



Top 10 Risk & Compliance Trends for 2023

A NAVEX
EBOOK

Table of Contents

3	Introduction SEAN THOMPSON
6	The Whistleblower Landscape – Reporting Trend Changes May Compel Organizations to Reassess Their Programs JANE NORBERG, CARRIE PENMAN
13	The Next Era of R&C Management: Data-Informed Decisions Through Digital Transformation A.G. LAMBERT
18	EU Whistleblowing Directive – Trends in Transposition and Adoption MARK ROBERTSON
22	Privacy in 2023 – What to Expect and How to Prepare JAMES CASTRO-EDWARDS, NANCY PERKINS
29	Addressing Risk, Compliance & Integrity in the Extended Enterprise MICHAEL RASMUSSEN
34	Third Party Risk in the Era of Sanctions Enforcement MICHAEL VOLKOV
38	New Expectations of Executive Leadership – How Will You Prove and Certify Your Program Works MATT KELLY
42	Joining Forces with Learning and Development Will Improve Ethics and Compliance Education INGRID FREDEEN, MEGAN TORRANCE
48	This Supreme Court Case Will Reverberate Throughout the Compliance and ESG World KRISTY GRANT-HART
53	Staying Ahead of ESG Disclosures – What to Expect and How to Prepare COLIN ETNIRE

Introduction



BY: SEAN THOMPSON
President and CEO, NAVEX

It is no secret that managing a truly effective governance, risk and compliance (GRC) program is challenging, and becoming more so every year. It starts with an increasingly complex regulatory environment but does not end there. Successful leaders also understand that customers, employees, and other stakeholders will reward organizations for operating ethically and reject those that do not. In short, leaders must recognize that operating with integrity is just as important as complying with regulations. So, it is fitting these factors would inform NAVEX's Top 10 Trends in Risk and Compliance this year.

With the twin pillars of **regulations** and **integrity** as guideposts, NAVEX consulted with industry experts – including several of our own thought leaders – to compile this annual assessment. It delivers their best thinking about what GRC professionals and other leaders should consider and prepare for in 2023.

With respect to regulations, the only constant is change. Sometimes the direction is clear, or at least consistent with expectations. For example, the following examination of the EU Whistleblower Directive lays out what is in place today, and what to expect as each EU country transposes. However, when it comes to the growing desire to codify environmental, social and governance (ESG) standards, we found the expectations are far less clear, with more confusion than consensus.


On the topic of business integrity, there are clear indicators that GRC professionals' responsibility for maintaining a resilient, ethical corporate culture will intensify. Going forward, this will extend well beyond the organization's employees and facilities to include suppliers and other business partners. The recognition that third-party risk is also your risk is accelerating. Our examination shows that successful GRC programs address this additional risk – not just during the supplier selection process, but continuously thereafter. Taken together, these trends show a growing focus on regulatory compliance via creating a culture of integrity. This continued focus, and the ongoing challenges of meeting regulatory requirements,

will undoubtedly elevate the Compliance function – positioning the role as even more critical to an organization’s long-term success than ever before.

On the topic of business integrity, there are clear indicators that GRC professionals’ responsibility for maintaining a resilient, ethical corporate culture will intensify.

But perhaps the most encouraging trend identified this year is the growing demand for more and better GRC data. This is driving a digital transformation in our industry. More organizations are using sophisticated GRC information systems to collect and analyze relevant data that helps inform decision making and achieve better outcomes. We expect this trend to continue for years to come.

Finally, we expect that some of the trends identified in this report may contradict current assumptions, while others will confirm suspicions. Regardless, we hope this year’s guide will provide valuable insight for any and all GRC professionals dedicated to meeting the challenges ahead.

A photograph of two women in a modern office hallway with large glass windows. The woman on the left, wearing a blue patterned sweater and jeans, holds a tablet and points at the screen. The woman on the right, wearing a grey sweater, an orange skirt, and headphones, holds a laptop. The background shows a glass railing and a view of trees outside. The image is partially overlaid by a dark teal rectangle on the left and orange rectangles at the bottom right.

"More organizations are using sophisticated GRC information systems to collect and analyze relevant data that helps inform decision making and achieve better outcomes. We expect this trend to continue for years to come."



The Whistleblower Landscape—Reporting Trend Changes May Compel Organizations to Reassess Their Programs

BY: JANE NORBERG

Partner, Arnold and Porter

CARRIE PENMAN

Chief Risk and Compliance Officer, NAVEX

Until recently, trends in whistleblower reports and behavior seemed to only break through into the news cycle when an extraordinary story made it into mainstream headlines. Now, reports of whistleblower actions and payouts are more frequently making news, and regulations protecting whistleblowers continue to take effect globally.

First, while legislatively protected whistleblowing for certain types of issues has been in place in the U.S. for some time, the international regulatory landscape is even more prescriptive than the U.S. on process and whistleblower protections. Ongoing global legislation, such as the EU Whistleblower Directive, Japanese Whistleblower Protection Act, and the Australia Corporations Act, is impacting organizations' processes to receive, investigate and follow up on reports. Keeping up with the new regulations is proving to be challenging, especially for organizations with multinational operations.

Second, tips to, and awards paid by, the Securities and Exchange Commission (SEC) Office of the Whistleblower are setting records and getting attention from both employee reporters and their organizations. Further,

a growing industry of plaintiff-side whistleblower attorneys feeding tips to the SEC and other agencies is capturing the attention of those who believe they haven't been heard internally or fear significant retaliation for raising a concern.

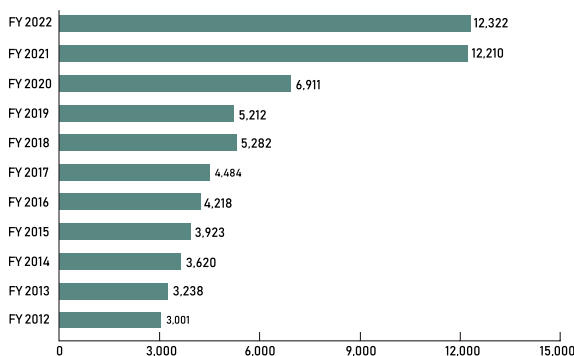
Add all of this to stresses and workplace changes resulting from the pandemic and remote work environments, and compliance programs are experiencing a changing whistleblower landscape. The recent SEC Annual Report, and data from over 1.4 million reports annually to NAVEX systems, provide some insights to help organizations understand the changing whistleblower landscape – both internally and externally – and prepare them to adjust their programs to address the changing landscape.

External reporting trends

On November 15, 2022, the SEC Office of the Whistleblower issued its [annual report for FY 2022](#). The same day, the [SEC announced](#) its enforcement results for FY 2022, which highlighted the Office of the Whistleblower as “an integral part of the Enforcement Program,” and the whistleblower program as a critical tool in the SEC's enforcement arsenal. Both SEC reports reveal that whistleblower tips are an increasingly important source for SEC investigations and enforcement actions.

The SEC reported receipt of 12,322 whistleblower tips in FY 2022. This was the largest number of tips received in any year in the history of the SEC's whistleblower program, which was established in 2011 following the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

During the two prior fiscal years, there were dramatic increases in the number of tips received. From FY 2020 to FY 2021, there was a 76% increase in whistleblower tips received by the SEC, and FY 2022 yielded a similar number of reports as the previous year. The chart below illustrates this stark increase in reporting to the regulator.



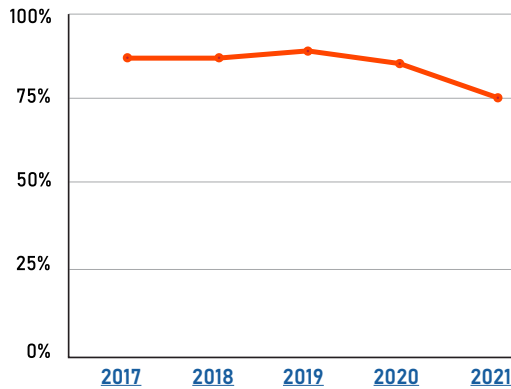
Although the reason for the increasing number of tips is not clear, one possible explanation is the prevalence of remote and hybrid working conditions that makes it easier for whistleblowers to gather evidence and report out to the SEC – such as taking screenshots of documents or emails. But even as many companies began to require a return to the office in some capacity, the number of tips reported out to the SEC remained very high and may reflect a “new normal.”

Global whistleblowing to the SEC – regulatory action and trends

As in prior years, the SEC's whistleblower program continues to have a global reach. According to the FY 2022 Whistleblower Report, tips were received “from all over the world,” with the highest number of foreign tips originating from Canada, the United Kingdom, Germany, China, Mexico, and Brazil. All told, the SEC received tips from over 130 countries worldwide since the beginning of the program. Companies should consider that employees in international operations may be inclined to report out to the U.S. regulator if they do not believe action is being taken internally to address their concerns. Therefore, policies and procedures around handling of internal reports need to encompass international operations as well.

Whistleblowers report internally prior to reporting to SEC

It is important to understand that most whistleblowers who received awards from the SEC first tried to raise their concerns internally or at the same time as reporting to the regulator. In fact, according to the [2021 SEC Annual Report to Congress](#), “more than 75% raised their concerns internally to their supervisors, compliance personnel, or through internal reporting mechanisms, or understood that their supervisor or relevant compliance personnel knew of the violations,” before reporting their information of wrongdoing to the commission. This represents a downward trend from 2020. Unfortunately, the SEC did not report this figure for 2022, however, historical information is illustrative of this trend.



Large whistleblower awards equal large corporate impact

The increase in tips may also be due to the very large whistleblower awards paid by the SEC. In FY 2022, the SEC awarded approximately \$229 million in 103 awards. Over the life of the program, the SEC paid out over \$1.3 billion in whistleblower awards. Of course, large whistleblower awards equate to large corporate impact. Successful enforcement actions brought as a result of whistleblower tips yielded more than \$6.3 billion in total monetary sanctions ordered since the beginning of the whistleblower program, including more than \$1.3 billion during FY 2022 alone. The incentives for whistleblowers to report out potential misconduct remains high, as does the cost to companies based on external whistleblower tips.

The SEC also announced a focus on large penalties to effectively punish and deter misconduct. They noted they will reward meaningful cooperation and remediation.

Proper handling of an internal tip from an employee is the first step towards potential remediation and cooperation credit. Conducting a thorough internal investigation and engaging in appropriate remediation can help position a company to respond effectively to an enforcement investigation and minimize potential sanctions.

Internal reporting trends

Recent years have shown changes in internal reporting trends as well. For example, organizations saw a continuous decline in anonymous reports before and during the pandemic, indicating employees are becoming more confident or emboldened to give their name. NAVEX reporting over the last two years also shows the profound impact of the pandemic and remote work on outcomes such as “The Great Resignation.” As of the end of 2021, internal reporting levels had not yet returned to pre-pandemic levels, yet, as described above, external reporting to the SEC has seen substantial growth. We expect to see internal reporting levels approach pre-pandemic levels when we publish the report for 2022.

Noting that many compliance programs view human resource matters as “not compliance issues,” it may be time to raise the profile of these types of matters within the compliance program and partner closely with human resource teams who we know are already well-aware of the increase in mental health issues facing their organizations.

We also observe that issues related to workplace behavior and civility are increasing. In 2021, internal reports of retaliation nearly doubled. Reports about whistleblower retaliation have always been a small portion of the total, but they shot up from 0.9% in 2020 to 1.7% in 2021. Reports about harassment also rose (to 5.6%, an all-time high) as did reports about discrimination (to 4.7%). Taken altogether, these findings suggest employees are more attuned to workplace civility issues. That would fit with external trends such as more talk about systemic racism, income inequality and political divisions, as well as increasing protection for whistleblowers and employees' awareness of those protections.

Keyword searches of reporting data show that other social and political issues are becoming topics for internal reporting, too. For example, issues such as the war in Ukraine and economic concerns around inflation, a potential recession, layoffs, stimulus, and student debt forgiveness are on the rise.

There is also a concerning increase in matters of workforce sentiment and mental health found in the keyword searches including anxiety, depression, exhaustion, mental health, pressure, quiet quitting, and bullying cases. Internal reporting systems serve as an emotional lifeline in some cases. Noting that many compliance programs view human resource matters as "not compliance issues," it may be time to raise the profile of these types of matters within the compliance program and partner closely with human resource teams who we know are already well-aware of the increase in mental health issues facing their organizations.

Addressing the changing landscape

To prepare for and address this changing landscape, organizations will need to test their mindset about reports and reporters (especially regarding anonymous reporters) as well as review their processes for managing cases.

