Top 10

Risk + Compliance

Trends 2024

NAVEX®

Contents

Executive Summary

By Matt Kelly

An effective corporate compliance and ethics program rests on two principles. First, the program must guide the company through today's complex regulatory environment; that's the compliance part. Second, the program must help the company to operate with integrity, a standard of behavior more important to customers, employees and other stakeholders with every passing year; that's the ethics part.

How can a compliance and ethics program operate on those two principles, while navigating the business, technology and social pressures of the day? That is the question NAVEX tries to answer in the annual Top 10 Trends in Risk and Compliance report.

To find those answers, NAVEX consults with trusted industry experts and internal thought leaders and practitioners. Those consulted were asked for their best thinking about what GRC professionals and other leaders should consider and prepare for in 2024. The result is this report in your hands (or on your screens).

Half of the insights in this year's report address the complex regulatory environment we mentioned earlier. For example, enforcement of economic sanctions has been marching up the priority ladder for the U.S. Justice Department – "sanctions are the new FCPA," to quote deputy attorney general Lisa Monaco – and compliance programs will need to adapt to that new reality somehow. The same will be true for new ESG reporting rules, expanded privacy standards, new compliance program guidance from regulatory bodies worldwide..

In other words, 2024 will be a year of compliance and ethics programs responding to specific demands from the regulatory world.

That's not all, however. The other half of insights in this year's report explore how compliance programs will need to respond to broader challenges in how businesses operate and employees work. Here we can look to the arrival of artificial intelligence. Even before regulators develop AI-specific regulations, businesses already have clear governance, risk management, and ethical challenges with how employees are already trying to use AI. Compliance officers can, and should, play a leading role in staying ahead of that challenge before it races beyond our grasp. Again, we can say the same for fraud risk in the distributed workforce, new types of cybersecurity risk driving CISOs and compliance officers to work together, and more.

In other words, 2024 will be a year of compliance and ethics programs responding to specific demands from the regulatory world.

So, we can also say 2024 will be a year for compliance officers to expand and embed their risk management objectives across the enterprise, too.

The good news is compliance officers can meet all these challenges, thanks to the digital transformation sweeping our industry. A modern, properly configured GRC information system can collect and analyze data so you and the senior management team can make better, more risk-aware decisions and achieve better outcomes – and we expect that trend to continue for years to come.

We hope this year's guide will provide valuable insight for any and all GRC professionals dedicated to meeting the challenges ahead.

Artificial Intelligence – The Good, The Bad... The Future

By Matt Kelly and A.G. Lambert

The rise of artificial intelligence – and specifically of **generative** AI, which can create entirely new images, sounds, and text with just a few prompts – was the most important technology development of this decade.

The challenge for 2024 (and years to come) will be how to put AI to profitable, gainful, ethical use in the corporate enterprise. The compliance function needs to anticipate everything that challenge will entail.

For example, compliance teams themselves could use AI to streamline or strengthen the compliance function. Other parts of your enterprise could find ways to put AI to good use in their own operations, too – or they could blunder forward recklessly, causing all manner of compliance and cybersecurity risks.

So even as compliance officers start using AI within their own function, they'll need to serve as trusted advisers to senior management and the rest of the enterprise, so those other parts of the business can use AI in a prudent, legal, and risk-aware manner.

Understand both the positive and the negative

The positive is that the technology behind ChatGPT and its generative AI brethren is enormously powerful. Generative AI first uses **natural language processing** (NLP) to let human users submit queries to the AI in the same plain language we use with each other. Then, based on vast troves of data it has already studied, the AI calculates the string of words, numbers, or pixels that are most likely to be a good answer to the user's question.

One can see the compelling use cases here. A business could essentially layer an NLP interface over its own data, so employees could ask questions such as: Which customers are our biggest spenders? Which job applicants have the skills most relevant to our needs? Which resellers ask permission to offer price discounts most often? And so many more. The AI would then return clear, straightforward answers immediately.

The negative, however, is that without strong guardrails, the AI might not always submit **accurate** answers. Or it might consume the information you provide it – including confidential information – to help it learn how to answer questions for the next user. It could interact with employees and customers in unexpected ways. It could learn from a flawed set of data, picking up bad intellectual habits and giving bad answers just like any human would. Remember what we said earlier: the technology behind generative AI is enormously powerful. Companies will need to channel that enormous power in the proper ways, or risk courting disaster.

The guardrails begin with governance

As we enter 2024, the immediate challenge for organizations will be to establish an enterprise-wide governance structure for how your business embraces AI. That is, some senior group within the company – let's call it a steering committee – needs to articulate the basic guidelines for how the company adopts AI in a sensible, compliance-oriented manner.

Remember what we said earlier: the technology behind generative AI is enormously powerful. Companies will need to channel that enormous power in the proper ways, or risk courting disaster.

Then other employees further down the org chart can develop the specific AI use cases that make the most sense for your business.

That steering committee should at least include the CISO, the chief compliance officer, your head of technology, the CFO, and the general counsel. Other plausible candidates (depending on your business model and objectives) might include the heads of HR, marketing, and others.

These steering committees could be a place for the chief compliance officer to shine. After all, most members of the steering committee will be strong on envisioning use cases, but **not** on understanding all the risks involved. You, the CCO, should be the consigliere guiding the committee as it maps out your AI adoption strategy.

For example, we already see some early instances of governments regulating how AI is used. In New York City, employers that want to use AI to screen out job applicants (including something as simple as automated keyword searches) must perform a "bias audit" on the AI and post the results online. If that rule applies to your business, does the HR team know about it? Who is working to assure the bias audit is conducted promptly and correctly?

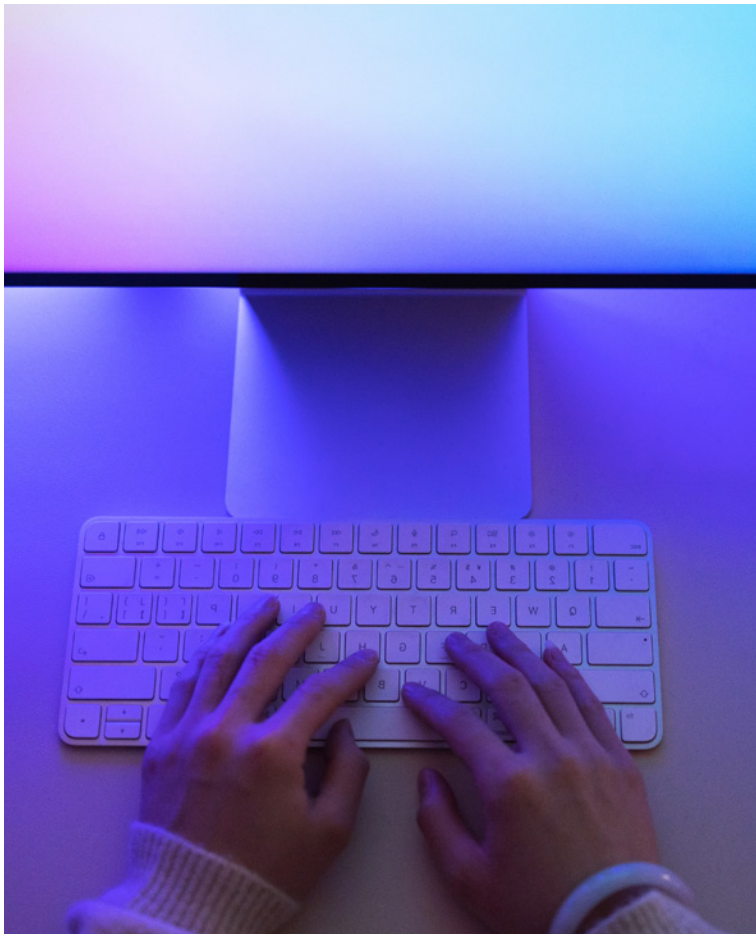
Those are the sorts of questions an AI steering committee can explore, and compliance officers can play a valuable role bridging the regulatory world and the business world. 2024 will be a year where compliance officers can help the enterprise adopt AI in an ethical, legal, sustainable way. Seize that opportunity.

A model for AI in the compliance function

Compliance officers can also spend 2024 figuring out how to integrate AI into your own operations. There's a lot of potential here.

We mentioned earlier that AI learns by consuming large piles of data. Well, corporations have data in spades. So, you could develop a generative AI tool that only studies **your own** data about transactions, third parties, internal employee communications, and more. You could then start asking the AI questions about compliance risks in simple, direct sentences. You'd get simple, direct answers in return.

Of course, this assumes your company has good data management practices, and that the compliance team has access to all of the data. This presents another goal compliance officers might want to set in 2024: work closely with other parts of the enterprise to build strong data



management practices, and be sure you have access to and management of all of the data so your adoption of AI can return maximum value.

What about AI regulation?

The regulation of AI is still in its infancy. We've seen some early attempts at the task – such as the aforementioned New York City law – but in both the United States and Europe, specific regulations are still rare.

It's possible we'll see more movement on that front in 2024. The European Union, for example, proposed the EU Artificial Intelligence Act in 2023, which would (among other things) require all generative AI to undergo external review before commercial release; but that legislation still has lengthy negotiations in front of it before going into effect. The Biden Administration also proposed several "pillars" of good AI use, but those are both vague and voluntary.

Then again, compliance officers don't need AI-specific regulations to keep themselves busy. AI is already here, seeping into business operations across the enterprise.

2024 will be a year for compliance officers to engage with senior management about how to adopt artificial intelligence, and for you to sharpen your own GRC technology capabilities to take full advantage of AI yourself.

AI is already here, seeping into business operations across the enterprise.

2024 prediction

As AI technology continues to develop and gain traction across the world, so will the proposed regulations to govern how it is used. We can expect these regulations to vary depending on the use cases, geographies and specific function of the artificial intelligence itself.

Artificial Intelligence will likely galvanize leaders who must be on the same page for how it is used in the business and how policies are enforced. We can expect more and more compliance and cybersecurity leaders to step up and uphold appropriate governance and security as AI becomes a staple technology to improve efficiency and accuracy in organizations.

About the authors

A.G. Lambert
A.G. Lambert is chief product officer at NAVEX, where he is responsible for driving the company's product vision and strategy. Helping NAVEX further its product innovation and leadership, A.G. is expert at optimizing product strategy to meet current and future needs of customers, partners and the industry.

Prior to joining NAVEX, A.G. served as chief product strategy officer at SAP Concur. He has also held positions leading product management and marketing teams at Saba, Infor, Extensity and Autodesk. A.G. earned a degree in physics and English literature from Washington University, and an MBA from the Haas School of Business at the University of California, Berkeley.

Matt Kelly
Matt Kelly is editor and CEO of Radical Compliance, a blog and newsletter that follows corporate governance, risk, and compliance issues at large organizations. He speaks and writes on compliance, governance, and risk topics frequently.

Data Privacy & Protection – Swimming into the Unknown

By Kristy Grant-Hart

If you feel like every day you wake up to a new data privacy law or piece of guidance, you're not dreaming. Regulation and rulemaking are happening faster than ever before. The complexities relating to ethical data usage are profound, especially in the emerging era of artificial intelligence (AI) and cyber-terrorism concerns.

Data privacy no longer simply refers to keeping data about an identifiable person secured. It extends to national security issues, deep fake media unfairly endangering reputations, and corporate databases broken wide open through misuse of biometric data.

Being a compliance, ethics, risk, or data privacy officer is challenging in this environment. So much has changed in the law, and so much more is going to change in the upcoming year. Let's look at where we are, emerging issues, what to do now, and our predictions for 2024.

Where we are now

Every part of the globe is now interested in data privacy, but some places are more focused than others.

Europe and the General Data Protection Regulation

Europe is ground zero for data privacy regulation. It was the first place to put a consistent, European Union-wide standard in place for data privacy, first with a Directive, and later with the 2018 General Data Protection Regulation (GDPR). Much has happened since the heralded law came into force.

The regulators have been highly focused on technology companies, with nine of the top ten fines being levied on social media and internet search companies. Enforcement is likely to continue at pace.

United Kingdom

In 2020, post-Brexit United Kingdom adopted the U.K. GDPR, which is substantially similar to the European GDPR. This is unsurprising, as it is critically important for the U.K. to maintain its EU-granted adequacy decision, which means the U.K. can transfer data into and out of the EU without any additional protections such as standard contract clauses.

