going toward people (with a mere 3 % toward legal technology). Continuing to justify head count can be a challenge, so GCs may have to position lawyers as helping advance the user experience for internal clients.

Although GCs would prefer to think about legal budgets in isolation, CFOs rarely do, so knowing what some of your corporate counterparts' **budget growth looks like is helpful.**

12. Don't Underestimate the Power of Your TruePeers™ in Budgeting— External benchmarking isn't a consistent business discipline across all companies, but many general counsel like to benchmark their budgets relative to industry peers or revenue peers. Over time, we've found that to be a necessary but sometimes insufficient benchmark. To create targeted accuracy and provide proper relevance, CEB developed a statistical model to isolate the factors that truly determine legal spending. Three factors—company size, complexity, and litigation—have a clear relationship to spending, while other factors (e.g., industry, regulation, business model, product volume) don't actually explain significant variations in spend. In essence, large, complex companies with more litigation spend similar amounts on legal services, as do small companies with few legal entities and less litigation. Broad demographics, such as industry, simply do not explain these budget differences as well.

With the demand for legal services continuously increasing year over year, leading companies are implementing some or all of these 12 guidelines to ensure the right resources are in place to achieve annual goals and cost-savings is realized to ultimately shape longer-term strategic priorities.

Contact us to learn more about the tools available to help you employ these insights.

The Three Biggest Barriers to Data Privacy Program Effectiveness

By Brian Lee, Managing Director, CEB Data Privacy Leadership Council

Despite growing concern about the likelihood of a data breach, senior executives underestimate the resources and structure necessary to create an effective data privacy program. The result is usually an ad hoc, overlapping set of responsibilities, activities, and management, which often leads to poor risk visibility. The best companies are consolidating responsibilities under a formal privacy function and creating realistic policies and training that reinforce the importance of keeping critical data secure.

With high-profile data beaches occurring on an almost-daily basis, senior executives are increasingly worried about their company's vulnerability to the loss of sensitive data. In the past 12 months alone, 43% of companies experienced a data breach. Whether caused by an external party or through the loss of laptops by negligent employees, the financial and reputational harm of a breach can be significant. In addition, most executives believe these data breaches will only become more prevalent, given companies' increasing use and collection of sensitive data.

Less than one-third of chief privacy officers are **satisfied with their company's current privacy efforts.**

Faced with higher expectations to manage privacy risks with limited resources, most chief privacy officers (CPOs) are unsatisfied with their company's current privacy efforts. CPOs point to three particular challenges that hinder the effectiveness of a privacy program.

