



NAVEX™

Top 10 Risk & Compliance Trends for 2022

- *Predictions & Recommendations for the Year Ahead*

A NAVEX
EBOOK

Table of Contents

3	Introduction CARRIE PENMAN
6	Risk & Compliance Management Expands to Include ESG CARRIE PENMAN
10	EU Whistleblowing Directive KARIN HENRIKSSON, JAN STAPPERS
15	ESG Disclosure Adoption: What Can We Learn From the EU? KAREN ALONARDO, VERA CHEREPANOVA
20	The New Normal Workplace (Part 1): R&C Management MATT KELLY
24	The New Normal Workplace (Part 2): Training and Policy Management INGRID FREDEEN
28	Holistic Third-Party Risk Management SUSANNA CAGLE, MICHAEL VOLKOV, CAROL WILLIAMS
36	Data Privacy: Frameworks and Implementation PAM HRUBEY, JESSICA WILLBURN
40	DEI Is Not “One Size Fits All” PATRICE PALMER
44	Compliance Sabermetrics: Data Will Change Assumptions that Plague Compliance KYLE WELCH
48	The Impact of IT Risk on Business Continuity: Making Businesses More Resilient CAROL WILLIAMS

Introduction



BY: CARRIE PENMAN

Chief Risk & Compliance Officer, NAVEX

Each year, NAVEX releases the Top 10 Trends in Risk and Compliance to provide leaders with guidance and insights on where to focus their initiatives and resources. While global disruptions over the last two years have been unprecedented, our observations and predictions for 2022 reflect some trends that have been years in the making. This year, legal and regulatory changes – both upcoming and recently put into effect – will expand the scope and responsibilities of compliance leaders. A few core themes emerge from the Top 10 Trends this year.

Businesses are continuing a transformation caused by the long-term impacts of COVID-19, which progressed from massive disruption to a permanent consideration of the business. Further, the employees who power our businesses have undergone a transformation as well, challenging the norms of work, work-life balance, and the definition of a meaningful career. The “Great Resignation” and shifting expectations of the workforce will continue to have a significant impact on organizational risk, culture and compliance.

If the last two years were a time of developing and testing business continuity, 2022 will show a continued focus on business resilience and growth in the new normal. While organizations work towards building a foundation that can withstand disruption, successful business leaders will also address the transformative shift in culture and stakeholder expectations. Risk and compliance teams will play a critical role here.

Consumer, investor and employee attention is highly tuned in to how organizations operate, and this theme is present throughout our predictions. Beyond public attention, there are additional regulations – both pending and recently adopted – in the EU and US ranging from ESG disclosure, to whistleblower protections, to data privacy and risk management. Though some standards and frameworks are already in place and continue to develop, the onus

is on the business to take appropriate measures to show results in areas beyond financial performance. In the end, strong risk and compliance practices lead to good business – and with regulators and the public paying close attention, risk and compliance leaders are well positioned to deliver on many of these efforts.


In the end, strong risk and compliance practices lead to good business – and with regulators and the public paying close attention, risk and compliance leaders are well positioned to deliver on many of these efforts.

With the expansion of legal and regulatory changes – specifically, those like the EU whistleblower directive, ESG disclosure directives and agreements, and pending SEC regulations – the scope and responsibilities of risk and compliance officers continues to grow. Staying ahead of these changes requires strong cross-functional partnerships and diligent attention to the regulatory landscape.

This year's observations and predictions build on those of the last two in many ways. One of which is embracing our humanity and recognizing that our employees bring their whole selves to work as we collectively adjust to a new normal. This is important now more than ever.

Today, we find ourselves in a highly politicized and divided world – inside and outside the workplace. Meeting employees and the public where they are is no easy feat. Considerations about remote onboarding and distributed workforces, coupled with the need to cultivate a diverse, equitable and inclusive workplace, pose significant human and business operational challenges. Additionally, maintaining security internally and with third parties, as well as upholding the latest data privacy laws continues to be a moving target for risk, compliance, IT and cybersecurity leaders.

The coming year will not be business as usual – this is business in the new normal and it is here to stay. Some may look at the ongoing disruption as a major setback (and for many, it was). However, the increased visibility into corporate responsibility, organizational culture and inclusivity, ESG efforts, and more, continues to redefine the role risk and compliance play and the direction of organizations worldwide. And this is a good thing.

A photograph of three business professionals (two men and one woman) leaning over a large wooden table, intently studying a large document or blueprint. The woman on the left is wearing a white button-down shirt. The man in the middle is wearing a grey patterned shirt and a dark tie. The man on the right is wearing a dark jacket and glasses. They are in a bright, modern office setting with large windows in the background. The image is partially overlaid by a dark teal rectangle on the left and a white rectangle at the bottom right, which contains orange geometric shapes.

“Clear and meaningful examples of how ESG impacts the culture of the business help to reinforce the importance of prioritizing ESG as a long-term initiative and investment in the future of the company.”

Risk and Compliance Management Includes Oversight of ESG



BY: CARRIE PENMAN

Chief Risk & Compliance Officer, NAVEX

In the last year, there has been much discussion about upcoming regulation of Environment, Social and Governance (ESG) public reporting because of the financial impact of socially responsible investing on the capital markets. There has also been considerable discussion in the compliance community about whether compliance should “own” ESG oversight.

Some are very much for it and see the synergies. Others believe that adding this responsibility will strain the already limited resources available to compliance functions adding risk to their organizations if the compliance function is further diluted. And to be frank, adding the need to become knowledgeable of a totally new and complex topic like environmental management is daunting.

All that said, oversight of ESG belongs with risk and compliance because overseeing ESG involves both risk management and compliance expertise and we will continue to see these responsibilities converge.

Risk and Compliance’s Role in Managing ESG

Risk and compliance leaders are already heavily involved with the social and governance management of ESG. Providing mechanisms for reporting wrongdoing, tracking data on

human and social capital, identifying and managing third-party risk, and handling the legal and regulatory aspects are all commonly the responsibility of risk and compliance professionals.

In addition, a recent OnePoll survey¹ of corporate compliance leaders across the U.S., U.K., France, and Germany shows 89% of respondents already include ESG reporting as part of their compliance program. And of the 11% of organizations that do not include ESG as part of their compliance programs, 71% strongly or somewhat agree that compliance should be involved with ESG management.

89%

of respondents already include ESG reporting as part of their compliance program

Chief Compliance Officers (CCOs) are a natural fit to be leaders of ESG programs because of their demonstrated ability to engage with multiple stakeholders and leverage cross-functional teams to ensure compliance with various regulations, and to report on the most pressing risks the business faces. For example, CCOs already engage with multiple departments on issues of discrimination, anti-bribery or creating an organizational culture that supports

¹ Source: NAVEX Press Release: Global Compliance Survey Highlights Convergence of Environmental, Social and Governance (ESG) and Compliance Programs

compliance with policies and regulations. Likewise, the scale and complexity of ESG drives the need for multiple stakeholders from across the organization to be involved and for this oversight to be managed.

A converging ESG and risk and compliance program does not assume CCOs become subject matter experts or tactical operators in bringing the three pillars of ESG together, but rather that CCOs leverage their existing line-of-sight across key business issues and tap into the experts who have the required information.

Increased Investor Attention and Disclosure Regulation Driving Need for Oversight Expertise

Consumer and investor attention to ESG matters in organizations, as well as in their supply chains, are at an all-time high. Upcoming regulation from the SEC around ESG disclosures will formalize the need for companies to define, track and report on their ESG progress with regulatory consequences for misleading or falsified information. Avoiding these risks and managing these requirements necessitates high-level and consistent oversight.

The historical lack of a standardized disclosure framework has led to organizations responding to requests for ESG information on an individual basis. Now, the formation of the International Sustainability Standards Board (ISSB) – announced at the 2021 COP26 summit – has a mandate to create ESG disclosure rules for companies in response to growing demand by stakeholders for greater standardization of ESG data. It's expected the new ISSB will issue its first set of standards in the second half of 2022.

The main objective of creating standardized ESG disclosure is so investors and other stakeholders have decision-useful, comparable metrics to measure performance. As jurisdictions determine the level of regulated disclosure informed by the ISSB, risk and compliance teams are well advised to organize their processes and prepare now to meet the requirements.

Mitigating Risk and Creating Value Go Hand-in-Hand

In practice, there is no single approach that will work to manage ESG because, just like with compliance issues, the ESG risk profiles of organizations vary widely. Risk and compliance functions are well versed in conducting risk assessments which identify and help mitigate issues that could have a negative impact on the business. Similarly, in the world of ESG, materiality assessments are meant to identify direct and indirect economic, environmental, and social impacts by the business. While the language may differ, risk and materiality assessments are effectively the same process that CCOs know well.

ESG risks are now recognized as financially material to the business. Common examples of material ESG topics include monetary losses from legal proceedings associated with employment discrimination and labor law violations – both of which are compliance and ESG issues. Negative environmental impacts and supply chain sustainability can pose significant risks to the business, as well as the direct effect on the environment by those involved throughout the supply chain.

The role of the risk and compliance function in reducing risk for the business is also one that creates value for the organization. Risk and compliance leaders who oversee ESG programs make material impacts to the business and bring consistency to the approach and processes, thus reducing risk and ensuring unified management of critical risk mitigation functions.

Turning Plans Into Action

Driving meaningful change in ESG programs also necessitates a cultural adoption across the organization. While there is no one “owner” of culture within the business, compliance is often the driving force that ensures the company code of conduct is upheld, and that regular employee training takes place – all of which are fundamental to the organization’s culture. And, of all factors impacting company culture and employee engagement, performance against ESG factors may be the most important especially as the organization’s own employees demand it.

Examples of how compliance can advance ESG efforts include improving adherence to ESG protocols by performing due diligence, determining corrective actions, and tracking progress on sustainability and environmental impact. Another example is a partnership with Human Resources to improve company-wide diversity, equity and inclusion efforts. Analysis of the baseline, development of a strategy to make improvements, and tracking and reporting progress are top priorities for most businesses and should be present in a unified ESG strategy.

Clear and meaningful examples of how ESG impacts the culture of the business help to reinforce the importance of prioritizing ESG as a long-term initiative and investment in the future

of the company. Not only are dedicated leadership and transparency necessary for ESG programs to make an impact, but they will also become table-stakes with upcoming disclosure regulations.

2022 Prediction

Organizations will continue to see increased public attention to ESG matters and will need to act quickly to get ahead of the disclosure regulation curve. Compliance’s role in ESG management will and should continue to grow as organizations prioritize the creation and growth of ESG initiatives.

Visionary CCOs will see ESG responsibility as an opportunity for more resources, more organizational influence and impact, and a chance to further shape an ethical business culture. CCOs can be the leader, communicator, and coordinator. However, this cannot be just an “add-on” responsibility. This ownership must come with the appropriate resources, access to subject matter experts and overall authority to be successful. On the positive side, the right tools and technology exist to centralize and simplify the consolidation of subject matter expertise, benchmarking of goals, and compliance requirements.

CCOs who recognize the significant overlap that already exists between ESG, risk and compliance will be well situated to take their organizations – and their careers – to the next level as ESG and risk and compliance continue to converge.

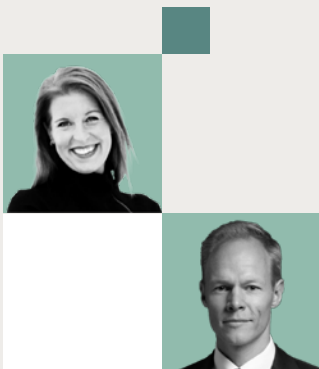
About The Author

Carrie Penman | Chief Risk & Compliance Officer, NAVEX

One of the earliest ethics officers in the industry, Carrie Penman is the Chief Risk and Compliance Officer for NAVEX Global. She has been with the company since 2003 after serving four years as deputy director of the Ethics and Compliance Officer Association (ECOA) now ECI. A scientist by training, she developed and directed the first corporate-wide global ethics program at Westinghouse Electric Corporation from 1994-1999. Carrie was recently awarded the inaugural Lifetime Achievement Award for Excellence in Compliance 2020 by Compliance Week magazine.

A man with curly brown hair and a beard, wearing round glasses and a headset, is smiling slightly. He is wearing a light-colored ribbed sweater over a blue and white striped collared shirt. He is sitting in a black office chair. The background is a bright, out-of-focus window. There are orange geometric shapes in the bottom left corner and a dark teal rectangle in the top right corner containing text.