U.K. politicians have talked about making the U.K. more data processing friendly to try to make it a more popular place for technology development and deployment. Thus far, little has moved away from the EU's version of GDPR.

United States federal law

Much ink has been spilled over the years in hopes of a federal data privacy law. Last year, this publication focused on the bi-partisan efforts in the U.S. Congress to agree on a federal data privacy law, but sadly, those hopes were dashed. There is currently no U.S.-wide law, nor do we anticipate one coming into force in 2024.

U.S. State law

Where the federal government has lagged, individual states have sprinted. California has been on the forefront of data privacy legislation ever since the California Consumer Privacy Act (CCPA) came into force in 2020. Unsatisfied that it went far enough, California voters approved the California Privacy Right Act, which uses a GDPR-like framework.

California created a brand new regulator, the California Privacy Protection Agency. While a new regulator, they have signaled a desire to be an aggressive protector of consumer and employee rights. News sources have commentated that the California privacy regulator is defining personal data extremely broadly – one which goes beyond the European Union's Artificial Intelligence Act and the GDPR.

A total of 11 states have now passed data privacy-related legislation, and many more are in the legislative pipeline. Unhelpfully, each is a bit different in application and requirements.

Data localization requirements

Data is a global currency, and some countries want to keep their citizens' data squarely under their control. Russia's data privacy law, passed in 2022, provides new rules for personal data processing and cross-border data transfer. It establishes mandatory requirements for data controllers and processors, including a new requirement on data breach notification.

China has become a hotspot for data privacy practitioners. China's Personal Information Protection Law (PIPL) includes a number of challenging provisions, including some data localization requirements. Additionally, the transfer of personal information overseas is subject to a security review assessment.

Emerging issues

Many exciting developments are on the horizon for 2024.

The US adequacy decision and Schrems III

In July, the data privacy world was jolted with the exciting news that the European Commission determined the United States had adequate protections for data transferred out of the European Union. President Biden signed the Executive Order on Enhancing Safeguards for United States Signals Intelligence Activities in October 2022 with an aim to meet the requirements of the EU for a positive adequacy decision. He was successful.

The adequacy decision allows companies in the U.S. to sign up with the Department of Commerce for the Data Privacy Framework Program. In exchange for agreeing to various terms, companies can now transfer personal data freely between the U.S. and the EU.

As exciting as this development is, litigation is brewing with a favorite character in the data privacy universe, Max Schrems. Max Schrems, through his organization, NOYB, has successfully challenged two previous U.S./EU transfer schemes at the EU Court of Justice – Safe Harbor and Privacy Sheild. Schrems will undoubtedly challenge

Data is a global currency, and some countries want to keep their citizens' data squarely under their control.

the legitimacy of the U.S./EU transfer agreement on the grounds that the U.S. continues to practice unreasonable surveillance against EU citizens.

It will likely take several years for the EU Court of Justice to rule on Schrems' next suit. In the meantime, the data firehose is flowing at full speed across the pond.

Artificial Intelligence regulation

With great power comes great responsibility, and AI holds tremendous power. The world's governments have noticed, and they are trying to respond by regulating an ever-changing landscape that seems impossible to control.

The European Union is in the process of passing the Artificial Intelligence Act. This Act will be the first large scale framework for the use of artificial intelligence. In June, the European Parliament adopted its negotiation position. Commentators expect that the final version of the Act will be passed by the EU relatively quickly, with enforcement likely by 2026.

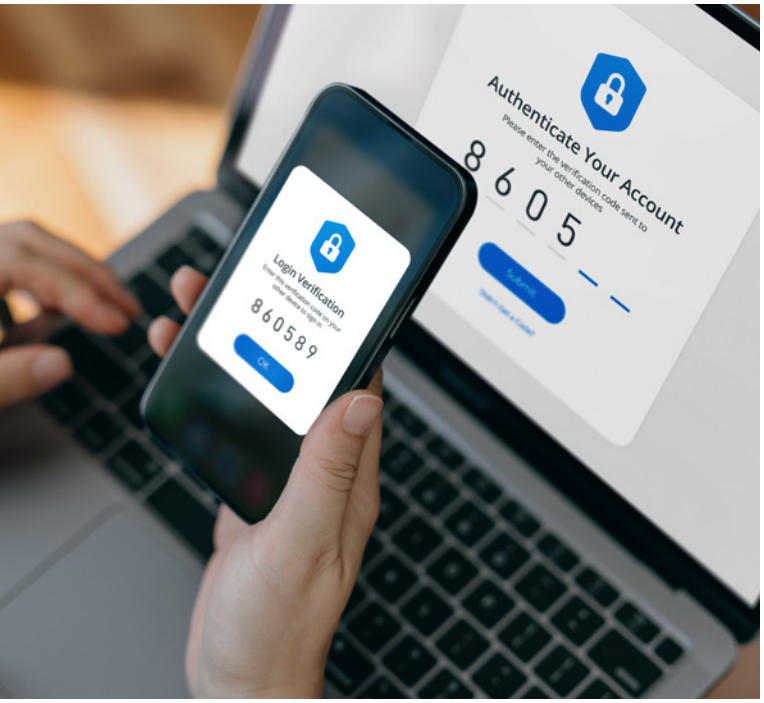
The U.S. government held a Congressional hearing with thought leaders like the creator of Open AI (ChatGPT), who implored Congress to put regulations in place for AI. Right now, Senators and members of the House of Representatives are trying to come up with legislation to manage an industry few of them understand.

Meanwhile, the states fill in some of the gaps. California and Illinois are leading the way in AI regulation in employment. Illinois has enacted the Biometric Information Privacy Act which requires a whole host of disclosures and consents, including a requirement for a publicly-available written policy that establishes a retention schedule for personal biometric information.

We anticipate more AI regulation, especially when it comes to the use of personal data.

More data localization requirements

As cyber-attacks escalate and sanctions regimes become more common and stringent, more data localization laws are likely. While the feasibility and success of these efforts are questionable, it is politically popular in many jurisdictions to try to localize data so it isn't vulnerable to bad actors in other parts of the world.



What to do now

Although there are many differences between current and upcoming regulations, the principles underlying data privacy laws are nearly universal. These include obtaining consent for the use of data by individuals, using the data in a way that would be anticipated by the individual, allowing for the correction and deletion of data, and agreeing to the sale of personal data to third parties.

Implement a principles-based approach to data use

Given the complexity of the laws, a principles-based approach is likely to be successful for compliance with most data protection laws. Look to the seven principles underlying the GDPR. They are an excellent place to start.

Complete data inventory and data mapping exercises

Work with the Information Technology department and assist them in completing a data inventory and data mapping exercise. A data inventory catalogues all of the categories of personal information used by the company by system. The inventory should be used to create maps showing the flow of personal data from the company into and out of various third-party systems.

A good data map is critical if your company receives a subject or consumer access request from an individual who wants to know what personal data is held about them by the company and how the company is processing and sharing it. Laws require a speedy turnaround, so complete the data inventory and map as soon as possible.

Review and update contracts

If your company transfers data to third parties (and it almost certainly does), review the contracts to ensure you have proper data breach notification and data security requirements. Keep the language broad so it expands to meet new legal requirements as they come into force.

Get it on the table

There's nothing like a real-life experience to help leaders realize how badly things can go wrong. Many companies perform annual or semi-annual data breach simulations (often referred to as table-top exercises) to help functions and leaders to practice their response to a crisis.

Ask your IT group to include a personal data breach in their next tabletop exercise. This will help focus attention on the importance of personal data protection, especially from an employee and customer perspective.

As cyber-attacks escalate and sanctions regimes become more common and stringent, more data localization laws are likely.

Follow updates

Find a reliable source for updates on proposed and existing laws, as well as enforcement actions. Review these materials and alerts frequently. Whether a law firm, consulting group, or industry trade association email, or news alerts, find a way to consistently learn of legal, regulatory, and enforcement updates so you're up to date on the latest requirements.

The only constant is change

It is said that nothing is certain in life except death and taxes. Change should be added to that list. The use of personal data will continue to evolve faster than ever. It's up to compliance, ethics, risk, and privacy officers to hold the line to make sure that, whatever the clever new use of personal data, it meets all current and likely future requirements.

2024 prediction

GDPR enforcement will continue, bringing higher and higher fines. Schrems will challenge the U.S. Data Privacy Framework Program at the EU Court of Justice, and AI regulation with respect to employees and consumers will keep coming.

About the author

Kristy Grant-Hart

Kristy Grant-Hart is an expert at transforming compliance departments into in-demand business assets. She's the author of the book "How to be a Wildly Effective Compliance Officer" and CEO of Spark Compliance Consulting, a London and Los Angeles-based consulting group which was shortlisted for Compliance Consulting Team of the Year at the Women in Compliance Awards. She is also an adjunct professor at Delaware Law School, Widener University, teaching Global Compliance and Ethics. Before launching Spark Compliance, Ms. Grant-Hart was the Chief Compliance Officer at United International Pictures, the joint distribution company for Paramount Pictures and Universal Pictures in 65+ countries.

How to Meet the Letter, Spirit and Intent of the DOJ's Evolving Compliance Program Expectations

By Daniel Kahn

With any new administration, the U.S. Department of Justice (DOJ) often shifts focus from one set of enforcement priorities to another. However, one area has remained a focus from administration to administration: guidance and expectations related to corporate compliance programs.

In fact, DOJ's guidance pronouncements are seemingly more detailed and its expectations heightened, particularly over the past year. This article addresses recent DOJ guidance pronouncements and priorities, and how companies can best meet the letter, spirit and intent of compliance program expectations.

Recent DOJ corporate compliance guidance and pronouncements

Clawback pilot program

In March 2023, DOJ announced a new three-year pilot program on compensation incentives and clawbacks, which includes two key components: (1) compliance requirements for criminal resolutions; and (2) credit for compensation that has been clawed back against penalties imposed in a DOJ resolution.

This suggests DOJ expects companies to put in place broad policies to allow it to recoup compensation in the event of misconduct, and to actually enforce those policies when misconduct occurs.

According to the program, every DOJ Criminal Division corporate resolution – whether it be fraud, foreign bribery, sanctions, money laundering, or something else – will now include a requirement that the company implement criteria related to compliance in its compensation structure and to report annually to DOJ on the implementation.

The criteria "may include, but are not limited to: (1) a prohibition on bonuses for employees who do not satisfy compliance performance requirements; (2) disciplinary measures for employees who violate applicable law and others who both (a) had supervisory authority over the employee(s) or business area engaged in the misconduct and (b) knew of, or were willfully blind to, the misconduct; and (3) incentives for employees who demonstrate full commitment to compliance processes."

The pilot program also offers discounts off of the penalty amount imposed by DOJ where the company fully cooperated and remediated and demonstrated it is seeking to "recoup compensation from employees who engaged in wrongdoing in connection with the conduct under investigation," or others who were supervisors and were willfully blind to the misconduct. In such circumstances, the Criminal Division will reduce the fine amount by 100% of any clawed back compensation.

Even where a company is unable to recoup compensation, so long as it demonstrates a "good faith attempt" to do so, prosecutors have the discretion to reduce the fine by up to 25% of the amount of compensation the company sought to claw back.

Revision to Evaluation of Corporate Compliance Programs guidance

In addition to implementing the clawback pilot program, the DOJ Criminal Division also announced revisions to its Evaluation of Corporate Compliance Program guidance (ECCP), which is one of the most detailed compliance guidance documents published by enforcement authorities. Among other things, the ECCP outlines questions prosecutors ask companies in evaluating their compliance programs. The revised guidance now incorporates questions related to financial compensation as a method to incentivize compliance, as well as policies and controls around the use of messaging apps and personal devices.

With respect to clawbacks specifically, DOJ asks whether a company has "policies or procedures in place to recoup compensation that would not have been achieved but for misconduct attributable directly or indirectly to the executive or employee," and "[w]ith respect to the particular misconduct at issue, has the company made good faith efforts to follow its policies and practices in this respect?"

In short, this suggests DOJ expects companies to put in place broad policies to allow it to recoup compensation in the event of misconduct, and to actually enforce those policies when misconduct occurs.