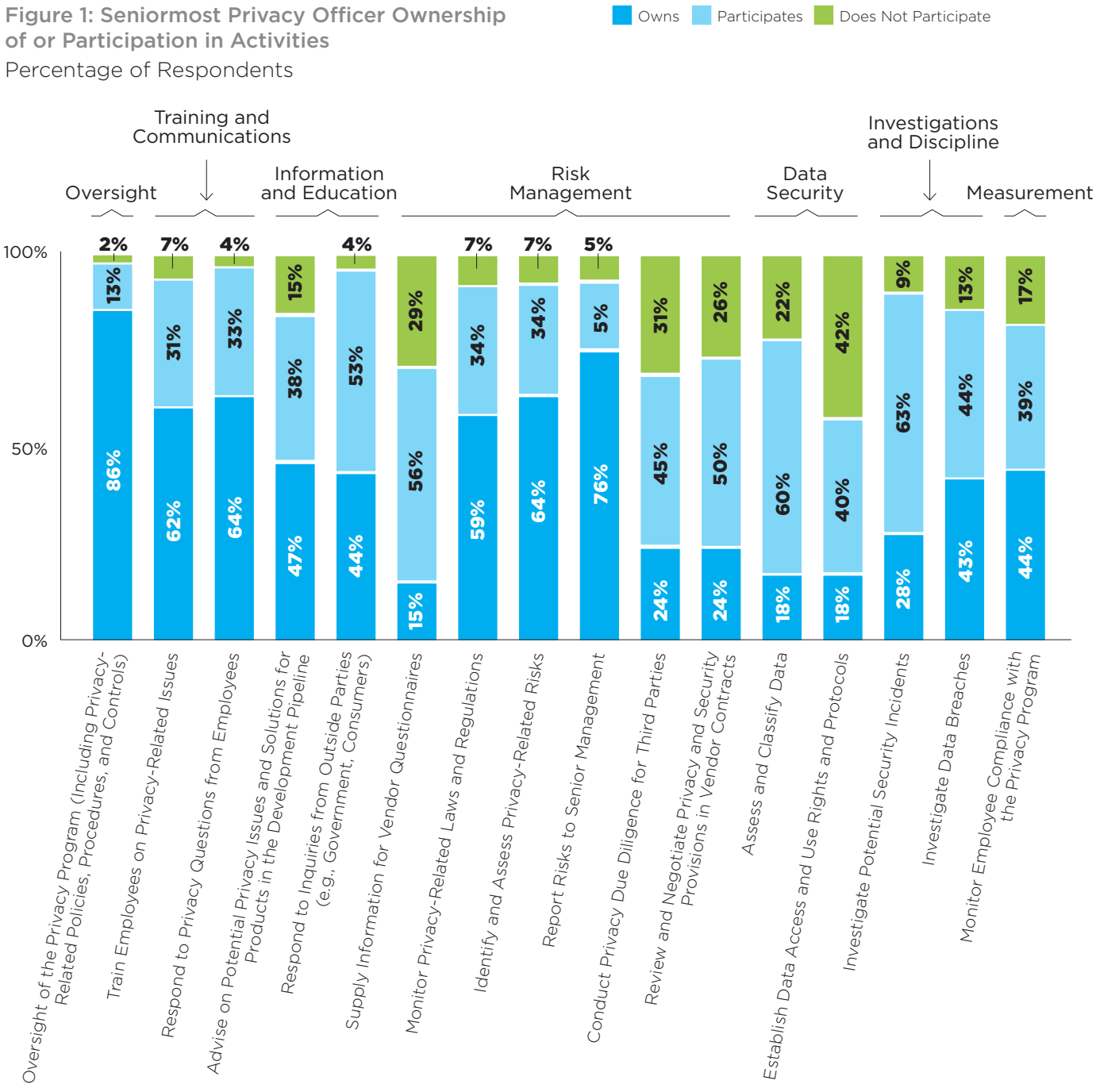
Challenge 1: An Inconsistent Mandate (and Set of Resources)

Although almost all directors and senior executives are concerned about privacy risks, they disagree on how to staff and resource the associated work. In fact, only 42% of large companies have a designated CPO, and, depending on the organization, the data privacy function can reside in any of 10 corporate functional areas, including Legal, Compliance, IT, and HR. To make matters more difficult, our research finds that most companies lack a dedicated head of Data Privacy; rather, that person maintains another role in addition to privacy responsibilities.

This lack of consensus extends beyond job titles to how companies resource these functions and, ultimately, the responsibilities they take on. Figure 1 outlines the typical responsibilities of a CPO. Interestingly, although the CPO most often owns areas such as program management, training and communications and some aspects of risk management, he or she is less likely to be involved in traditional legal or information security–related issues. That said, the CPO often participates in each of these activities to various degrees, creating confusion between the CPO and the functions that primarily own these activities.

Figure 1: Seniormost Privacy Officer Ownership of or Participation in Activities

Percentage of Respondents



n = 54–56.

Source: CEB 2014 State of the Privacy Function Survey.

Note: Totals may not equal 100% due to rounding.

