Top 10 Risk & Compliance Trends for 2021
Predictions & Recommendations for the Year Ahead
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Carrie Penman</td>
<td></td>
</tr>
<tr>
<td>2021 Brings Risk and Compliance Together Under One Roof</td>
<td>5</td>
</tr>
<tr>
<td>Haywood Marsh</td>
<td></td>
</tr>
<tr>
<td>Risk Management + IT Security in the Work-From-Home Era</td>
<td>9</td>
</tr>
<tr>
<td>Sam Abadir</td>
<td></td>
</tr>
<tr>
<td>A Coming Wave of Investor Interest in ESG (Environmental, Social &amp; Governance) Reporting</td>
<td>13</td>
</tr>
<tr>
<td>Karen Alonardo</td>
<td></td>
</tr>
<tr>
<td>A Year of Uncertainty Spurs Integrated Risk Management Adoption</td>
<td>17</td>
</tr>
<tr>
<td>Dr. French Caldwell</td>
<td></td>
</tr>
<tr>
<td>Global Privacy Regulations: Hot Spots to Watch in 2021</td>
<td>21</td>
</tr>
<tr>
<td>Dr. Tobias Schelinski &amp; Jessica Wilburn</td>
<td></td>
</tr>
<tr>
<td>Diversity, Equity, and Inclusion: More Transparency and Accountability</td>
<td>26</td>
</tr>
<tr>
<td>Chai Feldblum &amp; Emily Cuneo DeSmedt</td>
<td></td>
</tr>
<tr>
<td>The Post-COVID-19 Workplace: What Employers Should Expect</td>
<td>30</td>
</tr>
<tr>
<td>Scott Nelson &amp; Savannah Gibbs</td>
<td></td>
</tr>
<tr>
<td>Third-Party Risk and Resiliency: Building a Bridge Between Compliance and Supply Chain Management</td>
<td>35</td>
</tr>
<tr>
<td>Josh Reid</td>
<td></td>
</tr>
<tr>
<td>Training: More Complex, More Important — and More Pushback</td>
<td>39</td>
</tr>
<tr>
<td>Ingrid Fredeen</td>
<td></td>
</tr>
<tr>
<td>A New Age of Accountability: Global Whistleblowing on the Rise</td>
<td>44</td>
</tr>
<tr>
<td>Kristy Grant-Hart &amp; Karin Henriksson</td>
<td></td>
</tr>
</tbody>
</table>
The first passage of last year’s Top 10 Risk and Compliance Trends for 2020 e-book read as follows: “Every year as we prepare for this annual publication, we discuss how the social, political and environmental landscapes our businesses operate within are growing more and more complex. We explore the implications of new regulations, new enforcement of old regulations, and the nuances of human behavior growing more disparate in a strained cultural climate.”

But nobody could have predicted the events of 2020 and the profound impact they would have on our organizations and the risk and compliance profession specifically. So, before we outline our predictions for 2021, it is important to step back and reflect on what we have learned this past year.

Despite the turmoil of 2020, we got a few things right in our predictions for the year (although the intensity level was certainly much higher than expected).

The first was a no-brainer – we knew that we were in for some challenges in “Managing the Impact of Politics in our Organizations.” What we didn’t foresee was the need to add divisiveness caused by the pandemic and politicization of public health efforts to the mix. We also didn’t predict the social and political unrest, which will hopefully lead to more meaningful and lasting changes in our collective diversity, equity, and inclusion commitments.

Second, we addressed the “Impact of Digitized Environments and Modern Workplaces on Internal Investigations.” We said, “the investigative and forensic accounting field is going through a significant metamorphosis to track with the exponential expansion of the use of electronic data and technology.” Then in 2020, we moved many of our employees to work-from-home. Some will never return to a full-time office work environment. This requires nearly all investigations, including the very serious ones, to be conducted remotely, further challenging these processes.
Perhaps the most profound prediction we made for 2020 was “We need to Learn How to Train Humans, Not Employees.” Our humanness has been on full and vulnerable display in 2020. Employees turned personal spaces into home offices. Others risked their personal safety, and that of their families, to do their jobs as essential workers. They truly brought their “whole selves” to work. As employers, we need to ask if our collective communications with them have reflected and acknowledged this sacrifice.

