MIT SMR CONNECTIONS

STRATEGY GUIDE

# Staying Compliant in a Complex World:

## What Today's Business Leaders Need to Know

ON BEHALF OF:

EY Building a better working world

# CONTENTS



**MIT SMR Connections** develops high-quality content commissioned and funded by sponsors. We welcome sponsor input during the development process but retain control over the final content. MIT SMR Connections operates independently of the MIT Sloan Management Review editorial group.

# Staying Compliant in a Complex World: What Today's Business Leaders Need to Know

**In today's multifaceted regulatory environment,** ensuring that any organization remains ethical and compliant has become more challenging than ever. With regulations and enforcement increasing worldwide, the complexity of operations, exploding volumes of information to manage, and limited budgets, compliance teams are struggling to stay current.

"We're seeing an increase in complexity in global regulatory regimes, with regulations that are similar across jurisdictions but with variations that are just different enough to complicate the landscape for compliance," says Erin Kitchen, chief ethics and compliance officer at Dell Technologies.

In an uncertain economy, teams must make do with the resources they have, even when they've got more on their plates. They must ensure that they are complying with anti-terrorism, anti-corruption, and anti-money laundering laws in every jurisdiction where their organization and its partners conduct business. And they must adhere to ISO standard 37301 for compliance management systems, the World Bank Group Integrity Compliance Guidelines, data privacy laws such as the European Union's General Data Protection Regulation (GDPR), China's updated Anti-Espionage law, and a slew of evolving environmental, social, and corporate governance (ESG) rules with varying methodologies and measurements.

Another big challenge: For some regulators, communicating regulatory information and providing training sessions is no longer enough. Compliance officers are increasingly being asked to prove that their controls are working and that the compliance and ethics programs are entirely effective. Providing such evidence requires the use of sophisticated digital tools, platforms, and analytics, and many departments lack the resources and expertise to implement such technologies.

Under pressure to manage their mounting risk portfolios with limited means, it's no surprise to learn compliance officers are stressed. In a 2022 survey of 240 compliance officers conducted by Corporate Compliance Insights, 69% said they were anxious about the pace of regulatory change, and more than half reported that they were experiencing severe job-related stress. Fifty-nine percent described themselves as burned out.

Given the enormous constraints compliance officers face, what can they do to keep up with changing rules and emerging risks across the vast regulatory spectrum and ensure that their organizations consistently follow them?

Following are five best practices industry leaders recommend for creating a robust and agile compliance program — one that adjusts to change quickly, uses enterprise resources efficiently, and demonstrates to regulators and organization leaders alike that controls are keeping violations at bay.

### 1. Use technology to create a more meaningful and comprehensive risk assessment.

Sound compliance begins with a thorough, up-to-date risk assessment. An effective assessment must consider all aspects of the business, including internal, partner, and vendor risks across all operations and geographies.

"A risk assessment is the first step in a compliance program and the foundation for all decisions that follow," says Michael Ward, a partner at law firm Baker Botts, former federal prosecutor, and former chief compliance officer at Juniper Networks, Adobe, and Cisco. "The challenge for compliance officers is coming up with a coherent, holistic risk strategy and allocating resources to the most significant risks."

Traditionally, risk assessments were performed annually or even less frequently. However, today's regulators increasingly expect compliance teams to update the assessments based on continuous access to data, rather than taking periodic "snapshots," such as

those attained from spreadsheets. Some companies will need to update their technology to meet those requirements, identify potential blind spots, and respond to deficiencies or emerging matters.

"A lot of risk assessments are done on spreadsheets, and that can be OK depending on your size and maturity," says Jisha Dymond, chief ethics and compliance officer and head of the Ethics and Compliance Center of Excellence at OneTrust. "But the industry is moving towards automated, dynamic assessments." Automated assessments can be done with governance, risk, and compliance (GRC) software, which contains tools linking risks to business processes and controls. It also tracks changes as they are made, providing evidence to regulators that the organization is doing a good job of keeping current. Beyond that, such tools allow easy access to a larger audience and increase the opportunity for benchmarking and other statistical analytics.

In addition to satisfying regulators, digital tools help keep the organization safer, Dymond says: "Digitization makes risk mitigation more agile and efficient. With automated tools, risk owners can make adjustments immediately, as opposed to waiting for compliance to make annual changes on the spreadsheet."