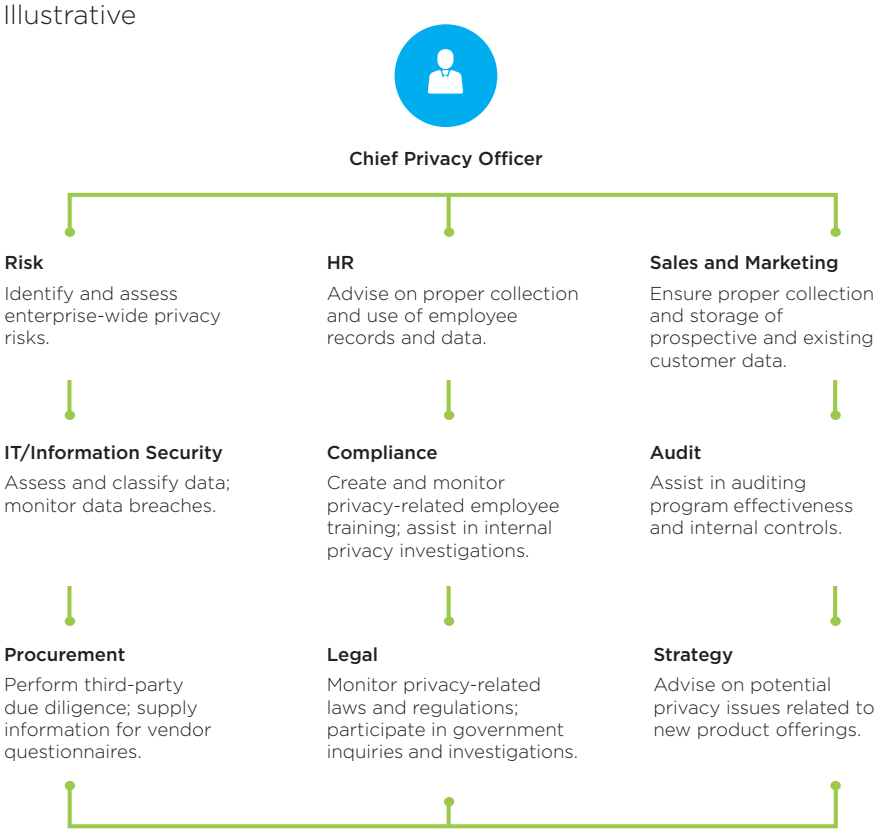
Challenge 2: Unclear Governance of Activities

Similarly, CPOs report difficulty in navigating across an enterprise-wide environment when managing privacy and information risk. The cross-functional nature of data privacy creates numerous problems with the ownership of even simple activities. In different organizations, accountability for activities such as determining risk appetite, tracking external risks, and overseeing third-party compliance can often be diffused among as many as 5–11 second-line functions. This scattered accountability creates serious confusion within the organization and can materially slow the response to privacy threats.

In addition, CPOs increasingly work with other functions to ensure data is properly categorized and protected. CPOs' success depends heavily on their ability to work with key stakeholders throughout the organization. Figure 2 shows several examples of how the CPO works with these stakeholders, from assessing and classifying data with IT or Information Security to ensuring social media campaigns and digital apps notify users of the variety of information collected by customers. Each of these initiatives require solid communication and relationship building, which can be challenging for even the savviest of CPOs.

Figure 2: Select Joint Initiatives Between the Chief Privacy Officer and Other Functional Heads

Illustrative



Source: CEB analysis.

Challenge 3: Lack of Employee Awareness

It's one thing to know the laws and regulations that govern privacy; it's another, however, to change employee behavior. Our research finds that the greatest risks associated with the use of sensitive data are related to employee negligence. In fact, almost 55% of data privacy incidents are unintentional, 42% of which because the employee was unaware of the requirements. This lack of understanding suggests that training should be a vital part of privacy risk management. Although most companies report that they already use some method of data privacy training, it often is too generic or technical for most employees to understand. Instead of focusing on specific behaviors and actions, training often cites laws and regulations, which causes employees to quickly lose interest. In addition, any information that employees retain after training is quickly forgotten without proper reinforcement throughout the year. Our research finds that, in general, only 36% of employees remember key lessons from training.