Finally, we talked about “People Risk, Business Risk, and Regulatory Risk.” We said, “the future of risk management will be in how we embrace risk through a holistic yet agile approach.” Well, if “pandemic” is the 2020 word of the year, “agile risk management” is surely the phrase of the year for risk managers. Organizations with robust business continuity plans were better able to respond and adapt quickly. Unfortunately, too many organizations realized that some of their “low likelihood” risks could indeed have a very “high impact” on the business. More attention needs to be paid to this risk category in 2021.

While we faced challenges, the events of 2020 created some high visibility opportunities for risk and compliance professionals we should all take into 2021. Business continuity responsibilities were added to the role of many compliance professionals. Ensuring that our organizations have a holistic and agile approach to risk management is now an imperative. Indeed, our first prediction for 2021 is that risk and compliance will come together under one roof. In 2021, organizations will need to integrate their compliance, IT, operational, reputational, third-party, and environment, social, and governance (ESG) practices. We expect more organizations to appoint Chief Risk Officers (CROs) or Chief Risk and Compliance Officers (CRCOs) to manage an integrated risk strategy.

This past year, issues of diversity, equity, and inclusion landed more squarely in our portfolio; we predict that this will continue in 2021. As Chai Feldblum, Partner at Morgan Lewis & Blockius, LLP notes in “Diversity, Equity, and Inclusion: More Transparency and Accountability” (p. 35), employers are examining their existing DEI efforts, acknowledging that simply prohibiting employers from considering race, gender, and other protected characteristics is not enough to achieve meaningful workplace diversity and inclusion. She further predicts that while some of the changes we saw in 2020 might be temporary, she is optimistic that efforts to improve diversity, equity, and inclusion will grow in the coming year.
Our 2021 predictions regarding global data privacy regulations start with an acknowledgment that change is the only constant. In the coming year, our authors predict (p. 21) that organizations - especially those with global operations - may find that a single, comprehensive approach to data privacy, in order to operate in this increasingly complex environment, is the most risk-averse.

Perhaps our biggest challenge for 2021 comes back to people – those bringing their “whole selves” to work – as we manage a strategic return to the workplace. As Scott Nelson and Savannah Gibbs of Hunton Andrews Kurth, LLP explain in “The Post-COVID-19 Workplace: Mission-Critical Decisions Ahead for Employers” (p. 30), what started as temporary work-from-home has, in the space of one year, become a paradigm shift in work culture. Ethical decision-making will creep back into our work as we navigate decisions around issues like vaccine requirements. Further, employee mental health challenges during this time may be more hidden now but could become more visible as we return to the workplace. This creates the need to be prepared for a variety of behaviors that add risk complexity.

A couple of other key predictions for 2021:

- “A Coming Wave of Investor Interest in ESG (Environmental, Social & Governance) Reporting” (p. 13): In the coming decade, we see an increase in climate-related disasters which will push businesses to adopt an array of ESG practices and procedures. This will have a profound impact on supply chain management, investment decisions, as well as operational and strategic decision making – not to mention the environment itself.

- “A New Age of Accountability: Global Whistleblowing on the Rise” (p. 44): In 2021, whistleblowers will come into their own in ways previously unseen: the “whistleblower hero.” We expect to see an explosion of whistleblower requirements in organizations, responding to a massive change in regulation, as well as a shift in the perception of whistleblowers.

We look forward to 2021 for many reasons. One of them is knowing that, while 2020 was challenging, our profession is forever changed – and for the better. Some of the risks that came to pass in 2020 were the anomalous result of a crazy year, but many were not. Some of the most difficult issues, such as the wave of social unrest in response to racial discrimination, are, sadly, not new. Perhaps 2021 will be the year we realize risk and compliance cannot be narrowly defined nor addressed. Integration, context, and cooperation may be the best tools organizations have to course-correct and prepare for the next chapter.
What started as temporary work-from-home has, in the space of one year, become a paradigm shift in work culture.
Corporations came under enormous strain in 2020. One primary source of that strain was the pandemic, but more destructive was the pandora’s box of other risks that the pandemic opened: cybersecurity, supply chain, health and safety, financial fraud, and regulatory compliance as well.

If the experiences of 2020 taught us anything, it’s that a federated approach to risk is not enough. Just a wildfire, individual threats, and crises can easily converge, feeding off one another and unleashing unpredicted destructive potential. This year may be over, but we still face many challenges. Compliance and integrated risk management will need to come together under one roof. The risks emerging before our eyes are interconnected and require the same in response.

