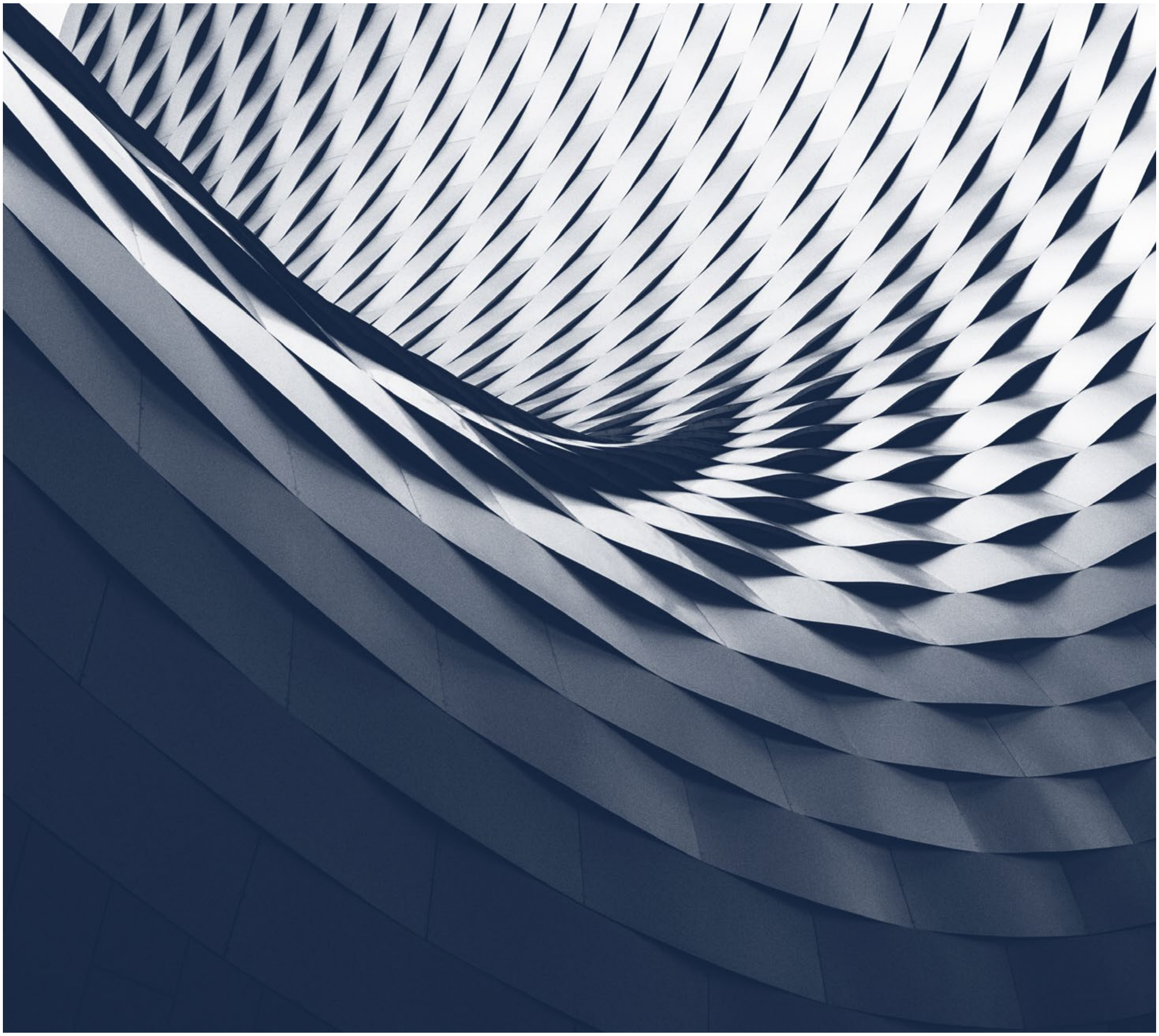


DLA PIPER'S 2018 COMPLIANCE & RISK REPORT

As Compliance Settles In, Personal Liability Concerns Persist and Technology Emerges as the Next Frontier

DLA PIPER

Foreword

Amid a period of strong economic growth, most compliance professionals say their resources and access to their organization's governing board are sufficient. So, why has their concern over their own and their CEO's liability increased over the past year?

DLA Piper's 2018 *Compliance & Risk Report* points to two potential and complementary explanations. First, the corporate world has been on a hot streak of late, closing a tremendous number of transactions over the past year. The pace and complexity of mergers and acquisitions may be a cause of CCOs' restlessness, not to mention the anxiety that comes with keeping the newly combined venture on track vis-à-vis its legal, regulatory and contractual obligations. Second, as the businesses they serve increasingly leverage technology solutions to drive productivity and efficiency, compliance departments largely have not followed suit – perhaps because the available technology solutions are not yet up to the task or cost-effective, or because compliance professionals have not yet figured out how to use technology to detect, prevent and mitigate compliance failures. And for those early adopters who have devised and implemented technological solutions to help, say, monitor transactions or detect operational snafus, there's the question of how to make sense of, let alone protect from misuse or disclosure, the troves of data that only exist because of the technological solutions.

Stasia Kelly
Co-Chair, DLA Piper's Governance and Compliance Practice
Managing Partner (Americas)

These and other insights are drawn from our third annual *Compliance & Risk Report*. Beyond exploring traditional compliance program features, this year we focus on how technology is used or not used to enhance the efficacy of compliance programs. We are proud to present the results, paired with practical guidance and pragmatic suggestions for compliance professionals.

Table of Contents

Executive Summary

As Compliance Settles In, Personal Liability Concerns Persist and Technology Emerges as the Next Frontier

Corporate compliance officers (CCOs) around the world are feeling better about many aspects of their companies' operations, particularly their allotted resources and organizational clout. But some complacency and difficulty finding the right technology solutions appear to be emerging – even as concerns about personal liability are again increasing.

That's according to DLA Piper's 2018 Compliance & Risk Report, the third survey in as many years that takes the pulse of individuals involved in corporate compliance. While the 2017 report showed the compliance function growing up, this year's findings seem to point to growing pains.

FIRST, THE GOOD NEWS

The CCOs surveyed feel good about their ability to do their jobs. 89 percent, the highest percentage in the history of the survey, say they agree to at least some extent that they have the resources, clout and board access they need. That's driven by 42 percent of respondents who agree to a great extent that they have what they need – a 12 percentage-point jump from each of the past two years.

89%

Say they have sufficient resources, clout and board access

But when specifically asked about budgets, only 55 percent of CCOs say what they have is sufficient to accomplish the goals that support adequate compliance programs. That's a 16 percentage-point jump from 2017 – perhaps fueled by companies providing more resources amid a strong economy – and 14 percentage points better than 2016.

"If CCOs use project management tools that include risk assessment, prioritization and project planning, then the activities that they think are obvious areas of residual risk can be discussed with the board to make the case for increased budget," one CCO said. "In other words, if CCOs have enough board access, they ought to use it."

Indeed, CCO overall satisfaction appears driven by their relationships with their boards and reporting regularity. After a slight decrease in 2017, 63 percent of respondents say they provide compliance metrics to their boards of directors and/or audit committees. More notably, quarterly reporting now appears to be the norm, with 68 percent of respondents saying they report on that cadence, up 14 percentage points from 2017 and 24 percentage points from 2016. Much of that appears to come from a decrease in the percentage of respondents who reported only annually or never in past surveys.

STRUGGLES WITH TECHNOLOGY

For the first time, this year we asked respondents how they're using technology. The results show that compliance departments are trailing other business units in embracing and leveraging technology. Why this is so is less clear.

80%

Don't use technology or automated tools to track and measure compliance training

About 90 percent of CCOs are using technology for training, far and away the most common application. While most companies are using technology for the training itself, only about one in five use technology or automated tools to measure compliance training participation among employees. This seems to be a fertile ground for expanding the use of technology, because the percentage of companies that penalize employees for not completing training or policy certifications improved to 56 percent. While employees are being disciplined more often for missing compliance training, their supervisors have largely escaped accountability. Only about a quarter of respondents say they evaluate managers or supervisors on whether their direct and indirect reports complete required compliance training.

While technology is being heavily used for training, the same cannot be said for compliance communications (51 percent), risk assessment (43 percent), and M&A due diligence and post-acquisition integration (26 percent). This could indicate that the available tools haven't yet advanced enough to be useful or cost-effective to CCOs, particularly given that about half of them have concerns about their budgets.

"We do look at external data to judge compliance risks, but not in a scientific fashion," one CCO said. For example, "we have not done any sort of scientific analysis … to see whether the trend for enforcement actions are up or down, whether penalties are increasing or decreasing, etc. "

26%

Use technology solutions for M&A due diligence and integration

Only about 40 percent of respondents use internal or external data to help forecast future compliance risks or measure the trajectory of future compliance risks. Nearly a third aren't taking steps to protect against unauthorized disclosure of information generated by the use of technology (despite a great deal of apparent concern about discoverability and disclosure). Only 5 percent are using mobile apps for training purposes.