Unlike the clawback pilot program, the compliance guidance goes well beyond the narrow topic of clawbacks, instructing prosecutors to consider compensation "structures that clearly and effectively impose financial penalties for misconduct," and that inject "positive incentives, such as promotions, rewards, and bonuses for improving and developing a compliance program or demonstrating ethical leadership." Likewise, the guidance asks, "whether a company has made working on compliance a means of career advancement, offered opportunities for managers and employees to serve as a compliance 'champion', or made compliance a significant metric for management bonuses."

With respect to messaging apps and personal devices, the revised ECCP focuses on three new topics: communication channels, policy environment and risk management. The ECCP also focuses on what communication channels the company permits and why, whether the company has given thought to how this should vary by jurisdiction and business function, and the mechanisms the company has put in place to preserve electronic communication channels (including with respect to the deletion settings on the apps).

Where companies have a "bring your own device" (BYOD) program, prosecutors will want to know what policies are in place and whether the company is permitted to review business communications on personal phones according to the BYOD policy. Prosecutors will also want to know whether the company has a policy requiring employees to transfer business-related data and information from a personal phone to company platforms, whether these policies are reasonable in light of the company's circumstances and profile, and whether these policies are actually being enforced. Prosecutors will also probe what type of controls the company has in place to monitor and ensure compliance with these policies, and what discipline the company has imposed for employees who violate the policies.

With respect to messaging apps and personal devices, the revised ECCP focuses on three new topics: communication channels, policy environment and risk management.

M&A due diligence guidance

More recently, DOJ announced new guidance on merger and acquisition (M&A) due diligence, providing for a safe harbor of sorts for acquiring companies that voluntarily disclose misconduct uncovered at the target company. So long as the acquiring company discloses the misconduct to DOJ within six months of the closing, fully remediates the misconduct within one year, and pays full restitution and disgorgement, it will enjoy a presumption of a declination.

This presumption will be afforded even if the misconduct at the target company involves aggravating circumstances, such as high-level executive involvement in the misconduct, and the misconduct disclosed under this policy will not count against the acquiring company as part of a recidivism analysis in future cases.

These benefits of the guidance will not be imparted to the target company, which can "potentially" qualify for a declination, and only absent aggravating circumstances. The presumption of a declination will also not be afforded when the misconduct was otherwise required to be disclosed or already public or known to the DOJ, and the policy will not protect against civil DOJ enforcement actions.

Speeches and focus on sanctions and data analytics

In addition to the new compliance guidance, DOJ officials are consistently beating the drum on the need for companies to focus on sanctions compliance and data analytics as part of the compliance program. Although these two priorities have yet to show up in DOJ's ECCP or other compliance guidance, DOJ officials have grabbed headlines with statements like "national security laws must rise to the top of your compliance risk chart" and "sanctions are the new FCPA."

DOJ officials have likewise emphasized the use of data analytics as part of an effective compliance program. Although they stopped short of stating that a compliance program must use data analytics or artificial intelligence in order to be effective, the clear expectation is that companies will use these tools as part of their compliance program if they are using them as part of their business.

Analysis of recent DOJ policy changes and pronouncements

It is noteworthy, and perhaps a little ironic, that regulators such as the U.S. Securities and Exchange Commission (SEC) have not released compliance guidance even close to the level of detail as DOJ. Especially because the SEC has the ability to bring, and recently has been bringing, enforcement actions based on compliance and control failures. DOJ, which does not have the ability to criminalize inadequate compliance programs, nevertheless has communicated significant guidance setting very weighty expectations for corporate compliance programs. Although this level of transparency from DOJ is admirable and provides insight into how DOJ is thinking about these issues, the guidance does raise some concerns.

Compensation clawback implications

The clawback pilot program and related guidance raises several questions and issues. Many countries restrict or preclude a company from clawing back compensation from employee wrongdoers, and thus the discounts accorded for clawbacks under the pilot program create incongruous and inequitable results for companies based solely on geography. Even when it is possible to claw back compensation, the process often entails protracted and expensive litigation, and can lead to the company being forced to turn over a considerable amount of confidential information (including from its internal investigation) to the employee.

Moreover, perhaps unintentionally, the pilot program's design will most likely benefit companies with the most egregious misconduct because it is often the more senior executives who receive the type of compensation that can be clawed back – i.e., bonuses and equity compensation – resulting in a greater potential for clawback and thus a greater discount when senior executives are implicated in the misconduct.

More about messaging apps

Like the clawback guidance, it is more difficult to adhere to DOJ's guidance on messaging apps and personal devices in certain countries than others as a result of employment, labor and privacy laws. Thus, regardless of whether a company has policies addressing these issues, they may be unenforceable.

Perhaps more importantly, there really does not seem to be a good solution to the problem of personal devices and messaging apps, and DOJ (and SEC, for that matter) do not seem to have one.

If employees use off-system communications channels and/or personal devices to engage in misconduct, there is very little a company can do to stop them, or even obtain those communications – and the cost of attempting to do so may be substantial.

DOJ officials have likewise emphasized the use of data analytics as part of an effective compliance program.

What does the new guidance mean for M&A?

With respect to the M&A due diligence guidance, there are significant limitations making the value and impact of the guidance questionable. Notably, the full benefits of the safe harbor only apply to the acquiring entity, not the target company – despite the fact the acquiring entity will likely own the target company at the time of any resolution with it, and therefore will ultimately bear the reputational and financial costs of any resolution.

Moreover, there are often circumstances where the acquiring company, even with good faith robust due diligence, will not learn of the misconduct or be able to fully remediate it within the allotted time. Although DOJ qualified that the deadlines "could be extended by Department prosecutors" on a case-by-case basis, the company would have to trust the reasonableness and discretion of the DOJ prosecutors when making the decision to disclose outside of DOJ's stated timeline. And the safe harbor will not protect the acquiring company from civil enforcement actions and will not apply if DOJ already knows about the misconduct.

Recommendations for companies on how to respond

The guidance described above does not mean companies should over-torque and necessarily devote significant resources to these areas.

Despite DOJ's claim that all companies should catapult national security to the top of their compliance risk chart, many companies may not have significant national security risk. Companies should certainly be attuned to national security risks, and DOJ's activity in this space is noteworthy and an important consideration. However, indiscriminately dedicating resources into this area without carefully assessing the company's risk may divert precious resources away from areas of significantly higher risk for a given company.

Likewise, as described above, clawing back compensation, depending on the circumstances, may not be worth the investment even with the increased incentives and expectations from DOJ. With respect to clawbacks, whether they can or should be pursued in any given case, in order to potentially benefit from the pilot program or DOJ credit in the future, companies can implement policies that permit them to recoup in appropriate cases.

Implementing an enterprise messaging app platform and sophisticated monitoring and control processes may help you limit the use of, and/or retain communications over, personal devices and messaging apps, and it may increase the credit you receive from DOJ and SEC if you should ever find yourself before them. Yet, it is impossible to know what actual difference this would make overall, much less in capturing or preventing the use of off-system communications to engage in misconduct, and it may not be the best approach for particular companies.

Nevertheless, companies can implement – where local law permits, at least – policies governing messaging apps and personal devices that address what messaging platforms and devices are permitted to be used for business communications. Recommended best practices regarding messaging apps include:

- Requirements and prohibitions for using personal devices and messaging apps for business
- Expectations for business communications that occur on non-approved platforms and devices, for example, that they be transferred to approved platforms
- Retention expectations for data and information on approved platforms, including what the deletion settings (to the extent the platform has them) should be set to
- Disciplinary consequences for failing to comply with these policies

Companies should further train employees on these policies and monitor and enforce violations of them. Monitoring does not need to take the form of sophisticated analytics, but instead may be as simple as including messaging apps and personal devices as a routine item for internal audits and something that is asked about during internal investigations.

Similarly, within the policies and pronouncements, there are reasonable steps a company can take to put it in a better position with the DOJ. For example, companies should ensure national security and sanctions are one of the areas considered as part of their risk assessment, even if it may not be an obvious risk. Companies that use data analytics to promote their business should consider ways in which those analytics can be leveraged for compliance purposes.

2024 prediction

Although 2024 will undoubtedly bring with it a number of surprises, it is safe to assume DOJ will continue to focus on corporate compliance, sanctions and data analytics. This will likely include continued speeches about clawbacks, messaging apps and personal devices, M&A due diligence, data analytics, and national security, and enforcement actions that look to highlight these issues. I also predict we will see DOJ become flexible with some of the guidance it has released to account for practical issues and obstacles that arise as it tries to apply these new policies and to incentivize the type of behavior DOJ is seeking to encourage.

About the author

Daniel Kahn

Daniel Kahn is a former senior DOJ official with more than a decade of experience in criminal and regulatory investigations and headed DOJ's Fraud Section and FCPA Unit. He represents companies and individuals in government enforcement matters, conducting internal investigations and in compliance matters.

The Wall Street Journal described Dan as DOJ's "most recognizable expert on the Foreign Corrupt Practices Act." At DOJ, Dan was acting Deputy Assistant Attorney General of the Criminal Division and Chief of the Fraud Section, and Chief of the FCPA Unit. He supervised matters involving the FCPA, money laundering, and digital currency, commodities, securities, healthcare and procurement fraud. At DOJ, Dan played a central role in developing enforcement policies on the FCPA, corporate enforcement, compliance and monitors. He worked with authorities around the world, and tried a number of cases to verdict. Dan co-authored a treatise on corporate criminal investigations, and teaches Corporate Criminal Investigations at Harvard Law School and Global Anti-Corruption at Georgetown Law Center.

Sanctions are the "New" FCPA – How this Era of Enforcement Shapes Third-Party Risk Management

By Michael Volkov and Alexander Cotoia

In the summer of 2022, Deputy Attorney General Lisa Monaco – a veteran prosecutor and currently number two at the helm of the U.S. Department of Justice (DOJ) – began to describe the enforcement of sanctions regulations as the "new FCPA". This sentiment is a not-so-subtle allusion to the DOJ's relentless commitment over the past decade to ramp up enforcement of cases implicating the U.S. Foreign Corrupt Practices Act (FCPA).

While Monaco's remarks seemed to generate additional angst among legal and compliance professionals, the DOJ's commitment to sanctions enforcement is a logical extension of the federal government's effort to use economic sanctions and trade controls as a means of depriving adversaries – particularly the regime of Vladmir Putin – of capital and resources needed to wage offensive operations.

The development of sanctions enforcement as the "new FCPA" has its roots firmly fixated in the decision by the Biden Administration to incrementally increase pressure applied on the Putin regime to cease and desist from participating in offensive military actions against the sovereign nation of Ukraine. Beginning in the spring of 2022, and continuing exponentially thereafter, the Biden Administration sanctioned a proverbial cornucopia of entities and individuals heavily associated with the ongoing Ukraine incursion.

In 2023, this trend continued, with the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designating even more individuals and entities on its ubiquitous Specially Designated Nationals and Blocked Persons (SDN) List. Those on the recently expanded SDN List are primarily Russian oligarchs with close Putin affiliations and entities providing financial material support for the war effort. To date, the inclusion of a massive number of Russian Federation parties on the SDN List substantially degraded the ability of individuals and organizations to profit from the war effort.

While foreign countries are not legally obliged to observe OFAC's SDN determinations, the sheer influence of the United States as a major international power, combined with the implicit threat of secondary sanctions, often compel international organizations to observe prohibitions that would otherwise bind U.S. persons only.

In 2023, this trend continued, with the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designating even more individuals and entities on its ubiquitous Specially Designated Nationals and Blocked Persons (SDN) List.

Emphasis on automated sanctions screening

The advent of sanctions enforcement as the "new FCPA" requires organizations to adopt novel approaches to the management of sanctions risk overall. This is especially true in the area of third-party risk management (TPRM), which must now elevate sanctions risks as among the most important to be identified and remediated – especially for organizations operating at an international scale.

Given the frequency with which organizations partner with third parties for a host of services and goods, it is imperative the company identify its highest risk areas from a geographic perspective. It must then ensure both an initial sanctions screening and daily rescreening are configured to provide the organization with actionable information. This information is needed to either evaluate the risk of entering into a prospective agreement with a new third party – or conversely, terminating an existing agreement with parties appearing on various international sanctions and watchlists.