Almost 55% of data privacy incidents are unintentional, with 42% of those unintentional violations occurring because the employee was unaware of the requirements. This lack of understanding suggests that **training should be a vital part of privacy risk management.**

What CPOs Should Do

In light of these challenges, CPOs must use resources throughout the organization. CPOs can maximize the effectiveness of their privacy programs by doing the following:

- **Clarify Stakeholder Expectations and Prioritize Critical Activities Accordingly—**The CPO's role has evolved from simply understanding and complying with the legal privacy landscape to translating that understanding into a realistic set of actions that business leaders and employees alike can follow. CPOs must work with key senior stakeholders to clarify their expectations and set clear goals for the program. In addition, once privacy department priorities are set, CPOs should benchmark their department's staffing and resourcing needs to better understand where they may be under-resourced.
- **Lean on Other Functional Heads to Maximize the Effectiveness of Privacy Initiatives—**The key to an effective privacy program is developing strong relationships with key stakeholders throughout the company. Data privacy functions that gather input from other functional leaders (and employees) often create more effective privacy policies while obtaining better senior management buy-in and employee adoption.
- **Maximize Training Effectiveness by Targeting High-Risk Employees and Delivering Actionable Training—**Training only works if employees retain what they learn. CPOs should first target their training efforts toward high-risk employees (e.g., employees who handle large amounts of sensitive data, social media users) to manage the risk of data misuse or mishandling. In addition, create memorable training by connecting them to real-life, applicable situations and tasks specific to employees' routine workflows.

The role of the CPO has evolved from simply understanding and complying with the legal privacy landscape to **translating that understanding into a realistic set of actions** that business leaders and employees alike can follow.

Setting Internal Audit Plans for 2015

By Ruth Shaikh, Associate Director, and Patricia Simione, Research Analyst, CEB Audit Leadership Council

Each year, we survey chief audit executives (CAEs) about their plans and expectations relating to budget, staffing, department operations, and priorities for the coming year. We have analyzed the results of this year's Budget and Head Count Survey and Agenda Poll to identify key benchmarks that support CAEs as they set departmental plans for 2015.

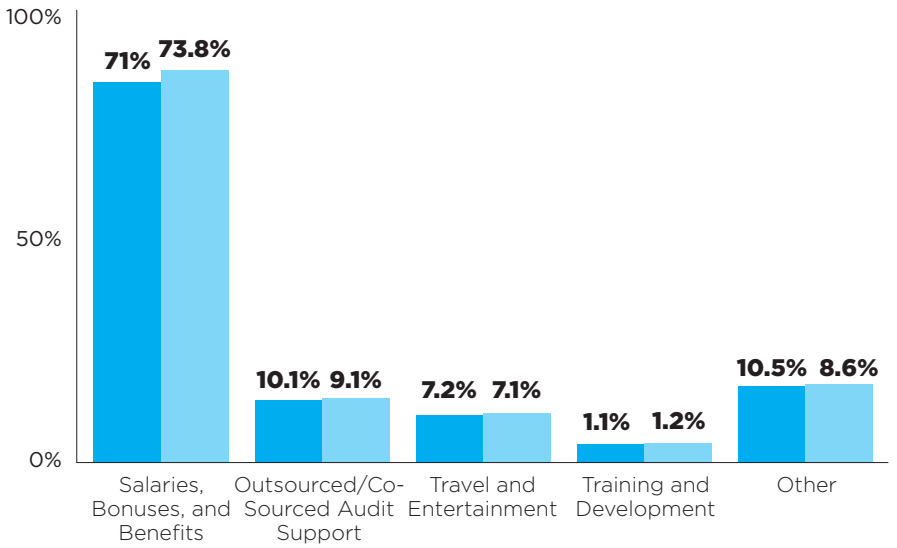
A Look Back at 2014 Resourcing Decisions

In 2014, most internal audit teams maintained level budgets and staffing compared to 2013. The median internal audit budget in 2014 was $3.57 million versus $3.75 million in 2013. Median head count also stayed flat at 2.67 staff per billion US dollars in corporate revenues.