### 2. Do a gap analysis of your current program.

Companies can also use digital tools to evaluate their current program and make improvements where needed. Making decisions is a complex undertaking that requires the compliance officer to analyze procedures and uncover trouble spots across the organization.

"A large organization is an amalgamation of hundreds of subcultures, some of them extremely risky and others less so," explains Eugene Soltes, McLean Family Professor of Business Administration at Harvard Business School and a specialist in corporate integrity and risk management. "You have to design your program accordingly."

For example, salespeople who travel abroad are more likely to interact with government ministers and, for that reason, warrant closer scrutiny to avoid running afoul of anti-bribery and anti-corruption laws. Software developers authorized to collect personal information for one product could fall prey to the temptation of using the same data to train other models — a violation of privacy laws in Europe and many U.S. states.

Digital tools can quickly spot and rank these and other risks, directing compliance officers' attention where it's needed. Such tools can proactively address common pitfalls and risks in targeted awareness communications.

"It's hard to manage the volume of issues and questions that fall under the umbrella of compliance without good sound technological systems in place," says Tom C.W. Lin, Feinberg Chair Professor of Law at Temple University's Beasley School of Law.

Compliance officers can also use data analytics to predict where compliance violations are most likely to occur, helping them arrive at confident, fact-based determinations for deploying resources to fill potential gaps.

Once digital tools are in place, they will not only be able to quickly gather the information compliance teams need but can enforce rules and shed light on new issues as they occur (see the next section).

Dymond sums it up succinctly: "If you get off that spreadsheet, it becomes a lot easier to make decisions."

### 3. Automate and verify controls.

To show regulators that their programs are working, compliance departments have traditionally documented their training programs and compiled data about reported incidents. But those practices are no longer good enough for today's regulators.

"In the past, it was sufficient to discharge your duties by ensuring you had reporting mechanisms in place, such as an ethics hotline. It was a reactive model," Ward says. "But in recent years, enforcement officials have expanded that approach. They want to see quantitative evidence that your preventative controls are being followed and tested and that you know they are being followed."

How can companies provide that evidence? Though the courts and agencies don't spell out a framework, documents such as the U.S. Department of Justice (DOJ's) latest guidance discuss the need to "evaluate periodically the effectiveness of the organization's program" by "testing of controls, collection, and analysis of compliance data."

For instance: "How are the results reported and action items tracked? How does the company measure its culture of compliance?" the DOJ guidance asks.

Other agencies, both in the U.S. and internationally, may soon call for similar control tracking for regulations such as the U.K. Bribery Act,

the Brazilian Anti-Bribery Law, France's Loi Sapin II law, and Hong Kong's Prevention of Bribery Ordinance.

The DOJ, along with the U.S. Securities & Exchange Commission (SEC), has always taken the lead, says Tyson Avery, former ethics and chief compliance officer at Starbucks and the global commercial real estate company CBRE. "Where they go, other regulators and other countries have a tendency to follow," Avery says.

Providing evidence about control effectiveness requires the use of automation and data analytics. In addition to demonstrating to regulators that controls are working, automated tools can improve efficiency. They can also warn compliance officers of problems and give them a better picture of how the overall program is working.

Here are some of the most important ways experts suggest using technology to improve compliance:

• **Unify data across silos with a common data model.** Because compliance regulations affect businesses in many different ways, compliance teams must coordinate with other departments to identify and analyze data and manage risks, which range from following employment rules and monitoring payments to keeping up with sanctions on international suppliers. Bringing this data together is often difficult because teams use different tools.

"Many organizations have legacy systems that have been built over time. It's like a silverware drawer where someone purchased different forks," Avery says. "It's better if you can monitor and manage compliance through the same lens. If you need to do disclosure, you can show consistency in your compliance program."

Companies sometimes already have solutions with existing tools but fail to take advantage of them, says Hui Chen, senior adviser at R&G Insights Lab, former compliance counsel expert at the DOJ, and former senior compliance leader at Microsoft, Pfizer, and Standard Chartered Bank. She cites the example of a high-tech company that used sophisticated tracking for customer transactions and activities but claimed it had no way to track employee expenses. When asked why it didn't apply its tracking tools internally, the company said its engineers were too busy with product development to set up internal controls.