While these processes may have been configured to operate manually in the past, an abrupt end to the days of lax enforcement now requires organizations to adopt automated solutions that can be used at scale to identify third parties posing a higher overall risk to the company. This includes, but is not limited to, NAVEX's own RiskRate system, which cross-references a host of international sanctions and watch lists to identify a third party currently subject to sanctions. These systems have the added benefit of rescreening each of the organization's third parties daily – ensuring recent additions to OFAC's SDN List, for instance, are completely captured.

This is critical given OFAC's relatively recent enforcement action against a small bank that failed to implement processes allowing existing customers to be screened against sanctions lists. According to a Finding of Violation released by OFAC, although the financial institution in question regularly screened new account holders, its review period of 30 days for existing customers was insufficient to satisfy its screening obligations. As a consequence, the bank in question processed a total of 34 payments for two individuals who were designated on OFAC's SDN List.

The critical takeaway here is that organizations still reliant on manual processes – including spreadsheet updates and ad hoc screening – are virtually guaranteed to run afoul of OFAC's sanctions regulations when engaged in activity abroad.

The critical takeaway here is that organizations still reliant on manual processes – including spreadsheet updates and ad hoc screening – are virtually guaranteed to run afoul of OFAC's sanctions regulations when engaged in activity abroad. Even companies with a continuous screening solution should work proactively with their chosen vendor to ensure OFAC's requirements – and the lessons of the recent OFAC enforcement action – are vigorously observed.

Expansion of screening responsibilities to ESG and due diligence

While the observance of sanctions regulations is certainly among the most important obligations of a company, 2023 saw a precipitous rise in activities that expanded sanctions screening to encompass a host of other issues outside of the sanctions space.

This includes, most prominently, a growing focus on environmental, social and governance (ESG) concerns like human trafficking and forced labor; egregious practices that some nations – including the People's Republic of China (PRC) – exploit with impunity by enslaving ethnic minorities and political dissidents to work in squalid conditions for little or no pay. The issue of forced labor and human trafficking was brought into clearer focus when, on January 1, 2023, Germany's Supply Chain Act (*"Lieferkettensorgfaltspflichtengesetz"* or "LkSG") entered into force.

Among other things, the LkSG requires companies conducting business in Germany to identify, prevent or minimize the risks of human rights violations and damage to the environment with respect to both direct and indirect business partners. While the requirements for dealing with direct suppliers is more stringent – owing to the ability of the contracting party to use financial leverage as an incentive to encourage compliance with the LkSG's goal of minimizing negative social and environmental impacts – the extension of certain requirements to an organization's indirect suppliers is equally challenging.

According to that portion of the LkSG, even indirect suppliers must be reviewed by a company for adverse human rights or environmental impacts when that company has substantiated knowledge the indirect supplier may be perpetuating abuses like those mentioned above. The adoption of the LkSG is a clear signal of a new era with respect to TPRM practices.

While it may have been sufficient for organizations to only screen for sanctions risk in the past, the evolving legal and regulatory frameworks around ESG concerns makes it imperative for organizations to move beyond basic screening to due diligence, where required.

But superficial scrutiny of an organization from an ESG perspective is becoming increasingly unwise, as legislators and regulators require a more robust assessment of ESG risks in concert with an organization's due diligence process. In the past, information elicited from a due diligence questionnaire was primarily focused on anti-bribery and corruption, as well as sanctions issues for companies having dealings with governments abroad. Organizations must now revamp those questionnaires to include more targeted questions about the counterparty's ESG practices, specifically in relation to human trafficking, modern slavery, forced labor and environmental degradation.

Since there is no commonly accepted definition of ESG concerns, let alone a centralized database of a company's ESG reputation, it is incumbent on the organization to do their level best to substantiate the information furnished by the supplier using a variety of both proprietary and public sources. With respect to contractual assurances, for companies known to operate in areas with poor human rights records, it is particularly important to insist the company's policies (not the counterparty's) will control in any definitive agreement ultimately reached. Those policies, in turn, should be detailed enough to leave no doubt in the supplier's mind as to the company's steadfast commitment to ethical and legal business practices.

2024 prediction (and beyond)

In a highly volatile geopolitical climate, it is virtually impossible to make predictions about the importance of certain compliance topics over others with any degree of certainty. Nonetheless, the trends from 2023 related to the growing prominence of sanctions concerns and the associated expansion of traditional ESG factors are likely to continue unabated.

While many nations have stopped short of a complete embargo of the Russian Federation – opting instead to employ the diplomatic weapons of economic sanctions and stricter trade controls – it is virtually certain the current number of sanctioned Russian parties will increase until the war in Ukraine is over. OFAC's recent actions also highlight the possibility that entities or individuals located outside of Russia may also be subject to sanctions, to the extent they contribute in any substantial way to Russia's war effort.

In short, we can confidently predict OFAC and its foreign counterparts will have no shortage of work in maintaining and adding to the existing sanctions list. With respect to ESG concerns, we anticipate the realm of activities that historically constituted ESG concerns will only continue to grow, as consumers drive the demand for details about a company's operations and its effect on the community at large.

About the authors

Michael Volkov
Michael Volkov, CEO of The Volkov Law Group, LLC, is a recognized expert in anti-corruption enforcement and defense, internal investigations, ethics and compliance, and white-collar defense issues with over 30 years' experience in practicing law. Mr. Volkov served for 17 years as an Assistant U.S. Attorney in the District Columbia and has served on the Senate and House Judiciary Committees as the chief crime and terrorism counsel to the respective Chairmen. He also served as a deputy assistant attorney general in the Office of Legislative Affairs of the U.S. Department of Justice and as a trial attorney in the DOJ's Antitrust Division. He also maintains the popular legal blog Corruption, Crime & Compliance.

Alexander J. Cotoia
Alexander J. Cotoia, regulatory compliance manager, has over sixteen years of experience in the legal and compliance profession. Prior to joining The Volkov Law Group, Alexander was employed by Richard Branson's company Virgin Galactic – a prominent suborbital space tourism company – in a multifaced legal and compliance capacity. Alexander joined The Volkov Law Group in 2021, and regularly assists the firm's clients with the resolution of trade compliance matters arising under both the ITAR and EAR, spearheads its due diligence efforts, and assists the firm's attorneys in advising clients with respect to sanctions regulations, the remediation of corporate compliance programs, and the conduct of internal investigations. Alexander earned an undergraduate degree at Purdue University Global and a master's degree in law with a concentration in compliance from Regent University School of Law in Virginia Beach.

The Vast World of ESG: How the EU is Leading Global Sustainability Trends

By Kevin Wilhelm and Holly Bridwell

In today's interconnected global regulatory landscape, Environmental, Social, and Governance (ESG) factors are becoming a fundamental consideration for organizations worldwide. While the European Union (EU) has always been a trailblazer in this arena, it is evident that two of the most recent requirements will increase in importance, influence and accountability for businesses across the globe — whether they are based in the EU or not.

As the United States grapples with new climate disclosures for organizations doing business in California and the much-anticipated pending climate-related regulations from the Securities and Exchange Commission (SEC), businesses across the globe would be smart to look at what is happening in the EU and to start taking pre-emptive action today. Even with all the "anti-woke" sentiment in the media today – these rulings underscore an undeniable truth: ESG is here to stay, and requirements are only going to get stricter over the years to come.

Examining the United States ESG landscape provides critical context for our discourse on the EU's trendsetting ESG disclosure requirements, how they inform other regulatory bodies, and what it all means going forward. This dialogue intends to help organizations understand current obligations and prepare for upcoming disclosure requirements.

The EU is leading the way

The "ESG discussion" is quite nuanced, but let's start by looking at it from two main areas the various laws endeavor to regulate: ESG data collection and disclosure and supply chain due diligence and monitoring – including human rights impact assessments and addressing modern slavery within the supply chain.

In 2023, we saw the landmark passage of several new directives. All of these will have potential global impacts, from directly affecting businesses in the EU or organizations that do a substantial amount of business in the EU, to serving as a global weathervane for what is likely to come. So, let's start with the core ESG regulations coming out of the EU.

What is the CSRD?

The **EU Corporate Sustainability Reporting Directive** requires granular and comprehensive disclosure of material ESG metrics as decided through a rigorous double materiality process. The CSRD went into effect in January 2023 and is mandatory for nearly 50,000 organizations (including around 3,000 U.S. companies). Data collection is to begin in FY 2024, with the first CSRD-aligned reports published in 2025, coinciding with firm financial statements.

Examining the United States ESG landscape provides critical context for our discourse on the EU's trendsetting ESG disclosure requirements, how they inform other regulatory bodies, and what it all means going forward.

Immediately affected organizations include those with over €20 million in assets, a net turnover of €40 million and/or 250 or more employees. Reporting will go into effect for companies with less than the above parameters, considered EU SMEs, in 2026, and non-EU companies with €150M net turnover and one branch or subsidiary in the EU in 2028. Under this Directive, organizations are required to accurately report on governance, strategy, impacts, risks and opportunities, and metrics and targets.

Additionally, companies must conduct a CSRD and ESRS (European Sustainability Reporting Standards) aligned double materiality assessment annually, and provide detailed measurements on subjects such as climate-related financial risks and greenhouse gas emissions to meet these requirements. The ESRS provides the disclosure framework to meet the needs of CSRD reporting. Companies must report on all ESRS disclosures that are material to the company or required as a general disclosure by the framework. For many, the reporting requirements will also extend throughout the value chain, further complicating information collection and solidifying that organizations will be held responsible for third-party actions.

What is the CSDDD?

Passed by EU Parliament in June 2023, the **Corporate Sustainability Due Diligence Directive** goes even further to expand on the value chain accountability of organizations and establishes reporting and disclosure mechanisms intended to increase obligations of the board and directors to ensure company compliance.

Organizations for which CSDDD would apply include EU companies with more than 500 employees and a global turnover of €150 million, and non-EU companies if they generate €150 million or more in the EU market annually. The CSDDD also applies to EU and non-EU organizations with 250 or more employees and €40 million in annual turnover in the EU if half of the turnover is from a high-risk sector. High-risk sectors include the manufacturing or wholesale of textiles, leather and related products, agriculture, forestry and fisheries, extractive industries, and the food industry.

The CSDDD would require applicable organizations to conduct due diligence in assessing environmental and human rights risks for suppliers, ensure third-party compliance, establish a mechanism to report grievances, risk identification and mitigation, and public reporting.

What is the German Supply Chain Due Diligence Act?

The **German Supply Chain Due Diligence Act (LkSG)** entered into force on January 1, 2023, and imposes due diligence obligations on companies to identify, prevent, or otherwise address human rights and environmental issues in global supply chains. Though focused on Germany, the scope of this law is broad and applies to companies with headquarters, a principal place of business, a registered office, or branch offices in Germany. Through 2023, the LkSG applies to companies with 3,000 employees, but starting January 1, 2024, it will apply to those with more than 1,000 employees.

The LkSG requires organizations to establish risk management systems, perform regular risk analyses, create a clear human rights policy, conduct remedial actions, and develop complaint mechanisms.

While this Act is directed towards organizations based in and doing business in Germany, it creates additional implications in several ways. First, the LkSG is one of many global regulations meant to protect the environment and human rights throughout the supply chain, thus strengthening the international position on ESG in the supply chain.

Similar to when California passed its Anti-Human Trafficking Law through the supply chain, it will require increased attention, action, training and monitoring of a company's suppliers regarding issues such as modern slavery and occupational health and safety violations.

Aligning on disclosure

Voluntary frameworks are unifying to support the increase in global ESG governmental regulations. The International Sustainability Standards Board (ISSB), established in November 2021 at COP26 in Glasgow, brought together multiple frameworks to develop a high-quality, comprehensive global baseline for ESG reporting. Focused on meeting the needs of investors and the financial markets, the ISSB will absorb the reporting requirements of the Taskforce on Climate-related Financial Disclosures (TCFD), seen as the standard for climate-related financial risk disclosures, as of 2024.

The ISSB standards build on the existing frameworks and standards for disclosure to address the information gap and issues with the reliability and comparability of ESG data. Since ESG data looks different depending on the organization and corresponding value chain in question, establishing a common taxonomy has long been an issue for compiling this information for disclosure. Merging the requirements of ISSB, TCFD and furthermore SASB (The Sustainability Accounting and Standards Board) will encourage easier and more efficient disclosure to better inform investors, lenders, insurance underwriters, customers, suppliers and vendors. Aligned frameworks will help provide ESG data to stakeholders who can accurately assess financial risks related to climate change and other ESG metrics.