"Despite the regulatory challenge, forward thinking companies and other organisations see that the Directive is not just about compliance."



EU Whistleblowing Directive

BY: **KARIN HENRIKSSON**

Director, WhistleB by NAVEX

JAN STAPPERS

Senior Manager, Partnerships, WhistleB by NAVEX

In December of 2021, the final EU Whistleblower Directive deadline was implemented into law. This piece of legislation focuses on encouraging and protecting whistleblowers who speak up about corporate misconduct. It acknowledges the value these people bring in helping organisations and states to uncover legal breaches at an earlier stage, thus preventing or minimising potentially harmful business losses and destructive behaviour. The Directive does this by placing the whistleblower at the centre, safeguarding their identity, prohibiting retaliation, and offering several channels for reporting.

In practice, the Directive requires organisations in all EU member states with 250 or more employees to establish a well-defined reporting channel and procedures to allow people to report concerns regarding illegal activities. Smaller organisations of 50 or more people will have until 2023.

While the Directive is a step forward in moving member states towards a unified legal framework, it may nonetheless result in a wide array of whistleblower laws. Responding to these will be a key challenge for compliance in 2022 – and beyond.

While the Directive is a step forward in moving member states towards a unified legal framework, it may nonetheless result in a wide array of whistleblower laws. Responding to these will be a key challenge for compliance in 2022 – and beyond.

Not Quite One Size Fits All

Though the deadline for the EU member states to incorporate the EU Whistleblower Protection into their national laws was December 17th, 2021, the vast majority of countries did not meet this date. Some proposals require additional consultation, and other countries have yet to start. Whether due to local political bureaucracy, down-prioritisation in the wake of the COVID-19 pandemic, or other obstacles – there remains significant work to be done.

The patchy timing across the EU is further compounded by the inconsistent starting point of each territory. Some countries already have their own extensive whistleblower legislation, such as the Netherlands and France. Others have laws that only apply to certain industries or company size. How local laws should align with the minimum standards of the EU directive, and the extent to which local laws should expand on the minimum standards, is hotly debated.

Another variable to consider is each territory has the freedom to expand on the scope of requirements stipulated at the EU level – in fact, this has been encouraged by EU regulators.

A Tougher Compliance Puzzle for Larger Organisations

National differences will arise, and monitoring and responding to these will create further compliance complexity for larger organisations and those operating across borders within the EU. For instance, what happens if the differences in protection lead to whistleblower forum shopping? This is when a person reports concerns in jurisdictions that are deemed to be more favourable, or where the scope of protected topics for disclosure better matches the person's issue.

Further, there is an additional requirement for legal entities with subsidiaries that employ 250 or more people. These subsidiaries need to have their own reporting channels and appoint separate recipients of reports for whistleblowers who do not want to report to a channel that is shared at the group level. While this may be more accommodating of the whistleblower, it creates a heavier burden for organisations. They will need to put the appropriate resources in place to handle reports at both subsidiary level and group level.

It is expected that in various countries, “effective, proportionate and dissuasive” penalties will indeed mean both natural and legal persons should look out for infringing the provisions related to whistleblowing. This goes both for retaliatory actions and for malicious whistleblowing.

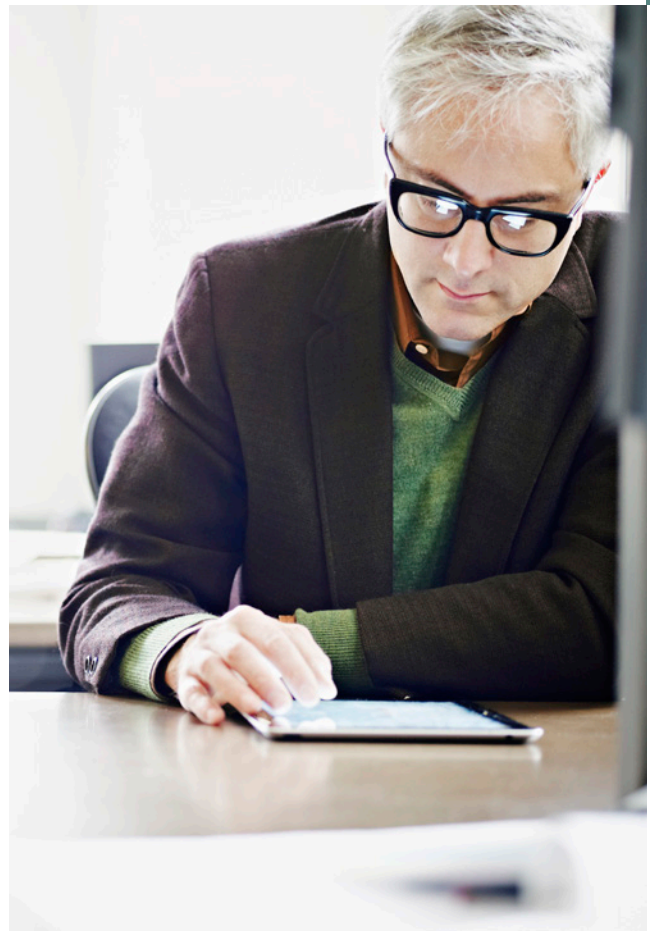
Clear Minimum Requirements Mean Progress Towards Compliance

Despite the above, inaction while waiting for territory transpositions is not recommended. The EU Whistleblower Directive clearly lays out a set of minimum requirements that will apply to all affected organisations in EU member states. Below we summarise these obligations and provide insight to go beyond compliance and gain further value from your whistleblowing program.

- **Provide secure channels for whistleblowing.** Organisations need to provide a reporting channel with a certain level of protection. It needs to be safe, and users should have multiple reporting options available – in-person, written or verbal – and resources should also be made available in the whistleblower's preferred language.
- **Maintain the confidentiality of the whistleblower and the data subject throughout the entire process.** Confidentiality is required by the Directive, and full anonymity is recommended – both increase the chances people will come forward to report and provide access to invaluable information.
- **Acknowledge receipt of the report within seven days.** This is a further indication of the importance placed on respectful treatment of the whistleblower. Organisations may opt for a system that alerts whistleblower report managers automatically. Accommodations must also be made to acknowledge receipt of anonymous reports, however member states may have differing requirements related to follow up.
- **Follow up on the case and provide feedback to the whistleblower within three months.** The Directive gives the whistleblower the right to know what is happening with their report, so it is important for cases to be monitored and followed up with.

Organisations will need to strike the right balance between sharing correct, but not too sensitive, information and providing feedback to the whistleblower throughout the process.

- **Maintain auditable records.** Consider a system that keeps a log of all case management activities carried out by all case handlers. Not only does this help keep control of investigations, it also provides evidence that the organisation acts compliantly and efficiently.
- **Protect whistleblowers against retaliation.** Retaliation is any form of negative consequence of filing a report. Ensuring retaliation does not occur may require training, policy or code of conduct updates, adequate security controls, and internal control. This is a key point of compliance, but more importantly contributes to ethical business and a healthy workplace environment.
- **Provide the workforce with information regarding the channel.** At a minimum this involves facilitating whistleblowing and informing users of the different country laws and their rights to report externally. More broadly this requirement may prompt a review of the corporate culture and whether it acts as a foundation for trust and transparency.
- **Allow reporting access to third parties.** The Directive defines a far wider scope of stakeholders as potential whistleblowers who would be eligible for protection. Organisations will therefore need to give reporting access to permanent and temporary employees, volunteers, former employees, contractors, family members of employees, and even suppliers.



- **Appoint impartial and experienced people to manage whistleblowing reports.** This presents a substantial challenge for many organisations. Typically, legal or compliance functions own this responsibility, and organisations should also assess whether it is safer or more efficient to use an outside party to receive reports.
- **Process any personal data in accordance with the EU GDPR requirements.** It is extremely important to take data security seriously as the whistleblower channel will contain personal and sensitive data. Organisations may want to find a system that helps to comply with this requirement automatically. Such a system would include functionalities to limit accessibility to data, store data in the EU, encrypt the data and ensure the organisation alone can unencrypt the data.

Go Beyond Compliance – Capture the Value of Whistleblowing

Despite the regulatory challenge, forward thinking companies and other organisations see that the Directive is not just about compliance. The Directive provides an opportunity for more ethical business, increased transparency, risk mitigation, reduced financial losses, brand enhancement, and talent attraction. All these benefits are outcomes of successful whistleblowing programmes, which in turn are wholly dependent on whistleblower trust.

To establish that trust, whistleblowers need to be considered valuable assets. For the first time ever, this Directive does just that. It positions the whistleblower as a hero, protects their rights and

requires structures that give them greater confidence to step forward and report concerns. Companies that go beyond compliance and truly embrace whistleblower protections stand to gain the most.

2022 Prediction

As member states and organisations within the EU adopt whistleblower programmes that adhere to the Directive, global attention will be paid to the future of whistleblowing. Organisations around the world will be expected – by the Directive, other upcoming legislation, and societal pressure – to go beyond compliance box-checking, and to create a culture where whistleblowers are encouraged to speak up, reports are managed professionally, and appropriate action is taken to correct any corporate misconduct.


About The Authors

Karin Henriksson | Director at WhistleB by NAVEX

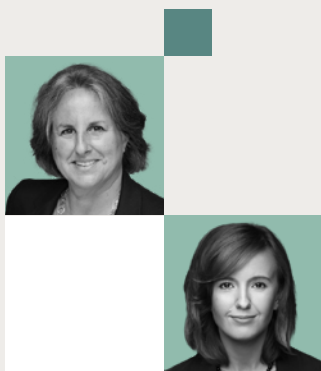
Karin is the co-founder of WhistleB, a global whistleblowing SaaS provider; now a part of NAVEX, Karin serves as the Director of WhistleB where the service is currently used by customers in more than 150 countries in 60 languages. Karin is also the co-founder of TripleB, a sustainability consultancy and has worked in the sustainability and compliance sector since 2006.

Jan Stappers | Senior Manager, Partnerships, WhistleB by NAVEX

Jan Tadeusz Stappers is senior manager partnerships for NAVEX Global's digital whistleblowing solution, WhistleB. More than 10,000 organisations and 50 million employees globally rely on NAVEX Global's whistleblowing solutions every day to safely report and manage their workplace concerns. Jan has authored various articles on new legislation concerning whistleblower protection and organisational whistleblowing best practices. Jan holds a Postgraduate Diploma (PGDip) from King's College London in the United Kingdom (EU Competition Law) and a Master's Degree (LL.M.) from Leiden University in the Netherlands (European Law). He is Certified Information Privacy Professional (CIPP/E) with the International Association of Privacy Professionals (IAPP).

A woman with long dark hair, wearing a light pink button-down shirt, is smiling and looking towards a man on her left. She is holding a black pen over an open notebook. In the background, another man is partially visible, looking down. The scene is set in a bright, modern office environment with large windows in the background. The image is overlaid with a dark teal rectangle on the left containing text, and two orange rectangles at the bottom right.

“There is a definite need
for greater clarity on
the substance behind
sustainability claims,
and the EU Commission
is leading the way.”



Environmental, Social & Governance (ESG) Disclosure Adoption – What Can We Learn From the EU?

BY: KAREN ALONARDO
VP ESG Solutions, NAVEX

VERA CHEREPANOVA
Ethics and Compliance Consultant, Studio Etica

EU Disclosure Requirements

The European Union has emerged as a leader in ESG with its Non-Financial Reporting Directive (NFRD) dating back to 2014. When the NFRD was passed, large European businesses were asked to undertake non-financial reporting on ESG matters for the first time. Flexibility was essential – companies were allowed to rely on various frameworks to produce their non-financial statements and report on a “comply or explain” basis. Today we see the downside of this: the lack of disclosure alignment is commonly cited¹ as a major challenge. The revised NFRD is expected to address this issue – but while we wait for it to pass, reporting under the NFRD remains the key source of non-financial information for EU-based asset managers.

There is a definite need for greater clarity on the substance behind sustainability claims, and the EU Commission is leading the way. One of the key elements of recent EU ESG measures is the Taxonomy line-item disclosure guidance (introduced in 2020), and a classification tool of economic activities that can be viewed as sustainable. Businesses now have to map their economic activities to the Taxonomy thresholds and assess if they contribute to or at least Do No Significant Harm (DNSHs) for each of the

Taxonomy’s environmental objectives. Financial market participants in scope of the recently adopted Sustainable Finance Disclosure Regulation (SFDR) need to disclose information on Taxonomy-alignment of their financial products.

