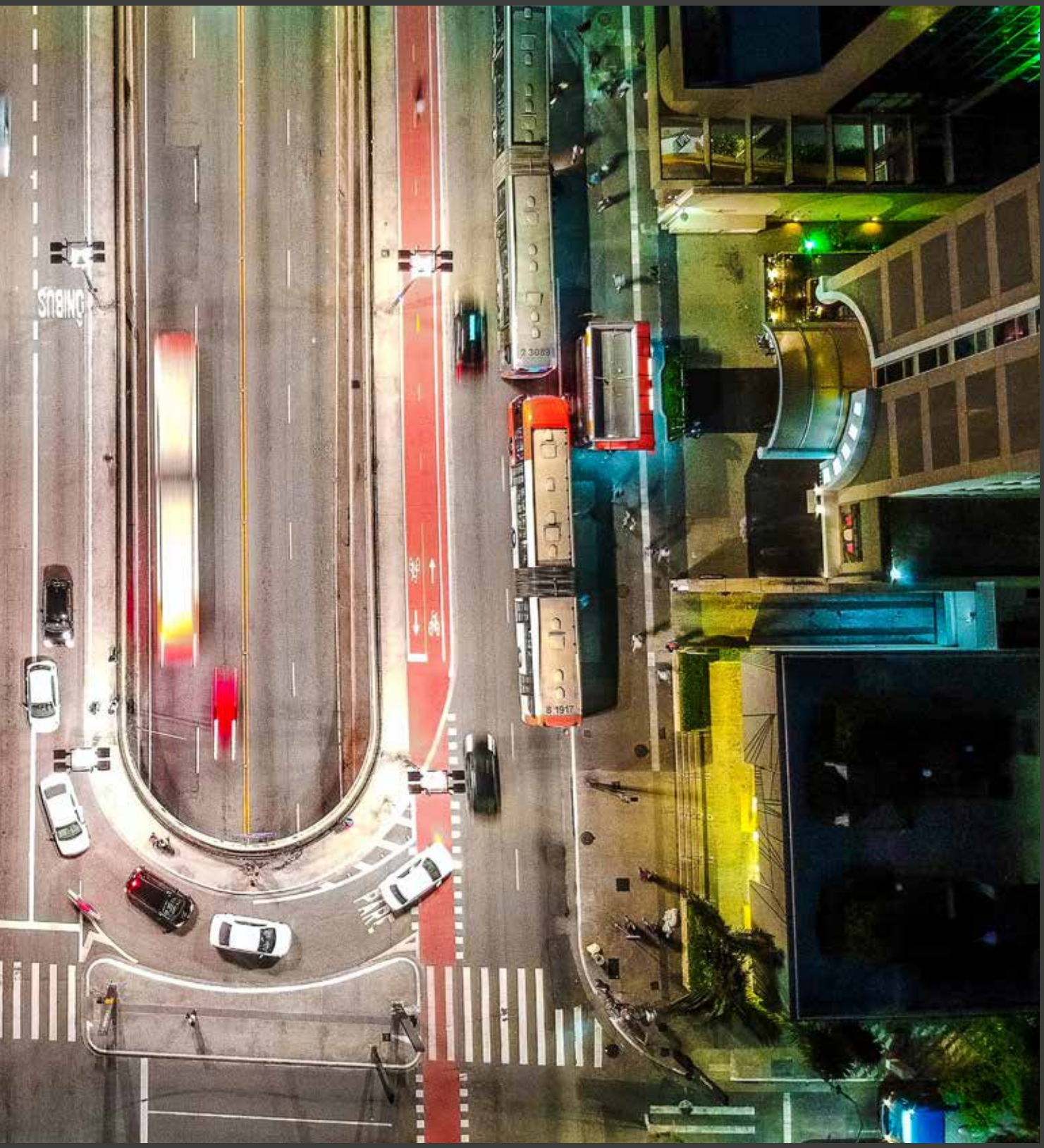
ROPES & GRAY

Data & behavioral sciences

A new approach to risk management

Contents


PARK

Introduction

For years, companies' risk mitigation efforts were typically reactive rather than proactive, involving policies and procedures rolled out by compliance departments to address regulatory shifts or new potential vulnerabilities. The onus was on employees to follow the rules without question, since compliance departments were often understaffed and teams spent much of their time simply trying to keep up.

Over time, a degree of inefficiency, frustration and even failure in compliance efforts risked becoming an accepted part of company culture. Despite tailored policies, procedures, training, testing and remediation, some employees still broke the rules. In some cases, non-compliance was even considered "the cost of doing business," especially in lucrative new markets where enforcement was lax and corruption was high.

Today, that approach to compliance looks dated and is ultimately bad for business. Regulatory enforcement is on the rise worldwide and the penalties for non-compliance can be severe. Monitoring of activity is more sophisticated, and not only among regulators – employees and customers alike now have a range of channels through which they can blow the whistle on questionable corporate behavior.

Our survey of 300 senior executives across the world reveals that compliance is getting better, but there is still room for improvement. Respondents from all sectors understand the challenges involved, but many remain focused on policies and procedures, rather than on examining the factors underlying compliance risks. In other words, what motivates employees to commit fraud or bribe officials when rules and regulations so clearly prohibit this kind of behavior?

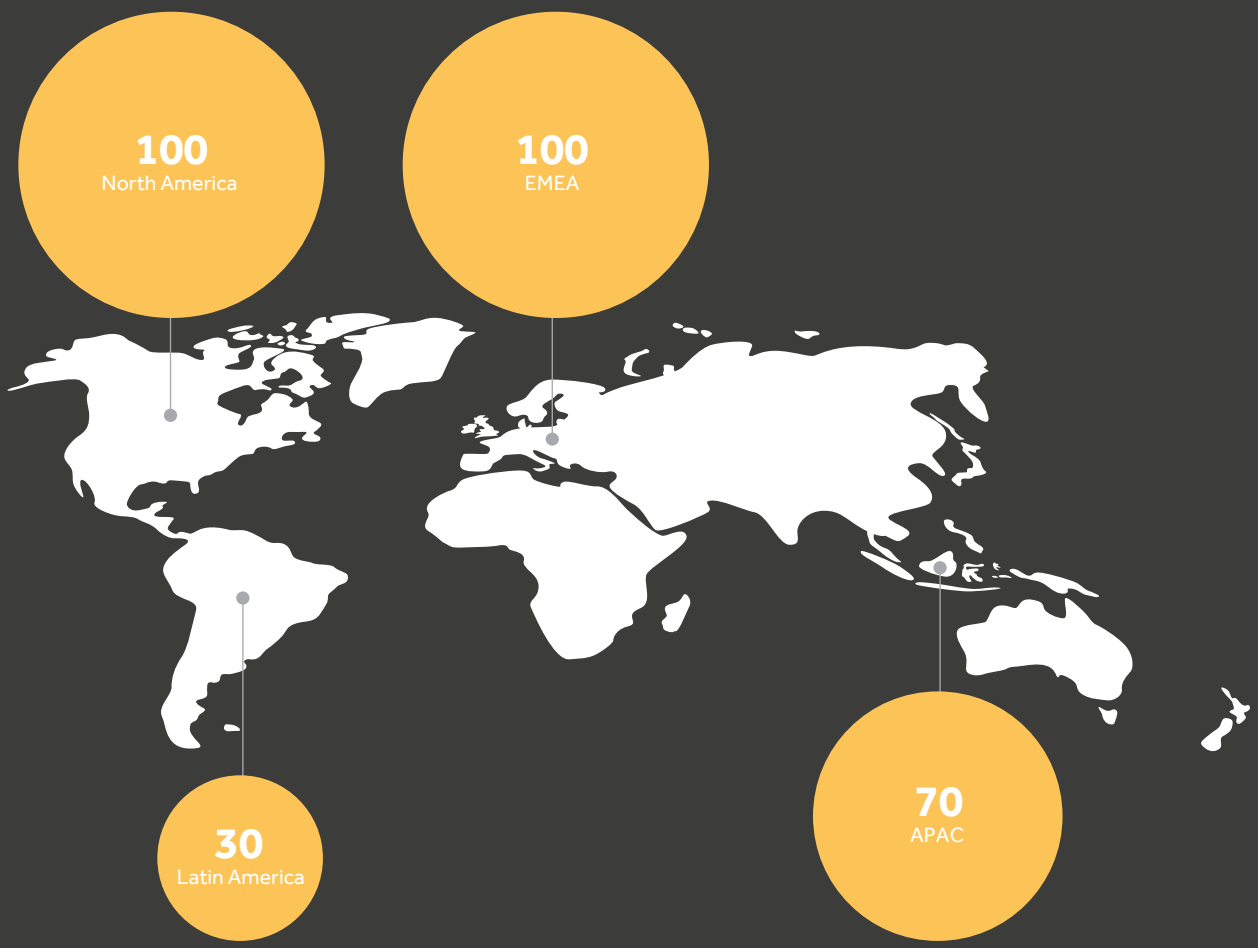
To answer these questions, companies increasingly employ data and behavioral sciences-based analysis to develop compliance strategies. While third-party and internal audits still play a role in compliance strategy formulation, companies now rely on improved data compilation and review to identify potential risk hotspots or trends. As a result, compliance efforts are moving beyond mere box-checking exercises and towards the creation of corporate cultures that empower employees to cope with risks, rather than compel them to read voluminous policies and procedures that attempt to account for every unforeseen risk.

Compliance offers a fundamental competitive advantage: From a public policy perspective, businesses are expected to operate in compliance with applicable regulations. If it cannot demonstrate a compliant culture, a company will not be able to secure funding, sell a business unit or advance its prospects significantly. This is more than just an approach to risk mitigation – ultimately, it is a strategy for building a business that can compete effectively on an increasingly challenging and competitive global stage.

Methodology

In the second quarter of 2018, Acuris Studios, on behalf of Ropes & Gray LLP, surveyed 300 senior executives on the topic of compliance and behavioral science approaches to risk management. Of those surveyed, 100 respondents were based in North America, 100 were based in EMEA, 70 were based in APAC and 30 were based in Latin America. The survey included a combination of qualitative and quantitative questions, and all interviews were conducted over the telephone by appointment. Results were analyzed and collated by Acuris Studios, and all responses are anonymized and presented in aggregate.

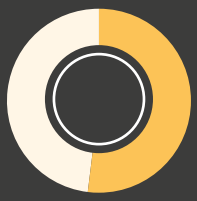
SURVEY RESPONDENTS BY REGION AND SECTOR



	North America	EMEA	Asia-Pacific	Latin America	Total
Asset Management	16	18	11	5	50
Banking	16	17	12	5	50
Life Sciences & Healthcare	17	17	11	5	50
Private Equity	17	16	12	5	50
Technology	17	16	12	5	50
Other	17	16	12	5	50
Total	**100**	**100**	**70**	**30**	**300**

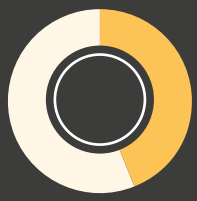
Key findings

Why do employees stay compliant (and how can companies keep track)?



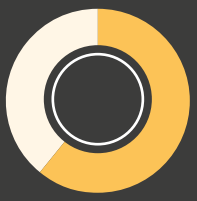
52%

of respondents say that employees are motivated to stay compliant out of an obligation to do the right thing



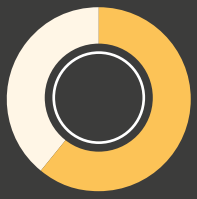
44%

say staff think it would be too time-consuming or expensive to try and get around the company's policies and procedures



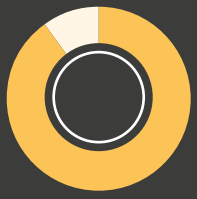
61%

say clear guidance regarding applicable laws and regulations is one of their top two considerations when helping employees understand compliance



63%

use HR records, such as disciplinaries, when planning compliance-related assessments



90%

use third-party audit and monitoring records to plan compliance-related assessments

Behavioral approaches to risk management: the next big thing?

55%

say they have heard of the behavioral approach to compliance

84%

think a behavioral approach to compliance would be helpful or very helpful

Compliance and monitoring

44%

of respondents overall say requests from government officials are one of their great compliance challenges (rising to 66% among asset managers and 58% among banks)

57%

say the culture of the region or country where their company operates is one of the biggest obstacles to implementing an effective compliance framework

49%

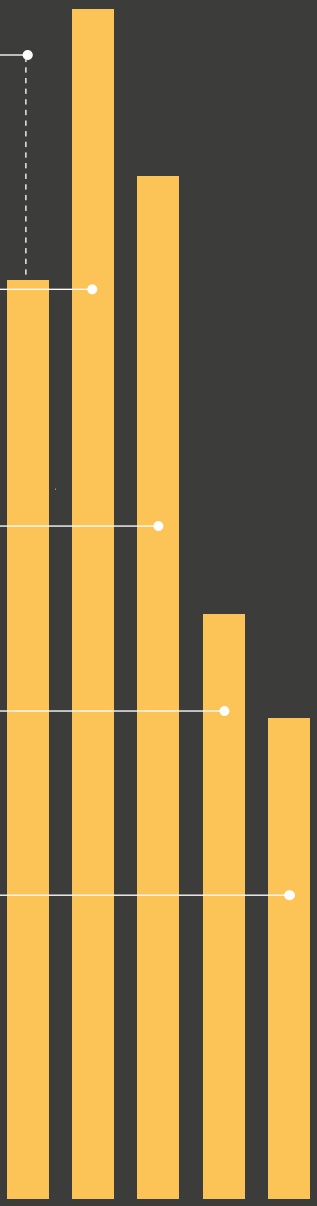
do not have an efficient, reliable, properly funded process in place for investigating allegations

28%

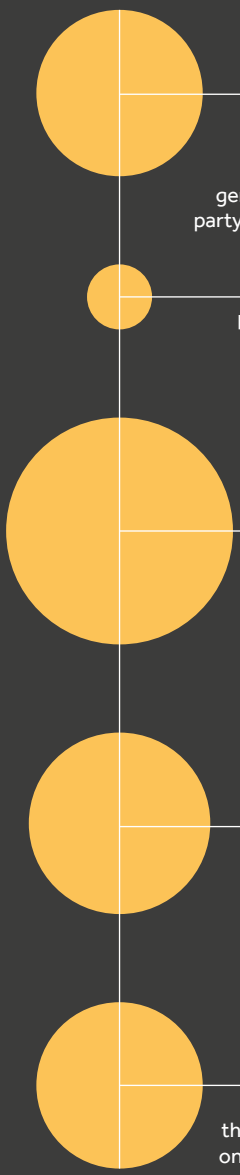
of respondents have a whistleblower hotline managed by a third-party vendor

23%

do not catalog all complaints and responses to allegations



Third-party risk management



46%

of respondents say the chief compliance officer, or the compliance department in general, is responsible for third-party due diligence and monitoring

7%

place this responsibility in the hands of individual business teams or units

83%

of respondents do informal background checks conducted internally when carrying out third-party due diligence

54%

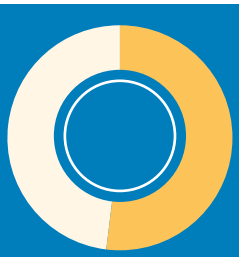
say one of the most important areas of due diligence is confirming that a third party is qualified to do the work that it has been engaged to do

55%

do not alter their level of third-party due diligence based on the type of third party or any red flags identified

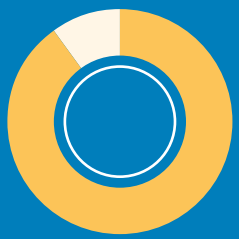
Section 01
Data, behavior and risk

How do professionals make decisions? Why do people break the rules? And how can a business encourage or discourage behavior beyond threats of punishment? Our survey reveals that legal, compliance and risk officers are now gathering, analyzing and applying an increasingly broad range of data in their policies and strategies, even as they struggle with incompatible legacy systems and stretched resources.