"Choices like that have repercussions for compliance teams and regulators," Chen says. "Technology should be employed consistently across the business."

• **Embed workflows with controls.** Teams can ensure consistent application of compliance rules by embedding employee workflows with built-in controls. For example, software can monitor customer discounts, which can be mischaracterized to create a slush fund for illicit payments — something regulators watch for. Embedded software can manage all discounts and show a completed approval chain for all those above a specified threshold. These metrics give regulators direct evidence that controls are in place and working.

"Process controls that are embedded into a workflow are not only more reliable, they create real-time documentation that the controls are being applied," says Ward, who has also served as an independent compliance monitor. "That evidence helps companies meet the escalating burden of proof."

They also make life easier for busy employees, who may forget or disregard compliance procedures (see "Preventing Fraud and Improving Business Processes With Embedded Controls"). When organizations implement embedded controls, the number of workers who miss compliance obligations drops by 58%, a 2021 Gartner study found.

In addition, controls can reduce the need for training sessions. Of course, training will never completely disappear; it's a crucial way of communicating and gaining commitment to compliance. But when automated controls steer workflows on the right path, fewer reminders will be necessary. By 2025, Gartner predicts, corporate compliance departments will reduce annual compliance training by 50%, displacing costs in favor of embedded controls.

• **Keep up with regulations and business partners.** Laws constantly evolve — and so do businesses as they expand into new areas. But

**Of course, training will never completely disappear; it's a crucial way of communicating and gaining commitment to compliance. But when automated controls steer workflows on the right path, fewer reminders will be necessary.**

foreign partnerships can backfire and lead to significant fines and reputational damage if companies don't monitor them carefully. For example, British American Tobacco was recently fined more than $600 million by the DOJ and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) for working with a subsidiary in Singapore that sold tobacco to North Korea, a sanctioned country, between 2007 and 2017. The company says it has since "transformed" its compliance and ethics program.

Automation can help companies avoid such problems by monitoring laws and sanctions lists maintained by the United States, the United Nations, the European Union, and other bodies, enabling companies to quickly modify embedded controls as necessary.

Companies can also monitor business partners, including vendors, to make sure they continue to meet company standards for creditworthiness, data protection, workplace safety, and insurance, receiving alerts if they fail to keep up and using machine learning algorithms to assign them evolving risk scores. Such management and monitoring tools will also become more important with increasing supply chain regulation, such as the EU's Corporate Sustainability Due Diligence Directive.

• **Solve problems with predictive analytics and human intelligence.** By analyzing data from across the enterprise, compliance officers can gain a better picture of the company's overall risk posture and receive early warnings of problematic trends.

They can also save time. "By leveraging analytics, you can have one person do the work of five, harnessing data to point you in the right direction for risk-based prioritization of limited resources," says Kitchen, of Dell.

As data accumulates, algorithms may be able to predict and prevent specific problems. The company can then seek a deeper understanding of the situation and implement solutions.

**"The ideal compliance program is data-driven and human-centered. At the end of the day, what you're trying to do is use data to understand human behavior."**

**HUI CHEN**
Senior Adviser, R&G Insights Lab

## Preventing Fraud and Improving Business Processes With Embedded Controls

Tying compliance rules to company workflows can nip fraud in the bud and save compliance teams countless hours of work.

But that's not all that practice can do. Embedded controls can also shed new light on business processes and help employees work smarter.

That's what a multinational engineering and technology company learned after working with consultants to integrate its compliance database with its business transactions — including those with business partners and vendors. The system was designed to prevent fraud and resolve issues associated with what accountants call "unwanted payments" — unintentional errors, such as incorrect figures or duplicate invoices, that many companies struggle to manage.

Company workflows are now monitored for dangers listed in the compliance department's risk assessment, as well as for unwanted payments and other issues. The monitoring software operates invisibly in the background, allowing employees to complete their tasks unimpeded unless a problem is detected. Then the controls swing into action.

If the problem involves potential fraud, the system may alert the business process owner, the compliance team, or the anti-fraud team, depending on the situation. A suspicious transaction may be targeted for investigation or blocked.

In addition, the system continually tracks partners and vendors against evolving compliance blacklists and media reports, immediately notifying anyone who is dealing with them of changes. In these ways, embedded controls save the company from dealing with unscrupulous parties and making illicit payments.