The direction of travel is clear: to support the transformation of the EU economy disclosure requirements as they get more rigorous. The legislative initiatives those adopted and forthcoming, are central to the EU plan to achieve its ambitious sustainability targets.

US and Global Focus on Integrated Standards

The US is following the EU and international directives to address global ESG initiatives through actions by the Security Exchange Committee (SEC) and International Finance Reporting Standards (IFRS). This month, the IFRS Foundation announced the formation of the International Sustainability Standards Board (ISSB)² which reflects the consolidation with the Carbon Disclosure Standards Board, an initiative of the well-recognized Carbon Disclosure Project, used by many US companies, and the Value Reporting Foundation. This is a huge step forward for global adoption of ESG disclosure that goes beyond traditional Sustainability management and reporting that has been an initiative for global companies for more than ten years.

¹ Source: PwC, “The growth opportunity of the century. Are you ready for the ESG change?”

² Source: IFRS Foundation announces International Sustainability Standards Board, consolidation with CDSB and VRF, and publication of prototype disclosure requirements

The Value Reporting Foundation, formerly the Sustainability Accounting Standards Board (SASB), was established several years ago to develop industry-level standards and materiality mapping to create a standard with investors in mind.³ With investor focus on ESG, the need for high-quality ESG disclosure standards will address the investor community's desire to make informed decisions beyond financial considerations. The plan is to complete the consolidation of these standard bodies by June 2022. When this is in place, global companies will be better positioned to meet the disclosure requirements needed for financial markets and investors to drive transparency and value creation, and mitigate risk. The technical groundwork to streamline corporate sustainability disclosures is in place for market adoption.

EU Climate and Biodiversity Action

On the climate change front, since the Paris Climate Accords in December 2015 the EU has been at the forefront of international efforts to fight climate change. It was instrumental in brokering this first-ever legally binding global climate change agreement – however, some of the member states took pioneering steps before that. Notably, Article 173 of the French Energy Transition Law passed in 2015⁴ required institutional investors to report carbon emissions and publicly listed companies to implement low-carbon strategies. Today, the EU continues to show global leadership in climate action, advocating an integrated approach to mitigate climate change and biodiversity loss.

³ Source: IFRS Foundation announces International Sustainability Standards Board

⁴ Source: Principles for Responsible Investment, French Energy Transition Law: Global investor briefing on Article 173

“By 2017, the EU had reduced its greenhouse gas emissions by almost 22% compared to 1990, reaching its 2020 emission reduction target three years ahead of schedule.”⁵ The European Green Deal that followed in 2019 provided a roadmap for legislative and non-legislative initiatives which should help to make Europe the first climate-neutral continent by 2050, safeguard biodiversity, establish a circular economy, and eliminate pollution. To further increase the climate ambition, in December 2020, the “EU leaders endorsed a binding EU target for a net domestic reduction of at least 55% in greenhouse gas emissions by 2030 compared to 1990.”⁶ To implement this, the EU Commission announced a raft of climate change proposals (including jet fuel tax, carbon border tariff, and many more) known as “Fit for 55.”⁷ These measures will likely have an impact on every citizen of Europe in almost every aspect of their lives.

EU Corporate Action

Ambitious sustainability targets are in the spotlight for the EU regulators, and this should translate into corporate action.

Although the NFRD doesn't require that, companies held up as exemplars driving ESG strategies in the EU (including Eni, Bayer, Unilever, and others) define science-based targets aligned to Paris Agreement and/or United Nations Sustainable Development Goals (UNSDGs). Research shows that many organizations still do not follow this best practice⁸, and increased regulation is expected to fix this. Envisaged NFRD amendments would require companies to define targets and report annually on progress against them.

The question of who should own ESG seems to be mostly sorted for EU-based organizations – back in the

⁵ Source: European Council, Council of the European Union, “Climate change: what the EU is doing”

⁶ Source: European Council, Council of the European Union, “Climate change: what the EU is doing”

⁷ Source: Legislative Train Schedule, Fit for 55 Package Under the European Green Deal

⁸ Source: Alliance for Corporate Transparency 2019 Research Report

days when ESG was still known as “Corporate Sustainability”. Whether it be a dedicated Chief Sustainability Officer reporting directly to the Board, or a Sustainability Unit inside of the Investor Relations – most large businesses in Europe have had this function in some form for years. The ESG paradigm, however, brought in the “G”, which has always been managed separately by ethics and compliance and/or legal counsel. At this point, working in silos is no longer an option: going forward, a coordinated approach will be key to integrated risk management.

US Action

The writing is on the wall with pending US regulation upcoming from the SEC.⁹ As companies realize the need to comply with investor pressure today without regulation, further adoption is inevitable across all industries. Historically, the US was driven by Corporate Social Responsibility (CSR), which focused on some elements of what we are seeing under the Social component of ESG today. The evolution continues with the recognized need to fully integrate environmental, social and governance. As corporations drive toward profitability, it's imperative they align with key performance indicators and metrics to determine how well they are performing in each of these categories.

US organizations have taken action without regulation as key stakeholders, like consumers, have demanded insights into how companies are conducting business when producing and selling products and services. As an example, Intel and other hardware companies launched a non-profit to focus specifically on conflict minerals. From that, the Dodd-Frank Act incorporated conflict

minerals¹⁰ compliance to identify if armed guerilla groups or forced labor were being used to extract minerals from mines to produce products like the iPhone and other technology.

In other areas, companies have taken the initiative to invest in CSR and Sustainability reporting using key frameworks like the Value Reporting Foundation, Global Reporting Initiative and others to get ahead of regulation (and because it made practical business sense). Once companies adopted these initiatives, they quickly realized cost savings, operational efficiencies, and increased brand recognition.

The movement around ESG will propel CSR and Sustainability initiatives forward as we now look at them from investor, financial and consumer lenses.

Next Steps – EU, US and Beyond

The recent COP26 summit in Glasgow, UK brought nations together to accelerate action towards the goals of the Paris Agreement and the UN Framework Convention on Climate Change. Although there is some disappointment among environmental groups over the conference outcomes, investor activism is clearly on the rise. More than 450 financial firms representing \$130 trillion USD in assets – or 40 percent of the world's financial assets – committed¹¹ to use their funds to work towards net-zero emissions by 2050. This means corporations will face greater scrutiny over their ESG policies.

The revised NFRD, soon to become the Corporate Sustainability Reporting Directive (CSRD), will considerably reinforce non-financial reporting requirements. Additionally, this will expand their scope to cover around 50,000 entities (compared to the 11,700 currently subject to the NFRD). Companies will have to report to new European Sustainability Reporting Standards currently developed¹² by the

9 Source: SEC Response to Climate and ESG Risks and Opportunities

10 Source: Responsible Minerals Initiative

11 Source: Glasgow Financial Alliance for Net Zero

12 Source: GRI welcomes role as ‘co-constructor’ of new EU sustainability reporting

European Financial Reporting Advisory Group (EFRAG) in close cooperation with the GRI. This unprecedented collaboration aims to contribute to further convergence between European and global sustainability reporting standards. In a best-case scenario, the CSRD can be adopted in late 2022.

Beyond the EU, the UK government has proposed¹³ UK companies should meet the Taskforce on Climate-related Financial Disclosures (TCFD) recommendations from 2022. Large Swiss firms will be required¹⁴ to report on their climate-related risks starting in 2024, and the mandatory guidance is expected by the end of summer 2022.

In APAC, vast political, economic, and social differences among countries translate into fragmented ESG regulations across the region. Navigating this is the primary challenge for multinational organizations. Leading countries have made commitments to achieving net-zero emissions within varying timeframes. South Korea, Japan and New Zealand plan to do so

¹³ Source: Gov.uk press release, "UK to enshrine mandatory climate disclosures for largest companies in law"

¹⁴ Source: The Federal Council press release, "Federal Council sets parameters for binding climate reporting for large Swiss companies"

by 2050, while China and Indonesia have pledged to become carbon-neutral by 2060. With the EU Taxonomy introduced in 2020, APAC regulators started working on green taxonomies as well. Earlier this year China announced¹⁵ a collaboration with the EU to adopt a common taxonomy for green investments. Following the EU lead on mandatory non-financial reporting more countries in the region are expected to set stricter regulations around sustainability reporting soon.

2022 Global Prediction

In 2022, the shift from ESG voluntary guidelines to binding regulations will continue and accelerate. Key new legislation including the CSRD and the pioneering EU Directive on Corporate Due Diligence and Corporate Accountability are likely to be adopted. Pursuant to the Taxonomy and SFDR requirements, asset and wealth managers will need to integrate ESG into everything they do moving to the next level of ESG integration at a product level. New regulations will require new data sets – effectively tackling the ESG data challenge will remain pivotal to success.

¹⁵ Source: Financial Times, "China reveals co-operation with EU on green investment standards"


About The Authors

Karen Alonardo | Vice President of ESG Solutions at NAVEX

Karen Alonardo, MSEM, is the Vice President of ESG Solutions at NAVEX Global, formerly the founder and CEO of CSRWare (acquired by NAVEX Global in 2020). Karen has held several key leadership and entrepreneurial positions at Fortune 500, private start-up, and high-growth companies, including Director of Online Operations and Information Systems and Technology at Electronic Arts and VP of Operations at Critical Path, the first technology company to deliver email as a hosted service.

Vera Cherepanova | Ethics and Compliance Consultant at Studio Etica

Vera Cherepanova is a former Regional Compliance Officer and author of "Compliance Program of an Organisation." Vera has worked on the ground in Eastern Europe, CIS and Russia, one of the key emerging markets. Taking her experience in addressing the cross-cultural challenges of ethics and compliance, Vera currently consults with international corporations, non-profits, wholesale and retail establishments, and small to large businesses, advising them on E&C programs. Vera speaks Russian, English, French, and Italian.



"Compliance leaders must demonstrate the importance of ethical conduct and make that message cut through all the other signals employees are receiving."

The New Normal Workplace (Part 1) – R&C Management



BY: MATT KELLY

Editor and CEO, Radical Compliance

Most businesses began 2021 with ambitions to return to the office. But in keeping with a trend of disruption, we are faced with new COVID-19 variants, questions on when and how schools will respond, a cultural shift towards flexible work, and more. Given this uncertainty, remote and hybrid work paradigms are here to stay for the foreseeable future.

This is where legions of companies landed at the start of 2022. The hybrid work environment is now the work environment for many; and for those with essential onsite work, the way work is done has forever changed. Compliance and risk concerns that arise from the new normal work environment are increasingly complex and challenging – and compliance leaders must work cross-functionally to stay abreast of changes impacting business operations. Three concerns stand out as perhaps the most important of these challenges.

Cybersecurity Will Be a Bigger Priority for Everyone

Cyber threats have existed for decades, and as one business process after another underwent “digital transformation,” each transition exposed more of the enterprise to those dangers. Moreover, digital transformation allowed businesses to collect more data: about customers, consumers, employees, third parties.

That spawned a wave of new data protection laws such as the EU General Data Protection Regulation and a bevy of state laws, such as the California Privacy Rights Act.

The pandemic, however, accelerated those digital transformations even more. Now essentially all business processes have to exist digitally to accommodate a combination of remote, hybrid and on- premises work. Businesses today must assume every business process happens digitally. Because of this, cybersecurity and privacy concerns permeate all business processes, all the time.

Now essentially all business processes have to exist digitally to accommodate a combination of remote, hybrid and on-premises work. Businesses today must assume every business process happens digitally. Because of this, cybersecurity and privacy concerns permeate all business processes, all the time.

Many organizations were already well along in their digital transformation journey, but the new normal work environment means companies can't rely primarily on physical office locations to provide strong cybersecurity. A distributed workforce means increased complexity to maintain cybersecurity across an unprecedented variety of work locations.

While IT security teams can continue to implement best practices such as a Zero Trust¹ approach to cybersecurity, companies also need to rely more on employees themselves adopting a security-aware mindset. In the same way companies have relied on the tone from the top, training, and incentives for anti-corruption; they'll need to do the same for cybersecurity awareness and training. Employees should be trained and coached to be vigilant about cybersecurity – because in the hybrid world it will take a collective effort to maintain.

