



# 2022 Top 10 Trends in Risk & Compliance

■ Kristy Grant-Hart, Founder & CEO, Spark Compliance Consulting  
Carrie Penman, Chief Risk & Compliance Officer, NAVEX

# Presenters



**Carrie Penman**

Chief Risk & Compliance  
Officer, NAVEX



**Kristy Grant-Hart**

Founder & CEO, Spark  
Compliance Consulting

# Overview: Top 10 Trends in Risk & Compliance

1. DEI Is Not “One Size Fits All”
2. Risk & Compliance Management Expands to Include ESG
3. ESG Disclosure Adoption – What Can We Learn From the EU?
4. Compliance Sabermetrics: Data Will Change Assumptions that Plague Compliance
5. EU Whistleblowing Directive
6. The New Normal Workplace – R&C Management
7. Data Privacy – Frameworks and Implementation
8. The New Normal Workplace – Training and Policy Management
9. Holistic Third-Party Risk Management
10. The Impact of IT Risk on Business Continuity – Making Businesses More Resilient

# DEI Is Not "One Size Fits All"

Written by  
Patrice Palmer





# Promising Practices

- Establish the goals
- Conduct a SWOT analysis
- Designate resources
- Start small



## 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."*

# Risk & Compliance Management Expands to Include ESG

Written by  
Carrie Penman



# Risk & Compliance Management Includes Oversight of ESG



Increased investor attention and disclosure regulation driving the need for oversight expertise



Mitigating risk and creating value go hand-in-hand



The evolution of ESG programs is following a similar track to the development of compliance programs

**89% of respondents in a recent, international survey indicate ESG reporting is already a part of their compliance program**



## 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."*

# ESG Disclosure Adoption – What Can the US and World Learn From the EU?

Written by  
Vera  
Cherepanova and  
Karen Alonardo





# ESG in the EU and the US

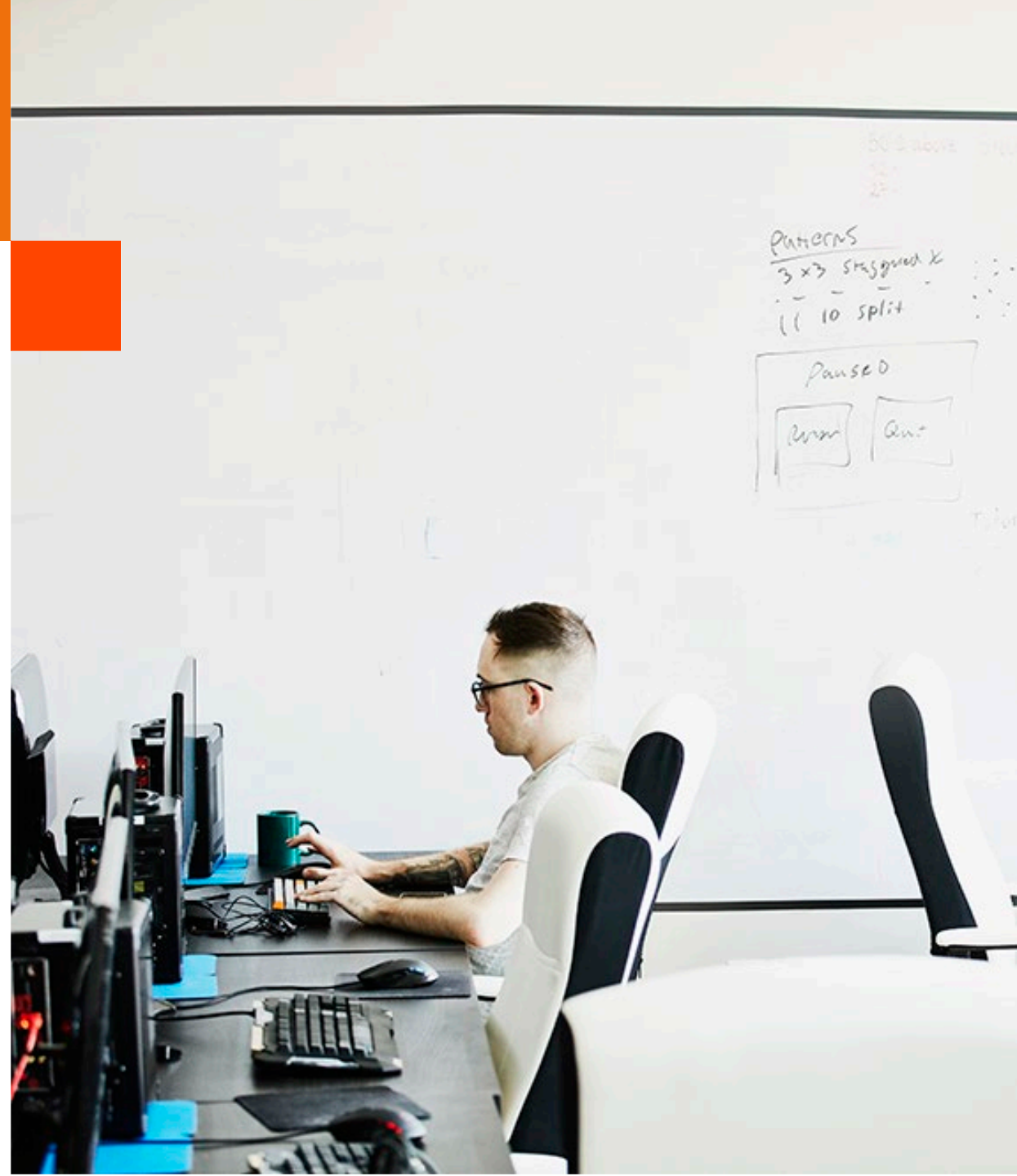
- Creation of a Common Taxonomy
- Greater Disclosure Requirements – no greenwashing!
- US – SEC and Value Reporting Foundation (formerly SASB)
- Consumer demand, financial services/investment focus and new regulations rule