For example, the ongoing economic conditions may lead to higher levels of anonymous internal reporting as employees fear retaliation for speaking up during periods of uncertainty. In our interactions with clients and customers, we continue to have conversations about the value and credibility of anonymous reports and reporters. We still hear about cases where the primary focus is determining who an anonymous reporter is rather than focusing on the issue raised. NAVEX data shows anonymous reports are substantiated at a rate close to those of named reports, indicating that while these reports may be more challenging to manage, they are valuable to our organizations.

We still hear about cases where the primary focus is determining who an anonymous reporter is rather than focusing on the issue raised. NAVEX data shows anonymous reports are substantiated at a rate close to those of named reports, indicating that while these reports may be more challenging to manage, they are valuable to our organizations.

Case closure time is another opportunity for review. The EU Whistleblower Directive sets out time limits for acknowledgement of case receipt and feedback to the reporter. We also know the directive places some

contingencies on who can view or investigate a report, adding complexity to processes that likely already have limited resources available to address. This is a good time to assess capability to handle more pressure and more complex cases. A focus on ongoing communications with reporters as well as a reduction in case closure times will help to build trust in internal programs which, in turn, may help reduce external and anonymous reporting.

One other program component worthy of attention is managing fear of, and preventing, retaliation. As noted earlier, cases of retaliation are on the rise. Yet, according to [NAVEX survey results](#), retaliation prevention is not a high-priority initiative for many organizations. The reasons for this disconnect are not clear as the purpose of much of the legislation we described earlier is to protect whistleblowers from retaliation. Indeed, the SEC recently filed an amended complaint [against the CEO of a company for retaliating](#) against an employee who raised concerns within the company, and also for attempting to impede that employee from reporting to the SEC by cutting off their access to the company's IT system, among other things.

Perhaps most concerning though, we expect to see continued growth in reporting of workplace civility issues including harassment, discrimination and retaliation, as the stresses and pressures of the ongoing political and economic climate continue. Organizations will also need to prepare for the internal reporting system to be used more often for social and personal mental health issues as the stress and exhaustion of the last few years continue. While these may not all be, by definition, "compliance issues," they certainly impact a culture of compliance.



2023 prediction

Whistleblowers (reporters) have shown in recent years they are more willing to take their concerns outside the organization if the issue is not addressed in a timely and appropriate way, as evidenced by the high levels of reporting to the SEC Office of the Whistleblower as well as the growth of social media sites like Glassdoor.

With the potential for a recession in 2023, we expect to see continuing changes in trends for both internal and external reporting. Further, as more countries pass legislation to protect whistleblowers, we expect to see a continuing shift in the number and types of reports that both organizations and external regulatory agencies receive. Particular attention is needed on retaliation prevention programs. Now is the time to step back and take stock of the changing reporting and regulatory landscape. If not, we could see external reporting escalate as the first option for whistleblowers. Further, taking a more holistic view of the individuals we rely on to maintain, and report on, compliance will serve our organizations well.

About The Authors

Jane Norberg | Partner, Arnold and Porter

As the former chief of the Office of the Whistleblower at the Securities and Exchange Commission, Jane Norberg brings her extensive experience to help clients navigate regulatory, enforcement, governance, and compliance issues associated with whistleblowers. As a former senior officer in the Division of Enforcement at the SEC and a former special agent with the United States Secret Service, Ms. Norberg also brings her unique background and insights to assist clients in bringing regulatory and governmental inquiries to a successful resolution.

Ms. Norberg represents public and private companies, financial institutions, individuals, and investment advisors on sensitive whistleblower and other complex matters, including internal and SEC and other government investigations; response to and defense of specific whistleblower allegations; securities enforcement and white-collar defense; whistleblower retaliation claims defense; proactive assessment and structuring of internal compliance mechanisms, policies and procedures; training boards of directors, management and workforces on internal reporting and retaliation; and crisis management counseling to mitigate reputational risk. Ms. Norberg also conducts sexual harassment and other sensitive investigations and educates boards of directors and executives about emerging whistleblower programs such as the Anti-Money Laundering Act whistleblower program and NHTSA automotive whistleblower program.

During Ms. Norberg's tenure at the SEC – she joined the SEC in 2012 as deputy chief of the office and was appointed to chief in 2016 – she helped develop and lead the SEC's whistleblower program since near its inception. Under her leadership, the office's staff expanded and achieved a record-breaking growth in both the number of whistleblower tips received and awards issued to whistleblowers under the program.


Ms. Norberg has extensive experience and knowledge regarding whistleblower retaliation and is the leading expert on agreements that impede reporting in violation of Exchange Act Rule 21F-17, having directly advised on all whistleblower protection cases brought by the SEC during her tenure. She advised senior SEC leadership on emerging whistleblower issues and policies, as well as reported to Congress regarding the program's activities. Ms. Norberg also had a substantial advisory role related to the amendments to the SEC's whistleblower rules and has advised other domestic and international regulators related to the development of new whistleblower programs. While at the SEC, Ms. Norberg also co-led a diversity and inclusion initiative across the Division of Enforcement.

Carrie Penman | Chief Risk and Compliance Officer, NAVEX

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.



"To prepare for and address this changing landscape, organizations will need to test their mindset about reports and reporters (especially regarding anonymous reporters) as well as review their processes for managing cases."

The Next Era of R&C Management: Data-Informed Decisions Through Digital Transformation



BY: A.G. LAMBERT
Chief Product Officer, NAVEX

The term “digital transformation” has been a topic of conversation for decades as organizations continue their path to modernization and optimization. This transformation is indeed a journey, including migration to cloud-based infrastructure, shoring up cybersecurity measures, implementing software solutions to provide valuable insights, and more. As digital transformation continues, it is no surprise that the most successful businesses today rely on a host of technological solutions to run day-to-day operations.

Managing risk and compliance across an organization is an area where digital transformation can provide a wealth of benefits. By embracing digital transformation of ethics and compliance programs, organizations are better able to evaluate the cultural health of the company, remove information silos, increase collaboration and eliminate redundancies in technology. Leading organizations leverage the immense value in data derived from ethics and compliance programs to create efficiencies and gain a better understanding of the company culture.

Simplify the complexity of data management

The amount of data any given organization produces can be overwhelming. When thinking of just the ethics and compliance data, this includes information such as hotline reports and related investigation outcomes, training and policy completion and attestation, conflict of interest disclosures, third-party supplier compliance (including sanctions compliance) – and that is just the tip of the iceberg. When these data points are woven together, we begin to see the story this tells about the culture and compliance health of the company. Further, we’re seeing a growing appetite for using these data points to benchmark against peers and present to executive leadership.

However, for many organizations, this data is being managed – but often this is done through siloed systems and multiple software solutions. Simply put, the vast array of data is far too complex for manual analysis and management. To do so via spreadsheets and emails will inevitably lead to something critical being overlooked. As an organization grows in employee count or to other geographies, this

problem gets exponentially more complex. The challenge this presents is twofold – the diminishing ability for inadequate tools to achieve even the bare minimum of data management for the expanding organization, and the growing difficulty of analyzing that data for any meaningful insight.

Given the breadth of this information, simplifying the complexity of governance, risk and compliance (GRC) data requires a consolidated information system, or GRCIS. More and more, we're seeing organizations that seek to gain a holistic understanding of GRC information migrating towards a consolidated platform to take advantage of the insights provided from ethics, compliance and risk data. Additionally, with increased requirements being imposed by the U.S. Department of Justice and other global regulatory bodies, having access to program data, and using that data to actively manage compliance risks, is vital to prove program effectiveness.

Arguably, the most important aspect of consolidating data from risk and compliance programs into a usable format is the ability to tell a story to leadership, employees and other stakeholders. When this data is scattered across multiple owners and resides in different systems, telling that story is made difficult. Most boards of directors receive periodic reports about compliance matters – in fact, 70% of respondents to [NAVEX's 2022 Definitive Risk & Compliance Benchmark Report](#) survey indicated this is the case – so being able to consolidate this data is imperative to telling the story.

Reduce cost and remove silos

Most organizations today have to deal with silos in at least some parts of the business – and the larger the organization, the more likely this is to happen. Further, for large enterprises, there is more likely going to be a robust tech stack collecting data from across the organization. While technology solutions are vital to business operations, too many solutions can inadvertently silo data and increase costs to the business. Throughout the journey of digital transformation, many organizations have continued to add solutions to their technology portfolio in hopes of gaining better insight and increasing efficiency. In some cases, it is years before leadership realizes all this has done is increase cost, create silos of information, and decentralize critical information.

While this conundrum applies to many departments in a given company, let's focus on GRC specifically. We're seeing a growing appetite for the consolidation of information related to ethics and compliance programs and risks, including hotline reporting, training, policy and procedure management, COI disclosure, third-party compliance, and more. Removing these silos is an important goal, and a much needed one for many organizations where compliance responsibilities are split across multiple departments – which accounts for 21% of the respondents to the 2022 NAVEX survey benchmark. A thoughtful and mature GRCIS can manage the wealth of data mined from these areas, thus reducing cost and removing the silos.

We're seeing a growing appetite for the consolidation of information related to ethics and compliance programs and risks, including hotline reporting, training, policy and procedure management, COI disclosure, third-party compliance, and more.

This is particularly helpful because the data within each area can be consolidated to paint a picture of the cultural health of the organization. While small- and medium-sized businesses tend to have fewer silos and fewer resources, large enterprises tend to have more silos and resources. In either case, businesses of all sizes greatly benefit from a consolidation of GRC program data from the cost savings and the elimination of siloed information.

Decrease redundancy and increase efficiency

Since budgets are typically allocated on a by-department basis, we'd be hard pressed to find an organization today that didn't have some redundancies in their technology portfolio. In years past, compliance programs were widely operating in shared drives with spreadsheets and email communications as the predominate method of management. Now, we're seeing an appetite for analytics and efficiency built into software solutions – something that is likely to increase as the potential for a recession continues to loom.

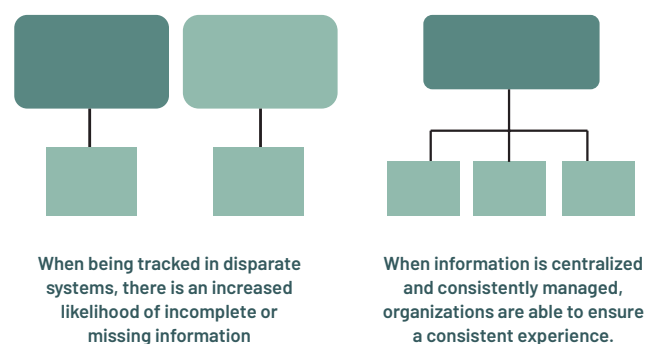
According to a global survey of over 1,400 IT professionals conducted by [Spiceworks Ziff Davis](#), even though half of surveyed organizations plan to take precautionary measures to prepare for economic slowdown, 51% are still planning to increase IT budgets in 2023. Also, according to the survey, common preparations for an economic downturn include “re-evaluating vendors or contracts”, and “decommissioning unnecessary infrastructure.”

While technology spending may be on the rise, it's clear that most organizations must make these choices thoughtfully and not simply add solutions to the tech stack. In this same survey,

26% of respondents indicated “consolidating redundant tech” as one of the measures their organization is taking to prepare for a potentially turbulent economy in 2023 and beyond. While this percentage may appear smaller than expected, when combined with “re-evaluating vendors or contracts” (30%), “strategic refocusing” (28%), and “adapting products or services” (26%), it is clear organizations are focused on decreasing redundancy and increasing efficiency.

There are several areas of overlap within GRC programs and other departments where redundancy can be reduced. For example, while compliance training is traditionally handled by the chief compliance officer or equivalent, employee onboarding is usually the purview of human resources. So, in this example, if completion and attestation for HR and Compliance trainings are being tracked in disparate systems, there is an increased likelihood of incomplete or missing information. Another common example is policy management, which, for many, is managed with emails and shared drives. The version control predicament this can create is not only inefficient, in some cases it can be dangerous (e.g., in a healthcare scenario where following proper procedure can be a life-or-death situation).

However, when information is centralized and access and version control is consistently managed, organizations are able to ensure a consistent experience – all while eliminating redundant information and creating a more efficient workflow.



2023 prediction

Increased regulatory enforcement for compliance infractions and growing public attention to how businesses operate will cause organizations to prioritize their ethics and compliance efforts. This is especially salient to compliance officers who are being asked to prove their program works in practice. The required level of transparency will require data from across the company in order to effectively tell the story to regulators, stakeholders, employees and the public. As organizations prepare for an economic downturn, the emphasis on efficiency will play a large role in how technology is evaluated.