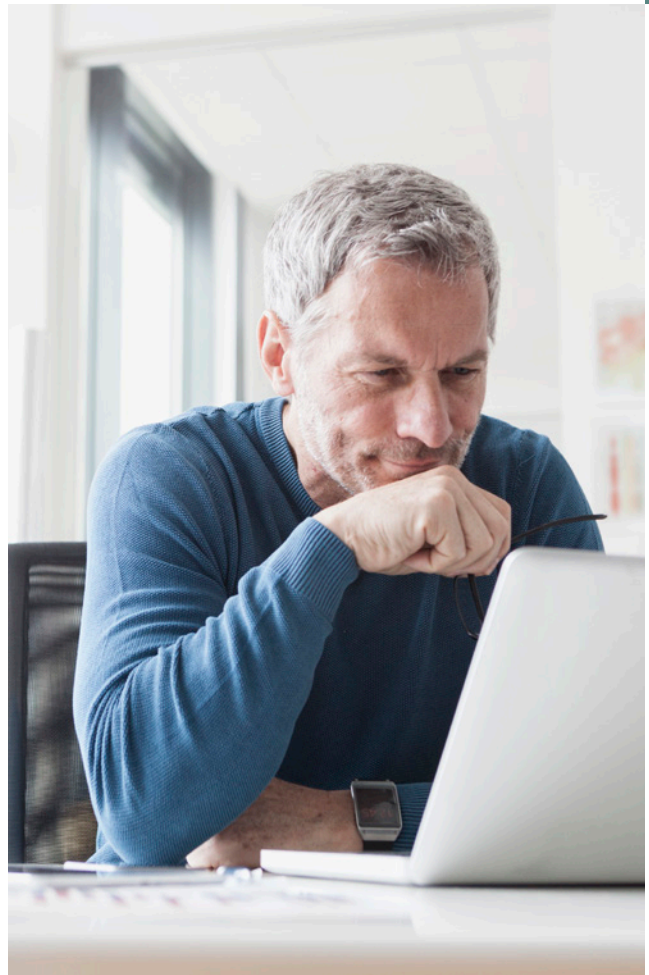
The Ability to Map the Company's IT Assets Will Be Critical

Mapping is the ability to locate where corporate assets exist, both physically in the real world and logically as part of your company's IT infrastructure. This includes data, devices, and critical applications. Prior to the pandemic, most IT assets existed in physical offices most of the time. In a hybrid work environment, those assets can be anywhere.

Compliance officers need to know where IT assets exist physically to understand privacy obligations and other regulatory compliance concerns. For example, China's new data privacy law requires that data collected in China about Chinese nationals must remain in China; so, you need to know whether employees have mistakenly transferred that data to a technology service provider based in North America. Or, if employees start using corporate IT devices on a home network, you need to know so you can implement security protocols such as extra password protections.

Risk managers and CISOs, meanwhile, need to know the "logical" map of their IT environment.

¹ Reference: NAVEX Blog: "Moving Beyond Borders, How to Achieve Information Security in a Time of Zero Trust"



That lets them understand which applications are mission-critical to operations; which applications were installed onto the network without proper permissions; or which troves of data need maximum protection from ransomware attacks.

Mapping IT assets is critical to regulatory compliance and business continuity. A hybrid work environment makes the task more complicated, so companies must assure they have strong capabilities on this front.

Cultivating an Internal "Speak Up" Culture Will Be More Challenging

We can never ignore how important the human element is to effective compliance and ethics. In the hybrid environment, however, it becomes a lot easier for the humans to ignore the fundamentals of ethics and compliance.

This is not to say employees don't care about ethics and compliance, because most still do. But working remotely can leave more employees feeling less connected to the organization — so when they do see misconduct, they may just report the matter to regulators directly, or not report at all. Compliance officers will need to work diligently and creatively to maintain those bonds of corporate culture and keep a speak up culture strong.

At the same time, internal reports about corporate conduct will be even more important for compliance officers to hear. The types of misconduct or risk that might happen in a hybrid environment will be more varied, and the compliance officer's ability to observe those activities directly will be more difficult.

Compliance leaders must demonstrate the importance of ethical conduct and make that message cut through all the other signals employees are receiving. Additionally, giving employees practical ways to report misconduct — whether they're working on premises, remotely, or in a hybrid capacity — will be capabilities compliance officers must make permanent in 2022.

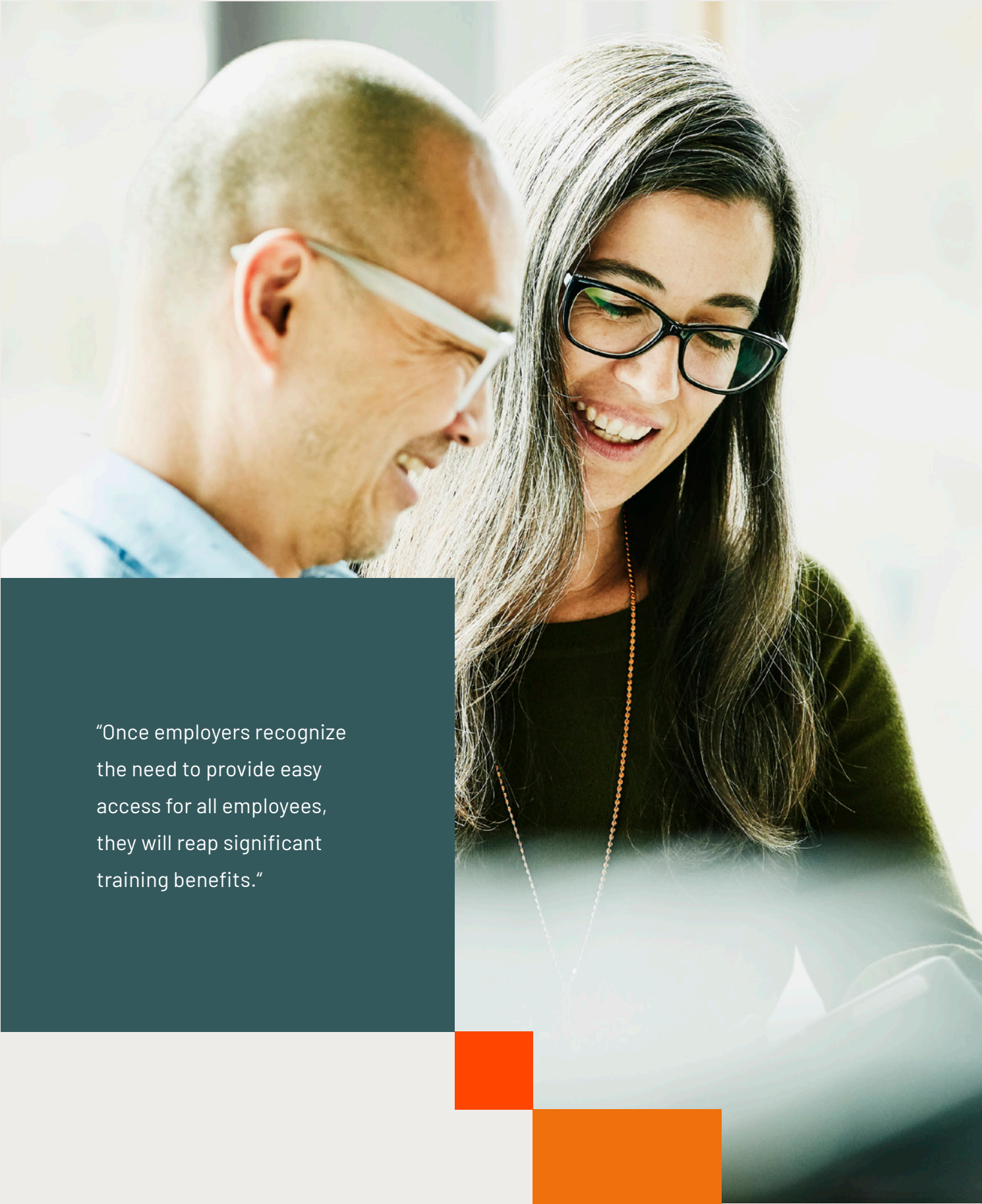
2022 Prediction

Ransomware and other cybersecurity attacks will become even more pervasive in 2022. The good news is risk and compliance officers now understand the tools they can employ against the threat, such as Zero Trust architecture and a security-aware corporate culture. The race is on to see whether compliance functions can execute on those ideas faster than the attackers can lay siege to your business.

About The Author

Matt Kelly | Editor & CEO at Radical Compliance

Matt Kelly was editor of Compliance Week from 2006–2015. Prior to his role at Compliance Week, he was a reporter and contributor on corporate compliance and technology issues for magazines such as Time, Boston Business Journal, eWeek, and numerous other publications. Matt now maintains his own blog, [RadicalCompliance.com](https://www.RadicalCompliance.com), and writes & speaks frequently on all things GRC.

A photograph of a man and a woman in an office setting. The man, on the left, is balding with glasses and is smiling. The woman, on the right, has long dark hair and glasses, and is also smiling. They are both looking down at a laptop screen. The background is bright and out of focus. In the bottom right corner, there are two overlapping orange squares.

"Once employers recognize the need to provide easy access for all employees, they will reap significant training benefits."

The New Normal Workplace (Part 2) – Training and Policy Management



BY: INGRID FREDEEN

VP, Senior Product Manager, NAVEX

A year ago at this time, we looked ahead to a year that was predicted to be more polarized, more distributed, and marked by more objections to training content. Last year undeniably delivered on that prediction – whether it was training about diversity, harassment, workplace violence and abusive conduct, active shooter training, or COVID-19 health and safety protocols, employees had opinions. The continuation of remote and hybrid work pressed organizations to move from a “wait and see” approach, to a “we must figure out how to train in this new environment” initiative.

Although the future of work in the long term remains fluid, focusing on these three strategies will help your organization weather 2022 much more successfully.

As we look forward to 2022, employers will need to focus on distribution of policies and training in the “new normal” state. The problem is it’s still not entirely clear what characteristics will define normal. And even when we feel like we have it all figured out, there is a high likelihood it will change again.

Although the future of work in the long term remains fluid, focusing on these three strategies will help your organization weather 2022 much more successfully.

Prioritize Access to Technology

Two forces are at play – remote work is here to stay for many workplaces, and in those workplaces where on-premises work is essential (such as service, manufacturing, hospitality and transportation) gathering people in one location for in-person training is in decline. To support this new normal, employers must focus on getting all employees access to the technology necessary to access training and policies. This includes employees who have no other need for technology in their work and don’t have corporate email addresses or personal devices. Without a commitment to providing access and an investment in technology, employers will continue to struggle with delivering training to all those who need it, and those who are required by law to receive it.

Once employers recognize the need to provide easy access for all employees, they will reap significant training benefits. Key among those benefits are more efficient learners, and delivery of a more controlled, consistent message around topics that are critical to the organization. This approach to training delivery helps ensure it is completed successfully, risks are discussed appropriately, and individual instructors do not influence the content with personal opinion or bias.

Adapt to Emerging and Evolving Risks

The risk profile of most organizations has evolved significantly in the past 1-2 years. New risks have emerged, and existing risks have become more

profound. COVID-19 protocols and compliance requirements; wage and hour off-clock work by remote workers; the growing need for active shooter training; harassment and discrimination with a focus on contemporary examples; and purposeful, deliberate approaches to diversity and inclusion are but a few of the topics that have taken on a new level of importance for all organizations. Addressing these risk areas successfully is not just about covering the topic, it is all about covering it properly. A course you may have deployed years ago is likely in need of new content, new approaches, and new messaging – and it should reflect where your organization is today with respect to the risk.

Other risks continue to evolve and gain attention too. For example, the Environmental, Social and Governance (ESG) frameworks that are rapidly evolving have brought new focus on the global impact that businesses have on the world around them. But like any other area of risk and responsibility, employers will need to assess and determine what kind of training they need to do to support their organization's ESG program.

Clarity of Expectations

Living in uncertainty is difficult for many people, and 2022 will be marked by ongoing uncertainty. Employers should do what they can to create certainty for their employees – even if it means some employees won't agree with the position being taken.

Policies and your Code of Conduct are a great place to set expectations and give employees a bit of clarity about the consequences they will face for their actions. Current policies may reflect what was good enough yesterday but are no longer sufficient in the new normal.