In short, these two voluntary frameworks overlap with the requirements coming out of the EU in significant ways, including disclosure of climate risks and opportunities, risk management and business continuity plans, climate targets, Scope 1 and 2 disclosures, and more. Because of the many material financial impacts ESG metrics have on capital markets, this reporting merger will provide disclosures that will be as essential as financial statements as practices advance.

What do EU ESG requirements mean for the U.S.?

Though the California and SEC decision on climate-related disclosures will have the greatest impact on U.S.-based companies, the EU requirements are important for the many larger U.S. companies doing business in the EU already meeting those requirements for the CSRD and CSDDD. These U.S. companies would do well to begin preparation for both SEC and EU reporting to avoid the financial and human capital constraints put upon a company when it becomes a laggard in meeting regulatory obligations.

Then, there is the question of enforcement. While the EU has enforcement mechanisms for many ESG regulations, how the U.S. will enforce ESG targets and disclosure is still uncertain and unpredictable. Part of the noise regarding ESG regulation in the U.S. concerns the looming elections and what will happen should a conservative administration take over in 2025. While this political shift is a distinct possibility, one thing is clear: ESG is not going away, and this information is quickly becoming as vital as financial disclosure, and global trends will continue to move in this direction, regardless of the political climate in the U.S.

California. SB 253, the Climate Corporate Data Accountability Act, will require all corporations doing business in California (both public and private) with more than $1B in annual revenue to fully disclose Scope 1, 2 and 3 in accordance with the Greenhouse Gas Protocol and get assurance on those greenhouse gas disclosures. SB 261, the Climate-Related Financial Risk Act, will affect public and private companies with over $500M in annual revenue, requiring biennial preparation of a climate-related financial risk report disclosing the entity's climate-related financial risk and measures adopted to reduce and adapt to climate-related financial risk. While smaller companies will be excluded from these bills, the regulations would have major implications for U.S. companies.

How can organizations prepare?

The following advice probably won't come as a surprise: start the work now and start getting audit ready. While your organization may not need to file ESG disclosures at this moment, it will eventually. We could publish an entire book about how to get started, but in simple terms, organizations can get moving by:

- Determining ESG topics material for your company – conduct a double materiality assessment
- Establishing a cross-functional committee to collect ESG data
- Gaining buy-in and educating the C-suite and board of directors (including securing adequate funding)
- Measuring your ESG impacts and greenhouse gas (GHG) emissions

- Adhering to any existing regulatory and customer/vendor requirements on ESG for your business
- Consolidating the information in a digestible format for audit-ready disclosure
- Aligning data and ESG efforts to ISSB and applicable regulatory disclosure frameworks

Of course, that all sounds easy in theory; in practice, those just now getting started have their work cut out for them. However, for companies where ESG practices and disclosure are not yet required, starting early will avoid the scramble once these requirements do come into effect.

2024 prediction

The global ESG landscape will continue to consolidate, enforcement will ramp up and be made more public, and stakeholders and regulators will continue to look closely at how businesses do business.

If history is any indicator, the EU will continue to lead the way with ESG regulation and enforcement – with the U.S. and rest of the world following suit. Publicly traded companies have a clear need to align on these requirements and disclosure frameworks, and private firms should also prepare now as this information is financially material and will impact future equity events.

Regarding the SEC decision – it will certainly be both imperfect and controversial, but it will soon impact companies operating in and likely those doing business with the U.S. in some capacity. There will likely be significant overlap with the disclosure requirements coming out of the EU and California, so aligning with the CSRD, CSDDD will be important, as well as using the ISSB and TCFD frameworks for disclosure.

About the authors

Kevin Wilhelm
Kevin Wilhelm is the Managing Partner of Point B's ESG practice and is one of the world's pre-eminent business consultants in the field of ESG and climate change. He was recognized in 2021 by Climate Change Business Journal with the Individual Award for Industry Leadership and in his previous role at Sustainable Business Consulting, he was named the Most Innovative CEO by CIO Magazine in 2022.

Kevin brings 23 years of experience working with leading clients to realize cost savings and brand value from better social and environmental practices. His list of 300+ clients include New York Life, Amazon, Delta and Alaska Airlines, Caesar's Entertainment, Nordstrom, Expedia, Kohl's, Carmax, IAC Global, REI, and many more.

He has taught 12 different courses in sustainability both in online and in-person formats at nine institutions including Harvard, The University of Washington and the University of Denver. He has two TEDx Talks and is the author of multiple acclaimed books in this field including: Return on Sustainability: How Business Can Increase Profitability & Address Climate Change in an Uncertain Economy, and the true guide to implementation Making Sustainability Stick.

Holly Bridwell
Holly Bridwell is an ESG Consultant with a focus on driving positive impact and helping businesses integrate sustainability into their operations and governance structures. She has professional experience in commercial banking, process development, event sustainability, and B Corporation certification in various fields.

Leaning into her experience developing and implementing ESG programs in commercial banks, Holly specializes in climate analysis, materiality assessments, and ESG reporting and disclosures. She is especially skilled in supporting clients with their climate transition and risk strategy, portfolio emissions, and reg. She has received a certificate in sustainable investing and supported sustainable finance initiatives across multiple industries.

Holly attended the University of Florida Warrington College of Business earning a Master's degree in Entrepreneurship and the Social Impact Scholar Award.

Supply Chain Regulations and Exposure – How to Manage Third-Party Risk and Beyond

By Kristy Grant-Hart and Florian Haarhaus

If the term "nth supplier" joined your vocabulary recently, you're not alone. If you haven't heard the term until now, don't worry – you'll be hearing it frequently soon enough.

The "nth" supplier is the mythical last provider of materials many layers down into the supply chain. Regulators expect companies to obtain (or divine) massive amounts of information from their suppliers' suppliers, then aggregate it magically into easily reportable sliced-and-diced data. The reality is much more challenging.

Supply chain due diligence regulation is exploding. So too, are stakeholder expectations around the supply chain, especially when it comes to environmental and human rights abuses. Gone are the days when the best price was the only consideration for product sourcing. Now, the review must consider many facets, including the environmental impact of production and the effect of production on the humans involved.

The current legal landscape

Unsurprisingly, Europe is leading the way when it comes to supply chain-related due diligence laws. We discuss some of the following regulations in light of ESG requirements in another section of this publication. This article focuses on how these regulations apply to supply chain due diligence, as opposed to ESG.

German Supply Chain Act

The German Supply Chain Act came into force on January 1, 2023. Where applicable, it obligates larger German businesses to identify and account for their impact on human rights, including forced and child labor, forced evictions, oil pollution, and land grabbing. The requirements extend to overseas direct suppliers and sometimes even indirect suppliers.

Due diligence procedures must be documented, and an annual report must be published and submitted to the Federal Office for Economic Affairs and Export Control.

Corporate Sustainability Reporting Directive

Just four days after the German Supply Chain Act came into force, the European Corporate Sustainability Reporting Directive did the same. While some rules are still being finalized, current reporting obligations relate to environmental matters, treatment of employees, respect for human rights, anti-corruption and bribery, and diversity of company boards (in terms of age, gender, educational and professional background).

The Directive has a staged approach for enforcement, with the first in-scope companies applying the disclosure rules to their 2024 financial year, with reports to be published in 2025.

The coming legal landscape

There are many laws on the horizon that are likely to impact supply chain due diligence and reporting requirements.

European Union's Corporate Sustainability Due Diligence Directive

The EU's Corporate Sustainability Due Diligence Directive (CSDDD) would introduce requirements for companies to identify, prevent, end, or mitigate the actual and potential negative impacts of their activities on the environment and human rights. It would obligate them to conduct due diligence on their own operations, as well as those of their subsidiaries and other entities in their value chains with which they have direct or indirect established business relationships.

Regulators expect companies to obtain (or divine) massive amounts of information from their suppliers' suppliers, then aggregate it magically into easily reportable sliced-and-diced data. The reality is much more challenging.

The law includes many disclosure requirements relating to due diligence and includes civil liability for companies if harm could have been avoided if proper due diligence had been performed. The law is completing negotiations and is expected to be finalized in 2024, with enforcement beginning in 2025.

United States Securities and Exchange Commission disclosures

The United States Securities and Exchange Commission is, as of this writing, continuing to finalize its new climate-related disclosure rules. When they come into force, they will obligate companies traded on U.S.-based exchanges to report information about their environmental impact. The rules will likely require companies to obtain information from their suppliers about their environmental impact, creating a wide-ranging impact.

Other states and countries

Human and environmental rights issues are hot political topics. Many state/country actors have stated intentions to require greater transparency from corporations. We expect to see many more formally proposed laws in the near future.

What to do now

The legal landscape is daunting, but there are many activities you can do now to prepare for disclosure compliance.

Map major suppliers using a risk-based approach

It's tempting to boil the ocean, but a better use of your time and resources is to use a risk-based approach for supply chain due diligence and management. There are different approaches to this.

The first is spend-based due diligence. To do this, go to procurement and/or finance and ask for information about the top suppliers by spend. Start with a number you can manage, whether that's the top five or top five hundred suppliers.

An alternative is to use a jurisdiction-based approach. For human rights concerns, the annual United States Trafficking in Persons report ranks countries by risk. Country-specific environmental protection risk may be reviewed using the Country Policy and Institutional Assessment (CPIA) data of the World Bank.

Another approach is to focus on higher-risk industries. Organizations like Walk Free, Amnesty International, and Human Rights Watch all provide good information for understanding supply chain risk.

Make it an inside job

Procurement/Sourcing should be able to give you access to information about key suppliers, but other departments will have important insights as well. For instance, Legal may know about the largest supplier contracts signed this year. You can read the terms and understand whether disclosure requirements or audit rights are present.

You can also ask IT for information coming out of their data flow mapping. If data is coming or going from higher-risk jurisdictions, that can be a lead you'll want to follow.

Ask your suppliers

Once you've identified your major suppliers, call their procurement or compliance teams, and ask for any disclosure information they have available. In many industries, disclosure is already common and/or required. Collect this low-hanging fruit to begin your information gathering.

Check your modern slavery disclosure requirements

Many companies are unaware that they need to disclose their anti-modern slavery activities if they reach certain legal thresholds. The United Kingdom, Australia, and California all have public disclosure requirements, and Canada recently joined that list. If you sell into or otherwise operate in any of those locations, check the rules to make sure your company is in compliance.

Create standard contract language

Work with the Legal department to create standard language in contracts relating to human rights, the environment, and deeper supply chain issues. A good approach is to have a catch-all "follow all laws, including all labor laws"-type clause in all contracts, with stronger contractual obligations for higher-risk and/or higher-spend suppliers.

Obtain an ESG baseline report

If you already know your company is going to be subject to disclosure obligations, consider hiring an outside expert to perform a materiality analysis and/or ESG baseline report from which to measure year-on-year.

Best practices

In addition to what you **need** to do now, some best practices include the following.

Create a supplier code of conduct

Create a supplier code of conduct that applies to all suppliers and ensure it is published on your website. Either attach or reference the supplier code for inclusion in all supplier contracts. Include language on PO's that states that submission of the PO indicates acknowledgment of, and adherence to, the company's supplier code of conduct.

Be sure to use a principles-based approach. Principles use universal language rather than didactic requirements. An example of this is choosing, "supplier agrees not to furnish any public official or private person with anything of value for an improper purpose" instead of, "supplier agrees to follow the company's gifts and entertainment policy." Many times, supplier codes include language requiring suppliers to follow the company's policies, when the company's policies aren't publicly available and/or conflict with the supplier's **own** policy limits. Using a principle-based approach solves this problem.

The legal landscape is daunting, but there are many activities you can do now to prepare for disclosure compliance.

Audit your highest risk suppliers

There's nothing like an on-the-ground review to understand what is really going on. When you've identified your highest-risk suppliers, make an audit plan and determine whether your internal auditors can include human rights/environmental review in their current plan, or obtain outside auditors to perform the reviews.

Many companies already perform quality audits of their important suppliers. Where that is already happening, add human rights/labor-related audit elements to the audit plan and train the auditors on red flags. Work with Legal to ensure that higher-risk supplier contracts include audit rights going forward.