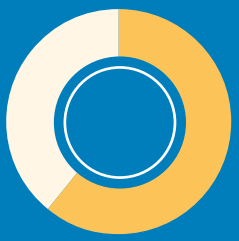
52%

of respondents say employees are compliant because they believe it is their obligation and the right thing to do



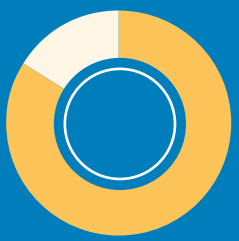
63%

of respondents use HR records, such as disciplinaries, when planning compliance-related assessments



61%

say clear guidance regarding applicable laws and regulations is one of its top two considerations when helping employees understand compliance



84%

think a behavioral approach to compliance would be helpful or very helpful

Our understanding of what drives decision-making is evolving. Historically, compliance has been a response to regulation – from anti-corruption to sanctions, and now data privacy – and a constant game of catch-up.

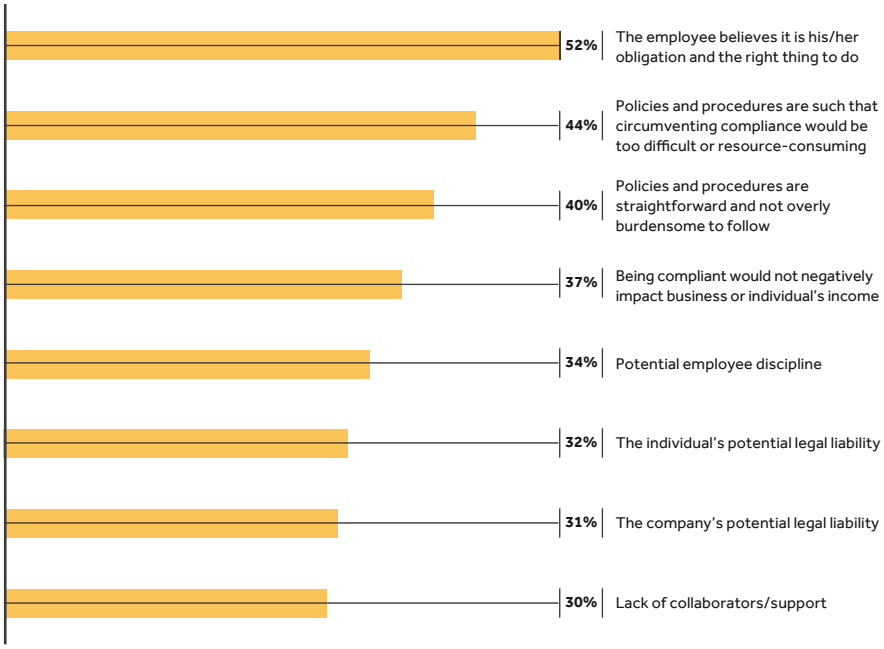
"It's hard to know where the real risks are – often we don't know where the real risk is until we or some other company runs afoul of it," says the managing director of a financial services firm in the United States. "The Wells Fargo situation prompted a sales practices review at every bank. Were we already doing a good job? Maybe we hadn't even classified sales practices correctly and instead we had a variety of different things like unfair or deceptive acts or practices and market manipulation and know your customer and suitability that piecemeal would have added up to that comprehensive review. But we are definitely influenced by enforcement actions across our industry."

Failure to comply can result in significant financial and reputational harm to the business, as well as legal risk. As a result, many companies have built compliance programs to address a specific regulatory focus, adding to it over time as new issues arise, without realizing the extent to which these policies have become siloed and disconnected.

"This can prove challenging, if only because it's difficult for employees to keep up – and it's already difficult for the ones drafting the policies and procedures to ensure they are responding quickly enough," says Amanda Raad, co-chair of the anti-corruption & international risk practice at Ropes & Gray. "It can be tough for employees trying to understand the risks, and what they are and are not supposed to do. Even if they are entirely well intentioned, they may violate company policy without knowing."

Respondents in our survey are not unanimous as to what motivates employees to stay compliant (Figure 1): 52% say that employees feel an obligation to do the right thing, while 44% say staff think it would be too time-consuming or expensive to try and get around the company's policies and procedures (though at times it can be equally time-consuming and expensive to understand company policy). Just over a third consider potential disciplinary action as a deterrent to non-compliance, with a similar percentage citing legal liability, whether personal or corporate.

FIGURE 1: **IN YOUR EXPERIENCE, WHY ARE EMPLOYEES MOTIVATED TO STAY COMPLIANT?** (SELECT TOP THREE)



"We tend to put more emphasis on the front end, on positive reinforcement," says the CCO of a North American medical technology company. "How can we make it easy and simple for people? Why is it important? And we make sure that there are checks and balances along the way."

In the process, businesses are learning that an effective and data-driven compliance program can be good for business.

"Standards for risk management have evolved and companies have learned that a better understanding and control over risk is an effective business strategy," says Heather Sussman, co-chair of the privacy & cybersecurity practice at Ropes & Gray. "Look at the lessons learned in cybersecurity: businesses have developed better risk assessments and training exercises that help them proactively evaluate where defenses can be improved; they're identifying weaknesses, whether in accounting controls or third party suppliers, that present a heightened cybersecurity risk; and they're learning how to prevent or stop potential attacks before they happen. So just as businesses developed these approaches to cybersecurity, they are now applying these lessons to compliance."

COMPLIANCE-RELATED MONITORING AND/OR ASSESSMENTS

Traditional approaches to risk management accept the assumption that bad behavior results from bad policy or a lack of understanding of policies.

Now, behavioral scientists are learning that professionals can be motivated by a variety of other incentives, such as high-pressure sales targets or government officials demanding rewards in exchange for a contract or other business opportunities.

Employees could put themselves and an entire organization at risk if they haven't been trained to identify risks or respond appropriately in difficult situations.

"Most employees are not going to work intending to break the law or do something that hurts the company," says Raad. "This is why, for example, employees aren't stealing money in many anti-corruption cases: they're using company money to try to help the business. Teaching them how to navigate challenges they might encounter in their work improves the corporate culture overall, as well as their working experience."

Compliance and risk officers are looking for new and better ways to identify potential compliance risk hotspots, as well as the underlying factors that may cause someone to break established codes of conduct – and data may hold the key. Companies are deluged with information, from sales contracts to regulatory requirements, internal audits and employee expenses, but using data to create a coherent picture of the business is complicated and can be unreliable if it is not processed and analyzed accurately.

"Over the past couple of years, we have seen companies begin to take a more data-driven approach to address compliance and oversight issues, rather than using anecdotal evidence," says Ryan Rohlfsen, a partner in the anti-corruption & international risk practice at Ropes & Gray. "I would not say there is a consensus on taking this approach, however, nor upon how to do it. Some companies are using historical data, others are taking a more forward-looking approach. But as a critical mass of companies have purchased key data analytics tools, they have come down in price, enabling more companies to pick off at least the low-hanging fruit."

According to our survey, executives are focusing their attention first and foremost on data surrounding third parties, suggesting a tight rein is being held on agents, distributors, consultants and suppliers. Some 90% of respondents say they use third-party audit and monitoring records when planning compliance-related monitoring and assessments (Figure 2). Given the number of recent high-profile fraud and related charges against major corporations that have stemmed from relationships with external parties, it makes sense that this is a priority.

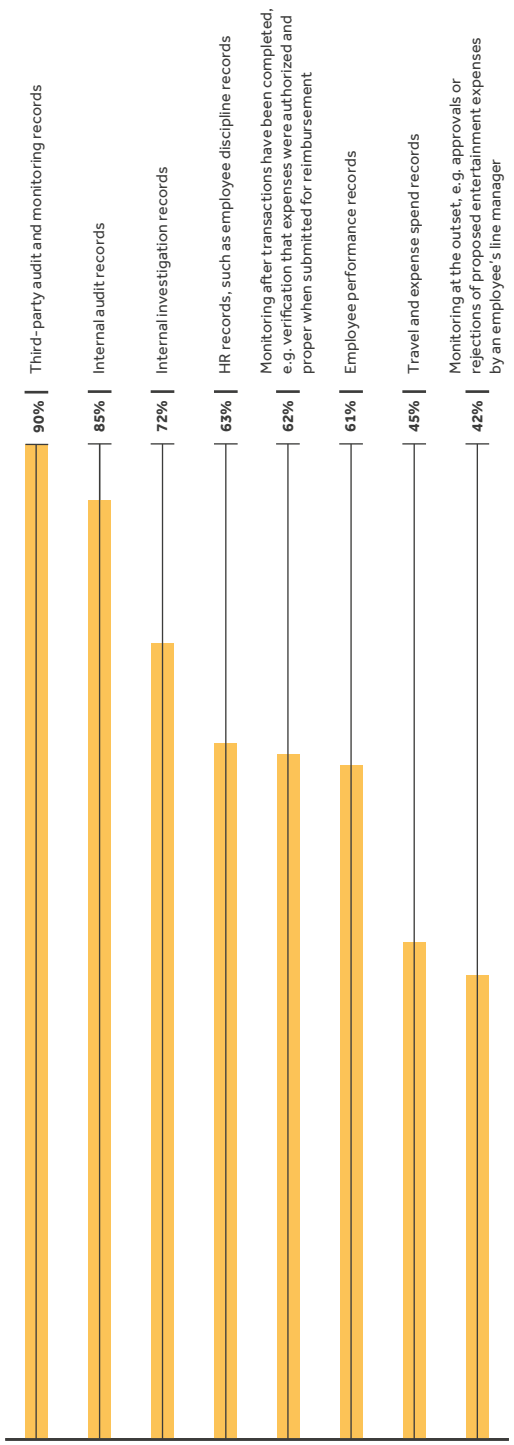
For example, in June 2016, Analogic Corporation, a Massachusetts-based medical device company, and its wholly owned subsidiary in Denmark, BK Medical ApS, agreed to pay more than US$14m under a non-prosecution agreement and settlement agreement with the DOJ and SEC, respectively. The company entered into these agreements to resolve FCPA charges for allegedly allowing BK Medical to be used as a "slush fund for its [third-party] distributors."

BK Medical's distributors routinely requested that BK Medical create "special invoices" to exaggerate the sales price of BK Medical's ultrasound equipment. After BK Medical received the inflated payments, it wired the excess funds to various third parties, as requested by the distributors, without determining whether there was an appropriate business reason for the payments.

In another example, the United Kingdom's Serious Fraud Office entered into a Deferred Prosecution Agreement (DPA) in January 2017 with Rolls-Royce for failing to prevent bribery committed by one of the company's third-party distributors. Rolls-Royce entered into a distribution agreement with a Nigerian company to distribute gas compression engines to an oil and gas exploration company. This agreement permitted the distributor to charge a markup on Rolls-Royce products, the proceeds of which the distributor used to make improper payments to Nigerian officials in one of the country's public entities that supervised the government's investment in the oil and gas sector.

When it comes to internal data gathering, the survey shows that old favorites still stand strong: internal audits (85%), internal investigations (72%) and human resources records (63%) – including disciplinary proceedings – are considered when designing or monitoring compliance programs.

FIGURE 2: **WHAT TYPES OF DATA DOES YOUR COMPANY CONSIDER WHEN PLANNING COMPLIANCE-RELATED MONITORING AND/OR ASSESSMENTS?** (SELECT ALL THAT APPLY)



Similarly, employee performance records are used by 61% of respondents, with a few more considering closed transactions or expenses that had been approved by a line manager (62%).

"There's a move to include the right kinds of data in risk assessments, which is a move in the right direction," says Raad at Ropes & Gray. "An effective risk assessment has to be data-driven; you can't just collect data, you have to use it. Historically, companies sometimes reviewed policies and procedures in a vacuum, without checking whether they were doing any good. Now data is being gathered to track how many internal investigations are being conducted and how many complaints or other compliance issues come up and where, pinpointing hotspots for compliance policy violations. It's being used to identify non-compliance trends. People are getting better at collecting, but there has to be real analysis about how it can be used effectively."

The bottom line, however, according to Raad, is that you can't analyze the data you don't have – "and I'm not sure businesses have all the data they need." For example, some companies don't keep a record of all allegations. Even if an investigation ultimately dismisses a complaint, it's still an important piece of data. These should be tracked to inform subsequent risk assessments.

"Something caused a person to log a complaint and maybe it's a disgruntled employee or just competitors being problematic in the jurisdiction, but without that information, you will never spot the pattern," says Raad.

FIGURE 3: **AT WHAT LEVEL IS THE DATA REVIEWED?**

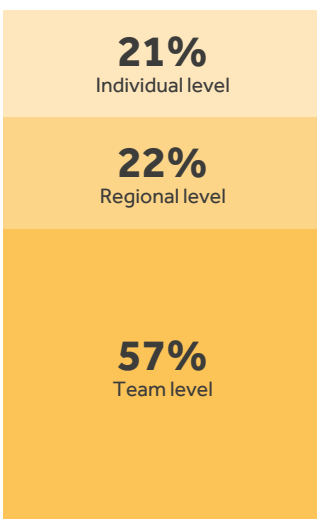
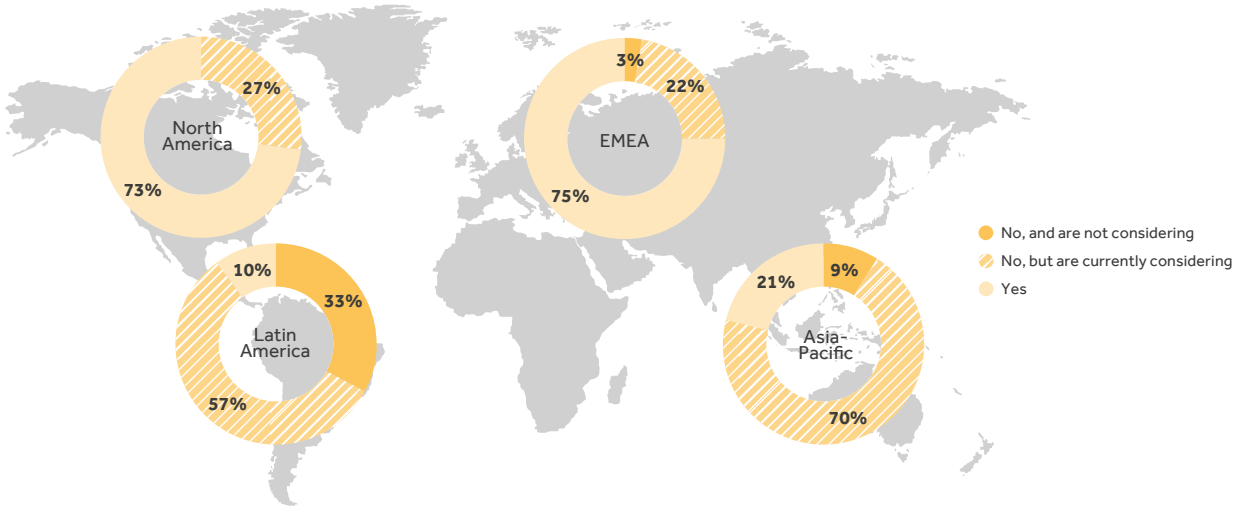


FIGURE 4: **HAVE YOU INCORPORATED DATA WHEN CONDUCTING COMPLIANCE-RELATED MONITORING AND/OR ASSESSMENTS?**



DEALING WITH DATA COMPLEXITY

The complexity around gathering, cleansing and creating a straight picture using this data is still a struggle for many businesses, especially those that have grown by acquisition and are tussling with legacy systems.

"Data is a huge enabler for any program – and not just compliance programs. But incomplete or inaccurate data is going to affect your results, and the refresh rate of that data can have an impact as well," says the CCO of a medical technology company in North America. "If you've got different systems, how do you connect those systems? If the data's not in the same format, that's a problem too. And that's just accessing the information – once you get it, not everybody looks at it the same way."