Policies should be viewed as a cornerstone for employees relating to conduct and performance – and consequences for their actions. Organizations must make a plan to critically assess and update key policies with the goal of making them more clear, usable and accessible

Policies should be viewed as a cornerstone for employees relating to conduct and performance – and consequences for their actions. Organizations must make a plan to critically assess and update key policies with the goal of making them more clear, usable and accessible. Think about what kind of content not only should be in your policy, but also needs to be in your policies in light of the shifts we have been experiencing. After which, it is critical to ensure to update appropriate training to include the most current reflection of your policy and key expectations. As you update policies, think about the events challenging the company, and consider whether your policy provides enough guidance for managers and employees to respond appropriately.

There are many contemporary examples of employee behavior that may seemingly fall into a gray area of where an employer can or should take a stand, for example:

- A racist rant posted on social media that was recorded while an employee was out with friends
- A manager who refuses to enforce the organization's policy relating to vaccine or face covering requirements
- An employee who posts threatening memes on a social media page not related to work
- A manager who holds personal beliefs that are contrary to the core values of your organization

Your policy and training may not lay out specific examples such as those listed above, but the language should contemplate the potential for events such as these. We will continue to see swift calls for employer justice when misconduct and misdeeds caught on video are posted on social media. But most importantly, employees should not be surprised when corrective action for behavior is issued.

2022 Prediction

In many ways this year will be a continuation of the last several, where employers work to continue to evolve and adapt training and policy to a highly polarized environment while also investing in technology and resources to ensure equity in education and enforcement across the workforce. Employers will continue to navigate a variety of training and conduct enforcement challenges. Effectively managing training and code of conduct policy requires a thoughtful approach and dedicated resources to ensure employees are reached equally.



About The Author

Ingrid Fredeen | VP & Senior Product Manager at 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 Global's online training course initiatives utilizing her more than 20 years of specialization in employment law and legal compliance. Prior to joining NAVEX Global, 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.

"A third party can either create additional risk to your company and its strategic plan or they can help reduce risk."



Holistic Third-Party Risk Management

BY: SUSANNA CAGLE, MICHAEL VOLKOV, AND CAROL WILLIAMS

Third-party relationships span a multitude of goods and services necessary for organizations to operate. Naturally, with these relationships comes a certain amount of risk, as these vendors expand the human capital footprint, technology access, environmental impact of the organization, and more. Increased public, investor, and internal attention to how organizations conduct business brings further scrutiny – not just of the primary business in question, but also the risks posed by its third parties.

Holistic risk management looks at three main categories of risk that third parties can expose their partners to: regulatory, enterprise, and environmental, social and governance (ESG). Here we discuss trends in holistic third-party risk management and considerations that organizations should make to assess and mitigate these risks for 2022 and beyond.

Regulatory Risk Management

WRITTEN BY MICHAEL VOLKOV



The exponential growth of the modern supply chain, coupled with expanding regulatory oversight, means third parties can expose an organization to numerous, far-reaching, and often severe risks. Organizations must understand the risks each third party poses to the business, and have a plan in place to effectively manage and mitigate them.

Risk assessments are a fundamental part of third-party risk management programs. They serve as a guide for the initial decision of whether or not to enter into a third-party relationship and are a core element of monitoring the relationship on an ongoing basis once established. It is a key step in an organization's efforts to comply with applicable laws, regulations, and guidelines and should be part of its overall compliance program to prevent, detect, remedy, and report misconduct.

The manner of due diligence depends on many factors, including:

- The risk profile of the countries at issue
- The industry

- The extent and nature of interaction with governmental or state-owned counterparties
- Whether the third party will retain other third-party agents or representatives in conjunction with its work for the company

Regular supply chain audits are necessary as liability can extend to unknown sourcing from prohibited parties and parties that are not in direct privity. Further, regulatory requirements frequently guide organizations on how to execute their third-party risk management program and what sorts of risks or red flags to look out for when transacting with third parties.

As a prime example, we've continued to see a rise in trade sanctions enforcement. Both direct and indirect transactions with sanctioned parties can trigger liability and lead to significant penalties under the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) regulations in connection

Risk assessments are a fundamental part of third-party risk management programs. They serve as a guide for the initial decision of whether or not to enter into a third-party relationship and are a core element of monitoring the relationship on an ongoing basis once established.

with the various sanctions programs established by the U.S. government. While many sanctions violations occur because a U.S. person exports a physical item to a sanctioned party, the provision of services to a sanctioned party can also be a violation. For example, it could be a violation of U.S. sanctions for a U.S. person to provide consulting services to the government of a sanctioned country or marketing services to a private business in a sanctioned country.

Any party engaged in or contemplating international business must understand how to navigate the applicable statutes, regulations, lists, and agency directives and guidance so as to ensure compliance with its U.S. sanctions obligations. OFAC specifically maintains a variety of sanctions lists, with the most extensive and restrictive list being the list of Specially Designated Nationals and Blocked Persons (the SDN List), which lists entities and individuals with which U.S. persons are generally prohibited from conducting any business. Common prohibited activities include:

- Importing goods from or exporting goods to a targeted nation
- Providing a loan or other financing to an SDN, or transferring funds to an SDN
- Facilitating any transaction by a non-U.S. person that would be prohibited if performed by the U.S. person or within the United States

In effect, this prohibition bars U.S. persons from taking any action to assist or support trading activity with a prohibited country, entity, or individual, unless specifically authorized. Furthermore, any activity that supports, authorizes, or otherwise assists in the conduct of a transaction by a non-U.S. person, where that transaction would be prohibited if conducted directly by a U.S. person, constitutes prohibited facilitation.

Prior to entering into any international business relationship, a company should conduct appropriate due diligence on the parties involved, including diligence on those parties' ownership and control. This includes screening international business partners, including distributors, customers, agents, brokers, and other third parties against applicable U.S. prohibited parties lists. The lists that should be consulted will vary depending on the scope and type of international business that a company conducts.

Increasingly, regulators expect U.S. companies to dedicate resources to their compliance functions sufficient to perform appropriate due diligence of all third parties, including intermediaries like resellers and distributors. For example, in March OFAC announced a settlement agreement stemming from an enforcement action with UniControl, Inc (UniControl). The company shipped goods to European trading partners when UniControl knew or should have known that some of its products would ultimately be re-exported to Iran.

It is important to remember that aside from sanctions violations, an organization may be liable for a third party's corruption, fraud, financial crimes (such as money laundering), unethical practices (including employment and human rights violations), actions causing environmental harm, and cybersecurity lapses or mishandling of sensitive data. This last item is of increasing importance, as third-party providers may access an organization's IT systems and/or handle personal information relating to the company's employees, contractors, customers, business partners, and other third parties. This past year, regulatory agencies have held entities responsible for the cybersecurity lapses of third parties that entity does business with, and this will become increasingly important come 2022.

2022 Prediction: Third-Party Risk – Regulatory Requirements

In 2022, third-party due diligence will constitute an increasingly important part of a compliance program's duties – and its budget. Periodic supply chain audits and screening against sanctions and prohibited parties lists will become a requisite for successful third-party risk management.



Enterprise Risk Management

WRITTEN BY CAROL WILLIAMS

Third parties play an important role in helping a company deliver on its core mission. All organizations rely on third parties for everything from raw materials to distribution, and more. Enterprise-level risks associated with suppliers, service providers, distributors, and vendors are becoming more numerous, with a rising impact on multiple areas of the company on as well. Considering the intangible (and therefore uninsurable) nature of some of these risks, a company could be exposed to crippling losses.

Even if not formally written in stone, every company has a strategic plan that consists of two channels – strategic goals and objectives, covering the next 1-5 years, and the business objectives, which focus on the day-to-day running of the company. And like the strategic plan, there are risks, whether documented or not, around each individual objective.

A third party can either create additional risk to your company and its strategic plan or they can help reduce risk.

Third parties can create and/or help reduce risk in a variety of areas, including:

- Operational
- Business resilience
- Cybersecurity
- Environmental
- Reputational
- Social

If not properly monitored and managed, these risks could prevent the company from reaching its goals. Additionally, more severe consequences include negative media coverage, scrutiny from regulators, steep financial losses, and, in the most extreme cases, company failure. Only 25% of Enterprise Risk Management (ERM) programs conduct proper assessments, monitoring, and management of risks from third parties.

While it is possible to outsource many processes, the risk associated with them cannot be outsourced and ultimately lies with the business.

There may be risks lurking under the surface with a particular vendor that could end up creating more problems for your company, which is why fully understanding and addressing these risks (potential to occur) and issues (occurring now) is so important.

To the average customer, mishaps caused by a third party are the problem of the organization, along with the resulting negative reputational impacts to both the organization and the third party. Therefore, third-party risks are passed on to their clients and demand due diligence to identify and mitigate potential issues. Therefore, understanding risks associated with third-party vendors – and being prepared to monitor and manage them – is as important as risks emanating from within your company.

All organizations should incorporate a vendor risk assessment as part of their vendor selection process. Due diligence should also include the use of established thresholds to prioritize those risks requiring greater monitoring and management.

These vendor assessments and risk thresholds will help organizations both better understand internal and external dependencies required for the third party to deliver its products and/or services, and ensure they are within an acceptable range to the company. If they are not, establish redundancies in the event the third party becomes unavailable.

2022 Prediction: Enterprise Risks and Third Parties

Third-party risks will continue to escalate in both volume and impact as companies further streamline in-house operations and focus on scalability. Growing uncertainty both within industries and in the broader economic landscape will elevate the need for a robust enterprise risk framework for both first- and third-party risks.



ESG Risk Management

WRITTEN BY SUSANNA CAGLE

Third-party risks are considered Scope 3 risks for ESG practitioners aligned to the Greenhouse Gas Protocol. The Scope 3 standard encompasses all emissions generated throughout the corporate value chain, including all aspects of the business beyond physical assets and people operations (which are defined as Scope 1 and 2 risks).

All ESG risks – including climate-related, social capital, human rights, and governance risks – apply to third parties as Scope 3 risks. From a measurement perspective, Scope 3 often represents over 80% of a company's greenhouse gas emissions and at least twice its human capital footprint (in terms of people who represent suppliers, distributors, and customers).

It is significantly more expensive and difficult to set and achieve ESG goals in Scope 3, because data related to a third party's environmental and human

footprint is not owned by your company, and funding projects – such as investments in renewable energy or improving wages to a living wage – are not directly affiliated with your company's balance sheet. Setting mutual goals with your third parties based on a mutual understanding of and desire for longer-term business partnerships can help address these difficulties.

All companies should consider climate-related risks and opportunities when assessing third-party risks. These risks may represent potential supply chain instability if suppliers are located in areas that face increasingly extreme weather events, significant sea level rises, or droughts as a result of climate change. It's important to understand upstream and downstream commitments and timelines. Where they don't exist or need to be expedited, work with their third parties to jointly address these risks, or consider doing business elsewhere.

Companies should also assess the human rights and modern slavery risk mitigation efforts of their tier 1 suppliers, as well as those of their contractors and sub-contractors. This is to ensure all employment is being managed legally and a fair and living wage is being paid under acceptable (and ideally better than "acceptable") working conditions.

From an ESG perspective, it is important to also include social capital when considering human capital. Social capital risks include the impact of third parties on their communities, and how your business with them affects that impact. There may be opportunities to partner with third parties to improve local infrastructure, assist in providing better education and childcare to the community, and mitigate environmental effects. All of these endeavors help secure the supply chain beyond basic compliance and improve communities for future generations.

In the next 2 years, businesses will have unprecedented supply chain interruptions in areas where they have not confronted third-party climate risk. Businesses that have addressed this will likely pull ahead in terms of revenue due to predictable operations and limited interruption.

Governance risks are also relevant to third parties. Explore procurement policies to encourage supplier diversity, codes of conduct to mutually align on ESG and general ethics and compliance goals, data acquisition through surveys or other tools. The latter is especially useful in helping organizations understand a third party's greenhouse gas emissions, compliance with modern slavery acts requirements, and its overall alignment to your ESG goals.

The recent COP26 summit made it clear countries and corporations around the world are not moving fast enough to mitigate unavoidable climate disaster. Some

(but not all) companies are acting on the basis of the Business Roundtable's conviction to do business not only for shareholder value, but more importantly for stakeholder interest. However, the current pace of change is too slow to avoid climate disaster as calculated by the scientists behind the UN's Special Report on Climate Change and Health¹.