> In 2014, Internal Audit's budget and staff levels were **largely unchanged.**

Unsurprisingly, the allocation of audit department resources changed very little as a result, with CAEs finding few new resources to invest in new activities without diverting coverage from elsewhere (Figure 1).

Figure 1: Audit Department Budget Allocation
Median Percentage of Total Department Budget

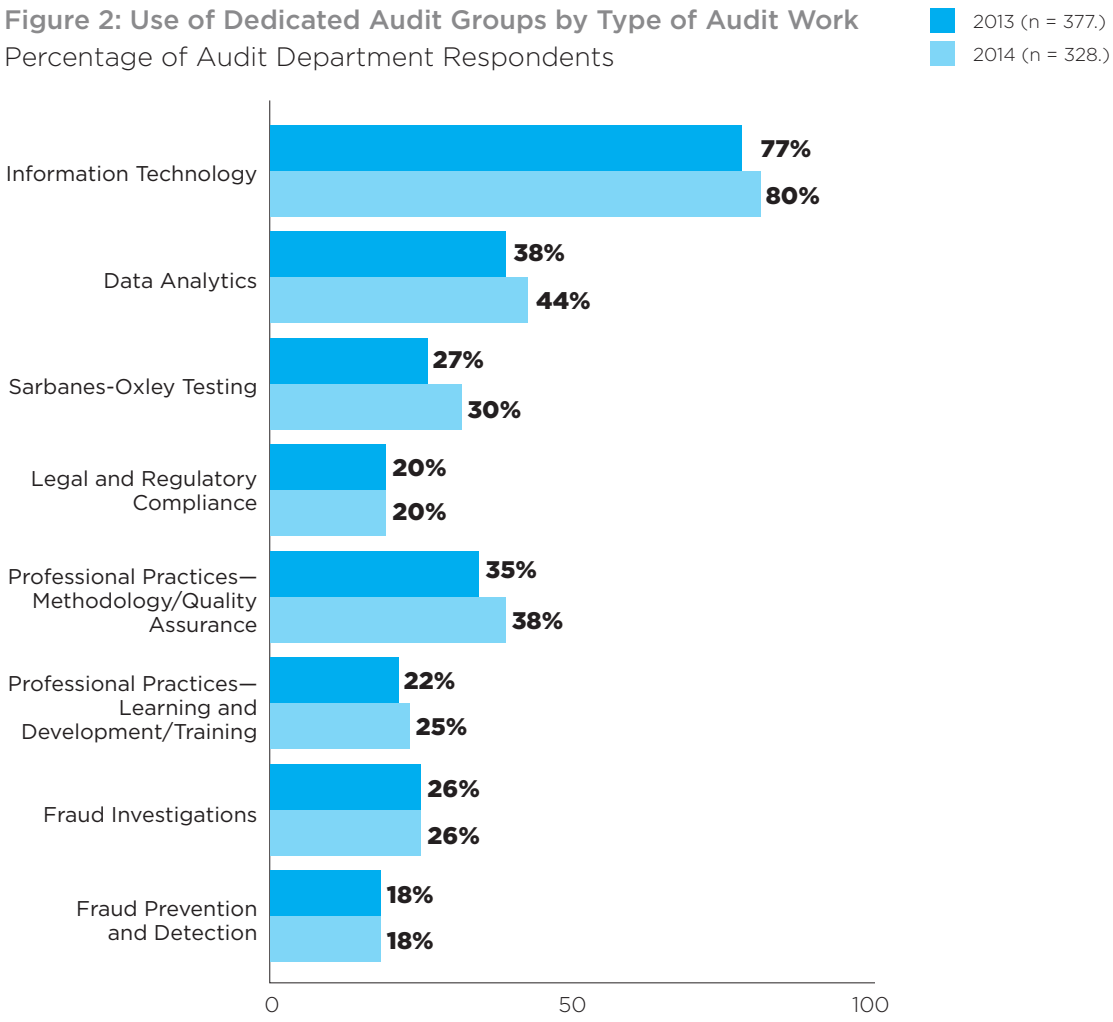


Source: CEB 2014 Budget and Head Count Benchmarking Survey.