It's hard to know how much of these findings stem from a lack of effective and affordable technology versus organizational reluctance. Either way, there's an opportunity for technology to strengthen compliance departments in the years ahead.

AND ABOUT THAT PERSONAL LIABILITY…

75 percent of respondents are concerned about their own or their CEO's personal liability. That's up from 66 percent in 2017 – and nearly as high as the 81 percent in 2016. A quick history lesson (and some economic prognosticating) might explain the trend lines.

75%

Of respondents are concerned about their personal liability or their CEO's

The 2016 survey was taken in the wake of the Yates Memo, a Justice Department document that declared the DOJ's intention to prosecute corporate executives for compliance failures. It was a big moment in the compliance world, but one that has resulted in little prosecution. The lack of enforcement, combined with a belief that regulators would be more business-friendly under President Donald Trump, could have calmed CCOs' nerves last year.

But savvy CCOs recognize that extremely high M&A volume carries risk as compliance personnel vet national and international deals by conducting everything from initial due diligence to operational integration – often with multiple transactions occurring simultaneously. And the first half of 2018 was especially hot, with more than US$2.5 trillion in global activity and more than US$1 trillion in the US alone, according to Thomson Reuters. It's possible we're seeing a sprint to close deals for fear of an end to the economic growth cycle that began in 2009. And if that volume wasn't enough to frazzle CCOs, the Department of Justice in July 2018 highlighted the extension of the Foreign Corrupt Practices Act (FCPA) to M&A transactions.

The frenetic M&A pace of 2018 won't continue forever, so its effect on CCOs will fade. But the resulting concerns – and apparent reluctance to use technology to address them – serve as a powerful reminder: There will always be another challenge, and technology appears to be a powerful weapon that CCOs have yet to fully exploit.

Guidance Section

What CCOs (and Boards) Need to Know

Taken as a whole, this year's survey reveals some interesting trends regarding the use of technology by compliance professionals. Although a given in most corporate functions these days, compliance has not yet fully embraced technology. While this presents an opportunity to implement technological solutions within the compliance function, how much to send on technology and how effective technology can be are open questions. And yet some of the same issues continue to challenge compliance professionals around the world – board interaction and support, training, reporting and communications. To assist compliance officers in dealing with these issues, we have assembled the following set of basic principles and best practices.

TECHNOLOGY

- **Have a plan.** When it comes to investing in technology, understand what you are doing and why. Think through what you intend to do with the information developed and how you will safeguard it from misuse.
- **Data without context is meaningless.** Technology, particularly data analytics applications, should help you better understand the business and its risks. But without partners from the business and service centers to help place the output into perspective, the information developed could more easily have you running in circles than speed you on the way to more sound and compliant operations.
- **Leverage existing tools.** Examine how other business units are using technology to compile and analyze data. The best solution for you or some form of it may already exist within your company.
- **Be patient and pick your spots.** Technology should make compliance professionals' jobs easier, create efficiencies and relieve resource strain. Don't just dive in because the business, other functional units or peers are implementing technological solutions. Do some research and benchmark. Wait until the technology meets your needs. There may be risk in being an early adopter.

BOARD EXPERTISE

- **Be selective.** In searching for new board members, consider their expertise and experience in compliance and, as appropriate, sub-specialties like cybersecurity.
- **Training.** Many boards are targeting key members to train on compliance-related matters. This may include subjects like compliance generally, privacy, cybersecurity, anticorruption and risk assessments.
- **Share the knowledge.** Once you've identified board members with the requisite compliance expertise, it is imperative that they share their knowledge and facilitate discussions at board meetings on those compliance issues. A company-wide "speak up" culture starts at the top.

BOARD REPORTING

- **Share more data.** Many companies regularly report only hotline statistics and investigation resolution information. While this is critical, more can and should be shared. Consider adding a data analytics perspective to identify trends and forecast risks before they reveal themselves in the hotline statistics and to provide context for the information.

- **Emphasize proactive risk management.** Apprising your board or audit committee of how you conduct risk assessments and presenting those results allows the members to better understand and challenge how the company is mitigating its legal and regulatory risks. Consider suggesting areas they may probe with other senior executives to better understand how compliance is perceived and what the business units are doing to operate compliantly.

- **Talk to your board/audit committee about resources and staffing.** In exercising their fiduciary duties, your board/audit committee needs to have a clear picture of how the compliance program is resourced and functioning. Ultimately, they will be held accountable for weaknesses in the compliance function, so make sure they know what resources you have and what you need. Benchmarking is hard to do without access to a network of industry compliance contacts.

BOARD TRAINING

- **Assume nothing.** Training is supposed to be educational and designed to ensure that all directors have a working knowledge of important compliance risks. Don't be afraid to spend a few minutes setting the table for a training discussion by first addressing the basic nature of the risks, the associated legal or regulatory context, and how directors can help.

- **Make it relevant.** Focus discussion around current and future risks, how board members' responsibilities and tactical strategies can help the company avoid major missteps, and what actions they should consider should a significant challenge arise. Directors are very busy people. Deliver the training in a manner designed to get the biggest bang for the buck. Strive for interactive discussions that draw comments from all directors. It may help to talk with them first to understand their backgrounds and what engages them.

MULTINATIONAL ISSUES

- **Calibrate your compliance program.** Directors should ask questions to ensure that the compliance program accounts for the geographic spread of the organization's operations and the value and risk profile of the business conducted in each jurisdiction. If the company's geographic reach is broad, discipline for compliance violations can be inconsistent if remediation is not tracked globally and reported to the board.

- **Be flexible.** Multinational organizations must remain nimble and avoid falling into the trap of applying one-size-fits-all strategies. What works in one jurisdiction may not work as well in another. Take into account changes in the business, such as new products, markets sales strategies and compensation plans.

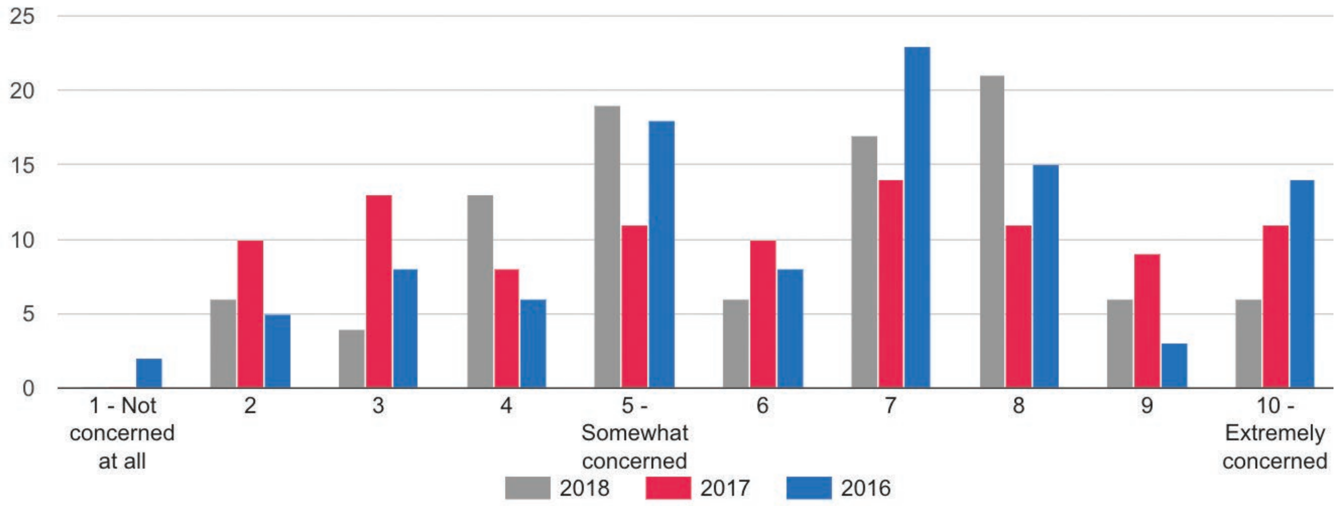
- **Acquisitions can quickly change the risk profile of a company.** Proper alignment between the compliance program and business development team can prevent unanticipated and unwanted liabilities.

- **Respect local laws, customs and language preferences.** Make sure your code of conduct and policies and procedures are available in the language(s) most commonly spoken among employees. Promote awareness of the hotline and the importance of compliance in a way that will resonate with the local employee population and confirm that reports are handled in a consistent and timely manner across all jurisdictions.

Survey Findings

Personal Liability

Q1: On a scale of 1 to 10 (with 10 being greatest), how concerned are you about your personal liability as a CCO or the personal liability of your company's CEO?



- The level of respondents who are at least somewhat concerned shot up to 75 percent in 2018, after falling from 81 percent in 2016 to 66 percent in 2017, despite more sanguine feelings among respondents about resources available to them.