In 2021, organizations will integrate their compliance, IT, operational, reputational, third-party, and ESG processes and practices. This holistic integration will require clear lines of communication and responsibility, and we expect more organizations to appoint Chief Risk Officers (CROs) or Chief Risk and Compliance Officers (CRCOs) to manage an integrated risk strategy. Additionally, board-level committees will be tasked with addressing enterprise-wide risk and risk strategy.

The Current State of Risk Integration

Regulators, such as the U.S. Department of Justice, scrutinize organizations’ ability to prevent misconduct from happening. Risks from climate change or supply chain failures threaten enormous operational disruption, even if those issues aren’t regulatory enforcement concerns. Social media enables advocates to draw public attention to corporate missteps, asking, essentially: How did the company not see this coming?

That’s a question corporate boards and CEOs never want to ask. In 2021, boards will require tools and information to assess, manage, and report enterprise risks.

Integration of risk functions isn’t a new idea, but the pandemic of 2020 has accelerated this corporate governance to a disorienting degree.

2021 PREDICTION

In 2021, organizations will further integrate their compliance, IT, operational, reputational, third-party, and ESG risk management processes and practices.
Integrated Risk Management is an Evolutionary Requirement

Governments have already begun to respond to the new complex risk landscape by pushing organizations toward increased transparency and accountability. In the U.S., the Biden Administration has already made clear that it wants to see more disclosure from corporations on climate change and racial equity. The European Union’s new whistleblower protection directive will go into effect at the end of 2021. Enforcement of anti-corruption, anti-money laundering, data privacy, and human trafficking laws increased dramatically over the past decade, and that won’t change in the next decade.

These dynamic social, regulatory, and economic pressures require an integrated approach to risk management. The board, senior executives, and business unit leaders should have a comprehensive understanding of organizational risks. Companies who are able to evolve and meet these new demands will have the advantage of informed decision-making and improved performance.

Steps for Organizations to Take

1. Cultivate Support for Integrated Risk Management

Integrated risk management affects many parts of the organization: legal, internal audit, IT, compliance, and any existing risk management functions the organization already has. Advocates for IRM need to identify and cultivate the support of in-house partners, senior management, and the board, which has the ultimate responsibility for assuring effective risk management.

2. Clarify Roles and Responsibilities

How will compliance and risk management functions intersect? Those can be delicate issues at many organizations, but clarity around roles and responsibilities determines decision-making hierarchy, and ultimately accountability. If you don’t have a CRO or CRCO, consider designating a member of senior management who can assume these duties.
3. Define Risks and Mitigation Steps

Leaders throughout the enterprise will need to use risk assessments to map risks to processes and requirements, including supply chain management, compliance risks, financial liquidity, litigation threats, workplace operations risks such as extreme weather events or pandemics, and more.

Use risk management frameworks to identify and mitigate risks. This can be an ambitious undertaking; role clarification is an important prior step.

4. Develop Monitoring and Reporting Capability

Risks need to be monitored on an ongoing basis, and new risks should generate an alert and be reported to key stakeholders. It’s also important to report regularly on all collective risks, so risk management leaders can clearly articulate the organization’s high-level risks and pressing concerns, as well as less urgent considerations.

It is tempting to view 2020 as an anomaly, and that’s not wrong. However, the trends driving the major crises of 2020 - growing international political instability, weakening institutions and norms, increasingly complex and interdependent supply chains, expansive trade wars and sanctions, ecological disruption, and accelerated global warming, just to name a few - will be just as urgent in 2021.

Businesses that isolate compliance risk from other business risks will not be able to strategically respond. Those that bring risk and compliance under one roof will be poised to thrive when the next once-in-a-century storm invariably hits – as it invariably will.

About the Author

Haywood Marsh leads the Lockpath and NetClaim businesses at NAVEX Global as General Manager. He leverages his experience in operations, marketing, strategic planning, product management and sales to drive the execution of Lockpath’s and NetClaim’s strategies.