Public attention is also likely to stay focused on how organizations operate – including misconduct, supply chain and third-party integrity, data security, and more. All of these forces combining means organizations will prioritize using digital solutions to monitor

the metrics that matter and take the data yielded to demonstrate their accountability and compliance. In this turbulent, 24/7 news cycle environment, companies that do the right things the right way will yield better results in the long term – and those that fail to prioritize ethics and compliance as a cultural pillar will eventually face regulatory enforcement and reputational damage. To that end, consolidating data from GRC programs and using it effectively will be key to enhancing cultural health within organizations and maintaining regulatory compliance as those requirements evolve.

About The Author

A.G. Lambert | Chief Product Officer, NAVEX

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, Extensify 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.



"Increased regulatory enforcement for compliance infractions and growing public attention to how businesses operate will cause organizations to prioritize their ethics and compliance efforts."

EU Whistleblowing Directive – Trends in Transposition and Adoption

BY: MARK ROBERTSON

Deputy Compliance Officer and Senior Counsel, NAVEX



It has now been three years since the EU whistleblower protection directive (“Directive”) entered into force. The Directive’s minimum standards are certainly no great mystery at this point – entities meeting the fifty-worker threshold must establish internal reporting channels and procedures for the receipt of whistleblower reports and protection of the whistleblower against retaliation.

What remains a challenging unknown, however, is the extent to which each member state’s transposition of the Directive meets or exceeds the Directive’s minimum standards. This is because of the staggered cadence of legislative enactments by EU member states and the failure of many member states to enact legislation at all. Now one year overdue, as of this writing, there remain 13 member states that have yet to transpose the Directive into national law. Multi-national organizations tasked with developing a harmonized approach to whistleblower reporting across the EU must do so with an incomplete picture of the legislative landscape.

But as we move into 2023, there is hope that this picture will be filled in. The majority of the 13 member states yet to transpose have published draft bills that are at various stages of the legislative process. The proposed bills provide a look at how these nations may codify

the Directive’s minimum standards. While the timelines of the enactments may differ among these nations, perhaps there exists some shared urgency as a result of the European Commission’s commencement of [infringement proceedings](#) against these member states (as well as some that have transposed, though only partially or untimely, as the European Commission tells it).

Despite the delayed progress across the EU, there are lessons to be taken from the Directive itself and the national laws that have been enacted in the past year.

Shared resources

One of the most impactful requirements of the Directive is for entities with 50 or more workers to establish internal reporting channels and designate an impartial person or department to perform the follow-up, which includes any resulting investigation. The Directive makes allowance, however, for entities with 50 to 249 workers to “share resources as regards the receipt of reports and any investigation to be carried out.” This ability to share resources was included in the Directive specifically because the commission was “mindful of the more limited resources of medium-sized companies . . . and with a view to helping them meet their obligations under the Directive.”

Thus far, we have seen nations that have transposed likewise be mindful of the potential resource strain in this regard and have incorporated this resource-sharing carve out in favor of medium-sized entities. For example, the national laws of Cyprus, Denmark, Ireland and Portugal all include express allowance for medium-sized entities to share resources in this limited respect. Spain's draft law legislation also includes this allowance in its present state. As more nations transpose, we can expect to see further adoption of this resource-sharing carve-out for medium-sized entities.

Initial assessments and additional communications to whistleblower

The Directive describes two distinct points in time when the receiving entity must communicate with the whistleblower. First, there must be an acknowledgement of receipt of the report sent to the whistleblower within seven days of report receipt. Second, the entity must provide "feedback" to the whistleblower within "a reasonable timeframe . . . not exceeding three months from the acknowledgment of receipt." This general framework – written acknowledgement followed by feedback – is apparent in the transpositions thus far.

These examples highlight the need to monitor each member states' draft and enacted legislation. As more member states transpose the Directive into national law, we may see additional nuances introduced that affect how organizations perform report intake and assessment and communicate with reporters.

There have also been additional steps required at the national level, including an initial assessment of the report and further communications to the reporter. For example, Ireland and Latvia both establish an obligation for the receiving entity to perform an initial assessment of the report and to communicate the results of that assessment to the reporter.

In the case of Ireland, the assessment should consider "whether there is prima facie evidence that a relevant wrongdoing may have occurred." Under the Latvian transposition, the assessment is to include a decision whether to recognize the report as a whistleblower report. Under both laws, the assessment is to be communicated to the reporter. Ireland also introduced a continuing obligation to communicate status updates to the reporter, if requested. These further communications are to occur "at intervals of three months."

These examples highlight the need to monitor each member states' draft and enacted legislation. As more member states transpose the Directive into national law, we may see additional nuances introduced that affect how organizations perform report intake and assessment and communicate with reporters expect to see further adoption of this resource-sharing carve-out for medium-sized entities.

Effective, proportionate and dissuasive penalties take shape

The Directive addresses at least one topic merely by describing the desired outcome, rather than through prescriptive rules defined by rigid timelines or worker counts: Penalties.

No specific punishments or monetary sanctions are set forth in the Directive. Rather, the Directive mandates member states "provide for effective, proportionate and dissuasive penalties applicable to natural or legal

persons” for hindering reporting, retaliation, bringing vexatious proceedings, and breaching the duty of confidentiality, and, in the case of reporters, for knowingly reporting false information.

This aspect of the transposition process has been keenly watched by industry observers to see what level of personal and entity liability is established. To date, the national laws have responded to this mandate in a few ways.

Some member states have established ranges of monetary fines that correspond to different violations. Portugal, for example, grouped violations into two tiers: serious offenses and very serious offenses. The latter, unsurprisingly, paired with the higher ranges of potential fines (i.e., €1,000 to €5,000 for natural persons and €2,000 to €50,000 for legal persons).

However, financial penalties against individuals are just one possible penalty under the Irish law. It provides – at least technically – for imprisonment of up to two years. One would have to think that imprisonment for violation of the duty of confidentiality would be a punishment reserved for the most malicious of intentional disclosures, but on the face of it, there is no element of scienter. In any event, consider this author dissuaded. The Irish law also creates two private rights of action.

A reporter may bring an action in tort against an individual who discloses the reporter’s identity to someone unauthorized to know it. Likewise, an individual may bring a tort action against a reporter who knowingly reports false information about the individual.

These penalties likely suggest more of what is to come when the remaining member states transpose the Directive. It seems safe to assume that financial penalties will be available in future transpositions against both individuals and entities when there is retaliation or a breach of confidentiality in which the reporter’s identity is made known beyond those authorized to know it.

2023 prediction


The coming year will continue to present challenges for organizations working to harmonize internal whistleblower programs across multiple EU members states, where some have transposed the Directive into national law and others have not. Organizations may wish to design or modify their programs to conform to the most protective of the national laws and, in any event, should ensure their programs are responsive to the Directive’s minimum standards. We can reasonably expect more member states will transpose the Directive in 2023, but whether it is all delinquent member states or just some remains an open question.

About The Author

Mark Robertson | Deputy Compliance Officer and Senior Counsel, NAVEX

Mark maintains the company’s risk and compliance program and advises the company on a wide array of legal matters, including intellectual property, compliance, employment, litigation, commercial transactions, and product development.

Prior to joining NAVEX, Mark was in private practice, representing artists, entrepreneurs, and performing arts organizations in the music business. Mark earned his J.D. from Loyola Law School, Los Angeles and served as editor-in-chief for the Loyola of Los Angeles Entertainment Law Review. He received his B.A. in communications from the University of Puget Sound.



"The coming year will continue to present challenges for organizations working to harmonize internal whistleblower programs across multiple EU members states, where some have transposed the Directive into national law and others have not."



Privacy in 2023 – What to Expect and How to Prepare

BY: JAMES CASTRO-EDWARDS

Counsel, Arnold and Porter

NANCY PERKINS

Counsel, Arnold and Porter

U.S. legal trends

Privacy law compliance in the United States today demands resilience, flexibility, and responsiveness. To date, the U.S. Congress has failed to enact broadly applicable privacy standards to govern companies uniformly nationwide. Seeking to fill the gaps in existing privacy regulation, the states are rapidly taking action, with one state in particular, California, leading the charge with a continually expanding set of privacy-related requirements to protect individuals residing in the state. California's initiatives have triggered other states to follow suit. In just the past two years, four other states enacted new consumer data privacy laws, all of which are scheduled to take effect in 2023. However, each state's version of consumer privacy law differs in various ways from the others. This means businesses will face an ongoing challenge in juggling privacy obligations under multiple regimes.

Adding to the complexity of the states' different privacy law frameworks, the Federal Trade Commission (FTC), which has broad jurisdiction over for-profit companies operating in the U.S., initiated a potentially far-reaching [rulemaking process](#) to address what it perceives to be major gaps in privacy and security protections for consumers. At the same time, the Department of Health and Human Services, which regulates

a wide range of entities in the healthcare sector with respect to the privacy and security of protected health information, is poised to [amend its privacy regulations](#). Further, the Securities and Exchange Commission (SEC), which regulates publicly traded companies, [proposed new cybersecurity rules](#), while the federal banking agencies issued new rules for financial institutions and their services providers for [notifications of cybersecurity incidents](#).

For companies doing business in the U.S., this multifaceted privacy law environment can seem daunting. As is the case with most major challenges, a framework for formulating fundamental principles can help make compliance and data strategy more manageable. With limited resources to invest, keeping a realistic focus on significant risks, rather than getting mired in the minutia of detailed requirements, can also prove beneficial. To help navigate this complex landscape, the paragraphs below suggest a conceptual roadmap for streamlining privacy efforts.

Common state law requirements

The five states that enacted broadly applicable consumer privacy laws – California, Colorado, Connecticut, Utah, and Virginia – have all embraced certain fundamental privacy principles and concepts, including many that are at the core of the European Union General Data Protection Regulation (GDPR) (discussed below). This trend is likely to continue in additional states.

Fueled by concerns that consumers lack knowledge of, and tools to control, how their personal data are being captured (particularly online), used and shared, the five states' laws all contain provisions requiring:

- Consumers be given **notice** (descriptions of what data is collected, and why, and who it is shared with)
- **Privacy rights** (some control over the use, disclosure and retention of their personal information and means to access and amend)
- Companies to implement **privacy-by-design** (ensuring privacy is considered up front and for specified purposes)
- **Purpose limitations** (forcing companies to collect and use data in accordance with a set of appropriate and lawful purposes)
- **Security** (protection of personal data)
- That companies are **accountable** (through enforcement and complaint mechanisms, documentation requirements, and oversight and auditing requirements)
- Adopting a clear, publicly available privacy notice that describes the companies' data practices and individuals' privacy rights
- Making that notice available to individuals before collecting their personal information (wherever collection occurs)
- Adhering, without exception, to the statements in that notice, including to respect people's privacy rights
- Engaging in privacy-by-design to ensure the ethical collection and use of data (in line with lawful purposes)
- Making third-party recipients of data accountable to follow your statements about data use
- Ensuring an internal privacy program that documents compliance efforts and risk determinations and allows for monitoring and auditing of same
- Maximizing the protection of data in accordance with its sensitivity and the threats thereto

These same principles are the backbone not only of the GDPR, but also of U.S. federal regulations governing the banking industry, healthcare industry, and industries handling children's information, among others. They thus serve as a reliable framework for designing a privacy program even while the legal goalposts and guardrails for that framework are still under construction.

Following these principles will go a long way in protecting against complaints from individuals or regulators. Key practical steps to implement these principles include:

New complexities under the state laws as of 2023

Although the five U.S. states' broad consumer protection laws have fundamental similarities, the scope of California's law, the [California Consumer Privacy Act \(CCPA\)](#), is notably more expansive than the laws of the other four states. This is due to the expiration of the law's previous exemptions for personal information about employees and business-to-business (B2B) contacts (such as customer representatives and vendor contacts). Further, the [California Privacy Protection Agency](#), which was established as a new CCPA administrative and enforcement authority in 2020, recently issued detailed draft regulations implementing the amendments to the

CCPA adopted pursuant to the [California Privacy Rights Act of 2020](#) (CPRA). Businesses subject to the CCPA will have significant work to do to ensure compliance with those regulations, the enforcement of which is scheduled to commence in the third quarter of 2023.

As noted, until January 1, 2023, the CCPA exempted from most of its requirements personal information about employees and B2B contacts. Until late August 2022, it was widely anticipated that the California legislature would extend these exemptions. Given these expectations, and because the other four states' consumer privacy laws contain permanent exemptions for such information, many companies have designed their privacy programs specifically to protect the personal information of consumers with whom they deal on a personal or household basis. Adjusting to the CCPA's new scope covering employee and B2B contact information as well will be a challenge for these companies.



In addition, both under the new CCPA regulations and other states' privacy regimes, businesses will need to grapple with restrictions on, among other things:

- Uses and disclosures of “**sensitive personal data**” (as defined in varying ways)
- “**Sales**” of personal data
- Sharing of personal data, including online tracking information, for certain **advertising** purposes
- Collection of personal information of **minors**

The specifics of these restrictions, and the requirements for implementing methods for consumers to opt-in or -out of these types of processing of personal information, may be similar across certain states, and can be handled in a uniform manner, but they will not be uniform across all states. Again, this underscores the need for a flexible posture with a focus on areas of highest risk.