Despite the availability of precise data, fewer than half of respondents say they consult basic details like travel expenses (45%) or rejections from line managers (42%) when building compliance programs.

Evidence of the barriers that legal and compliance professionals still face can be seen in the level at which this data is examined (Figure 3). While 57% look at data on a team level, fewer than a quarter of respondents say they either look at it on an individual level (which suggests there is too much data to go through) or on a macro level, possibly because homogenizing or standardizing data at a regional level to make it comparable poses too great a challenge.

As the in-house counsel of a consumer products company based in Latin America explains, "Team-level data is easier to look at, and we can make faster decisions on precautionary steps if necessary."

REGIONAL COMPLIANCE DIFFERENCES MAY APPLY

Companies are using a wide range of data for compliance purposes, with each sector and region choosing different elements that are relevant to their needs.

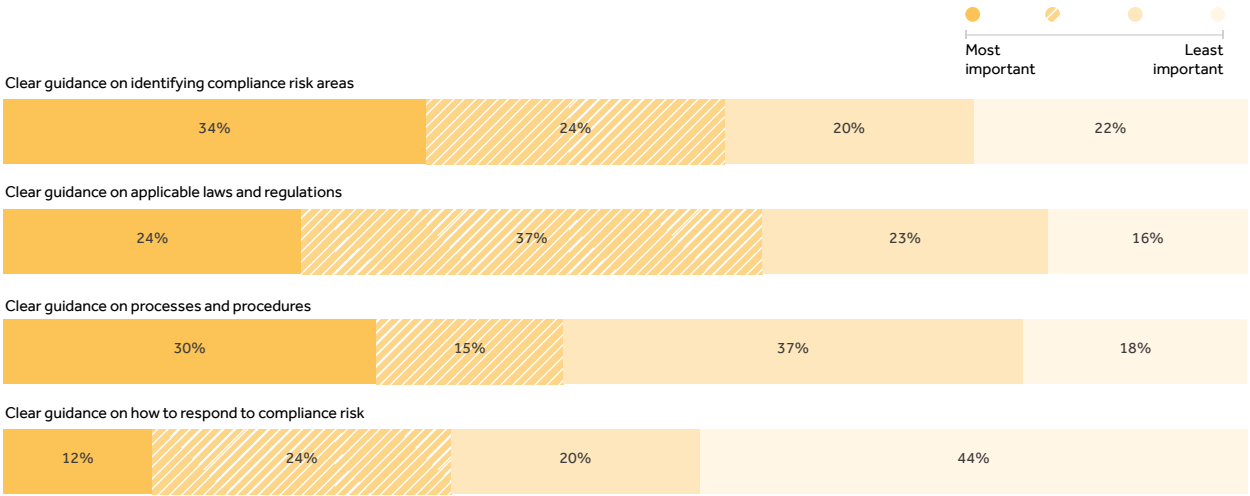
"A compliance data point in a pharmaceutical company in Canada might mean something totally different to a mining company or manufacturer based in China," says Rohlfsen at Ropes & Gray.

Much of this is determined by enforcement trends, as pointed out by Judith Seddon, a London-based anti-corruption & international risk partner from Ropes & Gray: "The U.S. and the UK have the most far-reaching extraterritorial laws and have been active in enforcement for the longest period of time," says Seddon. "As a consequence, companies doing business in the U.S. and in the UK may be more likely to make this a priority and to use data for compliance purposes."

While 70% or more executives in EMEA and North America say they have incorporated data when they have conducted compliance-related monitoring and assessments (and those few who have not used data in this way are actively planning to do so), just 21% have done so in Asia-Pacific and 10% in Latin America (Figure 4).

"APAC still lags behind EMEA and North America when it comes to incorporating data into compliance-related monitoring and/or risk assessments because 'compliance' is a relatively new concept in Asia, in terms of managing enterprise risk," says Mimi Yang, a Hong Kong-based partner in the anti-corruption & international risk practice at Ropes & Gray. "Companies haven't felt as much pressure from regulators as those in EMEA and North America.

FIGURE 5: **ORDER THE FOLLOWING FROM MOST IMPORTANT TO LEAST IMPORTANT WHEN HELPING EMPLOYEES UNDERSTAND COMPLIANCE** (1 = MOST IMPORTANT; 4 = LEAST IMPORTANT)



"Traditionally, companies in Asia have managed risk retroactively, meaning that they address compliance-related issues after they have occurred. Proactive monitoring and risk assessments, while certainly on their radar, have not yet been shown to provide value in the same way as investing in new technology or aggressive sales tactics. This is also in part because Asian regulators have not been aggressive in enforcing compliance-related regulation, such as anti-corruption laws, although that is certainly changing."

That change is reflected in the findings: 70% of respondents in Asia-Pacific say they are not using data in their compliance-related monitoring and assessments, but are actively considering doing so.

"It can be challenging to operate in countries where there isn't much enforcement," adds Raad. "Competitors may engage in practices that American or British companies may not. All the more reason to find a way to engage with your team on the ground in these jurisdictions and arm them with the tools they need to make the right decisions. A policy that just says 'Thou shalt not do X, Y or Z' isn't the solution."

HELPING EMPLOYEES UNDERSTAND COMPLIANCE

A compliance professional has to establish and implement compliance programs throughout the organization, and employees need to know that the issue is being taken seriously.

"This isn't just a question of putting a policy in place," says Colleen Conry, a partner in Ropes & Gray's anti-corruption & international risk practice. "This is about investing the time and energy to drill down to understand risk areas. Ultimately, the solution needs to come from employees. They are the ones who can say why they act in a certain way. Without their engagement and participation in developing compliance programs, it's not going to work."

Just over a third (34%) of respondents say clear guidance on identifying risk areas is most important when it comes to helping employees understand compliance rules in an organization (Figure 5).

As the chief risk officer of a life sciences and healthcare business based in North America says, "If risk areas are identified and noted, there will be extra caution taken in and around those areas."

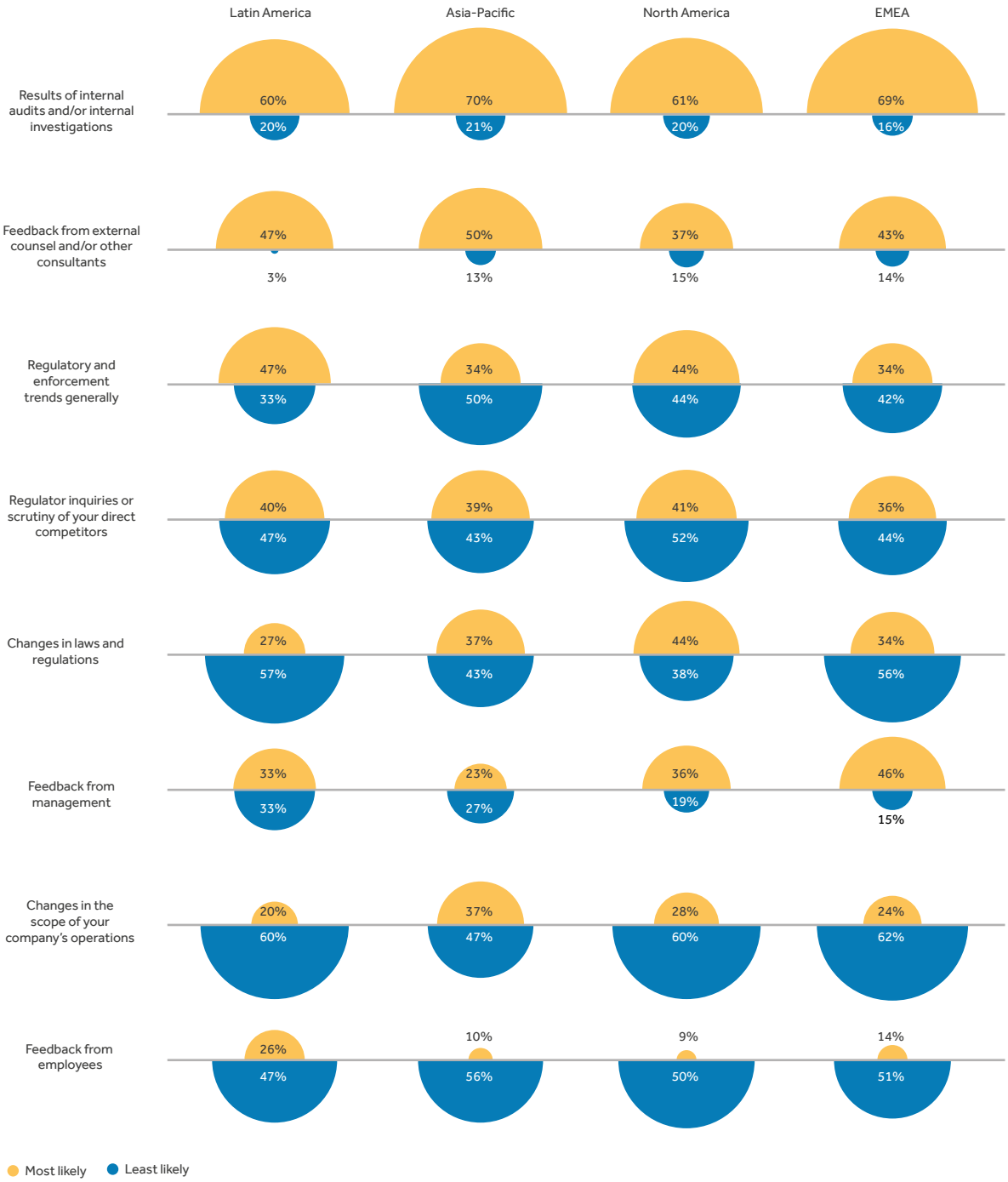
Conversely, just 12% say guidance on how to respond to compliance risk is the most important way to help employees understand compliance. This may be indicative of the fact that companies need to empower employees to identify risks and make decisions independently as compared to trying to prescribe a detailed policy, procedure, or training that will address every situation.

"When you discover anomalies, part of it may be due to training," says the CCO of a North American medical technology company. "Have you trained people on how to use the system? Have you explained why you need information, the frequency, why things need to be submitted in a certain way, and so on? If people understand the 'why,' they often become better at following the 'how.'"

KEY DATA CONSIDERATIONS IN ANTI-CORRUPTION POLICIES

When drafting or updating corporate anti-corruption procedures, a healthy majority of respondents say they are most likely to consider internal audits and investigations as one of their top three data considerations – particularly in Asia-Pacific (70%) and EMEA (69%) (Figure 6).

FIGURE 6: **WHAT ARE YOU MOST/LEAST LIKELY TO CONSIDER WHEN DRAFTING OR UPDATING YOUR COMPANY'S ANTI-CORRUPTION POLICIES AND PROCEDURES?** (SELECT TOP THREE)



IN CONVERSATION WITH...

James Hearty

Chief Compliance Officer, DaVita Inc.

Q. HOW DO YOU ENCOURAGE COMPLIANT BEHAVIOR?

We have more than 60,000 employees in more than 2,500 locations, so effective oversight and communication is a big challenge. At DaVita, our core values are an important part of the company's culture, not just from a compliance perspective, but in general. These core values are widely taught and frequently reinforced in every employee's performance reviews. We also have ceremonies where core value awards are presented to employees at big meetings.

Two of our core values are integrity and accountability. We link these core values to our compliance culture. We try to set the message that good compliance is good business, and that compliance is everybody's job. We are never going to be everywhere and have oversight over everybody, so having our employees embrace this culture is critical especially in such a decentralized business.

We also try to give people the tools they need. We spend a lot of time and effort on meaningful compliance training that adapts, changes and evolves with our business. We also try to tailor it to individual roles – compliance training for a patient care technician in a rural facility will be different than for a business development executive in our company headquarters.

Q. WHAT DO YOU HAVE IN PLACE TO FACILITATE THIS?

We have various tools, such as compliance policies and procedures easily accessible on our intranet. We promote a compliance question line as a way for employees to submit compliance questions via email.

We have an annual communications plan to target compliance messages to particular audiences that we reassess throughout the year. And, of course, we have a hotline if staff have concerns about non-compliant behavior – people can report these issues to a third party anonymously.

We track and monitor trends in hotline reports and substantiated compliance violations in various ways including type of issue and location. This enables us to determine whether there are areas where we need to educate our people with more training or communication. Maybe there is a gap in understanding our policies and procedures that we need to address or an issue with leadership tone. We use data to tell us about areas of confusion or increased risk, areas where we need to get more engaged from a compliance perspective, or that need some other remediation. Overall, we try to learn and get better, and improve risk mitigation practices in the company.

Q. HOW OFTEN DO YOU CONDUCT RISK ASSESSMENTS AND UPDATE YOUR COMPLIANCE PROGRAMS?

We conduct a formal and fairly exhaustive annual risk assessment for our compliance program, and then we update that risk assessment every quarter, without doing a complete new soup-to-nuts type risk assessment again. We look at any new things that have come up each quarter: are there things that would make us rethink the current risk assessment and audit plan? We continue to evaluate that throughout the year, and then we do a complete full new risk assessment annually.

One of the keys to an effective risk assessment is prioritization of external risk factors – it's easy to get lost in a morass of "what-ifs" and things that could happen. I think it is important to assess the likelihood and impact of the various risks to prioritize what our focus will be to mitigate those risks. We include many external risk factors in our assessment and rank them to determine where we can best use our resources to mitigate that risk.

"Audits are the best source of gathering relevant information on critical operations," says the CFO of a North American private equity firm. "Internal audits are like the final preparation before the curtain rises, making sure everything is aligned for external audits. These internal audits also supply information about where compliance is weak – such as where there are any cases of corruption – and the resolutions in place for these situations."

External input, on the other hand, can help companies see the bigger picture, as Ruchit Patel, an antitrust partner at Ropes & Gray in London, explains: "Law firms teach specialization and lawyers join corporations with those specializations in tow. There is real value in putting experts together to produce a more holistic analysis."

Respondents in all regions understand the value of feedback from external counsel and other third parties, with 50% in APAC ranking it one of their top three considerations, followed by regulator inquiries or scrutiny of direct competitors (39%).

Surprisingly, at the other end of the scale, when asked what they are least likely to consider when revising anti-corruption policies and procedures, almost two-thirds of respondents in Latin America, North America and EMEA include changes in the scope of a company's operation in their top three – despite the fact that any change in their scope of operations should introduce new risks.

One possible explanation is that businesses expanding their scope of operations, whether due to new business lines or entering new markets, assume their existing programs are sufficiently robust to address any new risks.

55%
say they have heard of the behavioral approach to compliance

84%
believe that a behavioral approach to compliance would be moderately to very helpful

The most concerning result for this question may be around employee feedback: almost half of all respondents say this is the least likely factor to be considered when drafting or updating corporate anti-corruption policies.

"We need to have an honest conversation with people on the front lines about specific high-risk situations – what do they need to make the right decision? What might lead to them making the wrong choice? Otherwise we're just running in circles," says Alex Rene, co-chair of the anti-corruption & international risk practice at Ropes & Gray. "There is more work to be done to understand what is driving people to make decisions before we can find solutions that will work."

One North American-based CCO of a PE firm says it is important to tailor a policy to the firm's business, including by getting input from the people executing the policies every day, instead of simply adopting a set or prescribed model: "We might gather a few examples of a policy and think about the various approaches in the context of our business, then we will speak to the people that these will affect to get feedback and buy-in."

Interestingly, changes in laws and regulations have relatively little importance when drafting anti-corruption policies and procedures. Just 44% of North American respondents cite rule changes as most important to their in-house rules – the highest vote of any region – with 57% of Latin American and 56% of EMEA respondents considering it one of the least important considerations.

However, "given the continuously shifting environment, we do see new regulations being issued that can require changes

across multiple areas of a firm's compliance program," adds the CCO of the North American PE firm.

BEHAVIORAL APPROACH TO COMPLIANCE

While data gathering is improving, the analysis of data alone is not the best approach.