Practice at the table

It's likely that your IT department does a data breach tabletop exercise each year to practice responding to a crisis. See if you can partner with IT to include a supply chain disruption with environmental or human rights-related challenges as part of the exercise. This will help people see the potential damage in a much more animated way.

Engage with industry associations

If your company is in an industry that is or will be subject to disclosure requirements, you're likely not the only company contemplating what to do. Engage with industry associations and advocacy groups to see if they have advice or guidance on complying with the disclosure requirements specific to your industry. If they don't, suggest that they start a working group to do so.

Acknowledge the limits

Unless your company is their most important customer, asking a secondary or tertiary supplier's supplier to disclose information to your company is going to be a challenge.

Over time, there may become uniform ways of disclosing information up and down supply chains that make it easy to comply with disclosure laws and to aggregate data in a consistent way. That day isn't here yet. Be patient and acknowledge the limitations of what is and will be available, then do your best to comply using what you have.

2024 prediction

Scrutiny of supply chains will grow stronger by all stakeholders, including regulators, employees, shareholders, other companies, and the public. Most companies will struggle to adapt to quickly changing requirements but will ultimately create successful strategies for doing so.

About the authors

Kristy Grant-Hart
Kristy Grant-Hart is an expert at transforming compliance departments into in-demand business assets. She's the author of the book "How to be a Wildly Effective Compliance Officer" and CEO of Spark Compliance Consulting, a London and Los Angeles-based consulting group which was shortlisted for Compliance Consulting Team of the Year at the Women in Compliance Awards (2016). She is also an adjunct professor at Delaware Law School, Widener University, teaching Global Compliance and Ethics. Before launching Spark Compliance, Ms. Grant-Hart was the Chief Compliance Officer at United International Pictures, the joint distribution company for Paramount Pictures and Universal Pictures in 65+ countries.

Florian Haarhaus
As international general manager, Florian Haarhaus is responsible for leading NAVEX's international business, spearheading strategic initiatives to extend NAVEX solutions across high growth markets. Prior to joining NAVEX, Haarhaus has 30 years of international experience in the software and SaaS industry, having built and run teams across Europe, the Middle East and Asia for companies like Oracle, Lotus-IBM, Salesforce, box and Nintex. His key area of focus is helping organizations across EMEA and APAC leverage leading edge SaaS technologies for better business outcomes.

Leveraging Compliance Data for More Effective Decision Making and Business Resiliency

By Anders Olson

For any business, the ultimate goal of collecting data must be to inform some decision-making process. Anything less would beg the question, "why bother?" But racing headlong towards the goal of "data-informed decisions," without considering the preceding steps, can lead to a misinformed decision-making process in which there is a great deal of confidence simply because it is "based on data."

Compliance data is unique in the breadth and depth of its impact relative to other data residing in your organization. Regulatory action and enforcement over non-compliance, negative social media exposure and insider threats are all unfavorable outcomes that can originate from any number of avenues – many of which are compliance-related at their core.

Identifying and collecting data alone is not sufficient. There must be a common framework to tie together data from different systems.

The best defense against unfavorable outcomes is comprehensive knowledge of your risk and compliance environment. But how does one go from data collection to comprehensive knowledge? This article explores how to build a foundation of compliance-related data in order to inform more effective decision making and business resiliency.

Capture data from multiple sources

The solution lies in active observation through multiple means. There are questions that need to be answered to gain comprehensive knowledge, some of which include:

- Where do people in your organization have conflicts of interest, perhaps with third-party vendors or competitors, and what potential risks do these pose to the business?
- Are there known risk factors associated with existing or potential third-party vendors?
- Are there existing policies being attested and adhered to at each level of site and level of the organization?
- Are policies and procedures accurately managed to ensure information is up to date and relevant?
- Are employees completing training on relevant compliance topics? How are employees voicing concerns?
- How are concerns investigated and followed up on?

Having systems in place to not only reliably capture data capable of answering these questions, but also provide a means of mitigation, are the foundations upon which comprehensive compliance knowledge is built.

First data, then action

Identifying and collecting data alone is not sufficient. There must be a common framework to tie together data from different systems. Locations, conceptual terminology, common elements which relate one datapoint to another. Put another way, context matters, and effectively using data means telling a story.

Consider the prior questions about which policies are being properly socialized and what sites have an outsized number of concerns being voiced. Now, imagine trying to relate the answers of these two questions absent a linkage. A wealth of siloed information can only provide siloed answers.

Data from each system should have at least one element in common with data from another, so events can be linked and categorized. Categorization allows for meaningful aggregation of data points.

In general, categories should be distinct enough to separate concepts but not so numerous as to make reporting uninformative. For example, being able to consider a policy, training, and set of whistleblower reports as related through a category allows for a whole host of action related to that category.

Imagine the category is discrimination; an outsized number of reports are coming in, policies are not being attested to and training scores are low. Having a way to tie together these data points means corrective actions can be targeted. The question of "what is wrong?" can be answered, rather than merely asked.

Data science doesn't have to be just for data scientists

Now, you may be thinking, "I'm a risk and compliance leader, not a data scientist!" Well, fair enough – but luckily there are sound core principles that can be easily leveraged by anyone – data scientist credentials or not. With a connective framework between datapoints, the scope of what is achievable with compliance data is widened immensely.

For example, spikes in certain keywords or phrases in hotline reports and inquiries can be identified and tied to a specific locations and then used to paint a picture for concerns that need addressing. Training results for employees at that location on topics most related to those keywords can be analyzed. A subsequent awareness campaign about workplace civility may be warranted.

Alternatively, consider the following situation: a new third-party vendor has been contracted in spite of the fact that it has a history of poor business conduct. Soon after, reports about product quality related to the parts provided by the third-party vendor start to surface. By cross-referencing conflict of interest disclosures, it becomes known that the employee in charge of procurement is related to the owner of the third-party vendor. Management now has a full picture of potential malfeasance.

Completing any of this analysis on its own is feasible, but a concerted effort aimed at uncovering root cause and remediation requires connected data.

Comprehensive data means comprehensive knowledge

Preventing embezzlement and fraud, avoiding financial penalties and regulatory enforcement by staying in compliance, preventing lapses in vital training are all tangible benefits of a well-functioning compliance program. While some benefits of such a unified approach may not always be easily quantified, less tangible does not equate to less impactful.

An employee who can trust their employer to do their level best to build a culture of compliance, rather than one that simply seeks to preserve a status quo, has far more reason to stay, grow, and speak up if they encounter a situation which presents a threat to the organization. Conversely, an organization may find itself accused of not doing enough, either by a regulatory body or in the court of public opinion. Data proving an organization's proactivity can help refute these accusations. Preventing or mitigating reputational risk is part of a risk and compliance program, but reputations do not grow or wither in a vacuum.

The art of storytelling

We covered how and why to collect the wealth of data, now let's talk about how to leverage it to make better decisions and improve company culture. First, without setting the context, data is effectively useless. When communicating findings, bear in mind the importance of the art of storytelling and don't forget to use tools at your disposal to paint a picture. Regurgitating data points is not an effective way to describe the nuance of a corporate culture, and a presentation full of bar charts is likely to make eyes glaze over.

Data from each system should have at least one element in common with data from another, so events can be linked and categorized. Categorization allows for meaningful aggregation of data points.

One such way to effectively communicate data is by relating it to trends in your industry and in your own data, and how your company performs against that benchmark. This sets the context and helps evaluate your performance and identifies areas of opportunity. Use the data to illuminate your audience, consider using business intelligence tools to create graphics that tell the story in an engaging way.

Other methods to use in helping tell that story include artificial intelligence capabilities such as Natural Language Processing techniques that can identify reports that look similar – or vastly different – to the norm. Think of the examples listed earlier and how just a few data points can provide valuable insight into the cultural health of your company. Data correlation will help analyze areas of risk and opportunity that may be hidden if data is only evaluated on the surface.

2024 prediction

Just as reputations do not exist in a vacuum, nor does the regulatory environment. Regulations such as the FCPA, German Supply Chain Due Diligence Act, EU CSDDD, Sarbanes-Oxley, GDPR, Sapin II, and others, will continue to drive the need for a robust compliance program. The scope and number of regulations has been growing for decades and is showing no signs of slowing. If we look at the recent DOJ guidance on compliance programs, much of it boils down to "you are expected to do everything that makes sense given your industry." That burden of proof will require data.

With the growing rate of organizations and executives being held accountable by both the public and by regulators across the globe, the need for data to effect change will continue to grow. With the rise in AI being used across businesses large and small, we expect to see a wealth of information being more effectively acted on – or at least, expected to be used to enact change.

About the author

Anders Olson
Anders transitioned from a career in banking to join NAVEX in 2020 as the company's inaugural data scientist. Since then, he has been instrumental in enhancing the data ecosystem, leveraging his expertise in applied economics to analyze and improve compliance-related human behavior data.

Risk & Compliance as a Strategic Imperative for the Board

By Carrie Penman and Shon Ramey

In an era marked by heightened global regulatory scrutiny and enforcement, the landscape of risk and compliance is undergoing an evolution making the strategic imperative for effective, risk-based compliance initiatives clear. From health and safety concerns, third-party risk management, cybersecurity, environmental, social and governance (ESG), bribery and corruption, and many more variable business risks, the risk and compliance function is increasingly involved in critical operations.

Beneath the surface of this risk landscape, a deeper narrative is taking shape – one that transcends the conventional perception of compliance as a box-ticking exercise. Now, more than ever, compliance as a strategic partner to the C-suite and board, and the intricate dance between data-driven precision and the compelling art of risk and compliance storytelling, is a strategic imperative. And specifically, it is a strategic imperative for the board of directors to effectively fulfill their oversight responsibilities.

The legal case for board involvement with Risk & Compliance

In early 2023, the Delaware Chancery Court issued a significant decision that impacts corporations and their C-suites. Now, corporate officers and boards of directors are held responsible for a fiduciary duty of oversight to their organization. This decision opens the door to legal action and liability for corporate officers to be held personally responsible for misconduct and/or third-party and shareholder lawsuits.

So, what does this mean for compliance officers? Well, in practice, for many that does depend on whether they are actually an officer of the company, something far from settled in the compliance field because many senior leaders in compliance are not technically part of the C-suite. In fact, data from the 2023 State of Risk and Compliance Report which surveyed more than 1,200 compliance leaders and professionals, shows only a quarter of organizations have a compliance function that is independent and part of executive leadership.

Personal liability aside, boards are indeed heading in the direction of more involvement with the risk and compliance function and need to be equipped to ask the right questions – some of which may yield uncomfortable answers. For example, when compliance professionals were asked in the same survey about management's commitment to compliance in face of competing business priorities, less than half (47%) stated senior leaders persisted in their commitment. This should beg the question, "is our organization operating under the "results at all costs" paradigm?" If the answer is yes, the realities of regulatory enforcement and accountability may mean your organization could eventually be at risk.

This increased risk exposure faced by businesses today, expanding with new regulations, sanctions, third-party risk concerns and the like, contributes to a sort of forced maturity for the function – similar to the path the cybersecurity function has been on for the last several years.

Now, corporate officers and boards of directors are held responsible for a fiduciary duty of oversight to their organization. This decision opens the door to legal action and liability for corporate officers to be held personally responsible for misconduct and/or third-party and shareholder lawsuits.

But in good news, there is compelling data and a legal imperative showing the compliance function is maturing. And as part of the maturity, more direct contact with and briefings for the board of directors are necessary to continue this strategic partnership.

What does program maturity mean?

At NAVEX, we spend a lot of time on compliance program maturity – from developing tools to assist organizations grow their program, to compiling data from risk and compliance leaders for use for benchmarking, and sharing information from customers and experts alike to further progress the maturity of the compliance function as a whole.

The U.S. Department of Justice (DOJ) offers specific guidance on what a well-functioning compliance program should look like, and also what role the board should play. Per the March 2023 DOJ guidance, "The company's top leaders – the board of directors and executives – set the tone for the rest of the company. Prosecutors should examine the extent to which senior management have clearly articulated the company's ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example."