Data transfers – the new EU-U.S. Data Privacy Framework

A new EU-U.S. transatlantic data flow agreement is expected to be finalized by the [spring of 2023](#). The EU-U.S. Data Privacy Framework will enable the flow of personal data from ‘data exporters’ in the EU to ‘data importers’ in the U.S. who have signed up to the agreement. The Framework offers a flexible alternative to the European Commission’s Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs), which multinationals with a presence inside and out of the EU must otherwise use to share personal data (absent some small exceptions).

The European GDPR prohibits the transfer of personal data to ‘third countries’ that do not guarantee an adequate level of data protection. ‘Third countries’ are countries outside the European Economic Area. The

European Commission declared a [small number of third countries](#), such as Switzerland, Canada and Argentina as guaranteeing an adequate level of data protection. Such an adequacy finding means personal data may be freely transferred from EU Member States to the adequate third country. However, the transfer of personal data to third countries which have not been granted an adequacy finding (such as the U.S.) is prohibited, unless appropriate safeguards have been implemented. Currently, the main appropriate safeguards are SCCs and BCRs, which may be onerous to implement or expensive and time consuming, respectively.

More flexible data transfers were available in the form of the Privacy Shield and the Safe Harbor scheme, which were invalidated following the Schrems II and Schrems I decisions in 2020 and 2015 respectively. Multinationals will welcome the EU-U.S. Data Privacy Framework, which offers a business-friendly alternative to facilitate transatlantic data sharing.

In October 2022, U.S. President Biden signed an [executive order](#), which mandates legal safeguards over U.S. security agencies' use of EU citizens' personal data. This is a critical and long-awaited next step in the progress of the EU-U.S. Data Privacy Framework.

Following the U.S.'s move, the European Commission will need to make an adequacy finding, which could take as long as six months. If and when it does take effect, the Framework would operate as a replacement for the Privacy Shield.

However, Max Schrems, founder of privacy non-profit NOYB, [already expressed reservations](#) regarding the level of protection guaranteed

by the EU-U.S. Data Privacy Framework and a third challenge seems inevitable. If Schrems' third challenge repeats his earlier successes, multinational businesses' access to a flexible EU-U.S. data transfer solution may be short-lived. Only time will tell, as this plays out over the course of 2023.

UK/EU divergence – the data protection and digital information bill

In the [Queen's Speech of May 2022](#), the British government announced its intention to reform U.K. data protection law. The government previously [expressed its desire](#) to take advantage of Brexit to realize the apparently conflicting aims of creating a more business-friendly data regime that promotes growth and innovation, while continuing to protect individuals' privacy rights.

The draft [Data Protection and Digital Information Bill](#) was published in July 2022, in an effort to realize the government's intentions. Notwithstanding the government's ambitious claims, the bill amounted to little more than an evolution of the existing U.K. GDPR, rather than a radical overhaul. However, the changes the bill would have introduced regarding international data transfers potentially threatened the U.K. adequacy decision the European Commission made in June 2021. The adequacy decision enables the free flow of personal data between the EU and the U.K. following Brexit.

The European Commission may withdraw the decision if the U.K. data protection regime diverges too far from European data protection standards. Such a withdrawal would mean that organizations in EU member states would be prohibited from sharing personal data with the U.K., which would be costly and disruptive for multinational businesses with a presence in the U.K. and the EU.

The draft Data Protection and Digital Information Bill looks set to make further progress, following the [November announcement](#) at the International Association of Privacy Professionals (IAPP) Congress 2022 in Brussels by DCMS deputy director Owen Rowland that the latest consultation on the Bill will commence shortly.

The need for reform is questionable; while the U.K. GDPR may not be perfect, it is fit for purpose in striking a reasonable balance between protecting individuals' rights and businesses' interests. The British government may dismiss the GDPR as overly unfriendly to business goals for data use. Yet, it seeks to give individuals choice and control over how their personal data is used and imposes heavy penalties on organizations that fail to abide by the rules. If the U.K. government pushes ahead with its proposed reform, resulting in a U.K. data protection regime that fails to meet European standards, leading to a revocation of the U.K.'s adequacy finding, companies will face a much-increased burden to enter into an appropriate data transfer solution, as well as carry out a transfer risk assessment, for transfers from the EU to the U.K. The inevitable costs to businesses are likely to absorb at least some of the purported savings (or increased revenues from new data uses) the new legislation would make. Whether the British government will press ahead with its proposed reform remains to be seen, so the best advice to multinational businesses is to watch this space.

2023 prediction

As noted, in recent years the U.S. Congress has considered but failed to pass various forms of federal privacy legislation. The new Congress taking over in 2023 is not likely to put a significantly new face on the prospects



for passage of federal privacy legislation. Regulated entities therefore would do well to focus on the trends in the states, as well as the anticipated FTC rulemaking and the agency's ongoing privacy enforcement actions under section five of the FTC Act.

The European Commission's adequacy determination concerning the EU-U.S. Data Privacy Framework is expected imminently; whether or not it survives the almost inevitable Schrems III challenge remains to be seen. Meanwhile, U.K. businesses that trade internationally may well be hoping that the government sees sense and leaves well enough alone, rather than risking the U.K.'s adequacy decision and the free-flow of data with Europe.

About The Authors

James Castro-Edwards | Counsel, Arnold and Porter

James Castro-Edwards provides counsel on global data protection compliance projects for multinational companies, advises on data protection issues, and helps companies respond to data breach situations. He represents a broad range of clients including financial, media and technology organizations, and medical device and pharmaceutical companies. In addition to advising clients on data protection issues, Mr. Castro-Edwards has created innovative data protection support, audit and training programs for clients.

Earlier in his career, Mr. Castro-Edwards was in private practice and served as a solicitor in the data protection group at PwC Legal. He is widely published in a variety of titles, a regular public speaker on data protection issues and wrote the textbook on the EU General Data Protection Regulation (GDPR) for The Law Society.

Nancy Perkins | Counsel, Arnold and Porter

Nancy Perkins focuses her practice on regulatory compliance and consulting on emerging policy issues, with a principal focus on data privacy and security and electronic transactions. Ms. Perkins regularly advises clients on compliance with a wide range of data protection requirements at the federal and state levels, including rules applicable to online communications and transactions as well as all types of uses and disclosures of medical, financial, and other sensitive personal information. She assists clients in structuring their activities, online service offerings, and privacy policies to comply with applicable laws and best practices, taking into account technological and intellectual property issues associated with the expansion of electronic commerce and Internet activities.

Among other laws, Ms. Perkins frequently provides counsel on the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act (as amended by the Fair and Accurate Credit Transactions Act), the federal E-Sign Act, the Children's Online Privacy Protection Act, and the Video Privacy Protection Act, as well as state privacy, security, data breach notification, and electronic signature laws.

"For companies doing business in the U.S., this multifaceted privacy law environment can seem daunting. As is the case with most major challenges, a framework for formulating fundamental principles can help make compliance and data strategy more manageable."



Addressing Risk, Compliance & Integrity in the Extended Enterprise



BY: MICHAEL RASMUSSEN

GRC analyst and pundit, GRC 20/20 Research, LLC

The structure and reality of business has changed. Traditional brick-and-mortar business is a thing of the past – physical buildings and conventional employees no longer define the organization. Instead, modern organizations are an interconnected web of relationships, interactions, and transactions that extend far beyond traditional business boundaries. Further, organizations rely on relationships with suppliers, vendors, outsourcers, service providers, contractors, consultants, temporary workers, brokers, agents, dealers, intermediaries, partners, and more, for critical operations. Even the smallest organization can have dozens of relationships they depend on for goods, services, processes, and transactions. In large organizations, this can expand to tens of thousands of third-party relationships with suppliers, vendors, partners, and service providers.

With businesses increasingly relying on a complex network of third-party relationships to thrive, the governance, risk management, and compliance (GRC) of third-party relationships is even more critical. Without effective GRC, organizations will fail to manage uncertainty, avoid disruptions, act with integrity, and achieve business objectives.

In a dynamic risk environment, resiliency requires agility and the ability to navigate great uncertainty. Effectively mitigating the exposure of potentially disruptive events requires real-time and comprehensive risk intelligence within and across the extended enterprise with insights to both assess the current and future risk landscape and drive sagacious action. Resiliency regulations such as in the U.K. with the FCA/PRA/Bank of England as well as the EU Digital Operational Resilience Act requires resilience of third-party relationships that organizations depend upon.

This is even more apparent in the age of ESG. The world is seeing a broad sweep of regulations impacting ESG in third-party relationships. Germany's Corporation Due Diligence Act which went into effect January 1, 2023, has organizations worldwide concerned about ongoing due diligence activities in the extended enterprise. With the corresponding EU Directive this is going to require every member country of the EU to pass similar legislation that impacts anyone doing business with organizations in these countries. Then there is the range of regulations that focus on aspects of ESG in the extended enterprise. These include the proposed SEC climate change rule, U.S. FCPA, U.K. Bribery Act, Sapin II, U.K. Modern Slavery Act, Australia's Slavery Act, California's Transparency in Supply Chains Act, Conflict Minerals in the Dodd Frank Act, and so many more. Privacy laws such as the EU GDPR and California's CPRA have an impact on the extended enterprise.

The inevitability of failure – fragmented views of third-party risk & compliance

Too often, organizations struggle to adequately govern their third-party relationships because of their reliance on outdated practices. Silos of documents, spreadsheets and emails give a false perspective of risk as they do not show the big picture. Technology enables organizations to be more effective and do more with fewer resources, but unfortunately, too many organizations have failed to seize the opportunity to evolve their third-party risk processes.

Failure in third-party GRC comes about when organizations rely on outdated risk practices including:

1 Silos of third-party oversight. Silos of oversight occur when an organization allows different business functions to conduct third-party oversight without coordination, collaboration, and architecture. The risk posed by a third party for one business function may seem immaterial but is actually significant when factored into multiple risk exposures across all of the business functions relying on the same third-party. Without a single pane of visibility into the risk in their third-party relationships, silos leave the organization blind to risk exposures that are material when aggregated.

2 Limited resources to handle growing risk and regulatory concerns. Organizations are facing a barrage of increasing regulatory requirements and an ever-expanding risk landscape. While risk functions are operating with

limited budgets and human teams, they need to do more with less. In reality, truly effective continuous monitoring and mitigation of today's dynamic and ever-expanding risk landscape is beyond human capabilities alone.

3 Overreliance on manual processes. When organizations govern third-party relationships in a maze of documents, spreadsheets, emails, and file shares, it is easy for risks to be missed amidst the extensive volume of data. In addition, when things go wrong, these manual processes neither support agility nor a robust feedback loop to improve processes going forward.

4 Limited view of risk vectors. Organizations often over-rely on third-party financial and cyber risk management and suffer from risk exposure in domains such as compliance, operations, ESG, location and Nth parties. To fully understand the complete risk picture, an organization needs to have full-spectrum risk coverage.

5 Scattered third-party risk solutions. When different parts of the organization use different third-party risk solutions, silos of risk data and intelligence are created that are difficult to assimilate, thus making it difficult to maintain, aggregate and provide comprehensive, accurate, and current third-party analysis. The resulting redundancies and inefficiencies make organizations less agile and impact the effectiveness of third-party risk programs.

6 Overreliance on Periodic Assessments. For many organizations, third-party risk analysis occurs primarily during the onboarding process at the onset of the business relationship with only periodic reassessment of risk over the length of the engagement. This approach fails to keep organizations informed in a timely manner

when the risk exposure changes between assessments. Without a continuous source of real-time risk intelligence feeds, the organization lacks the ongoing situational awareness necessary for proactive risk mitigation.

The modern business is dependent on third-party relationships and requires real-time and continuous awareness of its current and future risk landscape in the extended enterprise. A manual and point-in-time approach to third-party risk intelligence compounds the problem and can lead to elevated risk exposure. It is time for organizations to step back and move from legacy practices, defined by manual processes and periodic assessments, to a third-party risk strategy that includes integrated full-spectrum real-time views of situational awareness that impacts the extended enterprise and operations.

A dynamic business environment requires the capability to actively manage risk intelligence and fluctuating risks impacting the organization and its relationships. The old paradigm of uncoordinated third-party risk management is inadequate given the volume of risk information, the pace of change, and the broader operational impact on today's business environment and operations. Organizations need to address third-party risk management with an integrated strategy and an enterprise-wide information architecture that provides 360° third-party risk situational awareness. The goal is to provide actionable and relevant risk intelligence to support third-party risk governance and oversight to ensure the organization is agile, resilient, and acting with integrity in its business relationships.