"Companies need to conduct behavioral science-focused working group sessions, or discussions with employees, to help interpret the data and apply the findings to their compliance programs," says Raad at Ropes & Gray.

The notion of a behavioral approach to compliance – gathering data to analyze why individuals act in a certain way and using that to inform compliance programs – is becoming more widely acknowledged, with 55% saying they have heard of the method.

"With the introduction of data science, it's become far easier to look at behavioral data with a whole new perspective," says the CEO of a life sciences and healthcare company based in EMEA. "We can create policies that align with compliance procedures, making it easier for us to govern compliance activities."

If it's handled the right way, using behavioral science thinking to inform compliance programs could even bring down compliance costs.

"Behavioral science can help a business identify current and future risk areas and help people on the front lines make the real-time decisions they need to make," says Raad. "A people-focused, behavioral approach cuts down on policy redrafts and the need to jump through regulatory hoops by going deeper into a tailored solution. It becomes a business strategy, rather than a compliance offering."

This idea seems to be taking hold: 84% of respondents say the approach would be very or moderately helpful. As the North America-based CCO of a medical technology company says, "Where there are individuals who do not want to do the right thing, behavioral data helps you identify trends, risks or issues in specific locations or activities that you want to address quickly."

IN CONVERSATION WITH...

Daniel Moynihan

Chief Compliance Officer, Akcea Therapeutics

Q. WHAT ARE THE CHALLENGES OF GATHERING, ANALYZING AND USING DATA TO INFORM COMPLIANCE POLICIES?

One is centralization of data: you often need to pull data that has been saved in different formats on multiple systems. Companies that have grown through acquisition will have multiple enterprise resource planning systems or platforms. Bringing them together is costly and time-consuming. Some platforms allow you to bring feeds from different systems into a central reporting engine, but then master data management becomes a challenge.

We conducted a major risk assessment that required a lot of data, but we could not go to an individual source for it. And if you don't have an integrated data source, it must be done either manually or using a sampling approach, where you look at a data set to get a representative sample of whatever you're looking for.

Q. HOW HAVE YOU USED DATA TO ENSURE THAT PEOPLE FOLLOW THE RULES?

I've had great success in aligning our understanding of risk by using data up front and talking to the business in a language everyone understands. Getting leadership to look at the data, understand where we're going and why, and support that move, is a huge part of that success, rather than the compliance function simply dictating terms.

Taking a "you're-going-to-go-to-jail" approach isn't acceptable. People refuse to listen. You need to explain the stakes and potential consequences facing both the company and, increasingly, individuals, in a way that's not threatening.

Q. HOW DO YOU IDENTIFY THE BIGGEST RISK AREAS FOR THE COMPANY?

Enforcement agencies or regulators enforcing anti-corruption laws globally don't want to impose a one-size-fits-all compliance program. They expect you to understand and address the specific risks facing your company. This requires a thorough risk assessment, both qualitative and quantitative.

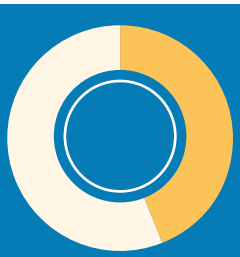
You may have a sense of the risks involved, but you must supplement that sense with data, including enforcement trends, by which I mean the likelihood of enforcement in certain jurisdictions.

If I were in an enforcement situation, I would feel much more comfortable backing up the rationale for our compliance using detailed data. There is an expectation among regulators that you are using all available data – because they will definitely be doing so. And if your competitors or the regulators can find information about your transactions, then other less scrupulous people can also likely see it. It's incumbent upon you to be sure of what your own data includes before other people can see it.

Section 02

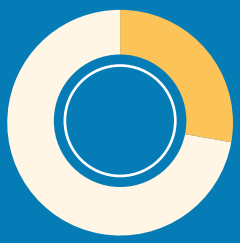
Compliance implementation and assessment

Risk officers are coping with both internal and external compliance challenges, from governmental requests to customer demands, as well as facing obstacles when they try to implement an effective compliance framework to tackle those challenges. Solving this puzzle demands a measured response.



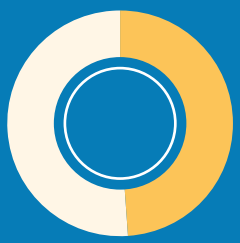
44%

of respondents say requests from government officials are their greatest compliance challenge (rising to 66% among asset management respondents and 58% among banks)



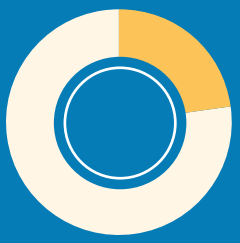
28%

of respondents have a whistleblower hotline managed by a third-party vendor



49%

of respondents do not have an efficient, reliable, properly funded process in place for investigating allegations



23%

of companies do not catalog all complaints and responses to allegations

Compliance is not a single issue. It is multifaceted and touches every part of a business. And it is not the same for every organization – different sectors face different compliance issues, some more obvious than others.

For example, requests from government officials are the greatest compliance challenge for financial services: 66% of respondents from asset management firms cite this as one of their top two biggest hurdles, while 58% of respondents from banks say the same (Figure 7). Just over half (52%) of respondents from banks also highlight customer requests as a major issue, twice as many as respondents from other sectors in the survey.

Almost half (48%) of respondents in life sciences and healthcare, meanwhile, say their biggest challenge is compliance requirements getting in the way of business operations.

Michael Beauvais, co-chair of the life sciences practice at Ropes & Gray, says companies in the sector are accustomed to complying with strict regulation, due to the nature of their business, and often have whole teams dedicated to legal requirements.

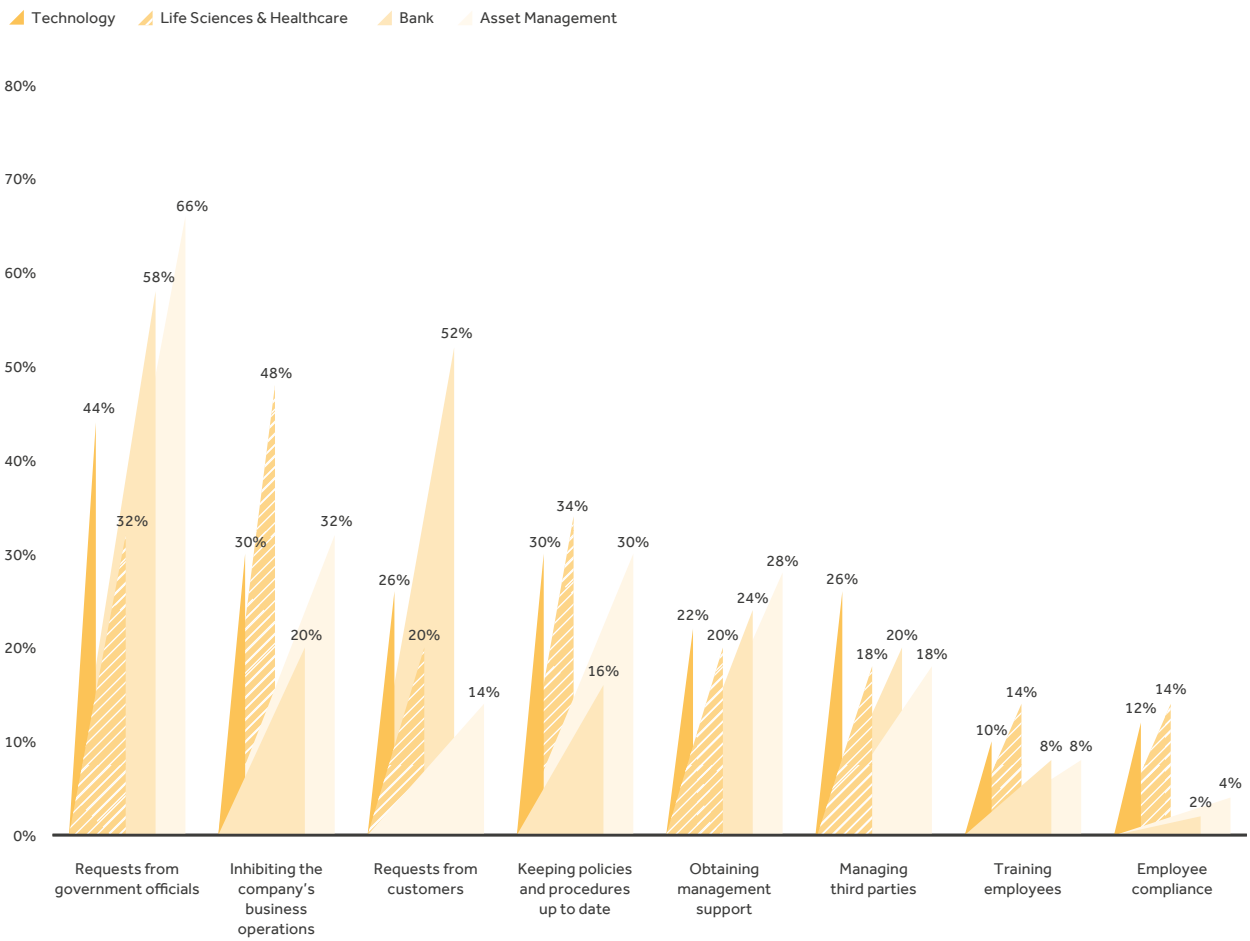
"That being said, like any industry, the life sciences industry must strike a balance between a robust compliance infrastructure and remaining competitive and nimble in the marketplace," says Beauvais.

Across all sectors, employee compliance was identified as the least serious compliance challenge, cited by just 2% of banking respondents. And yet, 52% of those same respondents say that their failure to understand why employees may choose to be non-compliant is a major barrier to implementing an effective compliance framework.

"Banks can be somewhat confident – certainly on the investment banking side – that they are hiring very high-caliber people and paying them well," says Rohlfsen at Ropes & Gray.

"Under those circumstances, they may assume employees are less likely to cheat – that's the theory, anyway."

FIGURE 7: **AS A COMPANY, WHAT ARE YOUR GREATEST COMPLIANCE CHALLENGES?** (SELECT TOP TWO)



OVERCOMING HURDLES TO IMPLEMENTATION

While addressing compliance challenges is difficult enough, implementing an effective compliance framework is an entirely different animal.

Culture may be the biggest obstacle to these efforts, depending on the various regions in which a company operates, according to respondents (Figure 8).

"Companies in APAC are less likely to conduct regular, compliance-focused audits or incorporate compliance metrics into the performance evaluation and review process because so much of the growth in Asia has been attributed to emphasis on sales or gaining market share," says Yang at Ropes & Gray.

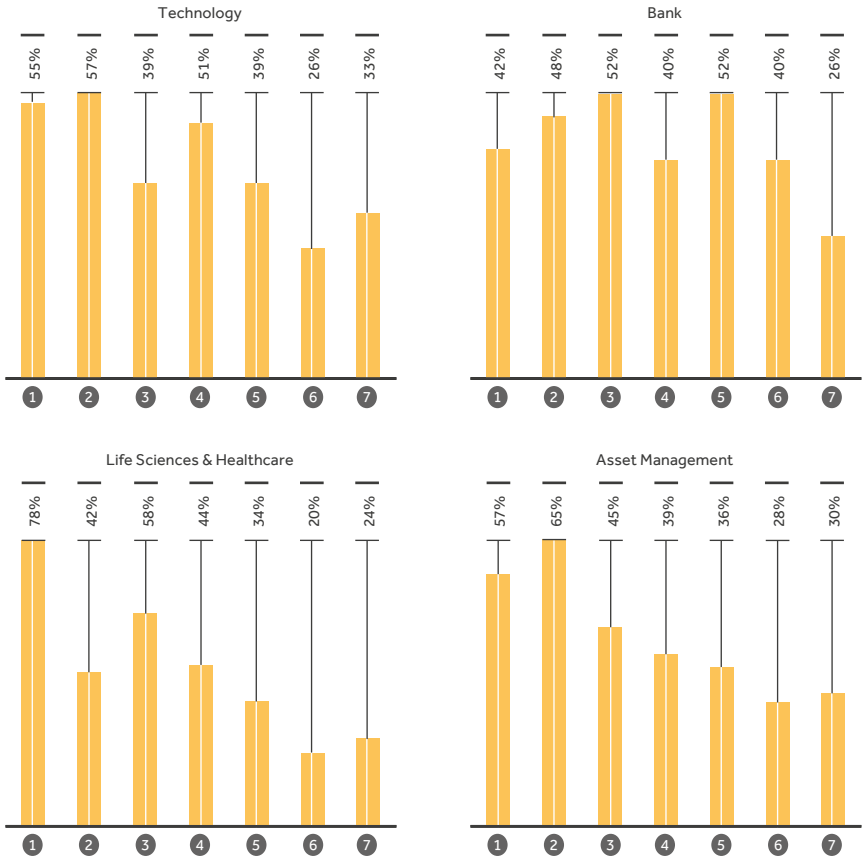
"Compliance and compliance-related departments are afraid to impede that growth, and certainly no senior manager wants to bear the blame for slowing revenue at a company. I think this is also reflected in the larger macro environment, where regulators have to walk a fine line between strictly enforcing the laws and making sure their enforcement doesn't slow down the growth of a country's economy."

But while this view is shared across all sectors, those in life sciences and healthcare feel this issue most acutely (78%).

"The life sciences sector is heavily regulated, and thus different countries' approaches to regulation impact the culture of the life sciences industries in such countries," says Beauvais at Ropes & Gray.

"For example, the U.S. has a uniform framework for the regulation of drugs and medical devices, meaning that pharmaceutical companies and medical device companies both function under regulation of the U.S. Food and Drug Administration and thus are accustomed to complying with its strict regulatory framework. In Europe and other jurisdictions, the regulatory authority for drugs is separate from that for medical devices, leading to a different culture."

FIGURE 8: **WHAT DO YOU THINK ARE THE BIGGEST OBSTACLES TO IMPLEMENTING AN EFFECTIVE COMPLIANCE FRAMEWORK?** (SELECT TOP THREE)



❶ The culture of the region or country where your company operates

❷ Ineffective use of resources (for example, failure to conduct effective audits that identify problems or trainings that do not engage the audience)

❸ Company culture (for example, inadequate tone from the top)

❹ Incentives for engaging in non-compliant behavior (for example, salary and bonus structures)

❺ Failing to understand why employees might choose to be non-compliant

❻ Lack of compliance resources

❼ Industry practice

Company culture is another sensitive spot for life sciences, according to 58% of respondents in the sector. Inadequate or inappropriate "tone from the top" can be a major obstacle.

"There needs to be commitment from the board at the most senior levels, running all the way through the organization," adds Raad from Ropes & Gray. "That commitment lets people know this must be taken seriously and that the board isn't just paying lip service to compliance."

Much of this boils down to resource allocation, which is cited as another major concern, especially in financial services – 65% of asset manager respondents and 48% of bank respondents say that an ineffective use of resources is their biggest barrier. This could mean they feel their companies are unable to conduct effective audits that identify problems or run training

IN CONVERSATION WITH...

Azish Filabi

Executive Director, Ethical Systems

Q. HOW IMPORTANT IS COMPANY CULTURE TO COMPLIANCE?

I think most people in business would agree that culture is a key factor in how they run their company – not just the effectiveness of their compliance programs, but all business outcomes (profitability, innovation, etc.). People intuitively know that culture drives their day-to-day behavior. The challenge is operationalizing it.

For compliance, it's important to keep ethics at the top of people's minds, and to design internal systems that will align with the company's stated values. Keeping ethics salient is important, but values need to also be integrated into day-to-day work systems and decision processes. For example, research shows that if you frame a decision as a "business issue" or using the language of "cost-benefit" analysis, it could lead to unethical outcomes that don't align with the values you intended to keep.