Prior to his current role, Haywood served as the VP of Strategic Programs at NAVEX Global, managing the Project Management Organization, Release Management and Business Systems teams. Immediately before joining NAVEX Global, Haywood led Marketing, strategic/ product planning and an Inside Sales team for a division of Danaher. Previous to Danaher, Haywood served in the Pentagon as a military strategy consultant and team lead for Booz Allen Hamilton, worked as the Director of Quality Assurance at SONEX Enterprises and ran a live military intelligence mission while serving as a soldier in the U.S. Army, among other roles.
In addition to regulations, which continue to proliferate, risk is now coming from more places than ever before.
The shift to remote work as a result of the COVID pandemic has increased the scope of risk and thus broadened the area of responsibility for risk managers. In addition to complying with regulations, which continue to proliferate, risk is coming from more places than ever before. The work-from-home (WFH) environment offers new opportunities for data breaches, policy violations, audit failures, and third-party risk, just to name a few IT risks resulting from a remote workforce.

This high-risk environment is challenging for compliance and IT professionals, who will have to keep track of more areas of risk in this new WFH environment.

Cyber attackers have seized this opportunity and significantly expanded their campaigns at a time when organizations are most vulnerable. It’s likely that the frequency of cyber-attacks, such as phishing attacks on remote workers and attacks on remote physical infrastructure, is likely to increase in 2021, as remote work continues and even becomes the norm for many companies.

In addition to increased threats to cybersecurity, the regulatory and risk-management environments are likely to shift next year, increasing the challenges for compliance officers, as recent regulatory changes come online:

- The recent California Privacy Rights Act (CPRA), expands data privacy rights in the California Consumer Privacy Act (CCPA). Other states are likely to follow.
- The Payment Card Industry (PCI) will be issuing a new version of its Data Security Standard (DSS) for credit and debit cards in 2021. PCI DSS 4.0 will update security rules for payments industry needs, support additional security measures, promote security as a continuous process, and enhance validation methods.
- NIST 800-53 rev. 5, published in September 2020, will be a good privacy framework option as organizations prepare for the many coming different privacy regulations.

**2021 PREDICTION**

The landscape of business risk in 2021 will be more varied, dangerous, and prolific than in years past. The pandemic-induced remote-work environment will continue to prompt a significant number of IT-related risks, going far beyond what many compliance professionals may be used to.
The scope and complexity of cybersecurity risk and compliance will continue to increase as WFH becomes a semi-permanent condition, even after vaccines control the COVID-19 pandemic. As a result, compliance and IT functions will need to find new ways to collect and communicate risk data, prioritize risk, and incorporate inputs and outputs throughout the organization.

The NIST CSF framework is designed to help translate IT risk to business and compliance risk. Simplify and strengthen compliance and cybersecurity together by tackling them with a compliance-focused infosec strategy.

**Steps Your Company Can Take**

1. **Join Forces with the IT Department**

A progressive risk-based approach requires compliance and IT departments to work closely together. Compliance has likely already mapped compliance requirements to processes; now it’s time to map IT assets to software and software to processes, which will create a Rosetta Stone for translating information security metrics into business risk and compliance objectives – quantifiable metrics they can measure and report on.

2. **Manage What Matters**

Not all IT events, processes, and compliance objectives need the same investment in risk management. Work with IT, risk management, and business leadership to help understand what is most important, where your risk management efforts exist today and where you need to make adjustments for the right risk management approach.

3. **Map Cybersecurity Risks to Controls and Operations**

Map IT processes to business processes and objectives. These mappings can translate information security findings to business and compliance terms and impacts. Next, determine and clarify IT and compliance roles to clarify responsibilities for IT compliance and other security issues, as they are identified.

**IT Frameworks Manage and Communicate Risk Data**

There are many different information security frameworks that compliance officers can adopt to help align the technical aspects and language of information security to compliance and business risk. Adopt a technology framework to translate information security into compliance issues; this will help compliance officers understand, measure, report on, and act to protect the organization from the heightened risks of a WFH environment. Risks are amplified by COVID and will continue to increase in the hybrid office environment after it goes away.

The shift to remote work as a result of the COVID pandemic has increased the scope of risk, and thus broadened the landscape for risk managers. In addition to regulatory compliance, risk is coming from more places than ever before.
4. Contextualize Risk Data to Support All Lines of Business

With a structure and flow of information in place between compliance and IT departments, you have an avenue to report and analyze cybersecurity data and efficiencies. It also becomes an easier task to report risk to different lines of business, such as legal, operations, and product development. Refer to the controls mapping to translate risk information to support and protect other lines of business.

The past year has demonstrated how interconnected and global risk really is. The landscape of business risk in 2021 will be more varied, dangerous, and prolific than in years past. The pandemic-induced remote-work environment will continue to prompt a significant number of information security risks, going far beyond what many compliance professionals may be used to ... and maybe far beyond what we can imagine.