The end goal in mature third-party risk management is agility. This is where organizations will find the greatest balance in collaborative third-party risk management and oversight. It allows for aggregation of third-party risk intelligence relevant to individual departments, business functions, and relationship owners with a common integrated risk intelligence information architecture that aggregates and monitors risk across these areas.

2023 prediction

Organizations in 2023 need to clearly implement a well-defined third-party risk strategy, process, and architecture that delivers agility through the ability to connect, understand, analyze, and monitor risks and underlying patterns of risk in context of relationships and services across the extended enterprise. Different functions participate in third-party risk strategy with a focus on coordination and collaboration through a common core risk technology and process architecture.

About The Author

Michael Rasmussen | GRC analyst and pundit, GRC 20/20 Research, LLC


Michael Rasmussen is an internationally recognized pundit on governance, risk management, and compliance (GRC) – with specific expertise on the topics of enterprise GRC, GRC technology, corporate compliance, and policy management. With 27+ years of experience, Michael helps organizations improve GRC processes, design and implement GRC architecture, and select technologies that are effective, efficient, and agile. He is a sought-after keynote speaker, author, and advisor and is noted as the “Father of GRC” – being the first to define and model the GRC market in February 2002 while at Forrester.

Michael has contributed to U.S. Congressional reports and committees, and currently serves on the Leadership Council of the OCEG and chairs the OCEG Technology Council, OCEG Policy Management Group, and the OCEG GRC Architect Group.

Michael is quoted extensively in the press and is respected for his commentary on broadcast news channels. He is an Honorary Life Member in The Institute of Risk Management for his contributions to risk management and GRC. In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in “Governance and Compliance: Saving the Planet and the Corporation” and as a “Rising Star in Rocky Times: Corporate America’s Outstanding Executives.”

Prior to founding GRC 20/20 Research, Michael was a vice-president and ‘Top Analyst’ at Forrester Research, Inc. Before Forrester, he led the risk/compliance consulting practice at a professional services firm, and prior to that has specific experience managing compliance and risk within commercial organizations.

Michael’s educational experience consists of a juris doctorate in law and a bachelor of science in business. Michael is currently pursuing a master of divinity at Trinity Evangelical Divinity School with a research focus in ethics and church history. He is a GRCP (GRC Professional), CCEP (Certified Compliance and Ethic Professional), and a CISSP (Certified Information Systems Security Professional). OCEG has recognized him as an OCEG Fellow for his contributions and advancement of GRC practices around the world.

A man with a beard, wearing a blue and red plaid shirt and black pants, is sitting in a modern office chair, working on a laptop. He is looking at the screen, which displays a map or data visualization. The desk is cluttered with papers, a smartphone, and other office supplies. In the background, there is a large window with sheer curtains, a potted plant, and a yellow cushioned chair. The overall atmosphere is professional and focused.

"The modern business is dependent on third-party relationships and requires real-time and continuous awareness of its current and future risk landscape in the extended enterprise. A manual and point-in-time approach to third-party risk intelligence compounds the problem and can lead to elevated risk exposure."

Third Party Risk in the Era of Sanctions Enforcement

BY: MICHAEL VOLKOV
CEO, The Volkov Law Group, LLC



An uptick in sanctions activity dominated the global compliance landscape in 2022. Precipitated in large measure by the invasion of Ukraine by the Russian Federation, sanctions have re-emerged as a primary means of facilitating foreign policy objectives, including a coordinated international response designed to cripple the Russian Federation's military-industrial capacity.

These sanctions range from substantial new additions to the Specially Designated Nationals and Blocked Persons List (SDN List) maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) to robust new export controls maintained by the U.S. Department of the Commerce's Bureau of Industry and Security (BIS). In addition, foreign jurisdictions – principally the United Kingdom and European Union – have leveled their own punitive measures against Russian oligarchs and industry for their complicity in the Ukraine conflict. Among other things, these restrictive measures include travel bans, financial prohibitions, export restrictions, and asset seizures.

In the third-party risk management context, risk-based due diligence of an organization's business partners – including, but not limited to, its suppliers, vendors, distributors, agents, service

providers, and other intermediaries – is part and parcel of mitigating the risk of incurring liability under international sanctions regulations. While the breadth and depth of such due diligence varies considerably based on factors like jurisdiction, industry, and third-party role, the common aim of all such inquiries is to ensure that the organization has insight into the **operations** and **ownership** of the due diligence target. Where companies lack such information, the risk of violating sanctions regulations is considerable, as such laws often target both designated entities and individuals with a **majority ownership** stake and/or **substantial control** over "blacklisted" organizations.

Complying with OFAC sanctions

Foremost among the global sanctions regulations organizations should be cognizant of are those enforced by OFAC. Long considered the most aggressive and far-reaching sanctions leveled by any jurisdiction, sanctions imposed by OFAC pursuant to both congressional mandates and presidential directives target myriad countries, regions, industries, entities, and individuals deemed to be participating in activities contrary to the national security or foreign policy objectives of the United States.

Under selective sanctions targeting the Russian Federation that were broadcast this year, OFAC imposed a series of incrementally more aggressive prohibitions that now forbid virtually any [new investment](#) by U.S. persons in debt or equity

of Russian Federation-based companies and the [importation of crude oil and petroleum products](#) of similar origin. In a new development coincident with the publication of this report, OFAC recently expanded the applicability of its Russia sanctions to encompass even ancillary activities that implicate the [maritime transportation](#) of Russian Federation-based crude oil below a predetermined price cap set by the United States and its allies. The intended effect of OFAC's recent action is to further constrain the ability of Russia to export energy products abroad, thereby reducing the critical revenue that the Putin regime relies on to fund its ongoing Ukraine excursion.

While the sheer complexity of sanctions leveled against the Russian Federation on its own warrants additional attention by the compliance functions of organizations, the threat of aggressive enforcement activity by the U.S. Department of Justice raises the stakes even further. As Deputy Attorney General Lisa Monaco emphasized in June of this year, sanctions [“are the new \[Foreign Corrupt Practices Act\],”](#) alluding to the fact the DOJ is prioritizing enforcement of sanctions evasion activity to a much greater extent than in the past.

As Monaco emphasized in the context of her remarks, the DOJ has dedicated significant investigatory and prosecutorial resources to enforcing Russian sanctions regulations, including creating a new task force – dubbed “Task Force KleptoCapture” – to prosecute intentional violations of U.S. sanctions regulations by Russian oligarchs. Monaco made it clear the DOJ would pursue such cases with “unprecedented intensity,” and explicitly cautioned all businesses with international exposure to take the issue of sanctions compliance more seriously.

Staying ahead of third-party sanctions risk

In such an era of heightened enforcement, it is imperative that all businesses with potential ties to Russia – however remote – adopt appropriate policies, procedures, and internal controls with the aim of advancing sanctions compliance as a signature operational concern. To the extent an organization's third-party due diligence program is lacking in any way, organizations should act swiftly to identify those deficiencies now, and devote appropriate resources to remediating them before a sanctions violation arises.

For instance, to the extent a company still relies on periodic manual screening of international sanctions lists to ensure its third-party partners remain compliant, such companies should plan on transitioning to automated screening utilizing a reputable sanctions screening solutions provider. Because sanctions regulations are subject to frequent change, organizations accustomed to more ad hoc, manual screenings are likely to find that their current third-party screening practices are insufficient to meet emerging regulator expectations. As one [recent enforcement action](#) demonstrated, even a modest interval between periodic manual screenings can result in significant violations of sanctions regulations.

Further, companies that have implemented automated sanctions screening should be cognizant that not all sanctions activity is list based. In some instances, international sanctions regulations prohibit companies from engaging in specified conduct. For example, furnishing maritime transportation services, engaging in certain financial transactions, etc. In these circumstances, more in-depth due diligence is required to ensure that the underlying activity itself is not prohibited by law.

Companies that lack a protocol for a more in-depth examination of third-party partners for sanctions risk should consider implementing one now. If internal

resources are insufficient, the company should consider outsourcing its enhanced due diligence activities to a reputable compliance solutions provider or law firm. While due diligence itself is not an absolute guarantee that a sanctions violation will not occur, companies that can demonstrate a good faith, consistent effort to comply with sanctions regulations are the most likely to benefit from leniency in any criminal, civil, or administrative proceeding.

2023 prediction


As mentioned above, sanctions enforcement activity remains a core priority of DOJ senior leadership. This emphasis is unlikely to shift anytime soon, as the Russian Federation's Ukraine incursion remains in full force. As a consequence, ethics and compliance professionals are charged with acquainting themselves with the basics of applicable sanctions regulations both domestically and internationally as they pertain to the operations of their respective organizations.

Moving forward, any transactions with even the slightest Russian Federation nexus should be subject to scrutiny. Moreover, as sanctions regulations are subject to frequent change, organizations that lack automated continuous screening of their third-party relationships should intend on devoting resources to that effort now. More importantly, organizations that lack a process for a more enhanced analysis of the sanctions risk involved in sizable transactions should plan on allocating resources to this effort going forward.

About The Author

Michael Volkov | CEO, The Volkov Law Group, LLC

Michael Volkov, CEO of The Volkov Law Group, PC, 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 award-winning legal blog Corruption, Crime & Compliance.

A woman with dark, curly hair is smiling and looking down at a tablet computer she is holding. She is wearing a white t-shirt and a necklace with a small orange pendant. The background is a bright, out-of-focus interior space with a curved ceiling. There are two solid orange rectangular shapes at the bottom of the page: one on the left and one on the right.

"Because sanctions regulations are subject to frequent change, organizations accustomed to more ad hoc, manual screenings are likely to find that their current third-party screening practices are insufficient to meet emerging regulator expectations."

New Expectations of Executive Leadership – How Will You Prove and Certify Your Program Works?



BY: MATT KELLY,
CEO, Radical Compliance

As compliance officers enter 2023, they need to learn how to handle a double-edged sword: the Justice Department's new requirement that as part of corporate misconduct resolutions, CCOs must certify the effectiveness of their compliance programs.

If you wield that sword correctly, certification requirements could be quite useful. They will force compliance officers and CEOs to think seriously about what an effective compliance program for their corporation should be able to do and then to marshal the necessary resources to bring that plan about.

Mishandle the sword, however, and you might end up skewered. What happens if you and the CEO disagree about the state of your compliance program? What data will you need to collect (from across the enterprise and your third parties) to satisfy the expectations of the Justice Department? Could CCOs face personal liability if their certifications don't hold up?

That's the challenge now facing compliance officers. You'll need deft moves and skill to prevail.

The logic behind CCO certifications

First, we should step back and remember precisely what the Justice Department has done, and why.

The requirement is that chief compliance officers and their CEOs will both need to certify at the end of a deferred- or non-prosecution agreement that the company's program "is reasonably designed and implemented to detect and prevent violations of the law ... and is functioning effectively." So said assistant attorney general Kenneth Polite [when he announced the requirement last May](#).

The intentions behind program certification are laudable, at least. By forcing the chief executive and the CCO to certify the effectiveness of the compliance program, that assigns accountability to those executives. It drives the importance of a culture of compliance up the company's priority list, ideally to the top.

Compliance program certification also helps the Justice Department's broader effort to crack down on recidivist corporate misconduct and nurture a greater appreciation of corporate compliance. Those CEOs who might need to certify their program also tend to sit on the boards of other companies; that helps to spread the message in corporate boardrooms that strong compliance programs matter. Moreover, when the CEO and CCO have to sign their names to a certification **under penalty of perjury**, that does tend

to focus the mind. Compliance officers and chief executives alike will want to convey the importance of effective compliance throughout the whole enterprise, and build the systems, policies, and controls necessary to meet that standard.

So, one can see why, from the Justice Department's perspective, compliance program certification is a compelling idea.

From the compliance officer's perspective, of course, things look quite different.

Facing new problems and perils

The primary question for compliance officers is obvious: What happens if you certify that your program is "reasonably designed and functioning effectively," and the company subsequently suffers a compliance failure anyway?

Right now, we don't know. The Justice Department only began imposing certification requirements in 2022. It might be years before an erroneous certification comes to light – and when it does, the Justice Department will evaluate that case based on the specific facts at hand. Compliance officers won't have that luxury. You'll need to certify your program **without** knowing what future scenarios might prove you wrong.

Meanwhile, compliance officers will face other, more practical headaches along the way. If you and the CEO disagree over the health of the compliance program, who settles that dispute? If you join a company in the middle of a DPA or NPA, can you review – or even redesign – the pre-existing compliance program, if you believe it isn't up to standard? Can you ask for directors' and officers' insurance to protect you from possible legal costs? What if

the company declines? When do you quit, rather than oversee a compliance program you believe to be substandard?