In the next 2 years, businesses will have unprecedented supply chain interruptions in areas where they have not confronted third-party climate risk. Businesses that have addressed this will likely pull ahead in terms of revenue due to predictable operations and limited interruption.

2022 Prediction: ESG Third-Party Risk

Leading companies in each sector that have already begun addressing Scope 3 emissions through their ESG function will be joined by mid-size companies that have achieved many of their own Scope 1 and 2 ESG targets. We will also see businesses more responsibly partnering with third parties to develop new and alternative financing vehicles or otherwise invest in the infrastructure of third parties. Such investments will include (but are not limited to) physical assets such as PPE and human capital in the form of increased safety, higher wages, greater education, and health benefits in order to produce more business continuity in their total value chain.

¹ Source: [UN Special Report on Climate Change and Health](#)

About The Authors

Susanna Cagle | Senior Product Manager for ESG at NAVEX

Susanna Cagle is a product strategist and ESG practitioner building solutions for companies who want to imbue sustainability into their purpose and operations. At NAVEX Global she oversees the design and development of ESG software and services and has previously worked at ENGIE, POLITICO, The Economist Group, and Anthem Insurance in product management roles. She holds a Master of Science in Sustainability Management from American University.

Michael Volkov | CEO at The Volkov Law Group LLC.

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

Carol Williams | CEO & Principal Consultant at Strategic Decision Solutions

Carol Williams is an Enterprise Risk Management (ERM) Consultant with 20+ years of experience managing risk in the insurance industry. Her firm, Strategic Decision Solutions, was founded to help companies design flexible—but optimal—strategies to make risk-informed decisions. Carol specializes in identifying strategic and operational opportunities for improvement and offers expert consulting which enable clients to achieve their corporate initiatives and strategy.



"2022 is primed to be the year many privacy program leaders will focus on implementing privacy frameworks as a way of insulating the privacy program from the winds of change that constantly buffet the organization."



Privacy and Data Protection – The Year of Privacy Framework Implementation

BY: DR. PAM HRUBEY

Principal, Crowe

JESSICA WILBURN

Data Privacy Officer and Senior Counsel, NAVEX

For those involved in supporting a privacy and data protection program, continued expansion of new regulatory requirements will likely be the biggest trend in the coming year. Whether it be new laws being discussed, pending, or already in place such as those in a U.S. state or at the country or regional level – privacy experts and the organizations they support cannot escape the constant change. Along with this continually evolving environment comes the need to adjust the privacy program to address new requirements. In addition, those in charge of privacy policy and implementation sometimes struggle to support frustrated line-of-business leaders who don't understand or appreciate privacy program requirements and see privacy as a distraction or barrier to productivity.

environmental, social and governance (ESG). Constant regulatory change is certainly part of the reason ethics and compliance leaders report that privacy continues to be a key area of focus. But the next logical question must be: how can privacy and data protection program leaders address the continuous external regulatory change impacting their organizations?

2022 is primed to be the year many privacy program leaders will focus on implementing privacy frameworks as a way of insulating the privacy program from the winds of change that constantly buffet the organization.

Choosing the Right Privacy Framework

Privacy frameworks help organizations deal with change. They provide a structure upon which to base both program fundamentals, and those critical processes necessary to fully support the privacy program and its stakeholders. Program leaders seeking to effectively leverage a privacy framework must have a clear grasp of the specific information requirements of the organization, and the relevant industry or industries the organization operates within. Using a privacy framework doesn't obviate the need to understand laws and regulations applicable to the business – but with a framework in place, it is easier to evaluate changes that could have a substantive impact on the organization. It is also important to be mindful of the organization's culture and values, as well as its appetite for regulatory risk.

66% of respondents indicated privacy, data protection and security as a priority

In a 2021 NAVEX risk and compliance program survey, 66% of respondents indicated privacy, data protection and security as a priority. This means privacy ranks right up there with other, more familiar, topics including conflicts of interest; antibribery and anticorruption; diversity, equity, and inclusion (DEI); and

Fortunately, numerous privacy frameworks are available, including:

- Fair Information Practice Principles
- Generally Accepted Privacy Principles (GAPP) Maturity Model
- ISO27701
- National Institute of Standards and Technology (NIST) Privacy Framework
- Organization for Economic Cooperation and Development (OECD) Privacy Framework

Additionally, work must be done to complete data maps (or records of processing activities) for the personal and sensitive data processed by the organization when implementing a privacy framework. Privacy leaders must consider the scope of the privacy program and how it aligns with the organization's values. It is also helpful to be aware of specific challenges the privacy program may face, including the potential for regulatory enforcement.

Buy-In and Implementation

First and foremost, the privacy program must have unmitigated buy-in from the organization's executive management. Privacy leaders should leverage departmental or functional champions where it makes sense and be sure to involve those privacy champions in related training events and workshops for senior management. There may be an additional organizational lift by creating a steering committee and deputizing other leaders to help carry the load associated with implementing the framework.

One of the first steps after selecting a privacy framework is to map out how the privacy regulations your organization must comply with overlap both with your framework and each other. In some cases, it may be helpful

to leverage more than one framework. Some organizations find it helpful to begin by replicating the work done by another portion of the organization – for example, the information security team's use of the NIST Cybersecurity Framework or ISO 27001. This can establish a stronger alignment in those spaces that naturally overlap between privacy and security. Mapping out control areas and then establishing connections within and across regulations can reduce the complexity that naturally exists in the global privacy and data protection arena.

Next is the creation of action items for the steering committee members and privacy stewards. These individuals will be in a great position to help map the controls from the selected framework into the organization's personal data-collecting processes. Privacy leaders should help the committee leverage existing policies, procedures and training. It is important to consistently communicate what is happening and why to truly gain buy-in. Roles, responsibilities, and descriptions created for the framework should be kept simple and clear. Members of the privacy program team with steering team members and privacy champions should be in alignment so they can be reliable evangelists for the program without danger of contradicting one another. Their involvement also provides the opportunity for personal and professional development. As with any effective compliance program, monitor regularly to evaluate the progress being made and check that the framework continues to be fit for purpose.

It will likely be necessary to tailor the chosen framework to the specific privacy risks and regulatory requirements the organization is obligated to meet. This is a natural part of the implementation process, and making these minor adjustments smooths implementation for everyone. When determining how to tailor the framework, be sure to involve those business partners that may be affected by, or must adhere to, the program.

Once the framework is implemented it can be leveraged every time a regulatory change happens – though the framework should still remain dynamic and flexible, as static frameworks become dated quickly. First, map the new requirements into the controls you have documented in the framework. Where there are gaps in controls (which can happen from time to time) adjust the controls. Then you'll be ready to rinse and repeat the next time a regulatory change happens.

In this day and age, true data privacy protection is not practical without technical automation. Nearly all data gathering, storage and use is already a technology-driven. Data control mapping should be done using software tools as well. The need for robust, yet flexible data control software

tools becomes even more obvious when considering the aforementioned rate of regulatory change. Manual, or only partially automated, control systems cannot respond as quickly change as a well-chosen software solution. As such, making necessary technology investments should be prioritized.

2022 Prediction

Data privacy regulation shows no sign of slowing. Organizations should prepare for changes by auditing existing privacy frameworks, investing in technology, and preparing to make changes as necessary. The coming year will yield increased attention to privacy programs, and current and upcoming legislation will demand dedicated resources and organizational buy-in to maintain compliance.


About The Authors

Dr. Pamela Hrubey | Principal at Crowe

Dr. Pamela Hrubey is a principal in the consulting group at Crowe and has more than 30 years of experience guiding innovation-based companies from discovery through commercialization. She assists clients around the world by leading and assessing complex business process development efforts in areas including data protection and privacy, ethics and compliance, transparency-related reporting, and anti-bribery and anti-corruption. Pamela has specific experience with developing global ethics and compliance programs, including the selection of key personnel, training and development, and engaging leadership. Additionally, she has led efforts to work with legal counsel and regulators including the DOJ, FTC, OIG/HHS, SEC, and international data protection authorities on enhancements of global ethics and compliance programs.

Jessica Wilburn | Data Privacy Officer and Senior Counsel at NAVEX

Jessica Wilburn is the DPO and Senior Counsel at NAVEX Global. Leading data privacy in-house, she advises on compliance across all aspects of global privacy law and regulations. Jessica spent 2017 in NAVEX Global's London office, working with individuals from around the globe on the impact of global data privacy laws. Jessica has worked in data privacy for more than 4 years, initially focusing on SaaS and data transfer and processing agreements. She now focuses on the management of NAVEX Global's international privacy program and operations, holding both CIPP/E (Europe) and CIPP/US (United States) certifications. She is a Member of Women Leading Privacy Advisory Board for the IAPP.

A photograph of a man in a wheelchair and a woman in a business setting. The man, wearing a maroon shirt, is seated in a wheelchair with green-spoked wheels, smiling and looking at a document. The woman, wearing a dark blazer over a yellow top, is standing and holding a large white sheet of paper, also smiling. They are in a bright, modern office environment with large windows in the background. A dark teal rectangular box is overlaid on the left side of the image, containing white text. At the bottom of the image, there are two solid orange rectangular shapes: a smaller one on the left and a larger one on the right.

"Genuine DEI ownership is
centered in honesty, integrity
and active change."

DEI Is Not “One Size Fits All”



BY: PATRICE PALMER

Assistant Dean, Colorado State University College of Business

There is no universal standard for diversity, equity and inclusion (DEI), and many experts and practitioners agree there are no simple best practices to implement either. This reality, and lack of clear direction can be troubling for leaders. Many create DEI strategies that aren't sustainable or completely avoid the issue with the unspoken hope the topic will fade from the headlines.

But DEI is here to stay, and with public and internal attention turned to how organizations respond, businesses must take steps towards meaningful and sustainable change.

Now, two years into a global pandemic and amidst a racial reckoning punctuated by a recent series of high-profile court trials, we must be thoughtful and intentional in what we want and – even more importantly – what we hope to accomplish.

In order for DEI initiatives to be long lasting and impactful, it is important to ask: how do we take our organizations to the next level? Where do we go from here – and most importantly, what does 2022 have in store for DEI?

As the world becomes more diverse, organizations must follow suit by paying attention to and acting on DEI matters. By 2030, 75% of the labor force will be made up of people

20-49 years old. This group is one of the most diverse in history, and they expect a robust DEI strategy. They are the market – and the market ultimately determines the value of an organization's offering – be it products or jobs. The world is calling for action and accountability through a DEI lens.

Intentionality in Brand Messaging

All stakeholders look for the intentionality that come with a well-defined plan, and look at the past stance an organization has taken with respect to DEI matters. It is critical to communicate where the company is currently positioned and where it hopes to make progress. If there is no stated goal for diversity, equity and inclusion, companies will be left spinning their wheels and hoping to avoid harsh public criticism.

Simply put, organizations should consider if the DEI program is reactionary to a trend, or if there are earnest efforts to put mechanisms in place to move the organization forward, leading with a DEI strategy that is flexible and sustainable.

Consumers also want to ensure organizations hold their people and suppliers accountable, especially on social media. Not only does it matter what is said by agents of the company, a lack of response from an organization can have consequences to the brand as well. Simply

put, organizations should consider if the DEI program is reactionary to a trend, or if there are earnest efforts to put mechanisms in place to move the organization forward, leading with a DEI strategy that is flexible and sustainable. In this light, it is advisable to be proactive in communicating DEI efforts; regular social media posts and persistent messaging on the corporate website are a good place to start.

Understand the Difference Between Genuine and Performative Coalition Building

The public is highly attuned to DEI matters as they frequently make front page news and can spot inauthentic allyship and empty gestures. Genuine DEI ownership is centered in honesty, integrity and active change.

If a program or initiative is not well thought out, or fails to encompass different perspectives and provide accessibility for different people, it will not go unnoticed. As a reaction to racial injustice around the world, and public cries for change, many organizations pledged to make impactful changes and embrace DEI initiatives in earnest. However, many of these same organizations remain silent, even when attention is drawn to their internal issues.

Inaction is gaining attention, sometimes more so than action. Organizations must go beyond the performative – genuine efforts require flexibility, sustainability and buy-in throughout the organization.