Q. WHAT MISTAKES DO COMPANIES MAKE WHEN BUILDING COMPLIANCE PROGRAMS?

Compliance programs are often built too narrowly to monitor and find bad behavior (i.e., the bad apples), or just focus on training employees about the rules. In the best case scenario, monitoring and/or testing transactions can find existing violations of internal compliance policies and limits. But how do you prevent employees from causing problems in the future? How do you get them to enroll in your organization's values and work to advance client interests?

I think partnerships between compliance and HR departments are really important. To help prevent problems, companies need to focus on corporate culture, ethical leadership and developing a values-based approach to compliance. Linda Trevino and her co-authors published a research piece called "What Works and What Hurts" in the *California Management Review* in 1999 – based on data collected from six large U.S.-based companies. They found that, in those companies where employees perceived that the purpose of the compliance program is to protect top management from blame (i.e., CYA), all of the outcomes associated with program effectiveness were negative. That includes outcomes such as observations of unethical behavior throughout the firm.

Getting employees to buy in to the purpose of your compliance program is key to its effectiveness.

Q. HOW DO YOU THINK COMPANIES SHOULD ADDRESS INTERNAL CULTURE?

I often hear people describe their organization's culture based on their "gut feelings" or their own personal experiences. But research shows that senior leadership is often not in tune with the organization's culture, particularly in those organizations where bad news travels up very slowly (if at all). People are too afraid to tell the boss what's really going on.

To manage corporate culture, you need to begin with an assessment. Especially for large companies, a full assessment that includes interviews, focus groups, and surveys can help leaders understand the mindsets and beliefs that govern day-to-day behavior. Based on those findings, you can then focus on problem areas, be they issues about perceived unfairness or abusive management, or geographic areas where you see sub-cultures forming that diverge from your broader organizational values.

In those cases where you've discovered misconduct, companies should use audit processes and investigations focusing on the root cause of compliance failures. Corporate investigators are good at finding who was responsible for misbehavior or connecting the dots on what led to a compliance failure, but often they're not uncovering the root cause of the problem. Even if you're able to find the wrongdoer and fire him, until you address the social context in which the misbehavior occurred, you haven't fixed the problem. Was there social pressure that caused the breach? Were the growth goals too aggressive? These are examples of the types of issues that should be addressed.

courses that fail to engage their target audience.

"Resource allocation is a huge obstacle," says Rohlfsen at Ropes & Gray. "Companies have to grapple with where and how they spend money. Those facing regulatory or criminal enforcement are going to put more resources into compliance to put out any fires. When you're not in that situation it is hard, but you have to justify the cost."

According to the CCO of a North American financial services firm, those with limited resources need a more targeted strategy: "The key is to approach things from a risk-based perspective, prioritize what to address first and how, and think about things in advance to the extent possible with an action plan of how to attack it."

Updating when necessary, rather than conducting a less frequent, but more onerous overhaul, would help balance out the burden.

"Policies and procedures are living documents," adds the CCO. "Updating them can mean tweaks here and there."

COMPLIANCE ASSESSMENT AND TRACKING: A GLOBAL PERSPECTIVE

Risk assessments, tracking high-risk transactions and the usefulness of compliance metrics are all viewed through very different lenses around the world. While most North American and European companies conduct robust reviews of potential risks and the tools they have in place to mitigate those risks, businesses in Asia-Pacific and Latin America seem less inclined to follow suit.

For example, almost all respondents in EMEA (87%) and North America (90%) say they carry out formal risk assessments to determine any compliance vulnerabilities in their company, as well as the state of their compliance controls. In Asia-Pacific, 60% say the same. In Latin America, that figure drops to 43% (Figure 9). Similarly, while a significant majority of respondents in EMEA (83%) and North America (80%) conduct regular, compliance-focused audits, only 57% do so in Asia-Pacific and Latin America (Figure 10).

"There is a lack of resources devoted to compliance and a lack of delineation of compliance duties in Asia, compared to Europe and North America," says Yang at Ropes & Gray. "It is difficult to conduct formal risk assessments when you don't have the manpower or are unclear about which department should be running the risk assessment."

90%

of respondents in North America carry out formal risk assessments to determine any compliance vulnerabilities in their company

60%

of respondents in Asia-Pacific say the same

The divide continues when tracking potential high-risk transactions, including those involving government officials, tenders and interactions with consultants. While 92% of North American respondents and 85% of those in EMEA do track them, more than a third (34%) of respondents in Asia-Pacific and almost half (47%) of those in Latin America do not (Figure 11).

In addition, more than a third of those in EMEA and North America say such transactions have heightened approval requirements, while in Asia-Pacific and Latin America stronger requirements are implemented by only 12% and 10% of respondents, respectively.

Again, this regional split is clear when looking at performance evaluation and review processes: between 55% and 60% of respondents from EMEA and North America say they incorporate compliance metrics into this process, while this falls to 19% in Asia-Pacific and 10% in Latin America (Figure 12).

"It's a combination of thinking about the transaction and the risks related to that transaction," says

FIGURE 9: **DO YOU CONDUCT FORMAL RISK ASSESSMENTS TO ASSESS YOUR COMPANY'S GREATEST AREAS OF COMPLIANCE RISK AND THE INTERNAL CONTROLS PUT IN PLACE TO PROTECT AGAINST THOSE RISKS?**

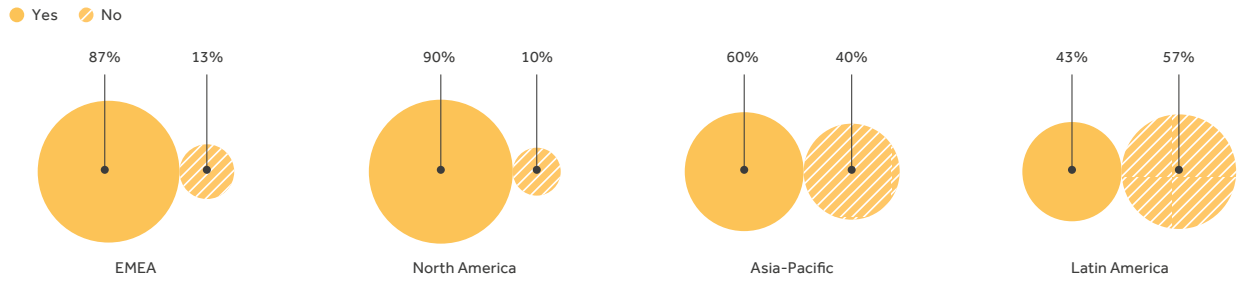


FIGURE 10: **DO YOU CONDUCT REGULAR, COMPLIANCE-FOCUSED AUDITS?**

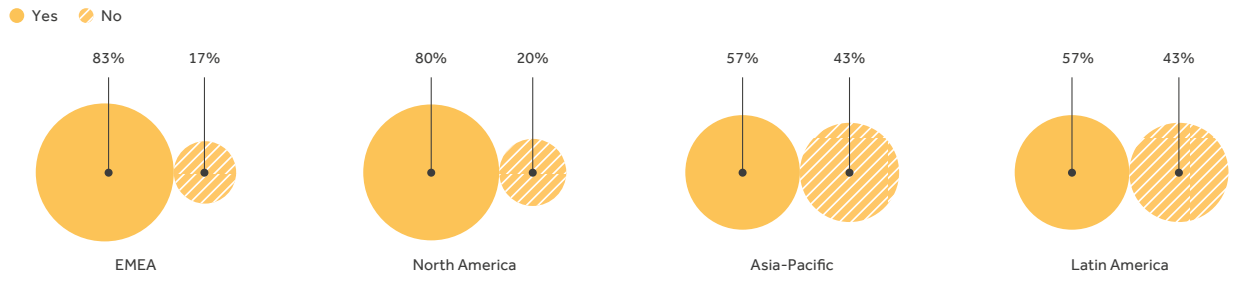


FIGURE 11: **DOES YOUR COMPANY TRACK AND LOG POTENTIAL HIGH-RISK TRANSACTIONS (FOR EXAMPLE, TRANSACTIONS WITH GOVERNMENT OFFICIALS, TENDERS, INTERACTIONS WITH CONSULTANTS, ETC.)?**

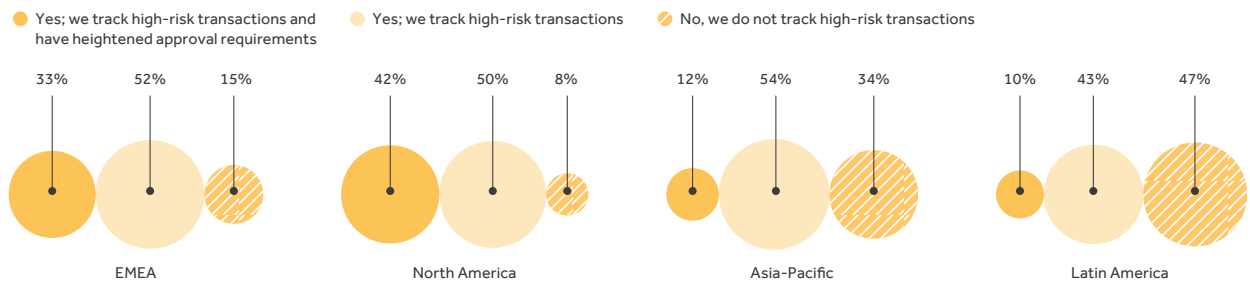
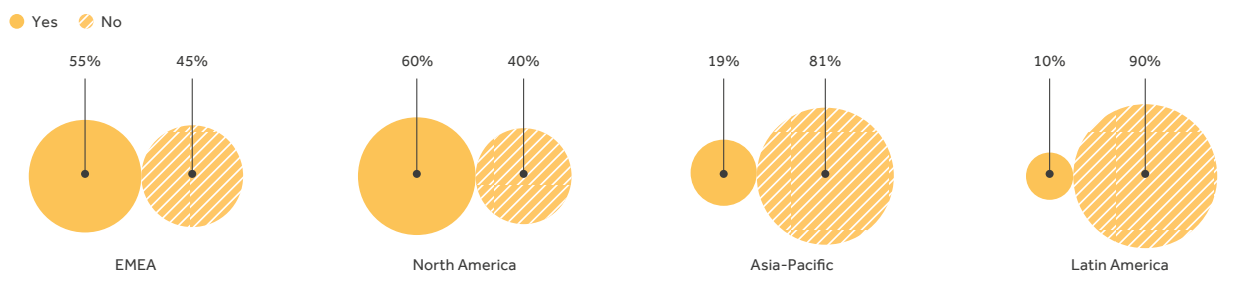


FIGURE 12: **DOES YOUR COMPANY INCORPORATE COMPLIANCE METRICS INTO THE PERFORMANCE EVALUATION AND REVIEW PROCESS?**



the COO of a medical technology company in North America, "and then looking for the data that will help identify anomalies or trends that may be of concern."

There is a stark difference in activity across the four regions, as some regulators are more advanced in their attitudes to creating or enforcing existing rules and regulations – however, this may be shifting.

"There are always going to be regional differences to compliance because people don't think the same way," says Rohlfsen at Ropes & Gray. "But there is definitely a move towards transparency and ethical behavior in global business."

REPORTING MISCONDUCT

The regional split is less defined when looking at how companies report – or ask their staff to report – misconduct. More than 90% of respondents from EMEA and North America have either an anonymous or third-party-operated system for reporting suspected or actual misconduct or violations of company policy (Figure 13).

Says the CFO of a life sciences and healthcare company based in EMEA: "We have an internal resource team that manages compliance-related monitoring and resolutions... and they maintain complete anonymity of the person raising a flag."

Some 70% of respondents in Asia-Pacific say they operate similar systems, with this number sitting at 60% among Latin American companies.

"There are many companies in Asia that do not see the value in confidential reporting mechanisms or think it fosters a better compliance culture," says Yang from Ropes & Gray.

"Some see whistleblowers as disgruntled employees making a last-ditch effort to keep their jobs, or worse, to take revenge against their supervisors and colleagues. Therefore, I think there is a reluctance among some Asian companies to give these employees a mouthpiece to amplify their grievances or disrupt the workplace."

Perhaps worryingly, only half (51%) of all respondents say they have "an efficient, reliable and properly funded process in place for investigating allegations". In addition, 23% of respondents across all regions and sectors say they do not catalog all complaints and document their company's response to allegations, which suggests they may be missing out on data that could be used to influence and improve compliance policy and procedures in the future.

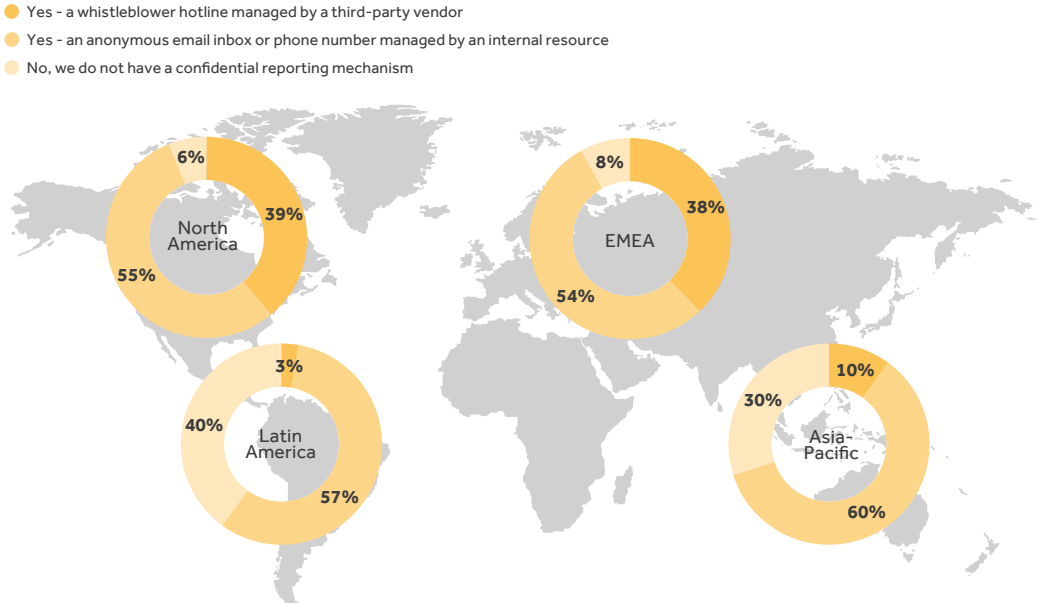
51%

of respondents say they have an efficient, reliable and properly funded process for investigating allegations

23%

say they do not catalog all complaints and document their company's response to allegations

FIGURE 13: **DO YOU HAVE A CONFIDENTIAL REPORTING MECHANISM TO REPORT SUSPECTED OR ACTUAL MISCONDUCT OR VIOLATIONS OF THE COMPANY'S POLICIES?**



IN CONVERSATION WITH...

Joseph Smith

Global Financial Crime Counsel, Barclays

Q. IN YOUR EXPERIENCE, WHAT MOTIVATES PEOPLE TO ADHERE TO COMPLIANCE RULES IN A COMPANY?

I think people want to do the right thing and that, increasingly, firms are ensuring people are positively incentivized to demonstrate good behaviors. In the financial services sector, there is an increased focus on individual accountability. In the UK, for example, the FCA brought in the new Senior Managers and Certification Regime (SM&CR) which places the onus on individual accountability for compliance at a senior level.

The challenge often isn't so much "tone from the top" – and the SM&CR helps to sharpen the focus at the top of the house – but making sure that it cascades through the organization so that you have the right tone in the middle. The middle management layer has to be empowered to do the right thing and build a robust corporate compliance culture.

Q. FINANCIAL SERVICES ARE SUBJECT TO SIGNIFICANT REGULATORY PRESSURES AND ENFORCEMENT – IS THIS CREATING A COMPLIANT CULTURE IN THE SECTOR?

Yes, although there are always opportunities to improve further. The sector is highly regulated and there are high expectations among regulators in terms of how firms are structured, their governance, systems and controls. All of this is mandatory – firms have to make sure they are compliant. The risk is that this leads to a tick-box culture where people are doing things simply because that's what the manual says they should do instead of taking a step back and asking whether it's the right thing to do.