## 2022 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. New regulations will require new data sets – effectively tackling the ESG data challenge will remain pivotal to success."*

# Compliance Sabermetrics: Data Will Change Assumptions that Plague Compliance

Written by  
Kyle Welch





# Data's Counterintuitive Insights for Compliance



Organizations receiving more reports per employee have better performance overall.



Findings show completeness (and therefore, quality) of reports increases with report volume.



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).

# 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."*

# EU Whistleblowing Directive

Written by  
Karin Henriksson and  
Jan Stappers



# EU Obligations for Whistleblower Report Management

- Secure channels
- Confidentiality and non-retaliation
- Keep information flowing
- Remember GDPR

## Major Challenges

- Local requirements

# 2022 Prediction

*"As member states and organizations within the EU adopt whistleblower programs that adhere to the Directive, global attention will be paid to the future of whistleblowing."*



# The New Normal Workplace – R&C Management

Written by  
Matt Kelly



# Risk and Compliance Management in the New Normal Workplace

- Cybersecurity will be a bigger priority for everyone
- The ability to map the company's IT assets will be critical
- Cultivating an internal “speak up” culture will be more challenging



# 2022 Prediction

*"Ransomware and other cybersecurity attacks will become even more pervasive in 2022. The race is on to see whether compliance functions can execute on those ideas faster than the attackers can lay siege to your business."*



# Data Privacy – Frameworks & Implementation

Written by  
Pam Hrubey and  
Jessica Willburn





# Privacy Program Buy-in and Implementation

- Adopt a framework and map requirements
- Leverage departmental or functional champions
- Action items for steering committee
- Tailor the framework for your risk and country laws



# 2022 Prediction

*"Data privacy regulation shows no sign of slowing. 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."*

# The New Normal Workplace – Training & Policy Management

Written by  
Ingrid Fredeen





# Strategies for Training & Policy Management

- Prioritize access to technology
- Adapt to emerging and evolving risks
- Set clear expectations with policy and a robust code of conduct

## 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."*



# Holistic Third-Party Risk Management

Written by  
Susanna Cagle,  
Michael Volkov and  
Carol Williams







# Third Party Risk Scope

- Regulators expect action and dedicated budgets
- Risks: operational, business resilience, cybersecurity, environmental, reputational, and social
- ESG-related risk comes from third-parties

# 2022 Prediction

## Regulatory Risk

*"In 2022, third-party due diligence will constitute an increasingly important part of a compliance program's duties – and its budget."*

## Enterprise Risks

*"Third-party risks will continue to escalate in both volume and impact as companies further streamline in-house operations and focus on scalability."*

## ESG 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."*

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

Written by  
Carol Williams





# Steps for Organizations to Take

- Determine if your company's technology is an impediment to its long-term resilience.
- Examine the company's technology strategy.
- Focus on the business of the company, not on becoming an IT shop that has a business.
- Recognize that technology risk is more than just cyber risk.

## 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. 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."*

# Thank you!

NAVEX™