It will be years before compliance officers have answers to all those questions, but even now, at the start of 2023, we can start to answer some of them.

Get better data, run better programs

The immediate answer is that compliance officers need to work on building an effective compliance program in the first place, **and then document why your program is indeed effective**. That's what the Justice Department will want to see if your company ever faces a government investigation: evidence that the program was designed thoughtfully and works as intended.

In that case, several specific capabilities become even more important:

- **Risk assessments.** You'll need to be able to identify new regulatory requirements and changes to your own company's operations, and do so swiftly. You'll also need the ability to test compliance controls.
- **Key performance indicators for the compliance program.** You'll need relevant KPIs, and an ability to track changes in those KPIs over time.
- **Data analytics.** This isn't simply about collecting data (from multiple parties, in multiple formats). You'll also need some way to turn that data into meaningful insights – about program weaknesses, problematic transactions, risk exposure, and the like.
- **Third-party due diligence and monitoring.** Third-party risk became an even more pressing issue in 2022, after Russia invaded Ukraine and the West responded with sweeping, fast-moving sanctions against Russian persons. More broadly, as third parties play ever larger roles for corporate

organizations, your ability to manage their compliance risks will become even more crucial.

- **Internal accounting controls.** Weak accounting controls are a perennial source of FCPA risk. Companies need to assess whether documentation and approval controls for high-risk payments are sufficiently strong, and for each transaction they need to confirm that employees follow the rules.

Aside from those program-specific needs, there's a larger issue here. Compliance officers will also need to forge stronger relationships with the CEO and the board. After all, the CEO's signature will be next to yours on the certification forms, and the board is the ultimate source of authority for the organization. In a roundabout way, certification requirements could help propel your compliance program up the maturity curve, since CCOs should (ideally) have more influence with senior management. You can then reorient corporate priorities toward that stronger culture of compliance.

The good news is that most CEOs and boards already value a strong culture of compliance, at least in theory; and most other senior executives do too. In 2023 and beyond, chief compliance officers will need to leverage that abstract enthusiasm into demonstrable, vocal, tangible support for the compliance program.

Then, with luck, we won't need to worry about what happens to a CCO who signs a certification form that later proves invalid, because you'll have that reasonably designed and effective compliance program in place.

2023 prediction

We won't see a lot of chief compliance officers certifying the effectiveness of their compliance programs in 2023, but only because the Justice Department settles only a relative handful of cases in any given year. Compliance officers will, however, need to have more frank conversations with their boards and senior management teams about investing in their compliance programs – because CCOs' unease about personal liability for program failures won't be going away. Compliance officers will need to think long and hard about how to assess risk and measure the effectiveness of their programs; and what their red lines will be for when they leave a job rather than participate in burying a compliance failure.

About The Author

Matt Kelly | CEO, Radical Compliance

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.

A man and a woman are standing in a modern office, looking at a tablet together. The woman is holding the tablet, and the man is pointing at the screen. They are both dressed in business casual attire. The background shows a large window with a view of a city skyline.

"Compliance officers and chief executives alike will want to convey the importance of effective compliance throughout the whole enterprise, and build the systems, policies, and controls necessary to meet that standard."



Joining Forces with Learning and Development Will Improve Ethics and Compliance Education

BY: INGRID FREDEEN

Vice President, Online Learning Content, NAVEX

MEGAN TORRANCE

CEO, TorranceLearning

Building a strong workplace culture – where people actively think about how to do the right thing and then follow through in their actions – is not something that happens organically. Rather, it is something that takes work and time. As we look to 2023 and beyond, it is clear that high-quality, impactful ethics and compliance learning initiatives and communications will be viewed as paramount in the pursuit of a strong workplace culture. With this focus comes a recognition that learning and development (L&D) professionals are key players and will increasingly have a seat at the table and help shape the direction organizations take. Their presence and expertise will help organizations create more powerful, impactful and effective adult learning and communication programs.

What is driving a greater recognition that L&D has unique contributions to make?

Ethics and compliance (E&C) professionals have long known the importance of educating the workforce in order to create and maintain a culture of ethics and compliance. It not only helps mitigate risk and reduce legal liability but also can help carry a message about an organization's own values and priorities. What's more, these learning experiences are among the

key activities in the E&C program that reach each and every employee – and in some cases external business partners as well.

As E&C professionals have charted a path and developed more sophisticated learning programs in the past five years, there has also emerged a recognition that something more is needed to actually help shift behaviors and drive a culture forward. Ethics and compliance programs are now starting to recognize L&D professionals can help take their adult learning education programs to the next level and help drive values throughout the organization.

Though E&C learning has traditionally been the purview of the compliance function, L&D's influence can be the key in supercharging a culture of learning and growth. In fact, there is a growing collaboration between the two functions to bring together the knowledge of L&D professionals in how to make learning experiences more engaging, memorable and effective, and the subject matter expertise of E&C leaders.

It is worth noting that not all organizations have the resources to staff a fully operational L&D function, and smaller businesses may only be deploying the necessary E&C learning modules to maintain regulatory compliance. However, through partnership with consultancies, organizations of all sizes are still able to infuse solid principles of adult learning to enhance

the efficacy of their E&C programs. So, while the conversation about L&D having a seat at the table with Compliance inherently speaks to large enterprise organizations, all organizations can see similar results with strategic partnerships.

For those organizations that embrace this emerging trend, L&D partners can help drive program improvements in three critical ways in 2023.

Driving quality over purely cost-driven considerations

First, developing high-quality, effective compliance learning can be difficult, and many competing factors must be weighed in order to optimize a program. Further, there is a cost whether the organization purchases virtual learning modules or builds their own. However, one practice that is increasingly becoming the norm is focusing on high-quality learning, and not just selecting the cheapest solution. This is because when poor quality learning tools are used, it not only wastes valuable employee time, but it may also actually harm the overall quality and internal reputation of the E&C program.

We have observed in the past six months, L&D is increasingly at the table in organizations of all sizes. They are seen as a resource and skilled member of the team and are helping organizations make better choices with their budget. In 2023, this trend will most certainly grow in strength as programs that got started early on this journey start to reap the rewards of a strong relationship with L&D and other programs see the value and engaging L&D as a resource.

This shift is the direct result of organizations viewing ongoing adult learning not just as a thing they must do, but rather as an opportunity to



engage each and every employee in their organization's values. Compliance communications and the related learning experiences are among the few activities that actually reach each employee on a regular basis and one of the best opportunities to drive knowledge and educate on expected behaviors.

So, how does L&D fit into the picture? L&D's very mission is to drive organizational performance by increasing skills and knowledge – and they have much to offer here. This is where a trained professional can help identify poorly designed or written content. Some of the most glaring issues they spot include use of ineffective gimmicks or gamification to mask poorly written content; disparities in design quality and consistency; poorly written questions that ask for regurgitation of a random fact rather than driving application of a lesson; and poorly designed analytics that track results but don't really measure employee knowledge, retention or risks.

Learning and development professionals know, despite their functional title, providing opportunities for learning can positively influence employee behavior – but alone it is not sufficient.

Creating a culture of learning that is employee-focused to drive better program results

Second, learning is not a “one and done” experience. A single course given once every handful of years is certainly better than nothing, but messages and expectations sink in better when there is a sustained and meaningful flow of communication and information. Further, the impact can be increased when learners have an opportunity to apply those lessons in real life.

In considering any learning event, identify the real objectives and outcomes to be achieved. If the answer is to check the compliance box, it's unlikely to influence the organization's culture.

However, if the objective is to enhance culture through meaningful content, fostering an environment that prioritizes ethics, respect – and yes, compliance – there is a much greater impact. If employees are at the center of these efforts (what they need, care about, and can use) then the organization is already on the way to creating a learning culture.



Organizations are embracing the concept of building a learning culture where meaningful and relevant opportunities to expand on skills and grow professionally are offered to employees. Also important to note, employees must be given allocated time and opportunity to utilize these resources to instill a true culture of learning. This includes covering important compliance-related content, but also learning opportunities that can enhance job performance and career growth. Learning events that are sandwiched in during other high priority initiatives will not receive the desired time and attention.

A great first step on this journey is to reframe the term “training”, the most used industry terminology, and instead focus on the greater goal: learning. The term “training” comes with baggage – frequently thought of as a boring, but necessary, task or used as a punitive action when expectations are not met. “Training” is pushed onto people. Instead, many leading organizations are now talking about these efforts as learning, continued support, and skill building for career growth. “Learning” is what employees do as they build skills and knowledge they can apply on the job. For this to work and permeate across the organization, it's imperative that time is allowed for learning activities and that the content is high quality, relevant and engaging to the workforce. In fact, this entire article excludes the term “training” in favor of terminology centered around learning and education. While this shift in verbiage may take some time and adjustment to adopt, it is an important step in creating a culture that embraces learning.

One approach that is becoming more widely embraced is adaptive learning. This personalization of learning gives an employee a unique experience with course content – adapting to what the employee already understands while providing more information where the employee is struggling. The goal of this type of learning experience is to make it relevant to the learner rather than a waste of their time.

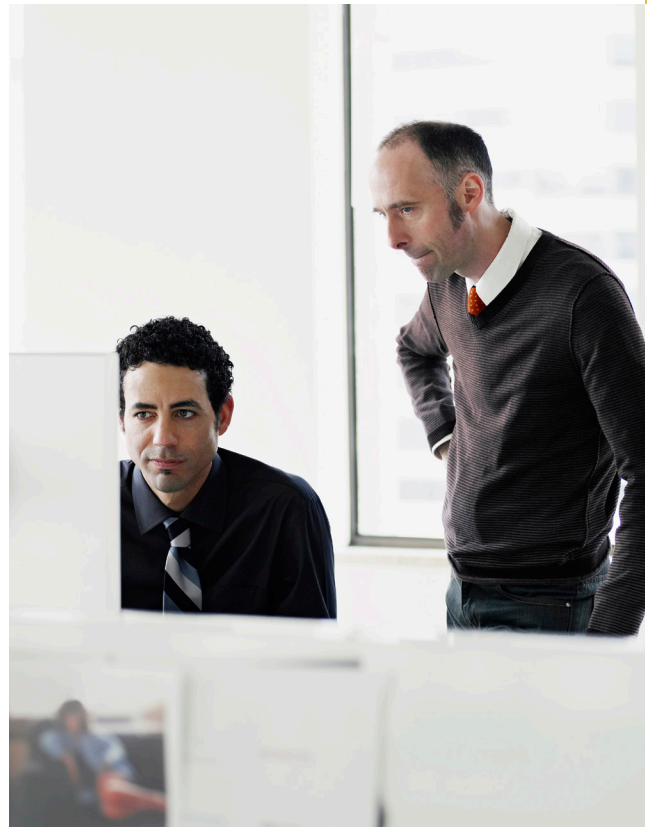
Another approach is self-directed exploration and skill development, including improving knowledge about compliance areas and risks important to your organization. This will help strengthen important corporate values while providing benefits to your employees. It may also encourage employees to seek more challenging roles and opportunities within the organization. Another benefit for the organization, and the compliance function, are helpful metrics to share about the importance of compliance, not only within the organization's leadership but also to employees.

L&D and E&C can work together to build a mutually reinforcing culture of learning and support each other's efforts. Employees rarely differentiate between learning content that comes from E&C and learning content that comes from their L&D teams or operational leaders. High-quality learning experiences from all sources contribute to the organization's overall messaging about the importance of learning and improvement.

Driving for year-over-year program improvements

A third, and important, way L&D contributes to the overall success of E&C learning and communication programs is through their relentless focus on year-over-year program improvements. This focus on improvement is aligned with similar concepts found in DOJ guidance, for example.

As noted above, ethics and compliance learning is among the few compliance initiatives that impact each employee every year – and these interactions often happen on a regular basis as new learning topics and communications are rolled out. When these interactions are viewed as



two-way communication (sharing information with the employee, but also getting information back from them), organizations create an ongoing opportunity to learn from employees through performance metrics, feedback metrics, and even follow-on effectiveness surveys.

This information is vital to identifying hotspots, areas that require additional time and attention, and making decisions about future investments – all of which contribute to driving program improvements. When organizations are able to further combine these data points with other compliance data (such as allegations of misconduct, or policy attestations) this creates a new view of the organization and the effectiveness of its E&C program. Further, this also helps to identify locations that may be struggling or where misconduct may be more widespread than an isolated report.

A talented L&D professional can help identify important data points and report on them so that programs can start (or even continue) the journey of making year-over-year improvements. L&D professionals leverage several solid models for learning experience evaluation, covering everything from satisfaction with the program and comprehension of the content, to on-the-job behavior, business results and return on investment. Benchmarking compliance learning initiatives against an organization's other L&D offerings can provide valuable insights on where and how to continue to improve.