In 2014, Internal Audit's time allocation also stayed fairly consistent with previous years. The five biggest areas of focus this year were operational audits (29%), financial audits (15%), Sarbanes–Oxley (SOX) or equivalent (13%), IT audits (13%), and regulatory compliance reviews (7%). The budgets for co-sourcing and outsourcing stayed flat.

CAEs use dedicated teams to increase specialization, role clarity, and audit execution quality. Figure 2 shows the prevalence of dedicated teams for data analytics, IT, SOX, legal and regulatory compliance, methodology and quality assurance, learning and development, and fraud over the past two years.

Figure 2: Use of Dedicated Audit Groups by Type of Audit Work
Percentage of Audit Department Respondents



Source: CEB 2014 Budget and Head Count Benchmarking Survey.

Audit's 2015 Resourcing Outlook

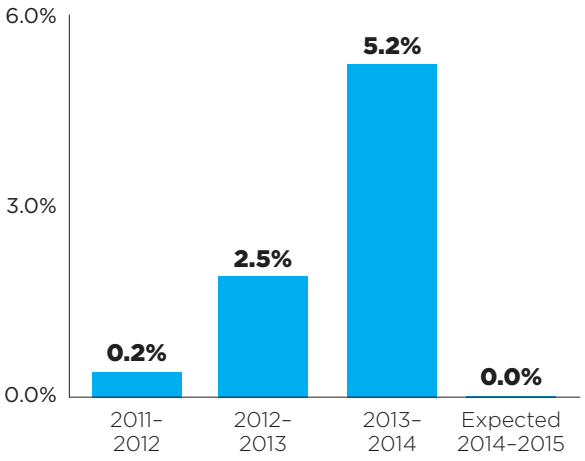
Audit department resourcing is expected to remain relatively flat, on average, in 2015 (Figure 3). Over the next 12 months, 47% of CAEs expect small to moderate 2015 budget increases, 38% expect budgets to stay flat, and 15% anticipate slight budget reductions.

Entering 2015, audit department budget and staffing are **expected to remain flat.**

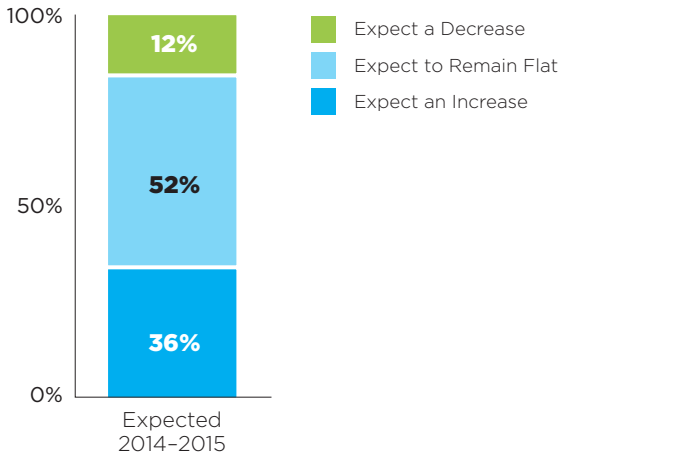
Consistent with the past four years, audit staff levels are projected to remain relatively flat; 36% of CAEs project head count growth, 52% project no change in head count, and 12% foresee small contractions. CAEs also expect an average staff turnover of 17%, excluding rotational auditor attrition.

Figure 3: Year-Over-Year Change in Internal Audit Resources

Median Change in Internal Audit Budget (n = 92.)



Percentage of Internal Audit Teams Expecting Staffing Changes (n = 91.)



Source: CEB 2012–2014 Budget and Head Count Benchmarking Surveys.

Audit's 2015 Audit Planning Outlook

Although the budget and head count figures suggest that Internal Audit's scope is unchanging, continuous shifts in the business and regulatory risk environment are causing CAEs to rethink time allocation for the next 12–24 months.