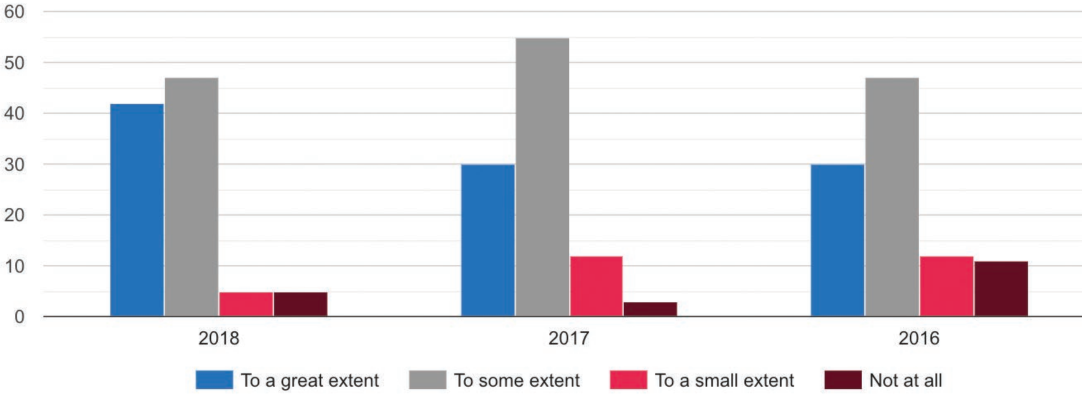
- The increased personal liability concerns are likely the result of CCOs struggling to keep pace with record M&A activity – which might be influenced by dealmakers moving rapidly before the current window closes. "It's … hard to ignore that the last two occasions when M&A activity reached similar levels were a year before the financial crash in 2007 and just before the bursting of the dot-com bubble in 2000," Jana Mercereau, head of corporate M&A for Great Britain at Willis Towers Watson, told Bloomberg.

- Concerns in the survey two years ago came in the wake of the Yates Memo, which signaled that the Justice Department would hold CCOs personally liable for compliance failures. But few prosecutions have occurred since, even after then-Attorney General Jeff Sessions said in April 2017 that the Trump Administration would largely maintain Obama-era policies regarding white-collar crime.

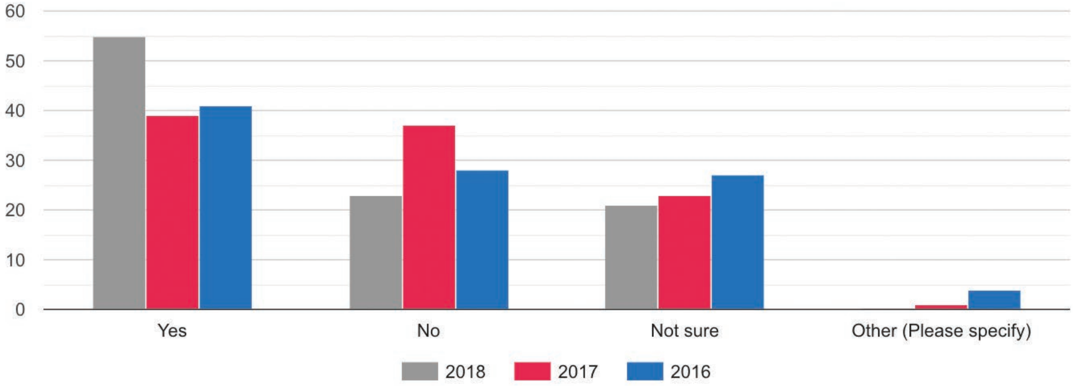
- Board members we surveyed were generally more concerned than CCOs, mirroring findings from the 2017 report.

State of Compliance

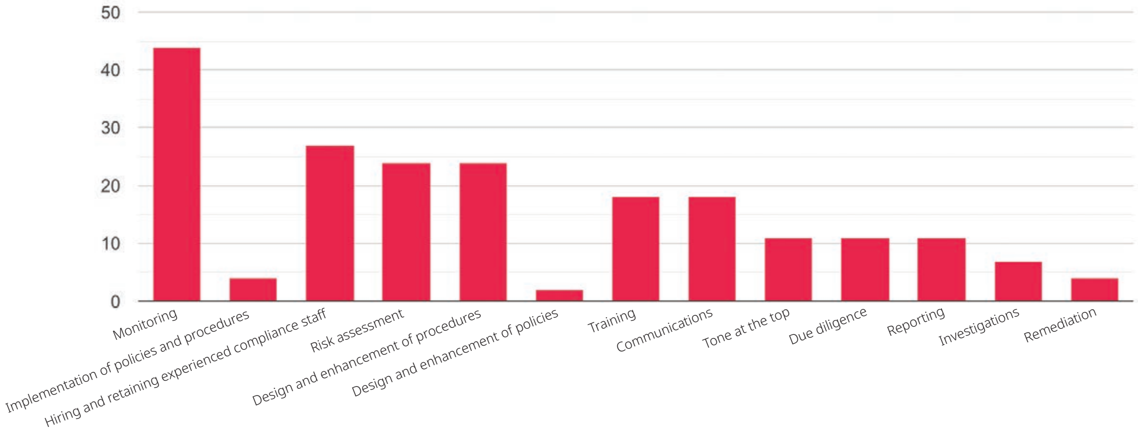
Q2: To what extent do you believe you have sufficient resources, clout and board access to support your ability to effectively perform your job?



Q3: In your opinion, is your budget sufficient to accomplish the goals you believe are needed for an adequate compliance program at your company?



Q4: In which of these areas do you feel your compliance program is weakest? (Check all that apply)



Q5: What aspect of your compliance program takes up the largest amount of your time? (Rank the top 5 with 1 being the greatest amount of resources)

RESPONSES	OVERALL RANK
Data breaches/data privacy	1
General increased regulatory risk	2
Cybersecurity	3
Regulatory	4
Third-party due diligence	5
Anti-corruption	6
Increased litigation risk and class actions globally	7
Whistleblowers	8
Theft, fraud, corruption	9
Increased competition	10
Rising use of technology and social media	11
Business interruption	12
Trade	13
IP and trademark protection	14
Antitrust	14
Employment and labor in the context of global expansion	15
Natural disasters and disaster recovery	15
Weak economy	16

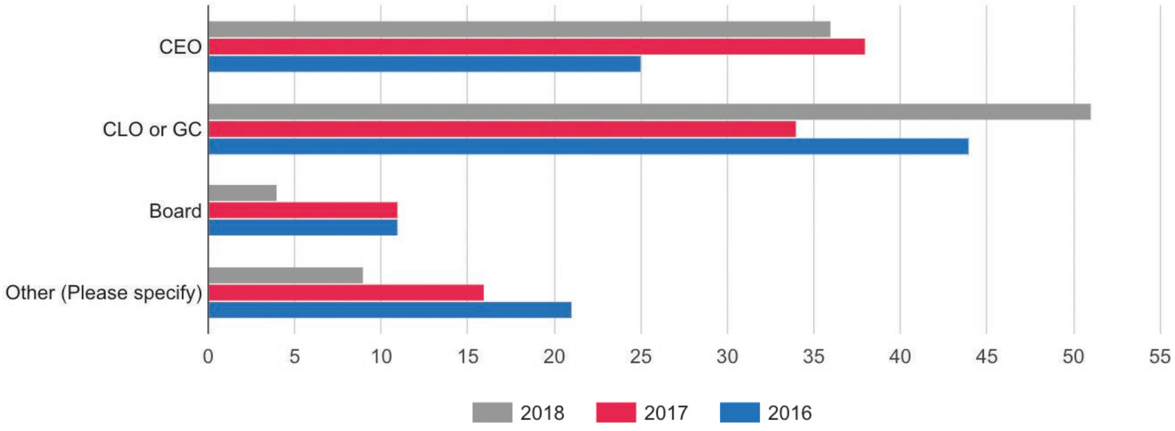
- CCO satisfaction in Question 2 reached its highest level in 2018, with a noticeable jump (from 30 percent to 42 percent) in respondents who strongly agree that they have what they need. This tracks with other findings in this year's survey that show CCOs are increasingly getting a seat at the table. Results from board members surveyed were largely in line with CCOs' assessment regarding resources, clout and board access.

- At the same time, there was a significant jump in the percentage of respondents who believe they have adequate budgets to accomplish their goals, from 39 percent in 2017 to 55 percent this year. This is likely the result of companies' willingness to add resources or personnel to compliance departments given the strong economy – but it shows a possible disconnect when CCOs are asked what they need to do their jobs generally, compared specifically with their budgets.