Organizations must listen to the needs of the constituents. For example, when creating a solution to ensure senior leadership is diverse and inclusive, it is important that the leadership is representative of the organization's workforce, otherwise this gesture is performative and inauthentic.

Transforming Rather than Changing

Transformation requires a methodical approach that enables intentionality in order to alter organizational behavior, rather than simply change the methods of delivery. This process takes competence, compassion and commitment.

With many long-term and far-reaching goals, forward thinking organizations are on a journey towards transformation. But it cannot happen overnight – it is a goal-oriented process that takes time and consistent effort. Also, it must be understood that there is no “destination” for transformation, it is a process intended to create a culture of inclusion and equity, then maintain it in what we all already know is a dynamic, ever-changing world.

There are no codified best practices for DEI implementation. But there are promising practices that can be put to use and refined over time; ultimately leading to common practices that are so well established in the culture they are a given.

Looking Forward

There are no codified best practices for DEI implementation. But there are promising practices that can be put to use and refined over time; ultimately leading to common practices that are so well established in the culture they are a given.

To start, organizations should consider these promising practices:

- Establish the goal of your organization's DEI strategy. What are you looking to gain? What are you willing to lose? What are the short-term measurable goals? How will long-term goals build brand value and consumer loyalty while adding to your bottom line?

- Once the goals are established, make a plan to reach them. An analysis of strengths, weaknesses, opportunities, and threats (SWOT) is a useful tool to outline that plan and determine where efforts should be directed. This understanding will help create buy-in and keep leadership team on an intentional path.
- Start small and gather incremental wins. This helps to build momentum and buy-in on all levels. This may be as simple as including space for pronouns in email signatures, or ensuring gender neutral language is used in all policies and procedures within the office. These are small, but they add up to sustainable change over time.
- Designate resources and appropriate staff support towards the goal. DEI is not a one size fits all plan; it is malleable but requires an intentional approach to be successful. Importantly, this approach must not be reactionary and needs to be well thought out. Make sure to be inclusive of the people who are supposed to be centered in this work, and remember that inclusion is not exclusionary.

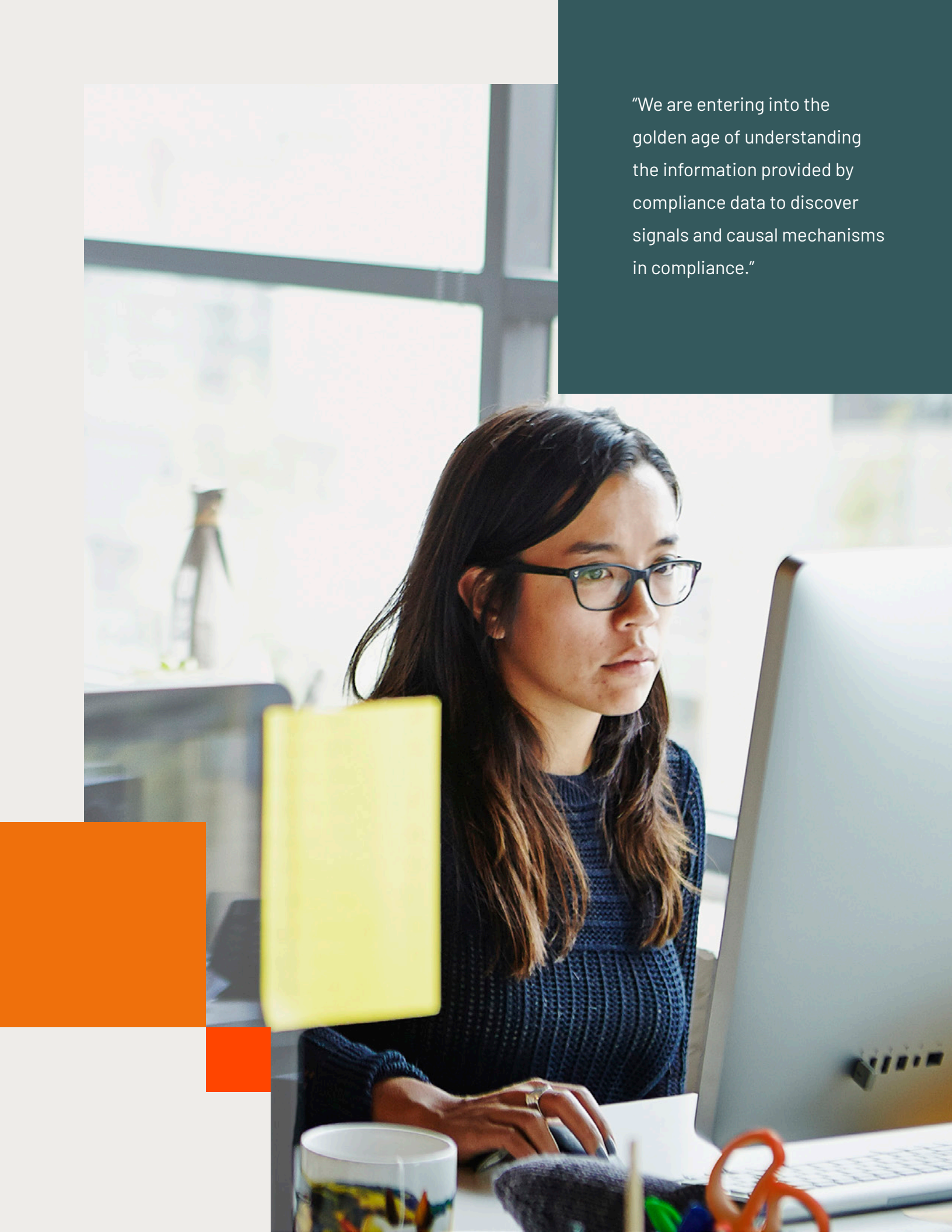
2022 Prediction

DEI is not a fading trend – on the contrary, it is becoming more informed. Words like transparency and honesty are taking on a new life as organizations are held to account for their actions (and inactions). The coming years will continue to shed light on the transformation organizations are undergoing. Employee, consumer and stakeholder attention to DEI in the workplace will continue to escalate and organizations will need to work diligently to ensure their programs are sustainable, well-resourced and authentic.

About The Author

Patrice Palmer | Assistant Dean, Colorado State University College of Business

Patrice M. Palmer (they/them/their pronouns) is an award-winning educator, speaker and author who has published works centered on diversity, equity and inclusion within higher education. They are a doctoral student in the School of Education at Baylor University. They are also the inaugural Assistant Dean and Director of Justice, Diversity, Equity and Inclusion Initiatives for the College of Business at Colorado State University. Patrice is also the founder and CEO of the DEI consulting firm, 'eROOT Consulting,' which helps SMB companies create a roadmap for integrated DEI success.



"We are entering into the golden age of understanding the information provided by compliance data to discover signals and causal mechanisms in compliance."

“Compliance Sabermetrics” – Data Will Change Assumptions That Plague Compliance



BY: KYLE WELCH

Assistant Professor, George Washington University School of Business

In 1969, the computer systems company Information Concepts Incorporated transformed the world of baseball with their creation of “The Baseball Encyclopedia.” The book (affectionately nicknamed “Big Mac” in homage to both its heft and its publisher, Macmillan) gave the sport its first fully comprehensive and rigorously researched compendium of baseball statistics – and inspired a generation of fans interested in baseball history and statistical research. In 1971, sixteen of these “statisticians” formed the Society for American Baseball Research (aka SABR or “saber”) and began using the Big Mac to develop new and innovative measures to compare players and predict outcomes. By 1980, this practice had been given a new name: sabermetrics.

Today, sabermetrics is an integral part of Major League Baseball. Virtually every MLB team employs sabermetricians, who replace “experience” and “intuition” with empirical data analysis. The approach has enabled teams like the Tampa Bay Rays and Oakland Athletics to build winning records on modest budgets (most famously illustrated in the 2003 book and 2011 movie *Moneyball*). This disruptive quality, along with its tendency toward counterintuitive maxims, has helped this “big data” approach to decision making capture people’s imagination.

A similar wave of change has started in compliance with data. For a long time, mostly due to data limitations, there was little examination into the cause and effect of different efforts in compliance systems. Even worse, there was no evidence for what compliance data was telling us about those systems. For example, are elevated hotline report volumes a good thing, illustrating an employee willingness to speak up, or a signal that the organization had deeper problems? Without additional information, this single statistic can’t tell the story. As a result, compliance officers have largely had to rely on their own experience and intuition when interpreting data. While these can provide valuable insights, they also open the door to incorrect assumptions and personal biases.

Uncertainty with decisions and data is beginning to change in compliance. We are entering into the golden age of understanding the information provided by compliance data to discover signals and causal mechanisms in compliance. Those at the cutting edge of this movement are giving birth to new rigorous data protocols in compliance, enabling compliance officers and organizations to more easily contextualize risk signals and better predict outcomes.

In other words, hotline reporting data is an incredibly valuable set of information to compliance leaders and executive leadership. Reporting information is the pulse check of organizational culture and should be weighed, analyzed, and acted on accordingly.

Data's Counterintuitive Insights for Compliance

A few counterintuitive insights have emerged from the initial efforts in this area. One of the most frequently noted is that firms with more actively used compliance reporting programs – those receiving more reports per employee – perform “better” in almost every measure (i.e., more profitable, better governance structures, less negative media coverage, etc.). Moreover, organizations with the highest volume of reports per employee were the least likely to suffer lawsuits and fines; and those that did paid less on average than their peers in fines and settlements.¹ These metrics undercut the widely-held assumption that more reports is indicative of more problems.

This may beg the question, “What does the data tell you about quality of reports as report volume increases?” Compliance officers are certainly aware of the misuse of feedback systems and may be rightly concerned with time and resources wasted on bad faith reports. Additionally, as with most business activities, there is almost always diminishing returns at larger scales of investment. The question is, has this happened with feedback systems?

In a crude analysis of report quality, we measured the prevalence of two factors as reporting volume increased: named (vs. anonymous) reporting and report completion. Previous analysis of reporting data has demonstrated that reports which include the identity of the reporter and those with fully completed information (e.g., fields including management involved, time it has been going on, how was it discovered, etc.) were most likely to be useful or informative,

or less difficult to examine.² Granted, it is not known how important each individual report in these two categories is, but there is a clear difference in the measure of quality in providing their own identity for follow up and including standard information details about the reported problem.

Ex-ante we would likely expect the information quality of reports to go down as volume increases. As more individuals make reports it seems natural for there to be more problems and limitations with those users providing that data. The chart below shows this is not the case.

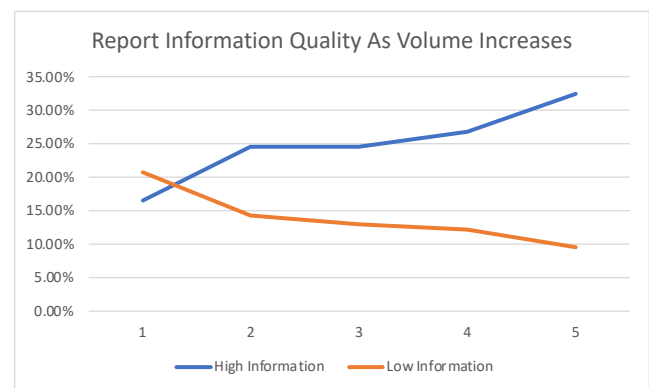


Chart Data

Quintile of # Reports per employee	High Information	Low Information
1	16.50%	20.70%
2	24.50%	14.30%
3	24.50%	13.00%
4	26.80%	12.20%
5	32.40%	9.50%

In the chart we separate the report volume by quintiles, with 1 being the lowest 20% report volume in a given firm year and 5 being the highest volume (top 20%), controlling for industry and other firm factors.

¹ See: Stubben, Stephen R., and Kyle T. Welch. “Evidence on the use and efficacy of internal whistleblowing systems.” *Journal of Accounting Research* 58.2 (2020): 473-518.

² Penman, Carrie, and Andrew Burt. “2021 Incident Management Benchmark Report.” NAVEX Global, May 2021.

Instead of finding what we would assume, we observe quality of information (i.e., completeness) of reports increases with report volume. This pattern, in combination with other evidence³ is consistent with the assertion that firms with higher reporting volume likely 1) have more training and information on effective use of reporting systems resulting in 2) higher levels of information in those reports and 3) more problems being uncovered before they get worse.