More frequently, the system helps companies avoid embarrassing but non-fraudulent mistakes. If an error occurs — such as an invoice naming the wrong client or a contract promising to deliver a shipment that supply records indicate is out of stock — employees involved in the transaction receive an email notification to correct it before the document is submitted.

By fixing problems earlier, employees avoid time-consuming and potentially awkward partner or client interactions. They also learn from the automated corrective emails explaining the errors, the company found, making fewer mistakes over time. Many become more proactive in solving problems — if they don't receive an automated approval in a few minutes, they know something is wrong and will often review their work and find and correct the error themselves.

Thanks to machine learning, the controls themselves are also improving. The more they are used, the better their performance can be analyzed. The company has already made tweaks to its algorithm, modifying alerts and making some remedial suggestions easier to understand. It's a cycle of continuous improvement, made easier by automation.

**For any compliance program to succeed, the company must create an enterprisewide culture of compliance and integrity. That starts with board officers and executives, who must set the tone for a culture that doesn't tolerate misconduct. Words alone won't inspire loyalty, or even participation.**

For example, Chen says, an organization might discover that misconduct is most likely to occur among first-level managers five years into the job. The organization could then monitor the actions of these people more closely to prevent problems or stop them at an early stage.

What data monitoring doesn't do, however, is explain why such problems occur.

"That's where the human aspect comes in," Chen says. "You've identified a systemic problem, and now you can start interviewing stakeholders to determine what's triggering it."

Perhaps frustration with a lack of career progression drives some people to become careless about following the rules as they prepare to leave the company, Chen says. "Now you have identified not just a misconduct problem but also a talent retention problem. If people don't feel valued, there are things the company can do to change that."

The example illustrates her vision of how compliance should work. "The ideal compliance program is data-driven and human-centered," Chen says. "At the end of the day, what you're trying to do is use data to understand human behavior."

### 4. Obtain the technology expertise you need.

Deploying automated controls and managing analytics can be tough for compliance officers, who aren't typically schooled in advanced technology.

"Most people running compliance programs have a legal background and thus are less experienced with technology and data analytics," Soltes says.

Augmenting teams with data analysts or data scientists can help, but such specialists are scarce and expensive. Compliance leaders should familiarize themselves with data management and controls as much as possible, he says. They can also work with consultants to develop a coherent, step-by-step strategy for integrating the tools they need for managing risk in accordance with evolving regulatory standards.

"Consultants can bring a new set of skills and help the organization make a lot of progress very quickly," Soltes says. "In the long run, teams need to build the internal knowledge and capacity to tackle problems as they arise. Consultants can help them get started with the right strategy."

### 5. Foster a culture of compliance and integrity.

All experts interviewed for this report noted that for any compliance program to succeed, the company must create an enterprisewide culture of compliance and integrity. That starts with board officers and executives, who must set the tone for a culture that doesn't tolerate misconduct. Words alone won't inspire loyalty, or even participation.

"Senior management can talk about compliance and ethics as much as they want, but it's more powerful and meaningful when people see them taking action according to those values," says Lin.

Leaders should practice good governance themselves and insist that others do, too. "If there is a double standard — if senior leaders fail to discipline other executives or high performers — employees will recognize that immediately because they pay close attention in those crucial moments," Ward says. "It's not in the regular blast email ethics messages from the CEO, but instead in those infrequent but painful choices, where a culture of compliance is created and sustained."

Midlevel managers, employees, and business partners all play a role in upholding the standards top executives set. In a culture of compliance, everyone has the confidence to confront irregularities head-on.

"Employees need to know that if they report a violation, something will be done about it, and they won't be retaliated against," Dymond says.

Underreporting is a serious problem. In a 2020 Gallup study of U.S. workers, 24% reported being aware of unethical behavior in their workplace, but fewer than half of those chose to report the problem. In a big company, that could mean hundreds or even thousands of potentially serious problems that leaders don't see.

Training and communications are also a critical part of maintaining a culture of compliance, but traditional methods don't always keep up with real-world demands. Employees may forget rules they've learned until they have to deal with issues such as expense management or interacting with officials on their own. They may not feel comfortable contacting a manager with questions covered in the training — or just feel overwhelmed by the number of policies and regulations that are addressed.