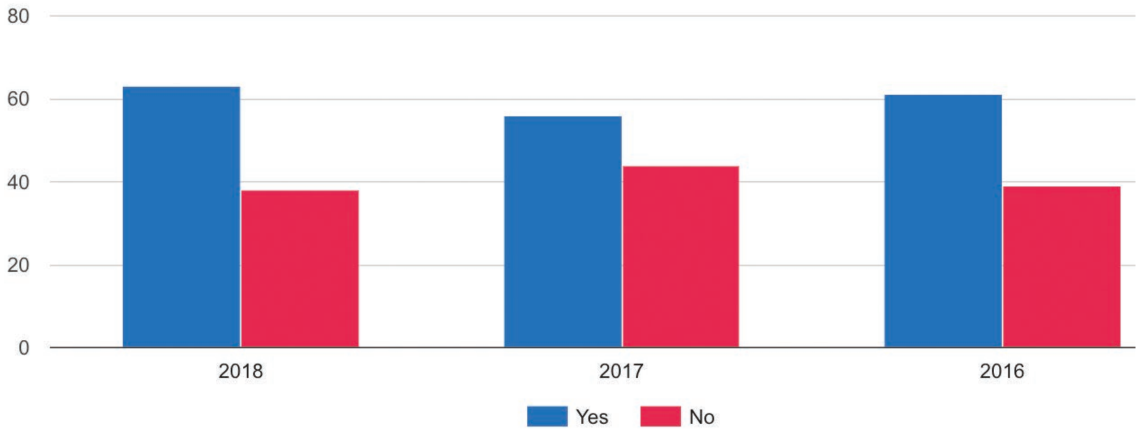
- We also asked respondents how they're spending their compliance budgets. Common answers were third-party due diligence, cybersecurity, training and hotline matters.

Reporting and Evaluation

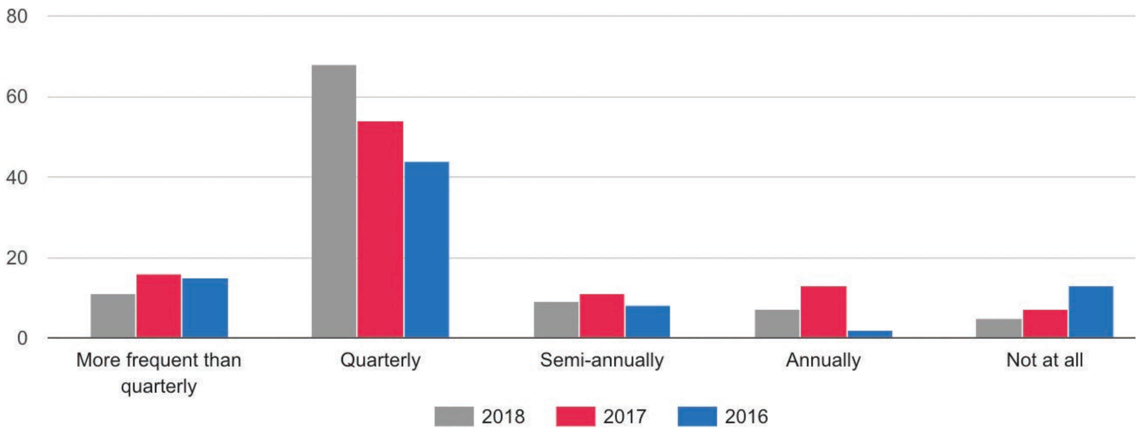
Q6: At your company, to whom does the compliance function report?



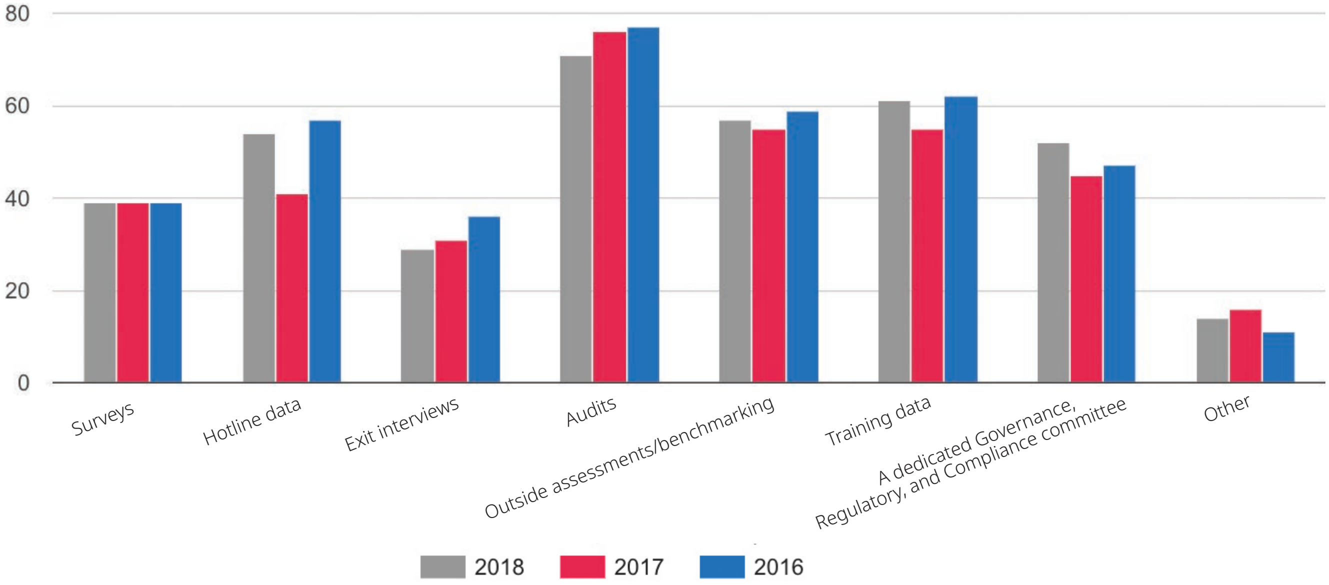
Q7: Do you report metrics to your company's board of directors and/or audit committee?



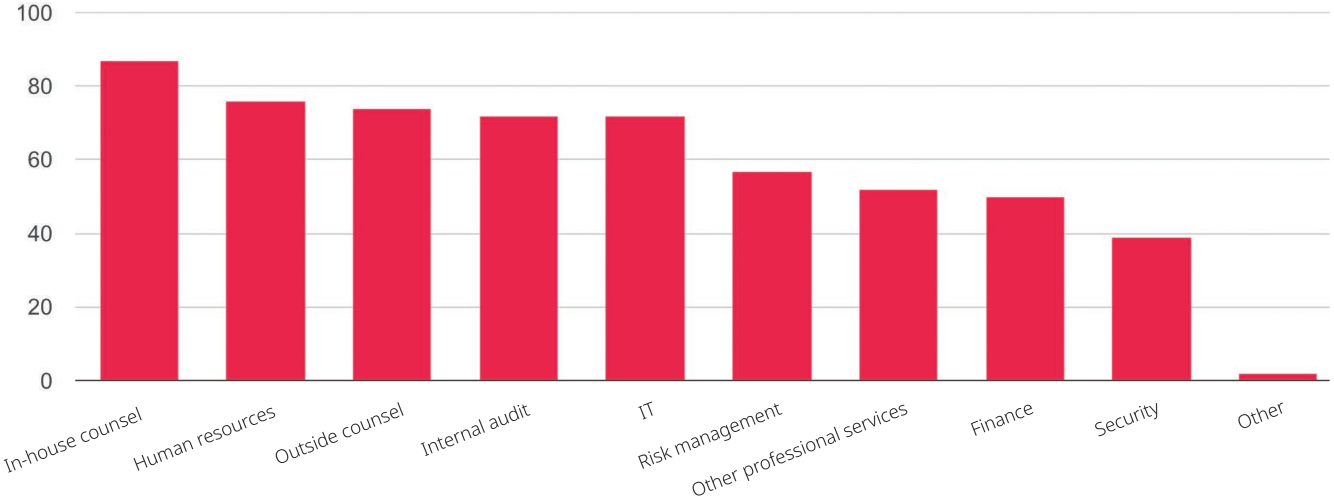
Q8: What frequency of reporting is expected from the compliance group?



Q9: What tools do you use to evaluate the effectiveness of your compliance program? (Check all that apply)



Q10: What resources do you currently leverage as part of your compliance program? (Check all that apply)



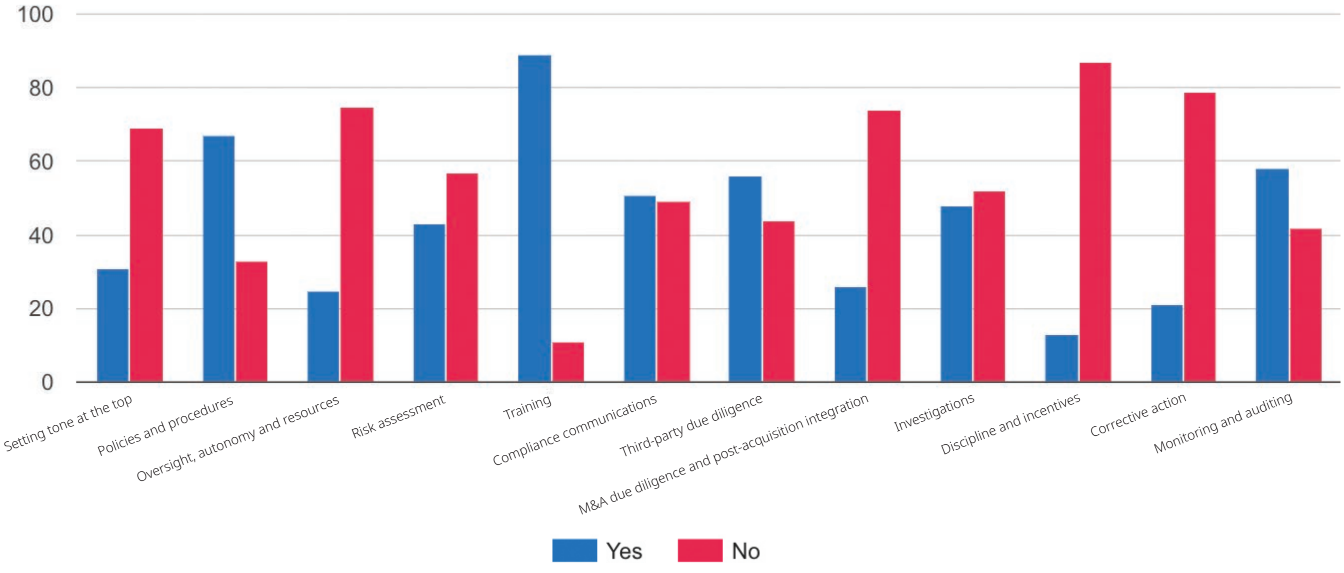
- When asked about the chain of command, directors surveyed had shifting thoughts regarding whom compliance departments should report to on a day-to-day basis. Some deferred prosecution agreements in the healthcare industry require that legal and compliance be separated. But this year's survey shows that legal is in vogue again.