Q. ARE MORE COMPANIES TURNING TO DATA FOR COMPLIANCE PURPOSES?

Yes, absolutely. We use data in different ways. For example, we are mitigating cybersecurity risk – which is part of our compliance requirements – through data by harnessing intelligence within the organization.

All major companies face a vastly increased threat from cyberattack. In the banking context that includes everything from theft of customer data to social engineering scams that prompt fraudulent wire transfers and data destruction that can shut down entire parts of a business. There's a risk of criminals breaking into your systems not just to steal data but to plant fake data that could corrupt business operations and prevent you from being able to compete in the market.

Financial institutions, including Barclays, have been investing significant resources in security functions, including command centers in multiple regions. These pool the threat data that they collect from different sources and use that data to monitor threats in real time and coordinate response efforts.

Part of the reason for pulling that data together is not only to understand and mitigate the threat that the organization faces internally but also recognizing that we have an obligation to support law enforcement to disrupt and prevent criminal activity, whether cyber-enabled, fraud or other types of crime. Data is only one component: you also need to develop thorough and thoughtful response plans and playbooks to respond to different types of incidents.

We've been looking at how we can better use our technology to get better at spotting and identifying potentially unusual or suspicious behaviors and transactions both in our internal staff members and customers. We're proactively profiling for risk, trying to look at the data that we have available to try and identify different types of threat.

We also have the risk of our customers not complying with the law whether that means dabbling in low level fraud or engaging in something like human trafficking, with the proceeds of that crime flowing through the bank for money laundering purposes. That's where technology is key. Good technology is better able to detect and steer action, which is a huge benefit in a large, diverse global business like ours. You need to be able to examine how these threats present themselves within your different businesses and jurisdictions, and respond accordingly.

Q. IS A MORE DATA-DRIVEN APPROACH TO COMPLIANCE, WITH A FOCUS ON BEHAVIOR, THE BETTER CHOICE?

I think you need both. Data-driven programs are invaluable when it comes to identifying emerging threats and risk trends, and being proactive in profiling for those risks. But they can't be a substitute for traditional top-down codes of conduct, policies, procedures and standards, and a very clear framework setting the expectations of behaviors.

Many years ago, there really was only one approach to compliance: policies, training and monitoring. You would conduct risk assessments based on what people told you was happening in the organization rather than empirical data. Now that the technology is available to take that to another level, organizations need to decide where they invest their resources.

No matter how good the technology gets, there will always be a need for human judgment regarding potential risks. For example, very sophisticated transaction monitoring tools can alert you to suspicious activity in transactions, but at some point, a person needs to look at that information and interpret it. I don't think compliance will reach the point where it's just done by computer.

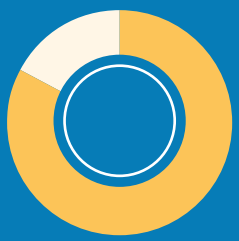
Section 03

Third parties and risk management

Working with third parties may be a fundamental part of business, but some regions are more keenly focused on regular third-party due diligence than others, while different sectors have different views on where specific attention is needed. Working with independent providers adds layers of complexity to an already complicated situation.

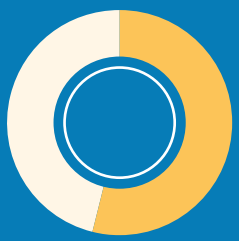
46%

of respondents say the chief compliance officer, or the compliance department in general, is responsible for third-party due diligence and monitoring



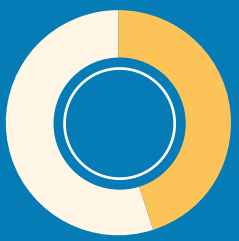
83%

of respondents cite informal background checks conducted internally as the top priority when carrying out third-party due diligence



54%

say one of the most important areas of due diligence is confirming that a third party is qualified to do the work that it has been engaged to do



55%

do not alter their level of third-party due diligence based on the type of third party or any red flags identified

Businesses understand that they have to address third-party risk, but many have struggled for years to determine what level of third-party diligence they need to conduct – and how that feeds into everything from contracts to third-party audit rights and how to use them.

"Anti-corruption laws do not distinguish third parties," explains Raad from Ropes & Gray. "If a third party is acting on your behalf and pays a bribe, you're on the hook, unless you can show that you did everything right in terms of due diligence, sufficient monitoring and checking. That's a heavy – but essential – burden for companies to bear, because most anti-corruption investigations, settlements and fines involve third parties – that's usually the way money is funneled. People don't want to do it directly, and think using third parties will protect them, but it won't."

DUE DILIGENCE AND MONITORING OF A THIRD PARTY

Who is responsible for third-party due diligence? The balance of power is split by region (Figure 14): in EMEA and North America, around 55% of companies hand this responsibility to the chief compliance officer, or the compliance department in general, compared to less than a third in Asia-Pacific and Latin America. Around half of respondents in the latter two regions give that responsibility to the chief risk officer or risk committee, while between a quarter and a third of EMEA and North American companies do the same.

Across all sectors, few respondents (11% or less) say any other department, including the legal or finance units, or the specific teams working with the third party themselves, took responsibility for due diligence.

FIGURE 14: **WHO IS ULTIMATELY RESPONSIBLE FOR THIRD-PARTY DUE DILIGENCE AND MONITORING?** (SELECT ONE)

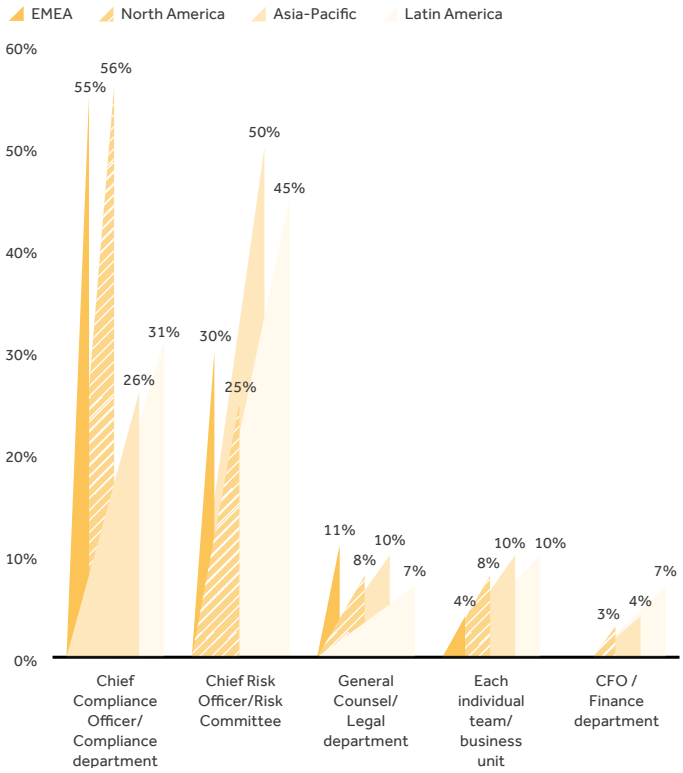


FIGURE 15: **WHAT DILIGENCE DO YOU CONDUCT ON THIRD PARTIES BEFORE YOUR COMPANY ENGAGES THEM?** (SELECT ALL THAT APPLY)

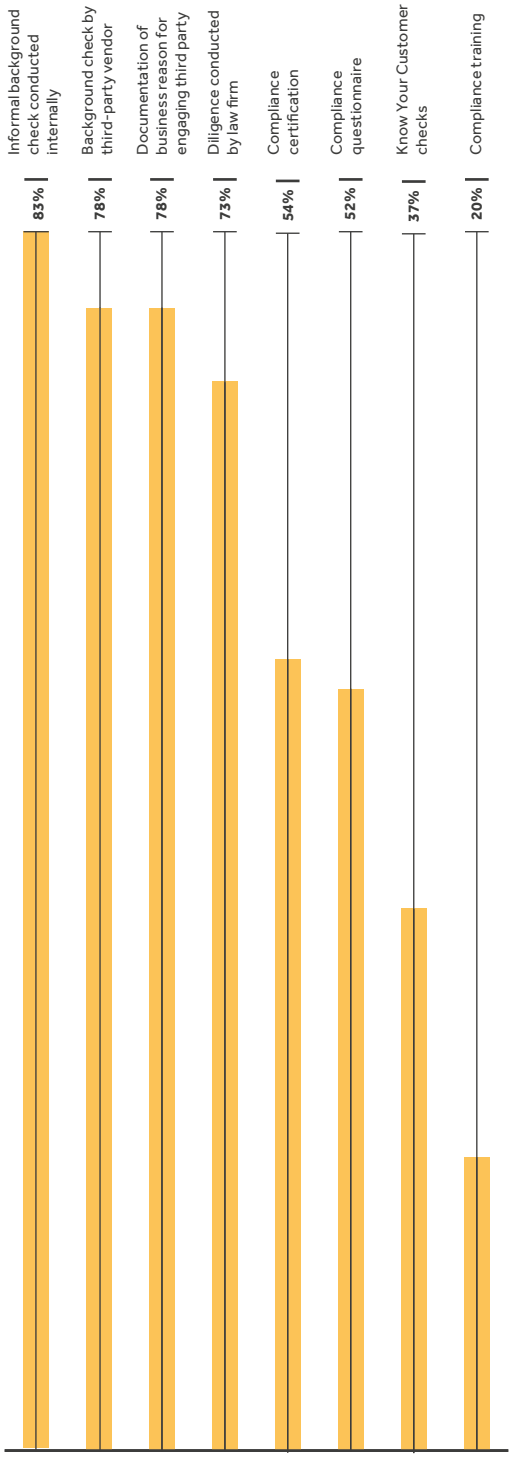
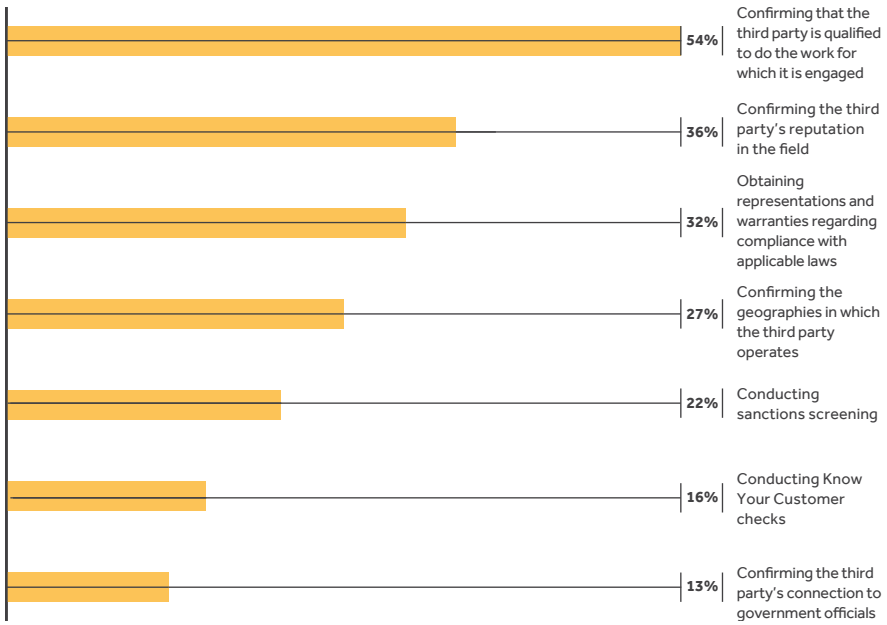


FIGURE 16: **WHICH OF THESE AREAS ARE MOST IMPORTANT TO YOU IN THE THIRD-PARTY DILIGENCE PROCESS?** (SELECT TOP TWO)



"This is somewhat concerning, as you really need the business working with the third party to commit to owning the risk, as the business remains on the front line," says Raad from Ropes & Gray.

Conducting informal background checks on third parties before engaging with them seems to be standard procedure, with 83% of respondents from all regions and sectors saying they do so (Figure 15). Some 78% say they have engaged an independent company to carry out a background check, while the same number checked and filed documentation memorializing the business reason for working with the third party.

Just under three-quarters of respondents (73%) say their company engaged a law firm to conduct due diligence, while just over half say they completed either a compliance certification (54%) or questionnaire (52%) with the new supplier or partner. Only a fifth carry out compliance training with a third party.

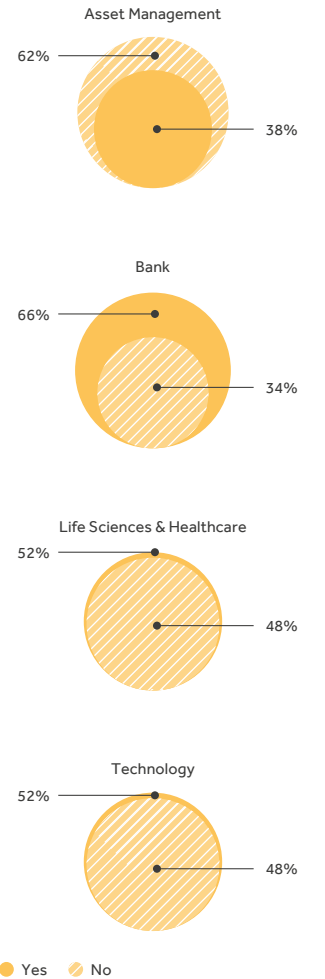
"Before we get on board with a third-party vendor," says the CFO of an asset management firm based in EMEA, "we conduct a detailed check to assess the vendor from different viewpoints. An external vendor does the dirty work for us, including documentation assessment of the third party."

Confirming that the third party is qualified to do the work for which it is being contracted is one of the most important aspects of third-party diligence, with 54% of respondents across all regions and sectors deeming it one of their top two priorities (Figure 16). Slightly more than a third say it is also essential to establish a new partner or supplier's reputation in the field before engagement, with almost as many obtaining guarantees of their compliance with applicable laws (32%).

Conducting "Know Your Customer" checks (16%) and tracking connections to government officials (13%) were the two least important steps for survey respondents – though these checks may well be handled as part of the broader background checks.

Just over half of all respondents (55%) say they do not adapt the

FIGURE 17: **DOES THE LEVEL OF DILIGENCE THAT YOU CONDUCT ON THIRD PARTIES VARY DEPENDING ON THE TYPE OF THIRD PARTY OR RED FLAGS IDENTIFIED?**



55%

say the level of diligence they conduct on third parties does not vary depending on the type of third-party or red flags identified

FIGURE 18: **HOW COMFORTABLE ARE YOU WITH THE RISK LEVEL OF YOUR THIRD-PARTY PARTNERS PRIOR TO ENGAGING THEM?** (ON A SCALE OF 1-10 WHERE 1 = NOT AT ALL COMFORTABLE AND 10 = VERY COMFORTABLE)

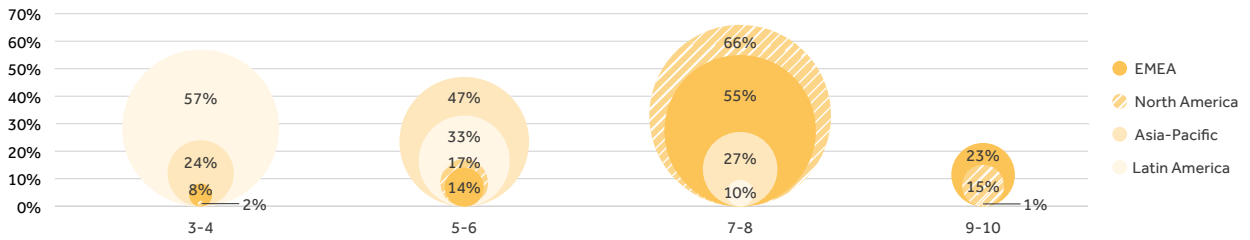
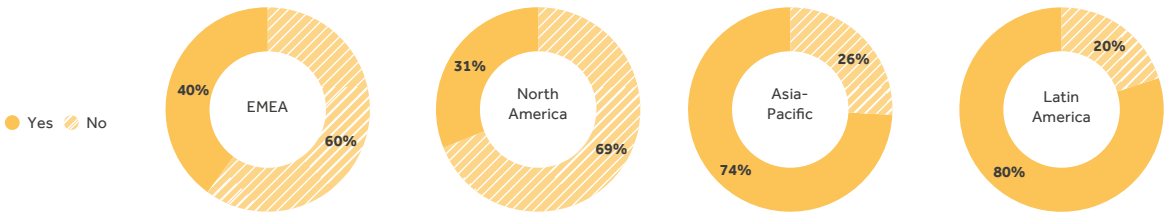


FIGURE 19: **DO YOU EVER ENGAGE THIRD PARTIES WHO MAY INTERACT WITH GOVERNMENT OFFICIALS ON YOUR COMPANY'S BEHALF?**



level of due diligence they carry out, depending on either the type of third party or the red flags raised by any investigation.