2023 prediction

As the world continues to adjust to the new normal and work is thought of differently than in years past, organizations will continue to evolve to meet the needs of the workforce wherever they are located. Organizations that can provide opportunities for personal and professional development within a culture that embraces authenticity and learning will find that they enjoy better employee engagement, performance and retention. Learning and development, and ethics and compliance education will continue to influence and reflect the conversation about organizational culture.

About The Authors

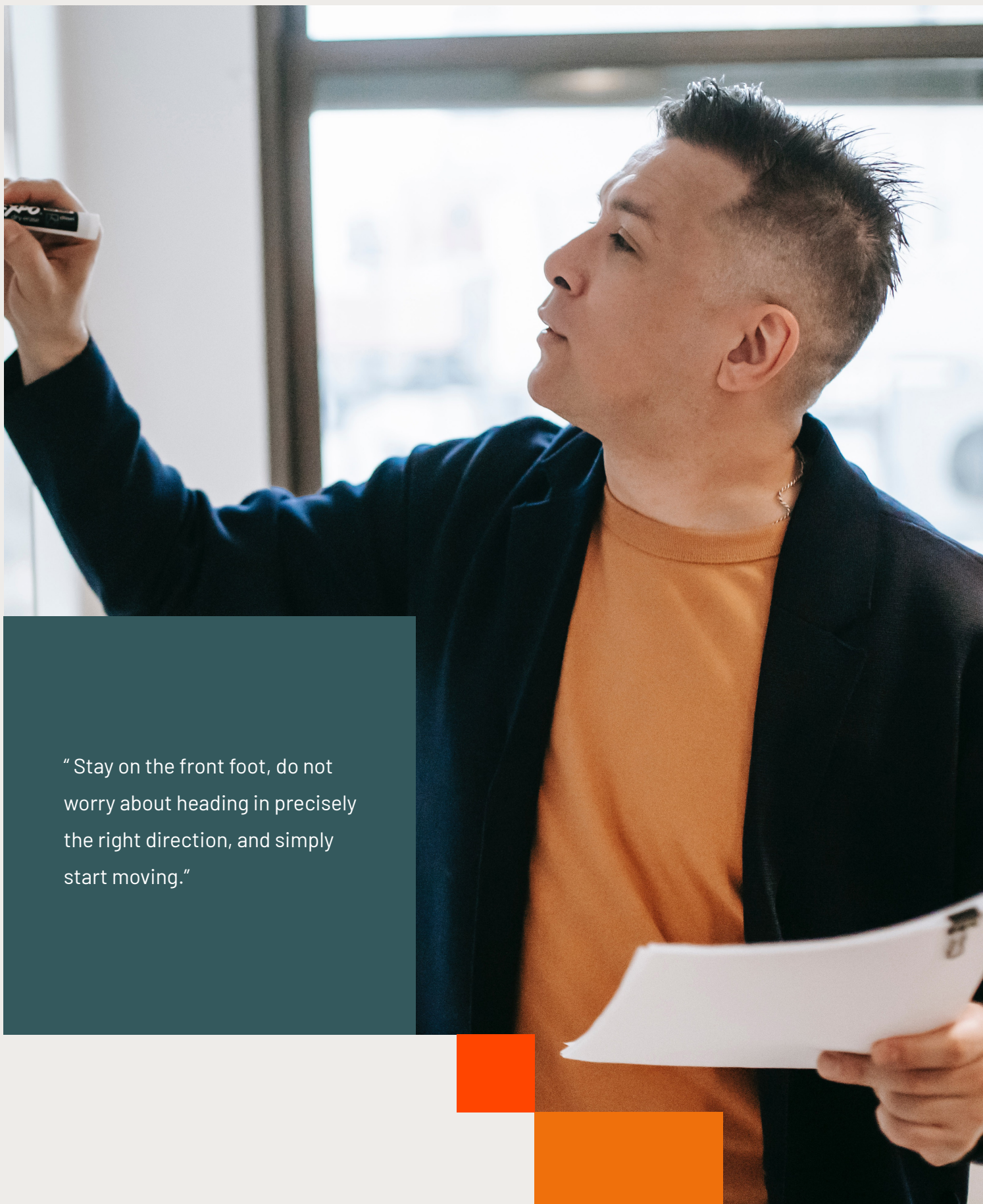
Ingrid Fredeen | Vice President, Online Learning Content, NAVEX

Ingrid Fredeen, J.D., vice president, online learning content, has been specializing in ethics and legal compliance training for more than ten years. She has been the principal design and content developer for NAVEX's online training course initiatives utilizing her more than 20 years of specialization in employment law and legal compliance. Prior to joining NAVEX, Ingrid worked both as a litigator with Littler Mendelson, the world's largest employment law firm, and as in-house corporate counsel for General Mills, Inc. a premier Fortune 500 food manufacturing company.

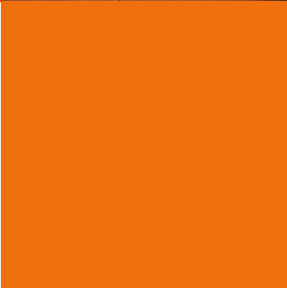
Megan Torrance | CEO, TorranceLearning

Megan Torrance is CEO and founder of TorranceLearning, and has over 25 years of experience in learning design, deployment and consulting. Megan and the TorranceLearning team are passionate about sharing what works so they devote considerable time to sharing professional development in her field.

Megan is the author of Agile for Instructional Designers, Data & Analytics for Instructional Designers, and Making Sense of xAPI. She is also a facilitator with eCornell's Women's Executive Leadership certificate, and courses in virtual teaming, team leadership and communication.



"Stay on the front foot, do not worry about heading in precisely the right direction, and simply start moving."



This Supreme Court Case Will Reverberate Throughout the Compliance and ESG World



BY: KRISTY GRANT-HART
CEO, Spark Compliance Consulting

Shockwaves hit publicly traded companies in March of 2022 when the SEC announced its proposed rule that would require public companies to include certain climate-related disclosures in their annual reports and registration statements. But now, thanks to the Supreme Court's decision in *West Virginia v. EPA*, those new rules – and many others – are seriously in question.

Recently, the Supreme Court has played a bigger and bigger role in shaping regulatory and compliance outcomes. Since 2018, when the Court unanimously held in *Digital Realty Trust, Inc. v. Somers* that internal whistleblowing did not qualify individuals to the Dodd-Frank protections against retaliation, the court's reach has become larger.

What happened in *West Virginia*

Over three presidential administrations, the EPA went back and forth with its Clean Power Plan, which was created to limit greenhouse gas emissions from power plants. The plan required increasing the use of cleaner energy like solar and wind and reducing the use of coal. The state of West Virginia and several other parties sued to block the regulations.

The Supreme Court took up the case and ruled in June 2022 that the EPA had overstepped its remit by enacting a sweeping regulatory scheme beyond that which had been authorized by Congress. They focused on the “major questions doctrine,” which, in a nutshell, says that when there is a question of “vast economic and political significance,” an administrative agency must identify a clear legislative statement made by Congress granting the agency the authority to use regulation to answer the question. Since Congress had made no such grant to the EPA to regulate the specific use of various types of energy, the Clean Power Plan could not be enforced.

Why this matters to compliance and ESG practitioners

Although this is the first time the major questions doctrine has been specifically relied upon, it follows a long list of cases upon which the core principle relies. This includes, notably for compliance practitioners, the decisions relating to the Occupational Safety and Health Administration's (OSHA) attempted COVID-19 vaccine mandate.

The major questions doctrine can, and will likely, undermine many proposed or contemplated regulatory schemes. The *West Virginia* ruling sets the scene for court fights that may reign in the power of

administrative agencies, especially when the agency's remit does not traditionally cover the area of regulation. The ruling goes well beyond the EPA. It affects all federal agencies and provides a potent tool for petitioners to argue against administrative actions.

These cases will lead to companies and compliance programs being stuck in limbo awaiting final answers from the court. What's worse? Some judges may stay the regulations while the cases work their way through the courts. Others may not, which means that the regulations may be in force for some time, while compliance and ESG practitioners wait to see whether the regulations will hold up in the long term.

Why the SEC's proposed disclosure rules are in question

Critics argue that the SEC's remit is to (1) protect investors, (2) maintain fair, orderly, and efficient markets, and (3) facilitate capital formation – not to regulate climate change disclosures. Of the SEC's proposed rules, [a Wall Street Journal opinion piece](#) stated that “the proposal would convert the federal securities regulator into a greenhouse-gas enforcer looking over the shoulders of exchange-listed companies' directors.” These critics state that the SEC's mandate only focuses on regulating the materiality of *financial* disclosures, not climate change. The SEC's position may be that, because so many investors care deeply about climate change, such disclosures are material to financial decisions.

Regardless, the major questions doctrine will likely be used to challenge the SEC's final set of rules governing climate change disclosure. The Court's *West Virginia* opinion states that congressional authorization is required for an agency to regulate matters of great political or economic significance. Climate change is most certainly a matter of great political significance, and companies have been publicly decrying the cost of implementing the proposed disclosure rules since they came out.

Absent a grant of specific power to the SEC to regulate climate disclosures, petitioners may be successful in their challenge. Congress has, thus far, *not* tasked the SEC with regulating climate change disclosures, and the divided house and senate are unlikely to do so in the upcoming term.

It's not just the climate change disclosures

Because the major questions doctrine applies to all federal agencies, other potential regulatory schemes may be challenged. After the recent collapse of the FTX cryptocurrency exchange and the resulting loss of over a billion dollars in customer funds, calls for the regulation of the cryptocurrency industry have grown louder. However, Congress has not tasked any administrative agency with tackling the problem, and therefore, under the major questions doctrine, until that happens, it may be argued that no agency has enforcement capacity.

Likewise, other regulations may be called into question. [One law firm wrote](#) that, in addition to cryptocurrency oversight, “other blockchain products, capital market regulations, FTC oversight, and antitrust and competition law” may be challenged in court using the major questions doctrine.

Congress may need to address how digital assets should be regulated, granting authority to the SEC or some other agency. If it does not, arguments will continue to rage about whether the SEC or other agency would be overstepping their mandate if they create new schemes or laws to regulate that market.

What about emerging threats?

The *West Virginia* decision calls into question new schemes meant to regulate new technologies or emerging threats. For instance, if the next generation of technology invades privacy in a way not currently contemplated within the mandate of the FTC, does that mean that Congress will have to grant authority specifically over the technology in order to regulate it? Quite possibly.

Global implications

American regulations aren't the only game in town, of course. The SEC's rules on climate change disclosure have pushed many American companies to ramp up their ESG efforts. However, slowing those efforts down due to Supreme Court action won't stop the ESG disclosure push from other parts of the world. According to the [Harvard Law School Forum on Corporate Governance](#), "Those who wonder what tomorrow's ESG regulation may be like should usefully turn to the EU, which has initiated significant reforms in this area for several years, most often based on the French model."

The same is true for the cryptocurrency market. In October 2022, the European Union took a major step toward regulating cryptocurrency when the European Council approved the comprehensive Markets in Crypto-Assets

regulation. While the vote in the European Parliament isn't expected until February 2023, the regulation, nicknamed MiCA, is widely expected to pass. In its current form, it would require crypto companies such as wallet providers and exchange platforms to seek authorization from national regulators within the EU.

What compliance officers should do now

All of this uncertainty puts compliance officers in a difficult place. To manage this challenge:

- **Identify the regulatory schemes that are likely to be challenged:** The first thing to do is to identify the regulatory schemes that are likely to be challenged, then determine if they affect your business. If they do, then...
- **Make a tentative plan:** Look at the proposed regulation and make a plan to comply with it. See if you can find synergies between other laws applying to your company in other parts of the world. Let them guide your planning.
- **Watch carefully:** Many law firms put out alerts when the courts rule on significant regulatory matters or Congress passes important regulations affecting businesses. Ask to be added to the lists of these firms so you are alerted to these changes.
- **Pay attention to the rest of the world:** When it comes to ESG, climate change, or privacy, look to Europe to guide your actions. Many European laws are, by design, meant to capture a company selling into the European Union even if the company has no physical presence in the bloc. By following European laws, you are likely to find yourself in compliance with many American laws when they come into force.

2023 prediction

The American regulatory landscape is likely to change in the wake of the *West Virginia* decision, but that doesn't mean the rest of the world will follow suit. We predict that if the SEC's rules are finalized in line with what was previously published, they may be challenged in court under the major questions doctrine, which might hold them up from being implemented or require revision. Other regulatory schemes may be challenged using the same grounds, which will cause uncertainty in the compliance and ESG world while the courts sort out which regulatory schemes can stay in place or be implemented. Pay attention, make a plan, and always follow the path of ethics and integrity to have a strong, defensible, and sustainable compliance program.