Regarding board oversight, the DOJ asks the following questions when investigating compliance failures:

- What compliance expertise has been available on the board of directors?
- Have the board of directors and/or external auditors held executive or private sessions with the compliance and control functions?
- What types of information have the board of directors and senior management examined in their exercise of oversight in the area in which the misconduct occurred?

Let's tie that to what we recently learned from practitioners from across the globe. This year, in the earlier referenced survey, we learned:

- 67% of compliance leaders deliver periodic reports to the board of directors
- 55% have compliance experience or expertise represented on their board
- 52% participate in private sessions with a board level committee
- 25% indicate Compliance is an independent function reporting directly to the CEO or board

These findings are somewhat concerning as boards are expected to oversee the organization's risk and compliance initiatives and these expectations have been in place since the original Federal Sentencing Guidelines for Organizations were issued. While (unfortunately) many organizations view their legal and compliance functions as cost centers, in reality, proper oversight, resources and action by those functions can save millions, or hundreds of millions, as recent enforcement demonstrated. Further, programs like the Securities and Exchange Commission's (SEC) whistleblower program, which is regularly making headlines with multi-million-dollar payouts to whistleblowers, means an internal issue can very quickly become a very public external problem – one that will quickly rise to the board level.

To overcome the cost center mentality, compliance officers must be seen as a strategic partner to the business leaders and the board of directors. One place to start is by helping your board and CEO know the right questions to ask.

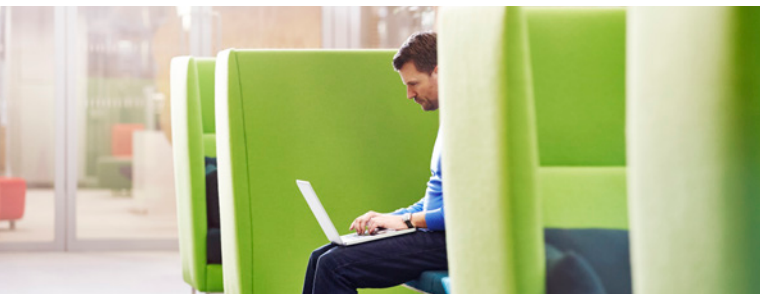
Some of those questions could include:

What information do you get to give you comfort that compliance risks are covered?

- Are there any risks that aren't being addressed as they should be?
- Do leaders set the right tone? How are they perceived by employees?
- Is candor rewarded or punished in our organization? What about fear of retaliation?
- How are we at discipline? Are top performers and high-level people held accountable to the code of conduct in the same way as other employees?
- Do you have the resources you need to do your job appropriately? Do you feel you have access to the CEO and board whenever you need it?
- What trends in issue types or company locations are you seeing?
- Is there anything we should know?
- What keeps you (the risk and compliance officer) up at night?

While this list is not exhaustive, it sets the general tone for the type of information board members should know about compliance. Then it's up to compliance leaders to tell a story that sets the context for the current risk and compliance strengths, opportunities and threats.

This combination of data (given in context), effective storytelling, and clear communication about the board and C-suite's responsibility to be informed about compliance needs will set leaders on the right path to being seen as a strategic partner.



2024 prediction

Boards are getting smarter and savvier about risk and compliance and will continue that trend. The increased attention to cybersecurity, data privacy, human rights, third-party risk, sanctions enforcement, etc., means boards will continue to become more fluent in compliance programs and will be more comfortable asking the right questions.

As case law continues to expand requiring more board involvement, directors will either willingly run –or begrudgingly be drug – to accepting responsibility, asking the right questions and vetting the answers. One way or another, board involvement with risk and compliance will increase as we head towards increased corporate accountability.

About the authors

Carrie Penman
As one of the earliest ethics officers in the industry, Carrie Penman has been with NAVEX since 2003 after serving four years as deputy director of the Ethics and Compliance Officer Association (ECOA) now ECI. A scientist by training, she developed and directed the first corporate-wide global ethics program at Westinghouse Electric Corporation from 1994-1999.

As Chief Risk and Compliance Officer for NAVEX, Carrie leads the company's formal risk management processes. She also oversees its internal ethics and compliance activities employing many of the best practices that NAVEX recommends to its customers.

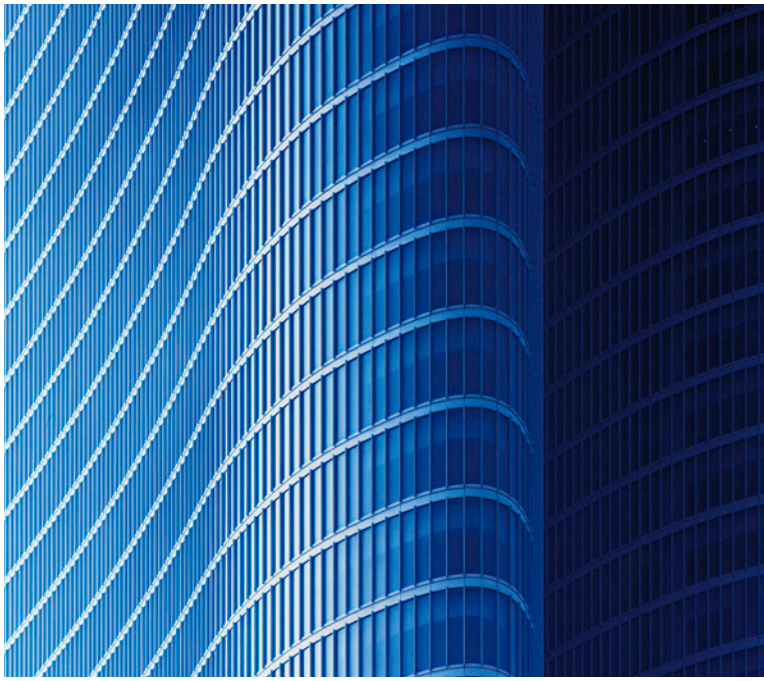
Carrie has extensive client-facing risk and compliance consulting experience, including more than 15 years as an advisor to boards and executive teams; most recently as NAVEX's SVP of Advisory Services. She has also served as a corporate monitor and independent consultant for companies with government settlement agreements.

Carrie was awarded the inaugural Lifetime Achievement Award for Excellence in Compliance 2020 by Compliance Week magazine. In 2017, Carrie received the ECI's Carol R. Marshall Award for Innovation in Corporate Ethics for an extensive career contributing to the advancement of the ethics and compliance field worldwide.

Shon Ramey

Shon has focused his legal career on corporate law and regulatory and compliance matters. In more than 25 years of practice, he has managed corporate law departments and counseled multi-national corporations on transactional and compliance matters. As NAVEX's general counsel, he is responsible for the legal department, and provides direction and oversight to the human resources and global privacy functions.

Shon previously served as general counsel for various publicly traded and private companies, with concentrations in technology and energy. Shon has also been a partner or senior counsel in some of the world's largest law firms, including Baker & McKenzie and SNR Denton (now Dentons). Shon is a graduate of Park University and the University of Virginia School of Law.



Compliance & Cybersecurity – Working and Worrying Together About the Intersection of People and Technology

By Bill Cameron

I'm not a cyber expert, but as a compliance professional with accountability for internal investigations of employee and third-party misconduct I've had a front row seat to the evolution of risk that has mirrored the mass adoption of new technology.

Protecting information used to be less complex. Keeping bad actors outside of an organization meant fences, door locks and security guards. While managing the risk of employees and other insiders misusing or stealing assets and information was a little tricky.

As artificial intelligence (AI) deploys and the risk of quantum computing looms, the push-pull of progress and risk has nudged corporate compliance and security functions, towards best friend forever status.

But good hiring practices, security cameras and simple physical access limitation policies worked pretty well. After all, stealing information meant physically taking or copying actual documents and walking out with them – or taking pictures with a camera and then getting the film developed. Pretty cumbersome and inefficient.

Now, that all sounds like ancient history although it's really not – the iPhone debuted in 2008 and, while the first banks appointed the first chief information security officers in the 90s, the position wasn't mainstream until the last decade or so.

Today we all walk around with a combination computer/camera/recording device in our pocket. Laptops replaced bulky PCs, and every business tool is generally smaller, faster and more capable of being both weaponized and breached.

The observation of Intel co-founder Gerald Moore, that the computer processing power of computers doubles every two years (Moore's Law) is often referenced to note the speed of technological advancement – and is, if anything, understated.

New technology, driven by the near universal connectivity of information via the internet, spawned a perpetual cycle of software development and other sophisticated products that drive productivity and efficiency.

The latest must-have technologies and software tease companies both large and small with endless ways to innovate and become more efficient and profitable. Which in turn, challenged the ingenuity of threat actors and encouraged governments to raise their expectations that companies meet the new information security risks.

As artificial intelligence (AI) deploys and the risk of quantum computing looms, the push-pull of progress and risk has nudged corporate compliance and security functions, both relative newcomers to the intense spotlight of government oversight and stakeholder accountability, from close associates, towards best friend forever status.

The evolving (and essential) relationship between Security and Compliance

As new BFFs, cyber professionals and their compliance counterparts increasingly see their areas of expertise and responsibility intersect and overlap. As greater swaths of critical information (e.g., customer data and other PII) are exposed, new compliance policies and cyber tools are rolled out to meet the risk. Tools launched by cyber insider threat programs spawn fresh categories of internal investigations and highlight new risk areas for compliance teams to address.

Government oversight expectations are also increasing as well. For example, the U.S. Department of Justice's Evaluation of Corporate Compliance Programs clearly contemplates the assessment and mitigation of risks presented by weak cyber controls including data loss, privacy, and operational impact. Further, the U.S. Securities and Exchange Commission recently adopted rules requiring publicly traded companies to disclose material cybersecurity incidents as well as their strategy for managing their cybersecurity risks.

So, the risks are real, the landscape is changing rapidly, and stakeholders – government, customers, employees and otherwise – are watching. Building and maintaining a corporate culture that embraces the vigilance necessary to meet those stakeholder expectations requires a strong partnership between compliance and cyber programs.

Embedding cybersecurity-related compliance into an organization's DNA isn't necessarily easy. Practically, trying to warn people about the risks of utilizing the tools they purchased as part of their push for innovation, cost savings, or even organizational transformation, can make cyber and compliance professionals feel at odds with business partners. This can be exacerbated when exercising the proper security hygiene requires the purchase of additional tools or use of other limited resources.

But a strong partnership between cybersecurity and compliance teams helps advance the cultural imperatives of both groups and the overall organization in a more effective and efficient way. Here are a few best practice areas where boots on the ground cooperation and integration pays off.

Compliance risk assessments

If you are doing comprehensive compliance risk assessments (and of course you should be) cybersecurity should be an independently assessed risk and not bundled with other operational or departmental risks. Additionally, if your core compliance team does not have cyber expertise, consider involving a cyber professional on the compliance risk assessment team.

Training

Compliance training and cybersecurity training should be complimentary and target overlapping objectives. Both teams should know what the other is rolling out and, where possible, should reinforce each other's critical messaging. Joint training projects, particularly regarding areas of overlapping accountability, can help punctuate a message and allow sharing of technical resources.

Communication

Similar to training, avoiding silos when communicating about cyber risk and related compliance expectations or initiatives is essential to avoiding confusing or contradictory messaging.

Mature organizations know that accountability extends far beyond discipline for policy violations. Deliberate and regular communication efforts are particularly important, versus only communicating in the aftermath of a security and/or compliance failure. Joint communications from cybersecurity and compliance leaders can increase both readership and the impact of essential messaging. Additionally, partnership with a strong communications team (if you are lucky enough to have one), can optimize message timing and prevent subject matter fatigue.

Third-party suppliers

Third parties are often in the back door friends of the company family. Contractors and vendors often have significant access to company systems and technology and are frequently essential to the completion of important projects or initiatives. Yet, compliance expectations, oversight and training of third parties often lag far behind that of employees.

So, the risks are real, the landscape is changing rapidly, and stakeholders – government, customers, employees and otherwise – are watching.

Cybersecurity and compliance professionals, working with internal supply chain stakeholders, as well as legal, should share the responsibility of defining acceptable training, oversight, and accountability of third parties with systems access. This means going beyond contractual terms and conditions to ensure vendors and contractors are trained with the same standards employees, and failures and missteps are tracked and become an accepted component of evaluating third-party performance. Supplier codes of conduct, which have proliferated as a result of ESG initiatives, are another potential vehicle for highlighting evolving cyber risk and compliance expectations.