Beauvais at Ropes & Gray points out that the level of diligence being exercised largely depends on the type of activity performed by the third party: "For example, if a life sciences company engages a contract research organization to manage its clinical trials abroad, it will likely exercise a great deal of diligence," says Beauvais. "For vendors performing lower-risk functions, such as conference planning, they tend to exercise less diligence."

But some sectors are more prone to adapt than others: two-thirds of banks do so, whereas just over a third of asset managers can say the same (Figure 17).

As the in-house lawyer of a North American asset management firm explains, "We have structured the system to test the third party at maximum, beyond which, we – being third parties to the vendors as well – are not allowed to conduct a due diligence check. So, the intensity doesn't change and is on the higher side all the time."

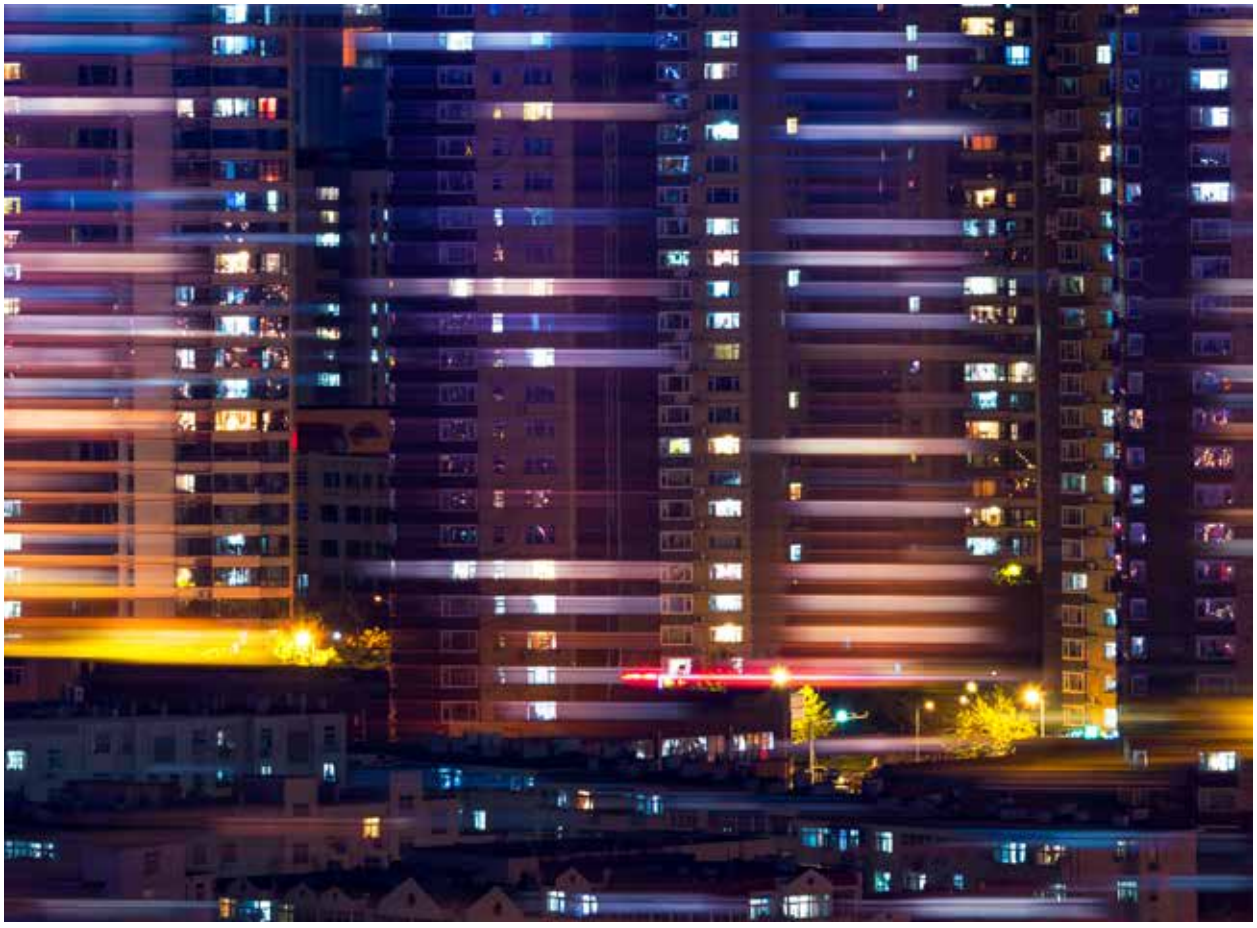
The majority of respondents in EMEA (78%) and North America (81%) are comfortable with the risk level of their third-party partners prior to engaging with them (Figure 18 - based on a rating of 7 to 10 out of 10). But the picture is very different among Asia-Pacific respondents, just 28% of whom give similarly higher ratings, and Latin American businesses, who are the least secure at 10%.

THIRD-PARTY RESTRICTIONS

When asked whether they engage third parties that may interact with government officials on their behalf, another clear regional split among respondents begins to emerge (Figure 19).

While 40% of respondents in EMEA and 31% of those in North America say this was sometimes the case, the numbers are much higher elsewhere. In Asia-Pacific and Latin America, 74% and 80%, respectively, engage in this kind of activity.

"Companies in Asia are more likely to engage third parties who may engage with government officials on their behalf, and they are less likely to monitor their third parties, leaving them vulnerable," says Yang from Ropes & Gray. "I think some companies in Asia don't have the resources to monitor third parties. Others may not understand that their company may be liable for the actions of third parties, and this may be partly due to a lack of clarity in regional laws. For example, China only amended its Anti-Unfair Competition Law last year to clarify that bribes made through a third party would also fall under commercial bribery."



Some respondents, however, are quick to point out that this is not necessarily a cause for concern. As the CFO of an asset management firm based in APAC says, "We have third parties who deal with the government for us. An external legal department is in place to verify our legal proceedings or basically do a security check for our legal team that is conducted by a third party."

MONITORING THIRD-PARTY RISK

"People are getting more comfortable with third-party risk, but the danger is that we're slipping into checklist mode – we did our due diligence, we have contract reps in the agreement and audit rights, and we're monitoring them, so we're fine. But you have to step back and check what the results are actually revealing," points out Raad from Ropes & Gray.

Analyze these results from a risk perspective instead of relying on the fact that diligence has been done. Check in with employees who have regular daily interactions with third parties. Put the responsibility on the business and those on the front lines to really own this risk: are they seeing anything that doesn't look right? If so, are they saying anything? If the third party changes its bank account details, are those employees flagging it or are they just filling out a diligence form that gets filed? If, right before you're trying to get a deal done, the third party says it needs an extra commission urgently, is anyone analyzing that from a risk perspective? Or is everyone relying on the fact that diligence was done and everything feels fine?

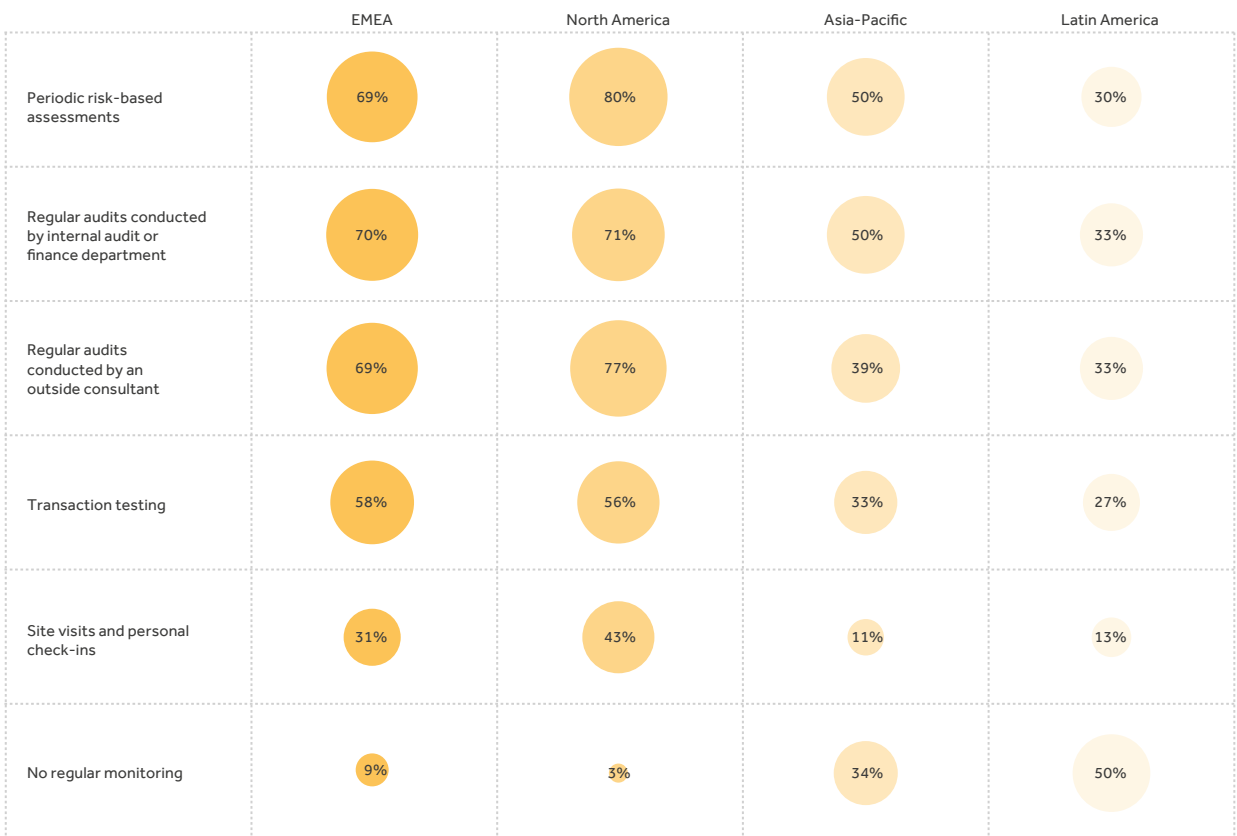
"The basics may be there, but businesses need to make sure that their employees don't have a false sense of security because of a checklist," adds Raad.

According to the findings, more than two-thirds of respondents based in EMEA (69%) and North America (80%) and half of those in Asia-Pacific are taking this approach, carrying out periodic risk-based assessments of their third-party providers (Figure 20).

The numbers are broadly similar among those saying they conduct regular third-party audits using internal teams in EMEA (70%), North America (71%) and Asia-Pacific (50%), or using outside consultants in EMEA (69%), North America (77%) and Asia-Pacific (39%).

However, Latin America is the outlier in this area: just 30% of respondents in the region conduct periodic risk-based assessments, with 33% saying regular audits are carried out by either internal or external teams. Half of Latin American

FIGURE 20: **HOW DO YOU MONITOR YOUR THIRD PARTIES?** (CHECK ALL THAT APPLY)



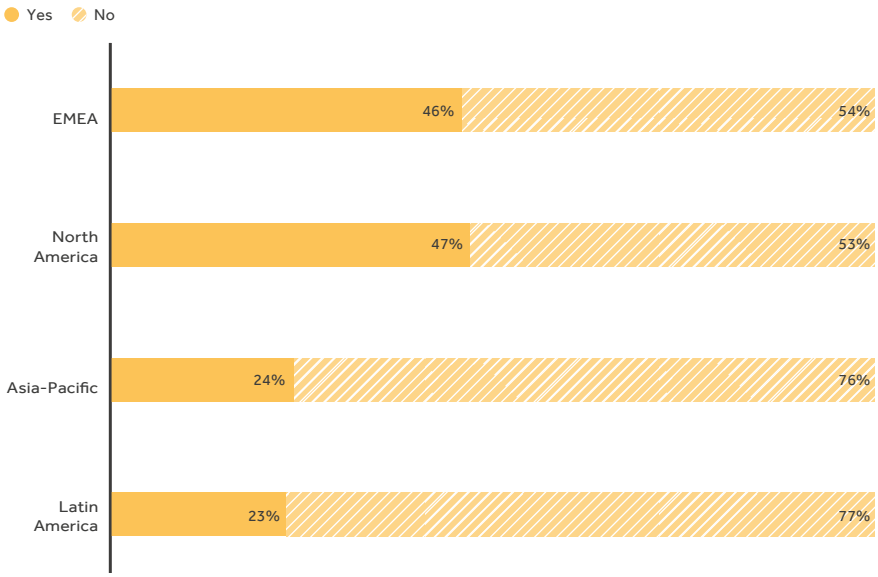
respondents say they do not carry out regular monitoring of third parties.

Additionally, unlike in EMEA and North America, where respondents carry out site visits and personal check-ins relatively commonly (31% and 43%, respectively), the results show that both Asia-Pacific and Latin American companies rarely do so (11% and 13%, respectively).

One other area where Asia-Pacific and Latin America are less stringent with their third-party controls than the other regions is auditing rights. Over three-quarters of Asia-Pacific (76%) and Latin American (77%) respondents say they do not require auditing rights when engaging with independent suppliers. Only around half of respondents in EMEA (54%) and North America (53%) say the same (Figure 21).

For those who do require these rights, almost two-thirds

FIGURE 21: **DO YOU REQUIRE AUDIT RIGHTS WHEN ENGAGING THIRD PARTIES?**



IN CONVERSATION WITH...

Alex Fell

Head of Strategy, Planning and Operations, Global Ethics & Compliance, GSK

Q. HOW DO YOU USE DATA IN YOUR COMPLIANCE STRATEGY?

When it comes to data, being a big company like GSK is an opportunity and a curse, because availability of global data in a company our size is sometimes more difficult than in a smaller company. We have evolved from tracking compliance performance to including additional audit training policy compliance metrics, as well as information about business activity, sales growth, revenue spends and profiles, to inform our risk assessments.

Our next evolution is to look at key risk indicators – including environmental, performance and behavioral factors – and use them to inform the board on how well risk is being managed.

There are things we would love to track but don't have the data, such as macro business intelligence that may not be captured in a way that a compliance professional would want to see it. We're getting better at this by examining what is available and looking at data more creatively.

Q. ARE THERE COMPLIANCE STRATEGIES YOU WANT TO IMPLEMENT BUT HAVE NOT YET BEEN ABLE TO?

Many of the things we can track are retrospective and not necessarily good predictive measures. We are behind the curve but think we can get better.

Marrying the data with the behavioral side is where value will be driven, and I think many organizations are moving toward this. They are identifying significant risks facing their company and measures they are taking to mitigate them. We are trying to get our behavioral data to a point where we can present it regularly to our board of directors. If you identify a compliance issue and create an online training module to deal with it, that isn't going to change employee behavior in the same way as using insight to create a discussion guide for your leadership. Something that talks about the ethical issues and helps to resolve the situation will work much better.