About The Author

Kristy Grant-Hart | CEO, Spark Compliance Consulting

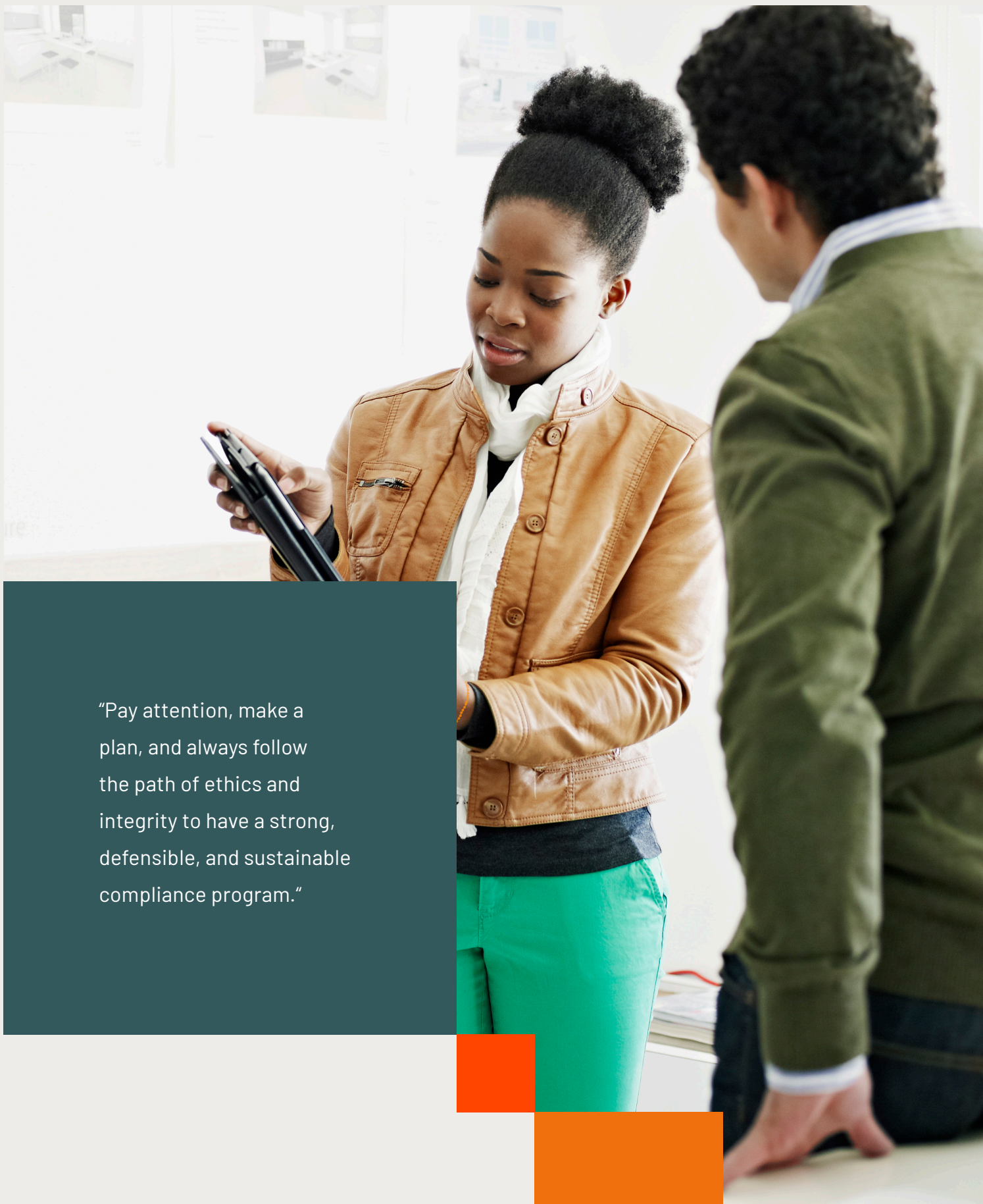
Kristy Grant-Hart is the founder and CEO of Spark Compliance and the author of several highly-acclaimed books, including the best-selling *How to be a Wildly Effective Compliance Officer*. She has advised Fortune 100 companies on international compliance and has created, implemented, and revamped compliance programs for major companies in Europe and the United States. Kristy was honored as a Trust Across America Top Thought Leader in Trust.

A powerful and inspirational public speaker, Kristy provides keynote presentations to organizations and conferences globally. Kristy has written for and been featured in publications including the *Wall Street Journal*, *Financial Times*, *Corporate Financier Magazine*, *Risk Universe Magazine* and on the cover of *Compliance and Ethics Professional Magazine*. She is a former adjunct professor at Delaware Law School, Widener University, teaching Global Compliance and Ethics. Kristy was shortlisted for the Chief Compliance Officer of the Year award at the Women in Compliance Awards and was shortlisted again for the Compliance Innovator of the Year.

Before launching Spark Compliance, Kristy was the chief compliance officer at United International Pictures, the joint distribution company for Paramount Pictures and Universal Pictures in 65+ countries.

Kristy began her legal career at the international law firm of Gibson, Dunn & Crutcher, where she worked in the firm's Los Angeles and London offices. While at Gibson Dunn, her team was nominated for Best Regulatory Law Firm of the Year at Thomson Reuter's Compliance Awards.

Kristy graduated summa cum laude from Loyola Law School in California. She holds certification as a Corporate Compliance and Ethics Professional – International (CCEP-I) and is a member of the California Bar.



"Pay attention, make a plan, and always follow the path of ethics and integrity to have a strong, defensible, and sustainable compliance program."

Staying Ahead of ESG Disclosures – What to Expect and How to Prepare



BY: COLIN ETNIRE
Head of ESG, BC Partners

When my private equity peers ask me how to handle ESG disclosures, my answer is typically, “don’t let the tail wag the dog.” What I mean is, it’s better to proactively report on what you know to be the most material and substantive representations of actual ESG performance for your companies, before being prompted to do so.

In my experience, investors appreciate thoughtful, proactive disclosures, which saves them time issuing and chasing completion of proprietary forms; further, it engenders trust based on open and transparent communication of these key metrics and considerations. While regulators require a more structured framework of reporting, I believe taking this proactive approach is still valid. Early movers in ESG disclosure will, at the very least, set themselves up better for inevitable regulation and made a head start, even if final requirements have a different total scope.

Fundamentally, all of these disclosures serve the same purpose: to inform better investment decisions.

The conversation around ESG has moved on significantly in recent years and it is no longer seen as mutually exclusive from strong returns. It is actually quite the opposite – it is seen as an essential lens through which to consider investment opportunities. In this context, the

imperative to accurately inform your investors remains more important than ever.

How disclosures are born

Understanding what informs disclosure obligations and how they evolve is essential in knowing how to approach them.

In the early days of ESG taking root in the private equity and wider investment industry, individual actors collected and reported information they deemed appropriate. These were informed largely by the practices in the (slightly) more established corporate sustainability sector that developed in collaboration with academics and NGOs. ESG officers at the various private equity firms collaborated informally, creating some consensus, but without formal obligations. Prominent asset owners, who are the primary investors in private equity funds, put out questionnaires or data requests as needed. Their counterparties, as well as smaller actors, frequently adopted the same approaches in order to streamline their work and maximize market acceptance.

Over time these informal collaborations became formal – though still voluntary – initiatives, notably the ESG Data Convergence Initiative (EDCI). These initiatives tend to be based on a set of key performance indicators (KPIs) deemed most essential and widely applicable, and were agreed across market actors through a consultation process. Processes like these

have fed into the formal regulatory rulemaking across industry that has produced legislation such as the EU Sustainable Finance Disclosure Regulation (SFDR). The EU SFDR includes a similar set of “converged” KPIs as the EDCI. In time, the different regional standards will revise themselves to become more interchangeable to make business easier for multinationals.

How to predict the future

The good news for your business is these convergences are not unpredictable; the requirements that win out generally come from good sense and can therefore be identified well ahead of time. In anticipation of what a business will be required to report, the following are helpful considerations:

- What issues are of generally universal interest, particularly within your industry?
- What issues are relatively easy to quantify in a substantive way?
- What issues have existing formal (voluntary or regulatory) initiatives in place globally?
- Assuming an issue has been identified, is there a manner of tracking it that reflects the realities of a business?

Greenhouse gas (GHG) accounting is a very straightforward example of the above. It's of universal interest across all industries, it's easy to quantify substantively, a large body of organizations already govern its disclosure, and accommodations to reflect business realities (such as reporting intensity metrics rather than absolutes) are well accepted. Taking a narrower example, in food and cosmetics supply chains, sourcing of palm oil is an important issue since it is linked to significant environmental degradation and other issues. While on the

surface this degradation may seem difficult to quantify, the fact that a voluntary framework already exists, the Roundtable on Sustainable Palm Oil (RSPO) allows for a percentage of RSPO-certified procurement to be reported.

Another factor to consider is that many who oversee ESG initiatives are not necessarily experts in the area. However, the good news is developments are not unpredictable if you keep your ear to the ground. Look back to the description of how disclosures typically are born: the early stages involve academics and NGOs. So, following media on particular topic areas will surface issues well ahead of time. Then, as practitioners begin discussing it, it will crop up in trade publications and conferences.

ESG matters such as climate change and diversity, equity, and inclusion (DEI) dominated agendas before they ever hit regulations. Around this point, you will begin to see formal requests from investors, customers, employees, NGOs, or other groups about the area, making the need for reporting on these topics very clear. By the time regulators begin discussing this, in what are typically lengthy rulemaking processes, you still have significant runway to prepare before you're required to formally report.

How to prepare

When you identify areas of increasingly urgent interest, keep in mind the adage “progress should not be the enemy of perfection.” It's always better to collect and report some information than none in this field – as long as it's represented accurately. GHG accounting is an infamously opaque exercise compared to its financial accounting cousin. However, while it does lean heavily on assumptions, using imprecision as an excuse to report nothing at all is much worse, both from a financial and environmental perspective.

Second, ensure access to adequate expertise on the topic area. While this may seem daunting at first glance, it doesn't necessarily mean hiring an army of new employees. Frequently, existing employees already work on the topic and have quite a bit of knowledge, and simply need a bit of guidance for how to convert that knowledge into a useful ESG disclosure. For example, HR professionals already live the day-to-day of DEI, and already frequently collect and report demographic information. Another example is the access to ESG reporting metrics such as energy consumption, which is typically already available to facilities personnel and needs to be consolidated in a more formalized fashion. For more resource-constrained organizations, an outside consultant can be used to steer what specific ESG areas ought to be tracked and what measures need to be implemented, in lieu of hiring an entire team dedicated to ESG.

Third, pick a framework that makes sense for your business and commit to it, regardless of what you think the future may hold. For example, biodiversity is an incredibly hot topic on the conference circuit at the moment and has essentially no universally accepted definitions or assessment frameworks, despite the fact the EU requires disclosures in its SFDR. As such, you'll need to look at what others are doing and pick a framework that is a good fit for your organization. In this example, perhaps you have a Europe-based business and define a biodiversity

sensitive area as a Natura 2000 space (EU-defined wildlife conservation area). You then use a spatial tool to look up if any of your operations are present in any of those areas and report the percentage that are.

Perhaps you accidentally got it exactly right and predicted what would later become the regulation. But even if you don't, you have investors appreciative of your proactive disclosures that still provide useful information – and are likely material to your business, even if you're not required to report on them. In the best-case scenario, your proactive leadership can encourage other market participants to adopt the same approach.

ESG disclosures do not have to be intimidating or burdensome. Imperfect disclosures now will help you comply with stricter and more complex regulations when they come down the road. The ESG field is relatively new and will mature in the years to come. Stay on the front foot, do not worry about heading in precisely the right direction, and simply start moving.

2023 prediction

For companies of any size, GHG accounting will become as normal and universal as financial accounting. Further, companies will realize (at least for Scopes 1 and 2) this accounting actually isn't particularly difficult. I also predict that biodiversity will finally get more widely accepted definitions of what constitutes biodiversity sensitive areas, and what basic procedures or resources can help assess businesses for their impact on them.

About The Author

Colin Etnire | Head of ESG, BC Partners

Colin Etnire joined BC Partners in 2020 as its Head of ESG and is based in the firm's New York office. Previously, Colin spent four years at The Carlyle Group as ESG Analyst, reporting to the chief sustainability officer, helping to implement an ESG program across Carlyle's platform. Prior to this, he worked for the New Hampshire Democratic Party and interned at the White House.



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](https://navex.com) and our [blog](#). Follow us on [Twitter](#) 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

4th Floor, Vantage London
Great West Road
Brentford, TW8 9AG
United Kingdom
info@navex.com
www.navex.com/uk
+44 (0) 20 8939 1650