On the other hand, if there were ever a good year to convince leadership and the board to prioritize risk-management initiatives, 2021 is it.

About the Author

Sam Abadir is the Director of Industry Solutions at NAVEX Global. He is a veteran of both the Big 4 Consulting world and the Software Development industry, with over 20 years of risk management experience. His work advances NAVEX Global’s Lockpath IRM platform; educates the world on governance, risk, and compliance; and helps organizations use the data and content around them to better manage risk.
Investment portfolios are now adding ESG information as part of their investment decision criteria and including it in newly created financial products.
A Coming Wave of Investor Interest in ESG (Environmental, Social & Governance) Reporting

By: Karen Alonardo
Vice President of ESG Solutions, NAVEX Global

Heightened interest in Environmental, Social, and Governance (ESG) has become a key topic during board room discussions, elevating Corporate Social Responsibility (CSR) and Sustainability to the next level. It’s now imperative for companies to take action by incorporating and rolling out a well-structured ESG program that aligns with market expectations and investor interest in ESG information on investment opportunities.

The increased interest at the board level has been driven by Bloomberg, Blackrock, the Sustainability Accounting Standards Board (SASB), and other investors and analysts. These groups have developed a common language and metrics that appeal to investors, the C-Suite, and other key stakeholders; SASB, for example, has developed over 70 industry-specific standards to align investors with corporate ESG reporting.

As a corporate leader, it is imperative to go beyond traditional CSR and Sustainability reporting. Stakeholders have much more awareness of concerns like diversity and inclusion, gender pay structure, donation programs, board composition, factory conditions, and how to mitigate climate risks.

Integrating ESG with the Rest of the Business

As ESG has evolved, increased integration across ESG, Sustainability, and other cross-functional teams is becoming more critical to the accuracy of the information. It takes more than one group to manage ESG efforts. Companies who align their ESG goals with business goals will have more long-term success as better information is collected by the appropriate professionals.

2021 PREDICTION

Boards and customers are becoming much more aware and demanding of metrics around diversity and inclusion, gender pay structure, donation programs, board composition, factory conditions, and how to mitigate climate risks. In 2021, organizations will need to move beyond traditional corporate social responsibility reporting, and include ESG issues.
According to a 2019 report, Climate Finance Strategy 2018-2023, from the Hewlett Foundation:

“To put the world on the path to solving climate change, the current level of funding for climate-friendly activities must be tripled to at least $1.5 trillion annually. Fortunately, the multi-trillion-dollar capital sources needed for climate already reside in the current global financial system many times over.”

ESG reporting is typically considered collecting “non-financial” data which presents unique challenges as to what type of information to collect and where to identify where that data lives.

Investors Care about ESG Ratings

For companies, ESG ratings have become a key driver for their Corporate Social Responsibility (CSR) and Sustainability initiatives.

The focus on ESG ratings is driven largely by investor demand for ESG data. Investment portfolios are now adding ESG information as part of their investment decision criteria and including it in newly created financial products to appeal to those who want their investments to align with their own values. Lacking ESG regulations, as of this writing, investors rely on ESG ratings to pressure companies to disclose corporate data, with the intention of standardizing criteria and providing that information to investors.

Ratings are simply intended to offer a high-level view into ESG performance, and disclosures around ESG concerns.

What are ESG Criteria?

Think of ESG as another level of CSR or sustainability reporting, with the added criteria of increased Social and Governance metrics. The areas typically covered by the current SASB standard and other frameworks, meant to provide guidance for the information needed to meet the requirements set forth by these non-profit organizations.

The three elements of Environmental, Social, and Governance (ESG) provide insights into the sustainability and societal impact of an investment in a company. These elements are used to determine the health of the business today and future considerations.

The three key ESG categories consist of the following (see chart):

<table>
<thead>
<tr>
<th>Environment</th>
<th>Social</th>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greenhouse gas (GHG) emissions</td>
<td>Diversity and inclusion</td>
<td>Board composition</td>
</tr>
<tr>
<td>Climate mitigation plans</td>
<td>Human rights</td>
<td>Corporate policies</td>
</tr>
<tr>
<td>Energy efficiency</td>
<td>Employee education</td>
<td>Executive compensation</td>
</tr>
<tr>
<td>Transportation (fleet, freight)</td>
<td>Philanthropic activities</td>
<td>Income inequality</td>
</tr>
<tr>
<td>Waste generations</td>
<td>Data security and privacy</td>
<td>Anti-corruption</td>
</tr>
<tr>
<td>Water management</td>
<td>Supply chain</td>
<td>Anti-bribery</td>
</tr>
</tbody>
</table>
Why is ESG Reporting Important?