With just-in-time and consumer-targeted training, employees can receive online instruction when they need it and with relevance to the respective job profile. For example, Dell has developed a smart mobile app that pops up specific training modules for employees, whether they are new to a role, traveling, or engaging in sensitive transactions.

Some companies are developing AI chatbots to answer employees' questions in real time. "The nature of this type of technology is such that the more people use them, the better they become," Chen says. However, she adds that chatbot answers to employee questions about ethics and compliance can be risky. A chatbot can easily respond to a simple question such as "What is the gift limit?" But more complex questions, such as "Can I give this gift to this person at this time under these circumstances," can be problematic. "I would not trust AI chatbots to answer that question," she says.

Another helpful technique is making the organization's code of conduct interactive, says Jonathan Rusch, a corporate-compliance consultant and director of the U.S. and International Anti-Corruption Law Program at American University's Washington College of Law.

"An interactive code of conduct is continually refined. Compliance can create and update questions and answers, and employees can submit examples of how they dealt with provisions in real-life situations," says Rusch, an adjunct professor at both American University and the Georgetown University Law Center.

Whether it's done through training, open discussion, or enforcement, a culture of compliance results from encouraging ethical behavior in day-to-day procedures across the enterprise.

"Everyone needs to realize that how the organization accomplishes its mission is just as important as accomplishing it," says Dymond. "It's everyday decision-making that builds a strong culture."

# CHECKLIST:
# NINE KEY COMPONENTS FOR STATE-OF-THE-ART TECH-DRIVEN COMPLIANCE

A sophisticated compliance program requires a strong, regularly updated collection of capabilities to allow it to go from data to insight to action, including:

- [✓] **A risk-scoring system** and anomaly detection to quickly prioritize compliance issues and design appropriate countermeasures. Prioritizing risks is an essential step in directing resources to places where they will have the greatest impact.
- [✓] **Standardized metrics and reporting** to create a holistic view of risk throughout the enterprise. When teams use a common set of tools and terms, they can work together better to solve problems.
- [✓] **Embedded controls** to ensure that good compliance practices are followed in company workflows, including approval procedures for third-party compliance and other risky interactions. No matter how much training you do, some people will forget or circumvent the rules. Built-in controls don't allow work to proceed unless the right procedures are followed.
- [✓] **Objective documentation** of program effectiveness. Today's regulators want to see evidence that safeguards are working. Collecting data on embedded controls will show enforcement in action.
- [✓] **Dashboards with automated "red flag" risk** to warn managers of suspicious activities. With compliance regulations touching nearly every facet of business operations, compliance teams need automation to keep up with risks.
- [✓] **Automated tracking of regulatory requirements** to keep compliance officers up to speed with proposed and effective changes.
- [✓] **Monitoring of business partner activities and media reports** to make sure all partners adhere to company standards. Companies can assign vendors continually updated risk scores.
- [✓] **Online interactive tools** to answer employees' compliance questions in real time. Tools can range from interactive Q&As to AI chatbots trained on the company's rules and code of conduct.
- [✓] **Data analytics and machine learning** to reveal trends. With data on all aspects of compliance readily at hand, compliance officers can foresee and prevent problems and make justifiable, data-driven decisions.

**Andreas Pyrcek,** CCEP-I, is a partner in EY's Forensic & Integrity Services practice. Based in Germany, he leads the global Integrity and Compliance Services group and serves as sector lead for telecommunications, media and entertainment, and technology. With more than 17 years of international experience, he is a thought leader for topics involving compliance, integrity, and ethical business transformation.

**Todd Marlin** is a principal in EY's Forensic & Integrity Services practice. He is the Global Forensic Technology and Innovation leader with a focus on forensic data analytics, cybersecurity, and electronic discovery. He and his team help clients develop custom models to identify, expose and demonstrate relationships, trends, and patterns within complex and disparate data.

EY Building a better working world

**SPONSOR'S VIEWPOINT**

# Fostering a Culture of Compliance

**No doubt about it: A culture of compliance starts at the top. But leaders can't just say compliance is important; they have to invest in it.**

Increasingly, effective compliance programs are data-driven, incorporating technologies such as AI and automation under the direction of skilled specialists. Growing demands from regulators, investors, employees, and other stakeholders have made doing the right thing even more critical for companies. Our experience with clients globally indicates organizations that successfully foster a culture of compliance have the following practices in common.