- As companies' strategies regarding the reporting structure for compliance continue to shift, one CCO for a consumer product company said he preferred reporting to the general counsel or legal department. "The legal department is the obvious place to house managing legal risk," he said. "There are a lot of synergies – and regulators see that and can accept it if it's set up the right way."

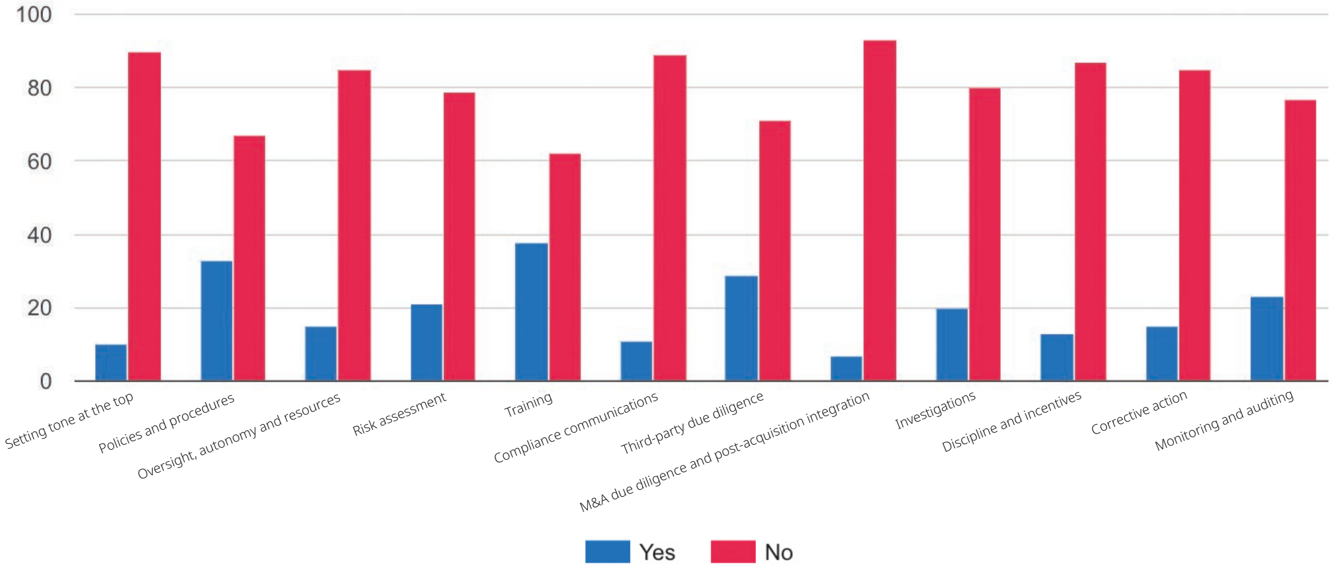
- Interestingly, directors surveyed say their CCOs report to the boards, and most of them think it should stay that way. This might be a difference in perspective of day-to-day reporting versus regular updates at board meetings.
- After falling slightly in 2017, the percentage of CCOs who say they report metrics to their boards of directors and/or audit committees increased to 63 percent. More importantly, the percentage of companies where CCOs report quarterly increased to 68 percent, 24 percentage points higher than in 2016 and 14 percentage points higher than last year. Most of those gains likely came from companies that formerly reported less regularly: Quarterly reporting now appears to be the norm. Directors also said there has been an increase in reporting frequency.
- Respondents note a wide range of metrics that they report, with a heavy emphasis on hotline data, investigations and training.
- Much of Question 9 indicates the settling in of compliance. But the reduction in audits as a tool is notable and could reflect a shift in compliance evaluation to more real-time monitoring.
- Notably, there continues to be an opportunity for compliance programs to better leverage peer functions. For example, only 50 percent of compliance programs reported that they leverage the finance department. Valuable data and analytics such as revenue figures (cut by business unit or product) and the economics of existing and new compensation programs are likely at finance's fingertips and could be reported to the compliance team – allowing it to better identify risk areas and pivot more quickly to head off issues before they become major problems.

Use of Technology

Q11: Do you use technology solutions for the following compliance program areas?



Q12: Do you plan to implement any technology solutions within any of these areas in the next 12 months?



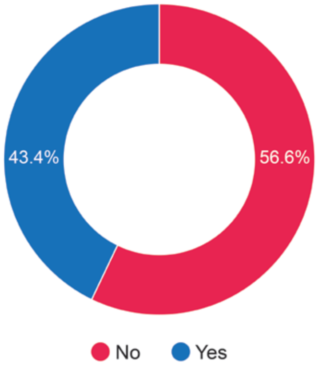
- Training is clearly the area in which respondents rely most on technology. But there are areas where the lack of technology being used is somewhat surprising. That such small percentages say their companies use it in risk assessments and compliance communications is surprising, and that only a about quarter use technology in M&A due diligence is even more so – especially in light of the high M&A volume in the past few years. Tools that evaluate where companies can improve their own compliance programs can be used for acquisition targets.

- There appears to be a belief that technology for evaluating M&A matters could be improved (an interesting finding given the heavy M&A volume in 2018), but it's not an area where most respondents are planning to spend next year (just 7 percent, according to Question 12).

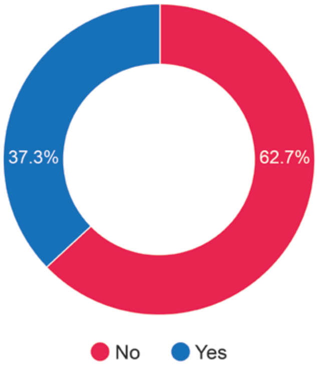
- In fact, the only two areas in which even 30 percent of respondents expect to implement technology solutions in the next 12 months are training and policies and procedures, although third-party due diligence was close at 29 percent.

- These are areas where technology has already proven itself. But it's likely CCOs aren't as ready to invest in less-established technologies.

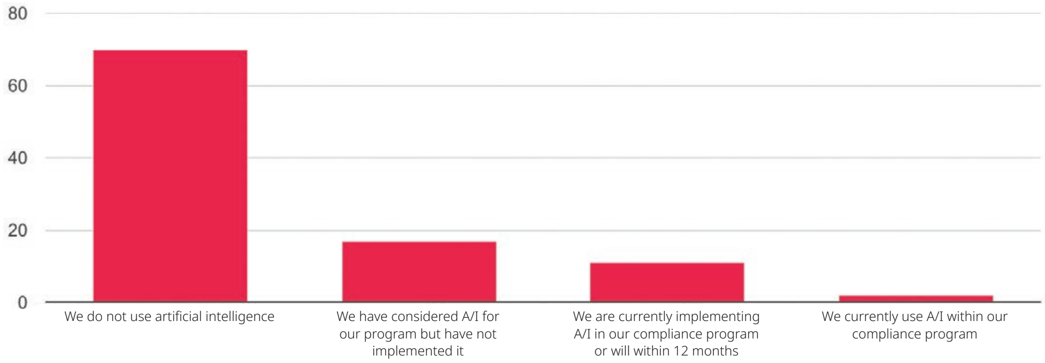
Q13: Are you using internal or external data to help forecast future compliance risks or measure the trajectory of current compliance risks?



Q14: Do you use technology or data analytics in your compliance program?



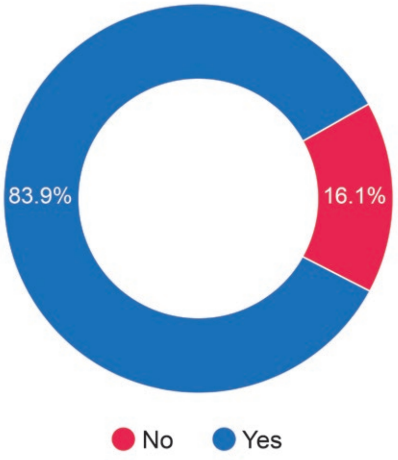
Q15: Which of the following statements best describes the current use of artificial intelligence within your compliance program?