One potential blind spot that audit teams are racing to cover is information security assurance; only 36% of CAEs believe they have enough staff to cover their greatest information security risks, and about half of audit departments plan to grow their IT capabilities over the next two years.

Functional Priorities for the Coming Year

Despite stagnant budget and staffing levels, CAEs are looking for ways to maximize value delivered to the organization. Three specific areas are highlighted as priorities for functional improvement in 2015: implementing data analytics, enhancing audit talent, and managing organizational change.

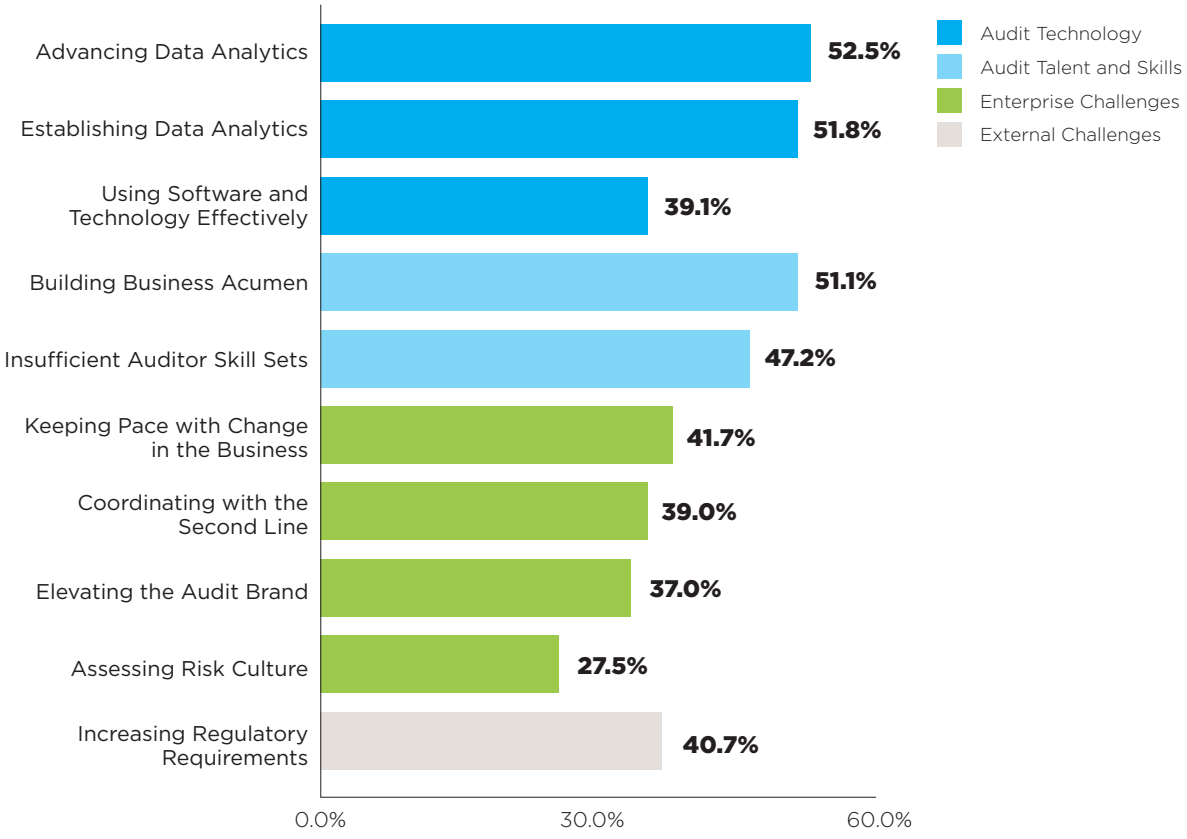
CAEs identified three distinct priorities for audit department success in the coming year: **data analytics, auditor talent, and managing organizational change.**

- **Data Analytics:** Fifty-two percent of CAEs identify the advancement of their data analytics capabilities as a high or very high priority for 2015, primarily because data analytics is seen as a key solution for making internal audit groups more efficient.
- **Talent Development:** Nearly two-thirds of CAEs are looking to improve alignment between auditor skills with their organizations' changing risk profile. Inadequate business acumen is particularly acute: 63% of CAEs reported this as an investment area for their teams.
- **Managing Organizational Change:** Most CAEs expect that changes in the organizational control environment—caused by cost cutting and shifts in company strategy—will significantly affect audit department coverage and operations over the next 18–24 months. Issues such as keeping pace with organizational change and coordinating assurance efforts with the second line illustrate the effect of wider organizational changes on Audit's activities.