**1. Both leaders and middle managers deliver consistent, meaningful communications on prioritizing compliance.** Most business leaders we work with strongly support compliance but minimize it in their communications. Both executives and middle managers should consistently deliver this simple message: "Compliance is the foundation of an ethical and successful business."

This thinking should be embraced not just by executives but middle managers as well so that they can reinforce it in language their employees understand. Managers should plainly say that doing the right thing is more important than meeting sales quotas or signing new clients. If people don't repeatedly hear this message, they may believe it's OK to bend the rules.

**2. Adequate resources are provided to develop a data-driven compliance framework.** Touting compliance is meaningless unless leadership provides adequate funding. For larger organizations, investing in technologies and talent that can leverage data is essential to creating a comprehensive, effective compliance framework.

Workplaces are drowning in data, making it difficult, if not impossible, to manually search for signs of misconduct. Instead, historical exceptions and knowledge of the organization can be used to build a training data set that monitors compliance through machine learning. Supervised learning models continually improve as more data is added, becoming increasingly effective at finding suspicious patterns and lowering false positives.

For example, we teamed with Honeywell International to create a digital scorecard that provided a centralized, actionable view of compliance, easily understood by key stakeholders.

**Managers should plainly say that doing the right thing is more important than meeting sales quotas or signing new clients. If people don't repeatedly hear this message, they may believe it's OK to bend the rules.**

Using more than 40,000 aggregated data points, this type of targeted approach is more effective and efficient than a rules-based system for finding exceptions.

Data and digitalization will be key to preventing and detecting potential fraud and noncompliance. With the opportunities AI brings to generate and analyze enormous amounts of data, organizations can simplify management procedures and add value to the compliance function.

But organizations must also invest in talent through both recruitment and training. While it's challenging to find compliance professionals with strong technical skills, it's entirely possible to teach data experts and tech-savvy business professionals to manage compliance.

In addition, compliance education should focus on relevant business practices rather than on laws and regulations. Create role-based courses that speak the practitioners' language, using anonymized organizational examples or publicized external cases.

Just-in-time courses can be delivered before an employee leaves for a certain country. It's also essential to educate contractors and supply chain partners whose misconduct can damage an organization's reputation and revenues.

Many organizations highlight course completion rates, which tell them nothing about effectiveness. The best way to measure training success is to determine whether exceptions decrease afterward.

**3. The compliance department has autonomy and independence.** Employees won't trust compliance professionals unless they believe their leadership supports a strong, independent function. However, misconduct can occur in even the best programs. An independent compliance department works with leaders to determine and address root causes. Executives who believe compliance is merely a tick-the-box exercise required by regulators might need some coaching.

While a board of directors may advocate a zero-tolerance approach to compliance, we have seen violators go unpunished because of strong business performance. More than 40% of board members surveyed in EY's Global Integrity Report 2022 said their organization tolerates unethical behavior in senior or high performers.

A lack of consequences for compliance violations will have a terrible impact on fostering a culture of compliance. If leadership is hesitant to impose zero tolerance, an independent compliance function can call for action.

**4. A strong whistleblower or confidential reporting program makes it safe to speak up.** If people don't believe they can report misconduct without fear of retaliation, they will stay silent. Nearly half of board members surveyed in EY's Global Integrity Report 2022 said it's gotten easier for employees to report concerns, but only 25% of employees agreed. While some employees may be more comfortable speaking to a trusted supervisor or HR professional, many whistleblowers prefer anonymity. Reporting tools should also be made available to contractors and vendors.

A whistleblower's complaint can be reviewed internally by the compliance or HR department if it is truly autonomous. External review by an outside forensic specialist, law firm, or ombudsman also provides strong protection.

**Conclusion**

Many companies have improved their compliance programs in the wake of the COVID-19 pandemic, seeking to reduce risk. Fostering a sophisticated, data-driven culture of compliance is becoming the standard for large organizations. It takes time and money, but we believe such investments will improve the enterprise's standing with key stakeholders and eventually lower compliance costs while reducing the risks of financial and reputational damages.

## ABOUT EY FORENSIC & INTEGRITY SERVICES

Our international team of more than 4,300 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisers. We strive to bring you the benefits of our leading technology, deep subject matter knowledge, and broad global sector experience. To learn more, visit **https://www.ey.com/en_us/forensic-integrity-services**.