Data sharing

As organizations continue to employ more sophisticated tools, growth often happens sporadically and in silos. HR systems, investigation databases and multiple GRC-related platforms are switched out or upgraded with increasing frequency. Often these systems are not integrated and sometimes can't be.

Most companies recognize sharing data from these sources across traditional governance functions offers expanded opportunities for trend spotting and potentially more reliable evidence to support (or disprove) anecdotally-based conclusions about potential risks. All of which makes the data more actionable overall. Providing cyber leaders meaningful access to broader risk related data enhances their tool kit and allows for more effective risk mitigation and cyber resource planning and deployment.

2024 (and beyond) prediction

As the cyber threat landscape intensifies and regulatory expectations increase, the partnership between cybersecurity and compliance leaders will be key to mitigating insider threats, protecting confidential information, and fortifying programs that can withstand governmental enforcement scrutiny.

Cyber and compliance professionals can (and should) play a joint role in breaking down silos, maximizing the use of available data and bringing key business stakeholders to consensus to ensure a nimble response to emergent issues and thoughtful cyber defense planning.

About the author

Bill Cameron
Bill Cameron is the principal of Cameron Advisory Services, a newly launched firm providing customized counseling and practical advice about all aspects of ethics and compliance programming.

Bill's lengthy in-house experience and deep network of compliance professionals provides a sharp lens for assessing and reducing overall risk, including identifying opportunities to strengthen corporate ethics and compliance programs and improve company culture.

Remote Workforces Create New Challenges for Investigators and Compliance Officers

By Scott Moritz

Though the world is no longer at a standstill due to COVID and our lives have returned to something resembling "normal," the pandemic forever cemented remote and hybrid work into existence. Indeed, such flexible work arrangements proved to embody the seldom-realized state of "mutually beneficial" for employers and workers.

Reported benefits include positive impacts on organizational culture, work-life balance, the ability to expand the candidate recruiting pool, and reduced real estate needs and related costs. But Sir Isaac Newton reminds us, "Every action has an equal and opposite reaction." Despite the benefits of remote work, there is an amplification of known risks, and the emergence of new ones.

These preexisting and new risks include:

- Lack of line-of-sight
- Network security
- Amplified opportunity for misconduct
- Training and professional certification fraud
- Increased confidential reporting and associated resource strains
- Investigation limitations

Lack of line-of-sight

One example of a risk that doesn't have a formal name is the "lack of line-of-sight". Remote and hybrid work largely nullified the positive impact of leaders and managers putting eyes on their colleagues – the resulting awareness of their presence or absence and productivity (or lack thereof).

Notably, line of sight isn't just about mitigating risk. It can also promote productivity and a positive culture. People profess to "keep to themselves," but in practice, most take an active interest in what colleagues are up to. Most of these interactions are inconsequential because the majority of employees have good intentions, want to add value (and be valued), take pride in a job well done, and want to be associated with an organization that is successful and well-regarded. While these dynamics are possible to support in a remote-work environment, line-of-sight makes them easier to achieve for in-person workplaces.

Where lack of line-of-sight collides with remote-work risk is for the outlier workers who might capitalize on the opportunity to behave unethically. The opportunists, the disenfranchised rationalizers, the financial trainwrecks, and the new age Charles Ponzis live and work amongst us. They also thrive in a remote work environment, with no one to overhear their conversations, look over their shoulders at their computer screens, or physically observe if they access sensitive information. While the risk of access to confidential information stored on the network or cloud environment is reduced by use of secure technology protocols, it is not reduced to zero.

Remote work essentially eliminated the "line of sight" control, and perhaps made failing to detect fraud seem more excusable.

Before the advent of remote workforces, there was plenty of fraud and other categories of misconduct, so what changed? Remote work essentially eliminated the "line of sight" control, and perhaps made failing to detect fraud seem more excusable.

Network security

Line-of-sight is not the only control that changed in the remote and hybrid environment – network security is now infinitely more complex.

In an ideal world, network security means only devices configured by the information technology department are granted access to the network. This means access control is maintained by means of virtual private networks, robust firewalls, multi-factor authentication and network monitoring. As organizations work to maintain business agility in remote work environments, these standard controls only become more difficult to maintain.

In addition, there are several known threats that have arguably been exacerbated by remote work. Business email compromise (BEC) schemes are major threats to organizations and continue to evolve as we get more savvy to the specific fraud indicators.

BEC schemes remain the biggest threats perpetrated using phishing attacks. The earliest and still very prevalent type of BEC scheme entails spoofing or hijacking of an executive's email address which is then used to target individuals who are authorized to send wires or automated clearing house (ACH) payments on behalf of the company. This scheme resulted in billions of dollars in lost revenue, but it has been running for over a decade, and the revenues derived from phishing may be tailing off as awareness grows. However, fraudsters are nothing if not adaptive.

The scheme referenced above is being supplanted by a more sophisticated form of BEC, known as "invoicing schemes." While there are a few variations, they all revolve around a central theme. Instead of impersonating executives, the threat actors impersonate vendors who interact regularly with the victim company. The fraudsters gather enough information through social engineering and malware to correctly conclude the target company owes a payment to the company they are spoofing, and then impersonate someone from the vendor or supplier and provide new (fraudulent) payment instructions.

Discovery of the fraud usually occurs well after the misdirected payment already occurred, often when the legitimate vendor starts to ask about the status of their past-due receivable. Organizations are even more susceptible to BEC schemes now than before the pandemic. Prior to widespread remote work, people could physically walk down the hall to the executive from whom the spoofed email appeared to originate and simply ask, "Did you send this?" Similarly, a payables manager who received a call or an email instructing them to change the payment instructions could ask a colleague or their boss, "Is this ok?" without having to call or email someone for advice.

Amplified opportunity

Fraudsters can commit their bad deeds because they are in a position of trust. Occupying a position of trust creates an opportunity to commit fraud. "Opportunity" is an important part of the often cited "Fraud Triangle," coined by noted criminologist Donald Cressey. Opportunity, along with "rationalization" and "pressure," make up the three sides of the Fraud Triangle, which represent the perfect storm for fraud.

When working remotely, without colleagues to overhear them or supervisors to observe their behavior, unscrupulous people can fully exploit their position of trust with far less concern of drawing attention.

While there are technology tools to monitor email, firewall logs and productivity, the lack of the "neighborhood watch" phenomenon that exists in a traditional work setting serves to amplify fraudsters' ability to take full advantage of their position of trust without fear of detection.

Training and professional certification fraud

At first glance, this category may not seem significant. And yet, falsifying continuing practice education or compliance training can result in serious consequences for organizations and the individuals involved.

Training and ongoing communications are hallmarks of effective compliance programs. Many professional licenses and certifications require a certain amount of training hours each year to maintain credentials and allow the individuals to continue to use their professional certifications and practice in their profession. Having others take exams for people, stealing and distributing copies of exams and otherwise circumventing the continuing practice education requirements of a profession can lead to long-term damage.

Remote work decreases the likelihood of discovery and may even play into participants' fraud triangle rationalization because of a belief that no one will ever know, or that faking training is harmless.

Increased confidential reporting and associated resource strains

According to the 2023 NAVEX Hotline & Incident Management Benchmark Report, confidential reporting is at an all-time high. After a brief uptick in reporters' willingness to identify themselves in confidential reporting during 2021 and the Great Resignation, reporters reverted back to reporting on a confidential basis more frequently, possibly signaling growing concerns over retaliation and general anxiety about remaining employed while still raising red flags.

Another important data point is that employees increasingly are looking at confidential reporting channels as a "lifeline" when dealing with personal struggles that may or may not relate directly to their work lives. Human resources and compliance personnel are increasingly working together to monitor the increased use of confidential reporting channels as unofficial crisis hotlines. As mental health issues stemming from the pandemic, financial uncertainty, and feelings of trauma from loss and isolation continue to unfold in the workforce, monitoring the sentiment coming through via hotline reports will remain an important endeavor.

Confidential reporting and investigations are one the hallmarks of an effective compliance program, and organizations must ensure there are sufficient resources allocated to review reports, triage immediate issues, and investigate reports warranting further review. Given the rise of mental health-related reports, this serves as an important reminder about the importance of sufficient resources to perform timely assessments and investigations, and the need to monitor and respond to the emergence of trends in the data.

Opportunity, along with "rationalization" and "pressure," make up the three sides of the Fraud Triangle, which represent the perfect storm for fraud.

Investigation limitations

Confidential reporting and investigations are inextricably intertwined. Reporting channels must include the ability to perform appropriate and timely investigations. Traditionally, investigations are conducted covertly until they reach an inflection point when it is time to start interviewing people and widening the circle in terms of who needs to know.

Prior to the advent of remote work, witness interviews were almost always performed in person. Likewise, records review, email collection and the forensic imaging of external storage devices, laptops and phones occurred in person. Remote work caused a tectonic shift in how investigations are conducted, and in-person investigations are no longer the norm.

While many authoritative studies suggest body language is not a reliable predictor of deceptive behavior, most investigators will still tell you in-person interviews are best – particularly when conducting admission-seeking interviews.

Physical cues are not as readily noticeable when conducting a virtual interview, and video conference interviews are far more likely to result in an abrupt end. In this case, there is no substitute for being in the same room for this type of conversation.

Despite the less-than-optimal phenomenon of remote investigations, investigators had to adapt – and adapt they have. Interviews performed via video conference are the norm, and the same is true with depositions and other legal and judicial proceedings. Aside from the occasionally hilarious mishap, the world settled into this new two-dimensional paradigm, and it is working well.

A silver lining to this for the investigators themselves and the organizations that must perform them is this: remote investigations are more efficient, less expensive and less resource intensive. They also result in reduced travel costs and freeing up of investigators, who can then carry a higher investigative case load. Even computer forensics can be completed fully remotely. Hard drive contents can be digitally imaged over the network without the need to physically lay hands on the device, and emails can be exfiltrated from the server or cloud storage and transferred utilizing secure file transfer protocols.

2024 prediction

How can we use the past three years to predict the future of matters requiring investigation and investigations themselves?

Progressive organizations will pay close attention to their own data and published trends to proactively address the emergence of increased susceptibility to fraud, new fraud exploits, red flags signaling the erosion of ethical culture, and the uptick in mental health issues. Leadership teams and middle management will be more proactive in seeking to engage remote workers.

Just like CEOs had to move away from fence straddling on social issues and take a stand on the important issues affecting their employees, customers and communities, so will they step forward and acknowledge the challenges of this new paradigm. This re-engagement of the workforce is the most important step of what will likely be a multi-step process, and will also entail empowering everyone to take ownership of creating a safe and ethical workplace.

Indeed, making sure everyone in the organization feels heard, supported and empowered to act ethically could head off at least some of the next round of fraud and misconduct.

About the author

Scott Moritz
Scott Moritz is the president of White Collar Forensic LLC, a boutique investigative, forensic accounting and compliance advisory firm providing turnkey investigative, financial analytical and compliance advisory services.

Mr. Moritz served as an FBI Special Agent from 1986 to 1996 serving in the Memphis, Tennessee and New York City field offices. Since leaving the FBI, Mr. Moritz has led and been involved in some of the most high-profile white-collar crime, money laundering and corruption investigations on behalf of some of the world's largest companies and their counsel. He is widely regarded as an expert in the performance and governance of internal investigations, forensic accounting analyses and regulatory compliance program remediation projects with domain expertise in the Foreign Corrupt Practices Act, USA PATRIOT Act and the Committee of Sponsoring Organizations of the Treadway Commission ("COSO") Fraud Risk Management guide.

NAVEX is trusted by thousands of customers worldwide to help them achieve the business outcomes that matter most. As the global leader in integrated risk and compliance management software and services, we deliver our solutions through the NAVEX One platform, the industry's most comprehensive governance, risk and compliance (GRC) information system.

For more information, visit NAVEX.com and our blog. Follow us on X and LinkedIn.

AMERICAS

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navex.com
www.navex.com
+1 (866) 297 0224

EMEA + APAC

1 Queen Caroline Street
London, W6 9YN
United Kingdom
info@navex.com
www.navex.com/uk
+44 (0) 20 8939 1650

NAVEX®