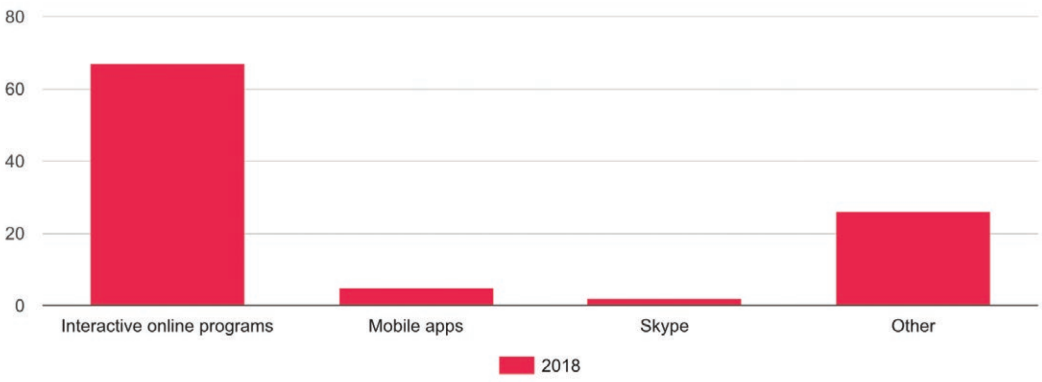
- Only slightly more than four in ten respondents say they use external data to forecast future risks or measure the trajectory of current risks. Given the quickly evolving landscapes when it comes to technology and compliance, this may indicate complacency – even if it isn't all that surprising given the difficulties in leveraging technology elsewhere.
- External data can be extremely valuable, but few companies appear to have the tools in place to use it effectively. And when it comes to data analytics, only slightly more than a third of respondents are using it. "We do look at external data to judge compliance risks, but not in a scientific fashion," one CCO said. For example, "we have not done any sort of scientific analysis … to see whether the trend for enforcement actions are up or down, whether penalties are increasing or decreasing, etc. "
- It's possible that artificial intelligence tools for compliance are too far away from being a reality, one CCO said. He recounted a session on artificial intelligence he attended at a recent conference. "No one even knows what A/I is, much less how to use it," he said.
- The CCO went on to note that A/I's use in other parts of companies – better screening of new employees to reduce the harassment claims or IT improving monitoring for cyberattacks – could end up aiding overall compliance, even if A/I within compliance departments is a long way off.
- And just 13 percent of respondents say they are using (2 percent) or implementing (11 percent) artificial intelligence in their compliance program. This is an area that companies are likely to continue to explore, especially sectors that involve big data.

Training and Accountability

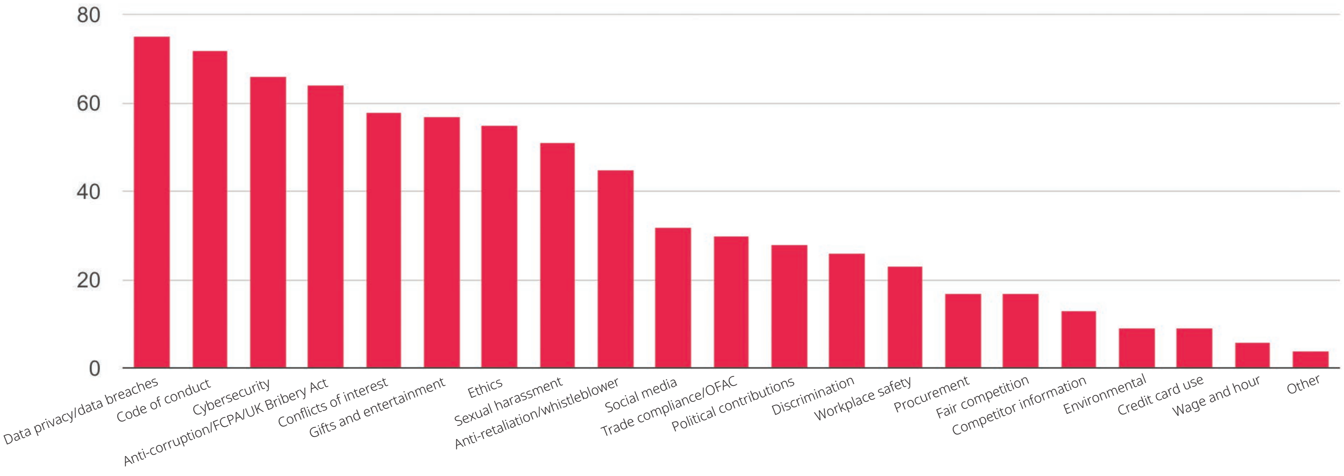
Q16: Are you using technology to help carry out your compliance training?



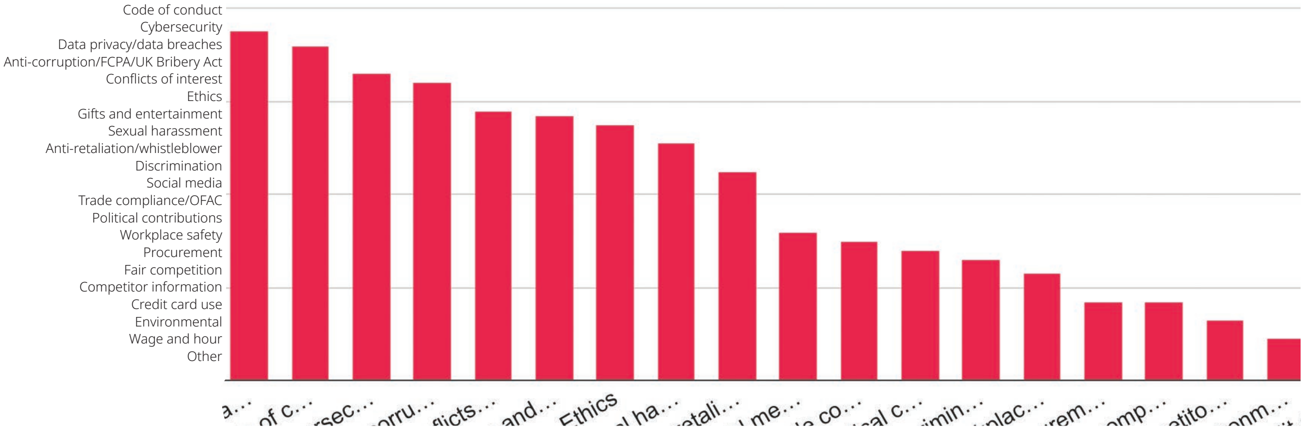
Q17: Which of the following technologies do you use?



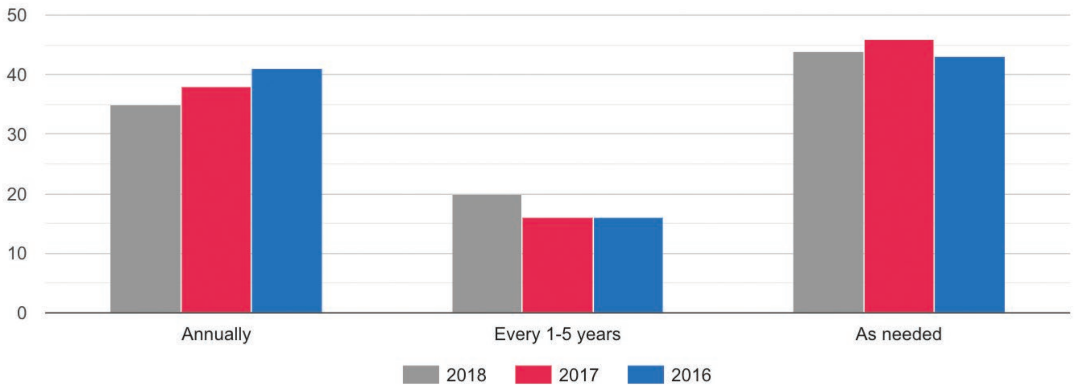
Q18: In terms of subject matter, what training programs has your compliance program updated in the last 12 months? (Check all that apply)



Q19: In terms of subject matter, on what does your compliance training program intend to focus on in the next 12 months? (Check all that apply)

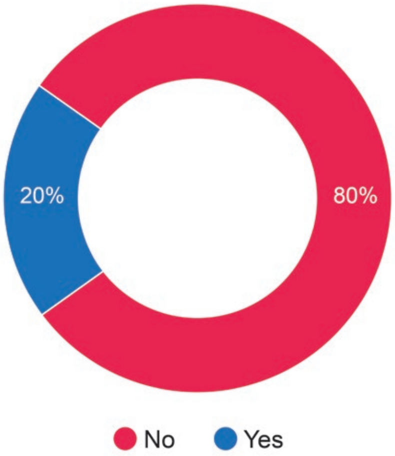


Q20: How frequently do you update or change any of your training programs?