Internal reporting data should be treated as the wealth of information it is. Creating a culture that allows for honest reporting and appropriate follow up to rectify problems should be prioritized by executive leadership.

This is just one example of the counterintuitive insights emerging from this field that are changing assumptions about compliance and employee feedback systems.⁴ The leading edge

³ See: Stubben, Stephen R., and Kyle T. Welch. "Evidence on the use and efficacy of internal whistleblowing systems." *Journal of Accounting Research* 58.2 (2020): 473-518.

⁴ For more see: Stubben, Stephen R., and Kyle T. Welch. *Throw Out Your Assumptions About Whistleblowing*. Harvard Business Review. 2020.

of the compliance industry is exploring what I call compliance sabermetrics – the use of big data to provide additional insights to management. These efforts are causing management to change their perspectives of compliance.

Under the old management mantra, when an audit committee observed higher-than-benchmark employee feedback through their reporting system, they might have wrongly asked, "Why do we have more problems than our peer firms?" The new wave of insights from data will cause a different question to be asked in the future: "Do we have the resources to make sure we are effectively investigating our increased information from employees?"

Internal reporting data should be treated as the wealth of information it is. Creating a culture that allows for honest reporting and appropriate follow up to rectify problems should be prioritized by executive leadership.

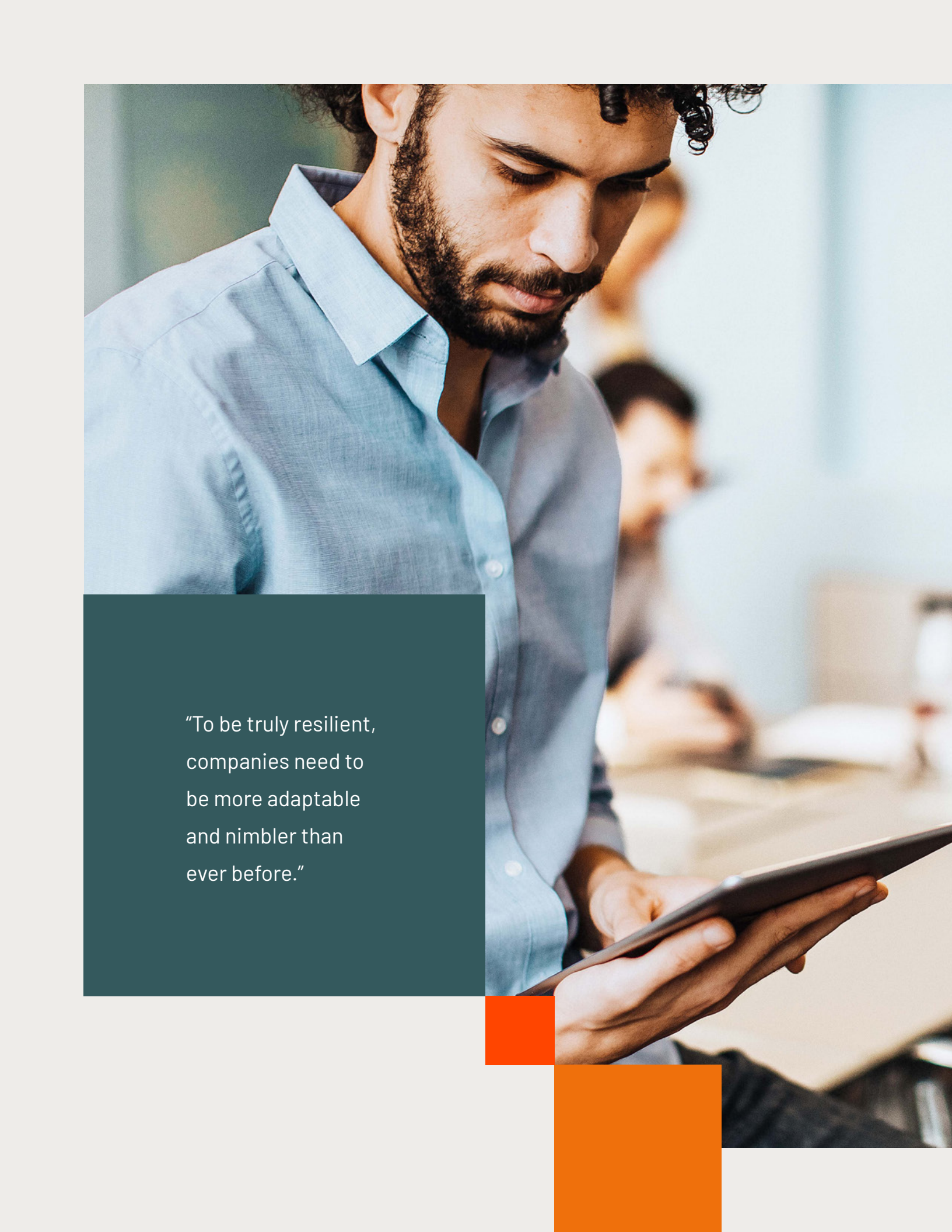
2022 Prediction

The increasing collection and analysis of compliance data will further challenge long-held assumptions about which metrics warrant attention and what they indicate about a company's organizational culture and health. Successful firms will invest in these efforts, de-emphasizing intuition in favor of empirical data analysis.

About The Author

Kyle Welch | Assistant Professor at George Washington University School of Business

Before becoming a professor at George Washington University, Kyle Welch worked on the investment team at the Stanford Management Company (Stanford University's endowment). While there he developed asset allocation and portfolio strategies. Professor Welch also evaluated public equity, private equity, venture capital, and hedge fund investment opportunities and fund managers. Prior to working at Stanford, Professor Welch worked at Standard & Poor's (S&P) in the Corporate Valuation and Consulting group (now part of Duff & Phelps).



"To be truly resilient,
companies need to
be more adaptable
and nimbler than
ever before."

The Impact of IT Risk on Business Continuity – Making Businesses More Resilient



BY: CAROL WILLIAMS

CEO, Principal Consultant, Strategic Decision Solutions

Since the beginning of the COVID-19 pandemic, business continuity has been top-of-mind for executives and managers regardless of their company's size, industry, or geographical location. Countless articles, whitepapers, webinars, and podcasts have discussed the necessity of robust business continuity plans.

While it is good that companies are focusing on this issue, business continuity has traditionally been more short-term in nature, especially when it comes to technology in the age of COVID-19, when companies were scrambling just to maintain a semblance of pre-pandemic operations in the new environment.

As first described by Professors Warren Bennis and Burt Nanus over 30 years ago, we live in a world characterized by volatility, uncertainty, complexity, and ambiguity, or VUCA. This is even more true today than it was then. Both surveys and first-hand observation confirm that our current era is marked with ongoing, increasing disruption and rapid change.

What Does This VUCA World Mean for a Company's Future Prospects?

To be truly resilient, companies need to be more adaptable and nimbler than ever before.

Like the redwoods of California or the majestic oaks of the southern U.S. that can live well over 100 years, companies must be able to "absorb and adapt in a changing environment." And like the environment consisting of a combination of sun, rain, wind, and other conditions that impact how big a tree gets and how long it lives, companies live in an "ecosystem" of their own consisting of suppliers, customers, employees, regulations, financial conditions, and many more.

To begin understanding the state of your company's long-term resiliency, it is important to closely examine the ecosystem in which your company operates. The main factors that can impact your company's ecosystem are:

- Social – customer values and priorities, social expectations, demographic trends
- Technological – automation, artificial intelligence, increased efficiencies
- Economic – prices (assets, raw materials, stock), market share, borrowing costs
- Environmental – emissions, energy use and costs, land use, water, climate change
- Political – legislation, regulations, leadership, public mood

Each of these factors within a company's ecosystem combine to have either a positive or negative impact on its long-term resiliency. It is possible that not all these factors will apply to your company since each

organization operates under its own unique structure, culture, industry, location, and more – its own ecosystem. But considering how interconnected companies and organizations are within an ecosystem, any changes or risks that impact just one of them will spill over into your company and may have even faster or larger effects.

Technology is one area that can have a significant impact, both positive and negative, on a company's ability to adapt and thrive.

Changes in your company's ecosystem can occur in the blink of an eye, which is why adaptability and flexibility of internal structures, suppliers, and other aspects within your control are so important, or as APAC IRM representative Gareth Byatt explains, "Even with robust plans in place to deal with disruption, if they are not aligned to a flexible structure and an ability to change when you need to deal with things in unexpected ways, they will not be truly effective when you need them."

While business resiliency is more important now than ever, it is not easy and may even seem impossible – especially if risk management processes are not fully developed.

The Impact of Technology on Business Resiliency

Technology is one area that can have a significant impact, both positive and negative, on a company's ability to adapt and thrive.

Technology in the form of software and hardware play an invaluable role in helping a company deliver value and accomplish its strategic goals. It can also be one of the biggest obstacles for a variety of reasons.

One such obstacle can be growth. As businesses grow, so to do their technology needs. The need for manual workarounds or processes for a fast-growing firm are costly from a financial and time perspective, inhibiting a company's long-term success.

It is also cumbersome and costly to maintain and update older systems, especially if developed in-house. Not to mention, these older systems make the company extremely vulnerable to malicious actors. Constant innovation and updates to technology also mean current tech tools are quickly outdated if not properly maintained and upgraded.

Utilizing multiple technology tools can also cause issues as well.

Companies with too many systems often fall victim to redundant information, which ends up hindering effective decision-making since there is no agreed-upon, single source of truth. Resources are drained because employees are confused and distracted from their day-to-day obligations, much less from pursuing strategic goals.

Steps for Organizations To Take

1. Determine if your company's technology is an impediment to its long-term resilience. You can't solve a problem until you acknowledge one exists. Ask the following questions:

- Is it difficult to obtain insights and information from our software and other technology systems?
- Are employees establishing manual workarounds, such as exporting data into spreadsheets just to enter it manually into another system?
- Do aging systems expose the company to increasingly sophisticated data breaches and other cybersecurity threats?
- Are workers diverting attention away from creating value and pursuing goals to focus on repeatable tasks that could be handled with adequate tech infrastructure?

2. Examine the company's technology

strategy. Determine if the technology strategy and the design of the IT department supports the business strategy or simply maintains the status quo. If the technology strategy is focused on the status quo, look at the long-term business strategy and determine the appropriate technology stance for the company to be resilient and relevant in the next 30 years.

3. Focus on the business of the company, not on becoming an IT shop that has a business.

Many companies feel they either need a miniscule IT department for tech support and minimal application support, or conversely, develop a large IT staff to develop and maintain in-house software. Minimal IT staff will not address the technology needs of any company in the VUCA world, and a large IT staff can drag down the business of the company if you aren't careful.

4. Recognize that technology risk is more than just cyber risk. Contrary to popular opinion, technology risk involves more than cyberattacks and data breaches –simply taking a tech only approach is insufficient in today's fast-changing world. Technology risks must be examined in the context of managing the company for success both in the short- and long-term.

Leading risk commentators and practitioners agree that risk management is not just about avoiding failure, but rather about ensuring the company meets or exceeds its strategic goals. In the past, focusing solely on preventing failure may have been sufficient, but in our increasingly VUCA world, this type of approach could be disastrous for a company's long-term resiliency.

By taking special care to understand your company's technology risk and investing in the right tools for your specific needs, your company will manage one of the biggest areas that could hamper its long-term resiliency.

2022 Prediction

The factors within each company's ecosystem will become more volatile, creating more uncertainty as companies look to the near-term for success. Customers expect both improved self-service and on-demand customer support with enhanced use of technology. The need to transform company operations and its supporting technology to become more efficient and cost-effective will skyrocket, leaving companies scrambling to juggle maintaining operations with significant internal change management.

About The Author

Carol Williams | CEO & Principal Consultant at Strategic Decision Solutions

Carol Williams is an Enterprise Risk Management (ERM) Consultant with 20+ years of experience managing risk in the insurance industry. Her firm, Strategic Decision Solutions, was founded to help companies design flexible—but optimal—strategies to make risk-informed decisions. Carol specializes in identifying strategic and operational opportunities for improvement and offers expert consulting which enable clients to achieve their corporate initiatives and strategy.



NAVEX is the recognized leader in risk and compliance management software and services, empowering thousands of customers around the world to manage and mitigate risks with confidence. NAVEX's mission is to help customers promote ethical, inclusive workplace cultures, protect their brands and preserve the environment through sustainable business practices.

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