Additional findings about CAEs' functional priorities for 2015—based on CEB Audit Leadership Council's annual membership poll—are illustrated in Figure 4.

Figure 4: Top 10 Audit Priorities for 2015

Percentage of CAEs Rating Priority as "High" or "Very High"



n = 117.

Source: CEB 2014 Annual Audit Membership Poll.

Leadership Councils

At the core of our membership programs are Leadership Councils. Through these we convene and provide support for decision makers in the following areas across legal, compliance, audit, and risk management functions:

CEB Legal Leadership Council

- Reduce Legal Department Spending
- Increase Legal Department Productivity
- Limit Enterprise Exposure to Legal Risks

CEB Risk Management Leadership Council

- Build Executive Support and Improve ERM Performance
- Save Time and Secure Budget for Key ERM Activities
- Reduce Enterprise Risk and Improve Decision Making

CEB Compliance & Ethics Leadership Council

- Improve Compliance and Ethics Program Effectiveness
- Save Time and Money on Compliance Training
- Reduce Compliance Risks

CEB Audit Leadership Council

- Access Strategic Guidance on Audit Issues
- Use Tools and Templates to Perform Audits Faster
- Train and Develop Your Audit Team

CEB Data Privacy Leadership Council

- Build and Resource an Effective Privacy Program
- Create Impactful Privacy Policies and Training
- Monitor and Measure Privacy Program Effectiveness

CEB RiskClarity: A Corporate Integrity Service™

- Create an Effective Channel to See Bad News Before It Goes Public and Becomes Costly
- Identify Cultural Weak Spots That Present Increased Risk and Missed Strategic Opportunities
- Determine Clear, Actionable Solutions to Mitigate Risk

CEB Support for Senior Executives Throughout the Enterprise

Featured Webinar

Q4 Emerging Risks Webinar (11 December 2014)
Hear how peer organizations are identifying and managing major risks on the horizon for their organizations.

For CEB Risk Management, Audit, and Compliance & Ethics Leadership Council members

Featured Diagnostic

Functional Data Privacy Maturity Diagnostic (Available January 2015)
Implement a tool that measures maturity levels for specific privacy activities and identifies opportunities to improve your privacy function.

For CEB Data Privacy Leadership Council members

Featured Meeting

Legal Risk Management: Building Your Organization's Legal IQ (17 March 2015)
Learn how leading general counsel build a culture of legal risk management to ensure critical business decisions receive necessary legal guidance.

For CEB Legal, Compliance & Ethics, and Risk Management Leadership Council members

Featured Research

Building a Risk-Based Monitoring Dashboard: Practical Guidance and Metrics (Available Now)
Learn how to measure the root causes of misconduct to improve your predictive monitoring capabilities.

For CEB Compliance & Ethics Leadership Council members

Featured Report

Audit Plan Hot Spots (Available Now)
Review the top 10 risks affecting audit plans in the upcoming months, questions to support discussions with management, and key risk indicators.

For CEB Audit Leadership Council members

About Us

CEB, the leading member-based advisory company, equips more than 10,000 organizations around the globe with insights, tools, and actionable solutions to transform enterprise performance. By combining advanced research and analytics with best practices from member companies, CEB helps leaders realize outsized returns by more effectively managing talent, information, customers, and risk. Learn more at **cebglobal.com.**

Contact Us

+1-866-913-8103

LRC.Support@
executiveboard.com

www.executiveboard.com/
legal-risk-compliance

CEB
WHAT THE BEST COMPANIES DO