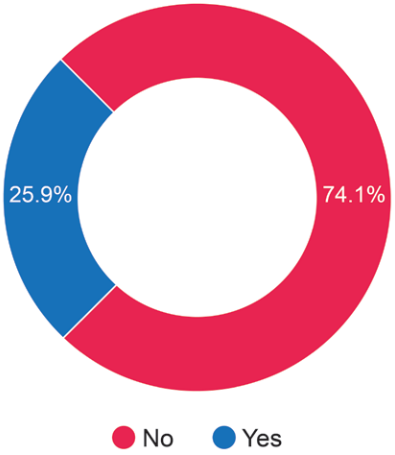


- Clearly, and as noted in Question 11, companies rely on technology to train their employees and managers. But despite new advancements – and a lot of excitement about apps – most companies are relying on interactive online programs.
- Data privacy and cybersecurity, as they have in past surveys, rank highly among areas for which companies have updated training programs. Codes of conduct, which are typically updated about once a year, ranked highly as well – and is the top area respondents say they plan to focus on in the next 12 months (followed closely by cybersecurity and data privacy and data breaches).
- The percentage of respondents who update their training programs annually fell for the second straight year – but the percentage who only update as needed has stayed about the same. That the biggest jump has been in programs that are updated every one to five years might be an indication of programs that are more established.

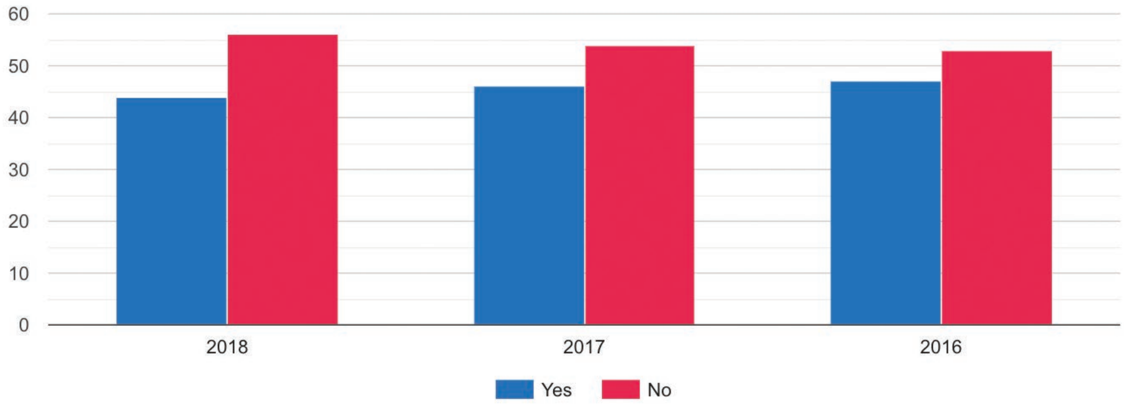
Q21: Do you use technology or an automated tool to track and measure compliance training participation?



Q22: Are managers or supervisors evaluated based, in part, on whether their direct and indirect reports complete required compliance training?



Q23: Are employees penalized for failure to complete training or certifications to policies?



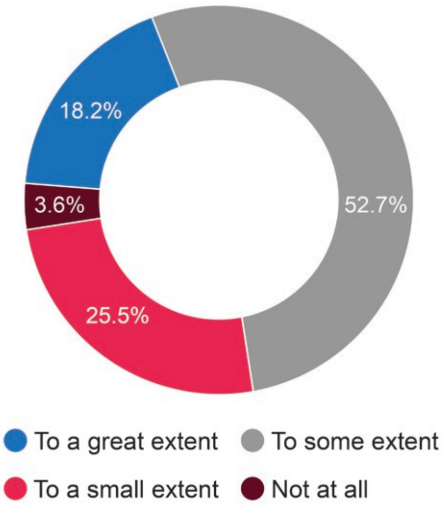
- It's noteworthy that only one in five respondents use automated tools to ensure their employees are participating in compliance training. But it makes some sense, given other findings.

- Nearly three in four respondents (74 percent) say they don't evaluate managers based on employees' participation in the training. Meanwhile, just 44 percent penalize employees (for example, via financial penalties or notes in their personnel files) for failing to complete trainings and certifications.

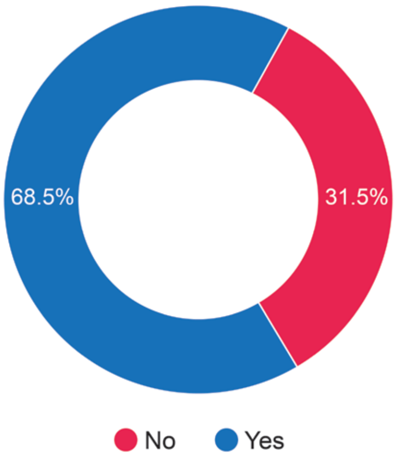
- Still, that last finding is an improvement over the past two surveys, giving reason to believe we're seeing an upward trajectory. The improvement shown in Question 23 indicates that measurement of such training is improving and that it's being more fully integrated into performance reviews. This is a positive trend, and one that will likely continue.

Discoverability

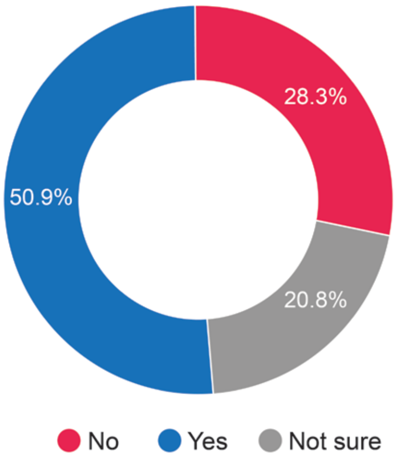
Q24: To what extent are you concerned about the potential discoverability or disclosure of information and data that is captured or generated through the use of various compliance technology solutions?



Q25: Is your compliance department taking any steps to protect from unauthorized disclosure information that is generated by the use of technology?



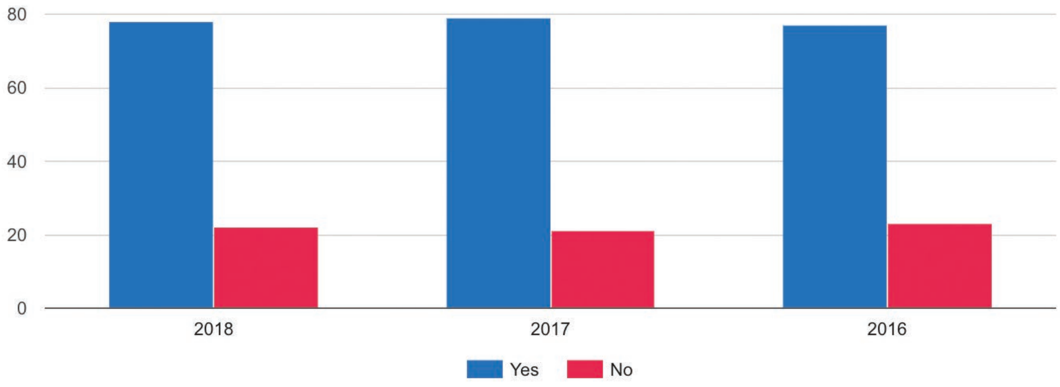
Q26: Do you have controls in place to protect any privileged information generated by the use of any of these technologies?



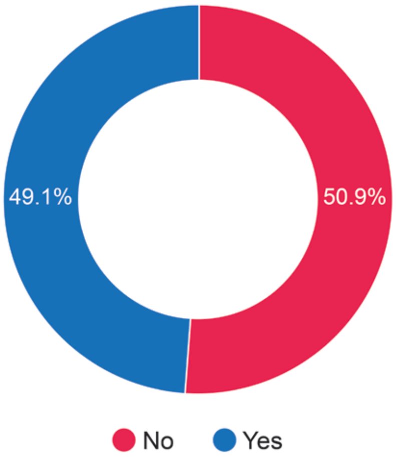
- There's a great deal of concern when it comes to discoverability, and more than two-thirds of respondents are taking steps to address it. Regarding the rest, it's possible parts of companies other than compliance departments (for example, legal or information security) are working on the issue.
- For respondents who are taking steps, actions included limits on the use of Dropbox, password protection controls and closer collaboration among departments. The "privacy team sits in compliance and works on data privacy/protection; we work closely with the IT security team on any applications/ data uses," says one respondent.

Crisis Management

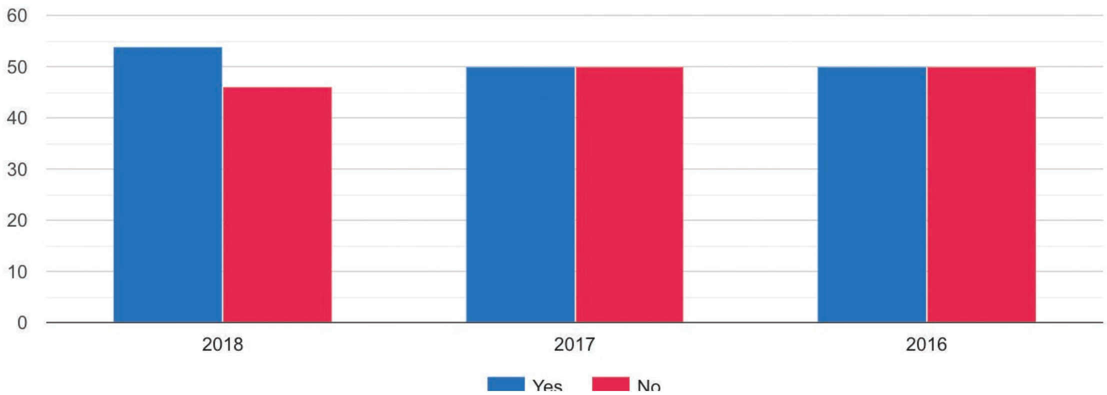
Q27: Do you have a Crisis Response Team identified in the event of a crisis?