62%

of those that require audit rights when engaging with third parties exercise these rights regularly and on a random basis

(62%) exercise them regularly on a random basis, rather than when there is an allegation or indication of wrongdoing.

As for the others, some apparently don't like to rock the boat: "We are eligible to conduct random audit checks on the vendors, though it's a freedom we don't like to exploit purely for business relations," says the chief risk officer of a bank based in EMEA.

"We have made it easier for the vendors by not exercising our audit rights rigorously but limiting to situational considerations," agrees the CFO of a North American bank. "If a flag is raised that concerns us, we will go ahead with a detailed check."

"Third-party audits are only conducted if there is an indication of any wrongdoing. We do not interrupt their general course of operations until we come across any findings that need specific attention," adds the director of risk management for a bank based in Asia-Pacific.

ACQUISITION DUE DILIGENCE

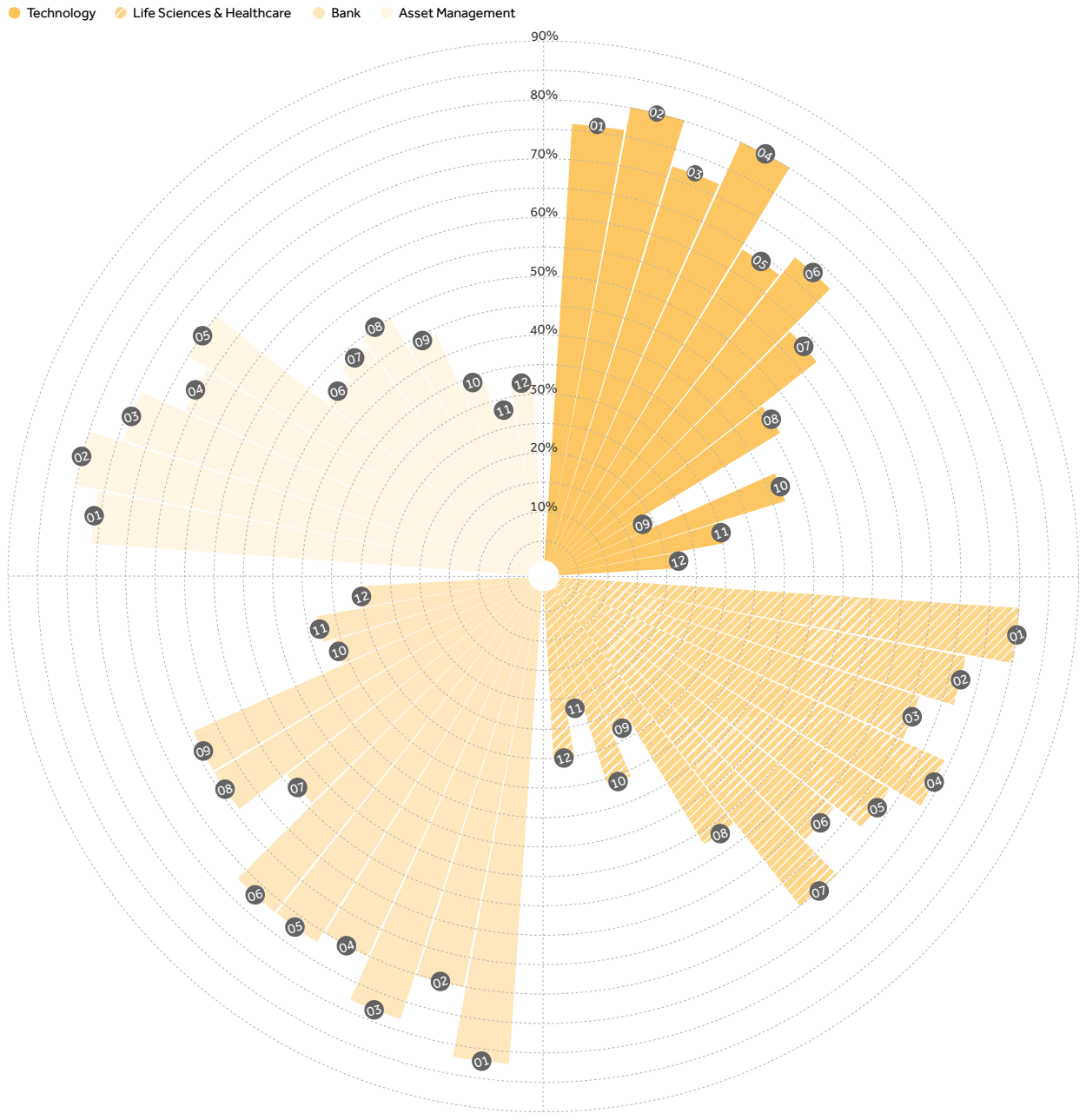
Before taking over or acquiring a stake in a new company, there are a range of diligence steps companies across all sectors consider essential.

The top requirement is an assessment of policies and procedures at the potential new company, with more than three-quarters of respondents ticking that box. Respondents from banks consider it to be their most crucial action, with a score of 82% coming from that sector (Figure 22).

Overall, the second most important requirement is carrying out reputational due diligence, with technology and asset management businesses considering it their top priority.

"These results confirm that investors and purchasers appreciate the value of assessing both the existing control framework and the culture at targets. Both reveal the extent of potential historical violations and ability of the company to efficiently integrate into or adapt to a newly defined framework," says James Dowden, co-chair of the anti-corruption & international risk practice at Ropes & Gray.

FIGURE 22: **WHAT DILIGENCE STEPS DO YOU TAKE BEFORE A POTENTIAL ACQUISITION OR EQUITY INVESTMENT?** (CHECK ALL THAT APPLY)



Negotiation of anti-corruption representations and warranties is in the top three overall, though interviews with compliance personnel at the target company edged slightly higher (80%) among technology companies. This may reflect their desire to protect themselves against future issues surrounding ownership of IP or customer data within the target company.

Just under two-thirds (64%) of bank executives believe that carrying out a litigation and news search, as well as a Know Your Customer review, is important to their businesses – higher than any other sector in the survey, no doubt due to the heightened risk of money laundering and attendant regulatory pressures.

Some 70% of respondents from life science and healthcare companies use regular sanctions screenings, whereas this is less important to respondents from the technology (58%), banking (54%) and asset management (48%) industries. Completing questionnaires and site visits are the lowest priorities across all sectors, of interest to less than a third of respondents.

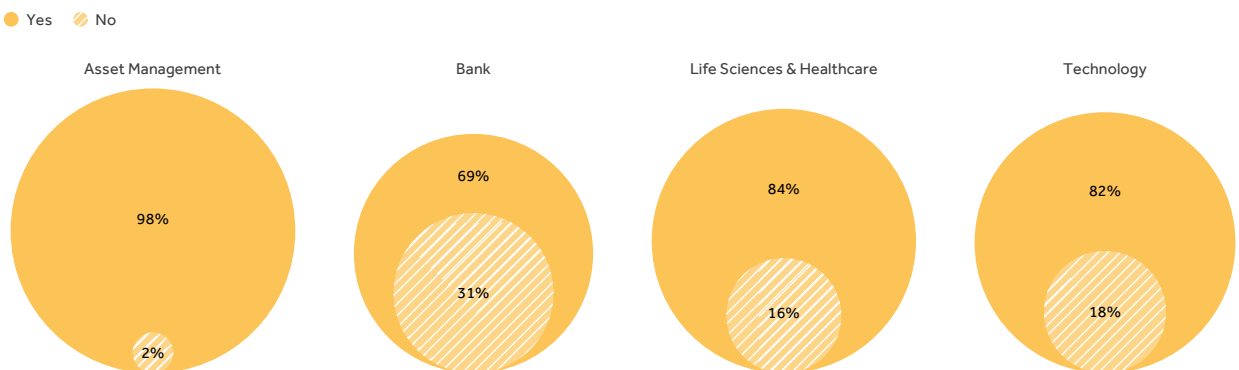
Outsourcing of all these diligence tasks is key for all sectors, with the clear majority engaging third parties to carry them out (Figure 23).

Asset management is most interested in bringing specialists on board, with 98% of respondents saying the process is carried out by an external provider. Life sciences and healthcare companies are the next most likely to engage a third party (84%), followed by technology firms (82%).

Banks, on the other hand, conduct much of this business using internal teams. Some 31% of respondents use their own staff to manage the diligence process when considering a corporate takeover or equity stake purchase.

"Every bank from big to small is looking for ways to automate their compliance efforts because it's a huge expense for the sector," says the managing director of a financial services firm in the United States. "Other sectors have a lot of regulation to deal with, but the breadth and differences of the jurisdictions we face, the levels of enforcement as well as the differences in the kinds of products we're delivering – for consumers, for institutions and so on – makes our compliance one of, if not the most, complicated there is. Our industry is more about investing in automating compliance processes than many other sectors. It's a 'tone from the top' culture here and we look at these as investments in risk reduction rather than as cost reducers – though that's ultimately the result."

FIGURE 23: **IS YOUR DILIGENCE PROCESS MANAGED BY SPECIALIZED OUTSIDE COUNSEL?**



IN CONVERSATION WITH...

Lindsay Antoniello

Deputy Chief Compliance Officer (U.S. & Europe) at TPG Global, LLC

Q. BASED ON SURVEY FINDINGS, PRIVATE EQUITY FIRMS ARE STRUGGLING TO KEEP COMPLIANCE POLICIES AND PROCEDURES UP TO DATE, MORE SO THAN OTHER SECTORS. WHY IS THIS AN ISSUE FOR THE SECTOR?

The regulatory environment around private equity is constantly evolving and the more jurisdictions in which a private equity firm operates increases the complexity of designing its compliance program. Changes in government leadership are typically accompanied by changes in regulation of financial services and private equity, particularly here in the U.S. Some changes can be more significant than others. And regardless of whether the changes result in an increase or decrease in regulation and oversight, all will result in a need to update policies and procedures accordingly.

To make things more complicated, many U.S.-headquartered private equity firms are global and subject to regulatory oversight in foreign jurisdictions. For example, compliance teams at firms subject to FCA oversight in the UK must monitor numerous new regulatory regimes coming out of both the UK and the EU (i.e., GDPR, MiFID II and various money laundering regulations) all while Brexit looms around the corner with no definite guidance on how it will impact the private equity industry. Therefore, the same challenges to keep up with policies and procedures reflecting the current regulatory environment in the U.S. also affect private equity firms in foreign jurisdictions.

Q. HOW ARE UPDATED POLICIES AND PROCEDURES FED THROUGH YOUR FIRM?

Our firm uses a number of different mechanisms for educating personnel and disseminating updates to compliance policies and procedures including live training sessions at firmwide meetings, small group sessions or one-on-one trainings, electronic communications, internal webpage postings and electronic learning (e-learning) modules. The means used for a particular training will generally depend on the depth and breadth of the subject matter being covered as well as the complexity of the underlying applicable law or regulation.

Q. ARE PRIVATE EQUITY FIRMS TAKING A DATA-DRIVEN BEHAVIORAL APPROACH TO COMPLIANCE?

More and more often, private equity firms are using a data-driven behavioral approach to compliance. One area where it is used quite often is in the development of compliance training programs.

It can be quite challenging for compliance teams to identify the most effective and efficient manner to deliver training on new or changing (and many times complex) laws or regulations. In addition, private equity professionals are constantly traveling and working on time-sensitive transactions, which cause scheduling and access challenges. When all of this is taken into consideration, the training content must be precise and impactful, and the delivery mechanism must be convenient and accessible for the audience.

One training method that many private equity compliance teams have been using is e-learning modules. E-learning platforms provide significant ease of use (accessible from PCs or any mobile device) and give compliance teams access to various data points that can be used to run detailed metrics on the effectiveness of the module (i.e., how long it takes for completion of the module or how long each user spends answering each quiz question). This data can be used to analyze where to improve or clarify content areas in the module.

We might do an analysis of new portfolio prospects – we send out a questionnaire to the companies involved to gain insights into their respective compliance programs. We take that information and conduct a detailed analysis to determine potential risks to our portfolio. Are we confident that their program is adequate or is there a way that we can help them make enhancements?

That's a good example of where we take data and analyze it to drive growth in deals: put the portfolio companies on a page together and figure out where we need to focus our attention for potential areas of risk.

Section 04

Conclusion: turn compliance into a business opportunity

Compliance efforts should not solely look to the past or the damage done, nor should they be driven by punishment or fear. Instead, the goal should be to learn why something happened, and how to enable employees to do the right thing in the future.

Most companies have systems in place to identify and investigate non-compliant behavior, whether through monitoring of accounts or random audits. Few, however, can prevent similar lapses from occurring again, much less identify the reasons why some employees choose to break the rules.

For a compliance program to succeed, companies need to collect, compile and analyze data to identify behaviors they want to encourage or prevent. The next step is to design and implement a system that promotes or stops these behaviors accordingly. That way, people not only understand the consequences of their actions, but also have the tools to independently address any obstacles they encounter.

By taking a data-driven approach to compliance, supported by behavioral sciences strategies, companies will be better-positioned to avoid unnecessary risks without burying employees in policy.

Instead of using blanket one-size-fits-all procedures to develop a compliance program, it is important to examine a company's compliance history and conduct a more robust, data-focused risk assessment, with the ultimate goal of also identifying the company's culture. Audit reports, HR records, corporate structure and data from internal investigations can all help paint a more complete picture of problematic behavior patterns.

A behavioral science approach involves direct communication and engagement: Once trouble spots have been identified, it is essential to meet with employees in those areas to explain why they are particularly vulnerable. Companies should seek straightforward solutions that protect employees without impeding business growth, and implement clear guidance that gives employees the tools they need to take responsibility for their own compliance, instead of waiting for corporate directives.

If businesses continue to rely on policy and procedure alone, without examining the factors underlying risky activities, employees will simply attempt to comply with the specifics of the policies, rather than own their individual behavior. The more policies change or are updated, the more complicated this effort becomes, leaving employees prone to inadvertently falling afoul of the rules.

In the end, a behavioral sciences approach can help redefine perceptions of compliance, transforming it from a burden into an integral part of the business and culture. This is a change that will benefit everyone.

About **Acuris Studios**

Acuris Studios, the events and publications arm of Acuris, offers a range of publishing, research and events services that enable clients to enhance their brand profile, and to develop new business opportunities with their target audiences.

For more information, please contact:
Simon Elliott, EMEA MD
Acuris Studios
Tel: +44 (0)20 3741 1060
Email: Simon.Elliott@acuris.com

About **Ropes & Gray**

Ropes & Gray is one of the world's premier law firms, with approximately 1,300 lawyers and legal professionals serving clients in major centers of business, finance, technology and government. The firm has offices in New York, Boston, Washington, D.C., Chicago, San Francisco, Silicon Valley, London, Hong Kong, Shanghai, Tokyo and Seoul, and has consistently been recognized for its leading practices in many areas, including private equity, M&A, finance, investment management, hedge funds, real estate, tax, antitrust, life sciences, healthcare, intellectual property, litigation & enforcement, privacy & cybersecurity, and business restructuring.

www.ropesgray.com

ROPES & GRAY

Contacts

Amanda Raad
Co-Lead, Risk Management
Amanda.Raad@ropesgray.com

Ryan Rohlfsen
Co-Lead, Risk Management
Ryan.Rohlfsen@ropesgray.com

About
Ropes & Gray's Risk Management Practice

Ropes & Gray provides a comprehensive suite of risk assessment and advisory services. By focusing on the entire enterprise rather than on specific areas of risk or particular geographies, we enable organizations to identify, monitor, and mitigate or eliminate risks at all levels. To evaluate potential risks across your enterprise, Ropes & Gray interviews key stakeholders throughout your global operations and produces a comprehensive report on your risks in various areas. We then make recommendations by practice area and assist with their implementation, monitoring and reporting. By leveraging all of our deep experience, we are able to quickly and effectively translate our analysis into action, maximizing time and cost efficiencies while dramatically reducing your risk exposure.

www.ropesgray.com