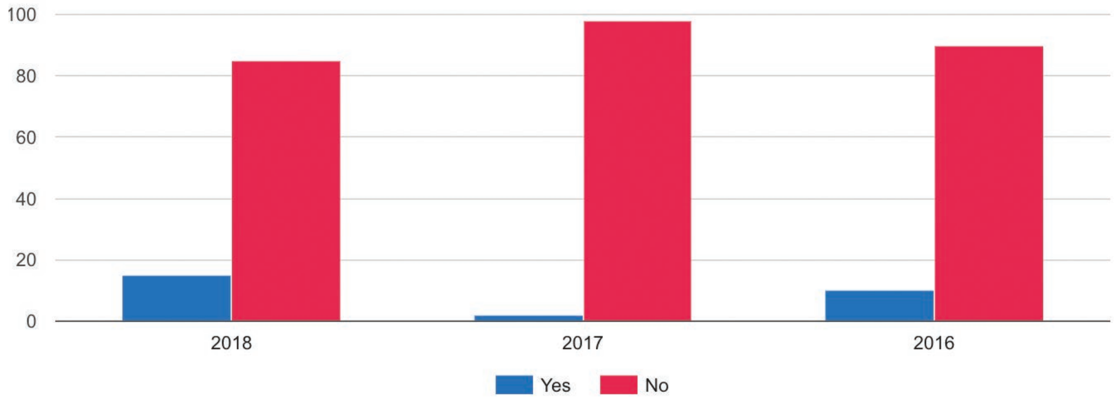
Q28: Does data privacy and cybersecurity fall within the responsibilities of the corporate compliance department?



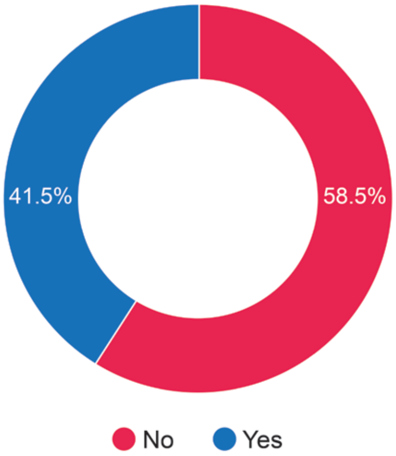
Q29: Do you have cybersecurity insurance?



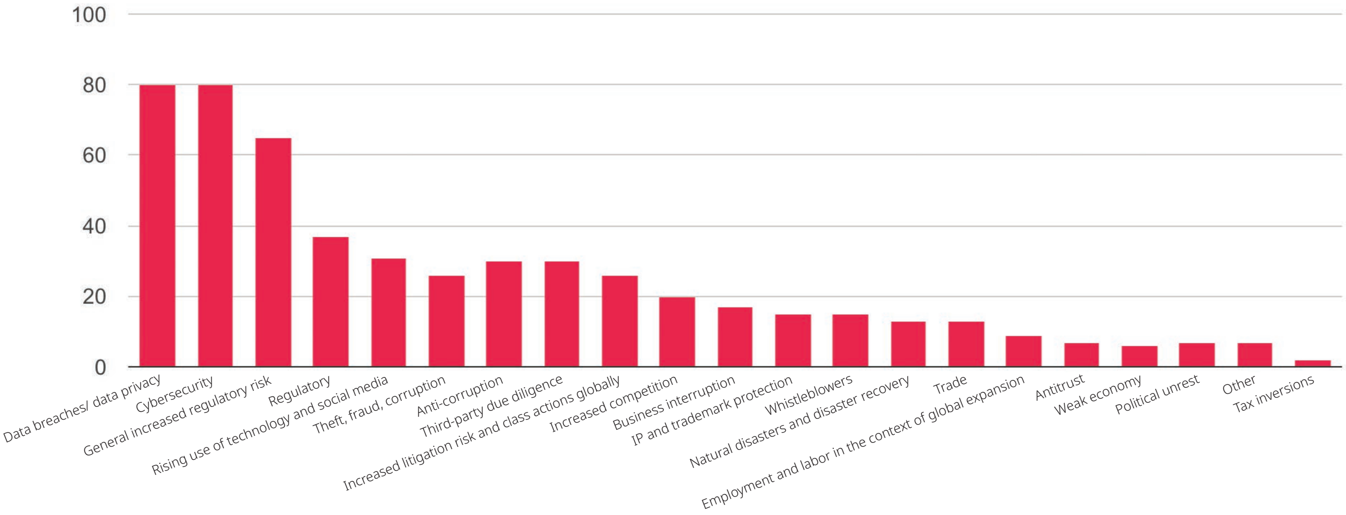
Q30: Has your company ever filed a claim against that policy?



Q31: Has your company experienced a cyberattack?



Q32: What are the biggest compliance risks that your company faces today? (Check all that apply)



Q33: On which of these compliance risks is your company spending the most resources? (Rank the top 5 with 1 being the greatest amount of resources)

COMPLIANCE RISKS	2018 RANK	2017 RANK	2016 RANK
Data breaches/data privacy	1	2	3
Cybersecurity	2	1	1
General increased regulatory risk	3	3	2
Increased litigation risk and class actions globally	4	9	7
Third-party due diligence	5	5	6
Regulatory	6	4	4
Increased competition	7	10	14
Anti-corruption	8	6	5
Theft, fraud, corruption	9	7	8
Rising use of technology and social media	10	8	9
Business interruption	10	12	12

- If data privacy doesn't fall under the purview of the compliance department, it's often the responsibility of IT security and/or legal, according to respondents.
- More companies are getting cybersecurity insurance and filing claims. This likely indicates growing concerns about cyberattacks and perhaps even more awareness of when they occur. 42 percent of respondents say they have experienced such an attack.
- With that in mind, it's not surprising that data breaches and data privacy topped the list of top compliance risks, with cybersecurity being among the top concerns for the third consecutive year.
- That these findings largely track with the results from Question 5 (regarding time commitment) shows companies are generally aligned correctly when it comes to priorities.
- And, in a somewhat hopeful sign, companies do seem to be putting their money where their risks are. For the first time, data breaches and data privacy are areas in which respondents are devoting the most resources. Cybersecurity, the top choice the past two years, was second in 2018.

Methodology

During the second quarter of 2018, DLA Piper distributed individual surveys to corporate in-house counsel, compliance officers and members of boards of directors at companies large and small, public and private, to better understand how they function, what risks they face and how they are positioning themselves and their organizations to succeed in an era of heightened focus on corporate conduct. The results were tabulated, analyzed and released in fall 2018.

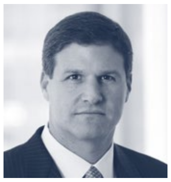
Respondents identified themselves as chief compliance officers, compliance professionals, general counsel or chief legal officers, deputy or assistant general counsel, in-house counsel, and directors. In total, 65 individuals completed the survey, and subsequent qualitative interviews were conducted to add commentary and insights to the analysis of the results. We thank all of the participants for their responses.

46 percent of respondents' revenue comes from North America, followed by 22 percent from Europe, the Middle East and Africa, 21 percent from Asia-Pacific and 7 percent from Latin America. Half of the respondents were from publicly traded companies.

Percentages in certain questions exceed 100 percent because respondents were asked to check all that apply. Due to rounding, all percentages used in all questions may not add up to 100 percent.

Contact

Stasia Kelly
Partner, Washington, DC
Co-Chair, DLA Piper's Governance and Compliance
Practice Managing Partner (Americas)
stasia.kelly@dlapiper.com
T +1 202 799 4239



Brett Ingerman
Partner, Baltimore
Co-Chair, Global Governance and Compliance
brett.ingerman@dlapiper.com
T +1 410 580 4177

Brian H. Benjet
Partner, Philadelphia
brian.benjet@dlapiper.com
T +1 215 656 3311

T. Brendan Kennedy
Partner, Baltimore
brendan.kennedy@dlapiper.com
T +1 410 580 4196

Angela J. Crawford
Partner, Miami
angela.crawford@dlapiper.com
T +1 305 423 8503

Bob Martens
Partner, Brussels
bob.martens@dlapiper.com
T +32 (0) 2 500 1503

Michael D. Hynes
Partner, New York
michael.hynes@dlapiper.com
T +1 212 335 4942

DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information please refer to www.dlapiper.com.
Note past results are not guarantees of future results. Each matter is individual and will be decided on its own facts. Attorney Advertising.