Many studies have been conducted over the past few years to illustrate the value of ESG to both investors and companies considering adoption. These studies have identified that assessing ESG practices can drive better valuations over time, drive down operating costs, identify potential risk to brand reputation - and allow companies to get ahead of potential issues that could cause business disruption, from product manufacturing to corporate performance.

What Your Company Can Do

1. The first step to building an ESG program is to assess your current state, identify potential risks, and map metrics to corporate goals.

2. Once you understand specifically what you’d like to accomplish, use a materiality analysis to engage with key internal stakeholders and establish priorities around strategy, goals, and metrics.

3. Collect and consolidate information for reporting. While ESG is progressing forward, corporate ESG and Sustainability professionals must systematize responding to a wave of third-party ESG ratings and sustainability frameworks questionnaires. It will be increasingly important to consolidate auditable, accurate data that can be submitted through questionnaires and made public through Yahoo Finance, Bloomberg terminals, and other financial institutions.

Successful organizations may wish to prepare for a coming wave of consumer demands and investor interest in ESG information by creating a scalable ESG policy now.

About the Author

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.
“Businesses should not mistake this as a return to normalcy.”
A Year of Uncertainty Spurs Integrated Risk Management Adoption

In the last five years, integrated risk management (IRM) has gone from buzzword to practice. The primary driver of IRM across industries is uncertainty. IRM mitigates uncertainty and improves business decision making by integrating risk intelligence with business intelligence.

And 2020 was the year of uncertainty.

• **IRM is a process that improves decision-making and enhances business value by integrating risk intelligence into activities across the enterprise, such as strategic planning and strategy execution, investment decision making, project portfolio management, enterprise performance management, third party performance management, and information governance.**

• **Risk intelligence** is risk data or information that is applied through IRM initiatives to business activities beyond risk management, compliance, audit, and other defensive programs.

Over the next year, organizations will re-direct some GRC-related resources from compliance to a risk-focused approach that supports strategic and operational decision making. This shift will be accompanied by increased investments in the collection and analysis of real-time risk intelligence, enabling companies to better identify and respond to rapidly changing events and more fully embrace IRM practices and processes. However, businesses should not mistake this as a return to normalcy.

**STEEP Analysis**

It is tempting to view 2020 as an anomaly, a self-contained series of chaotic circumstances that can be fixed and forgotten. However, a STEEP analysis (social, technological, economic, environmental, and political) of the current business environment highlights persistent factors of uncertainty that will continue to drive change and impact businesses in the coming years:

**2021 PREDICTION**

Organizations will direct GRC-related resources from compliance to a risk-oriented approach, to support strategic and operational decision making: such as increased investments in the collection and analysis of real-time risk intelligence.
Social

Around the world, social unrest has escalated to levels that are unprecedented in the last 50 years, and there is no resolution in sight.

Technological

Social media has made it easy for anyone to capture and share unfiltered opinions and events and promote real and fake news. Big Tech has come under fire for anti-competitive practices, and many tech companies face increasing scrutiny from lawmakers and regulators over the next several years.

Economic

Perhaps at no time since the Great Depression has economic uncertainty been higher. COVID-19 lockdowns, followed by government and bank interventions, have caused national economies to whiplash from crash to recovery with swings of annualized 30% of GDP or more. National debt and central bank debt portfolios have swollen to unprecedented peacetime levels. Some industries will never recover fully, and small business failures are accelerating.

Environmental

Extreme recent environmental events have given new urgency to the issue of climate change, while governments struggle to balance health and safety needs against the negative economic effects of COVID shutdowns. With effective vaccines, COVID-19 should be under control by year-end 2021; climate change, however, will not.

Political

In many democracies, political polarization and populism have increased over the last few years, creating an environment conducive to nationalism. While the uncertainties facing society, business, and government have been building for over a decade, in the past they have occurred in waves that peaked at different times.

The events of the past year led all STEEP uncertainties to peak simultaneously. Though that may not happen again soon, these uncertainties remain, and boards and senior executives are demanding better risk intelligence to support effective business decision making.
**Steps You Can Take**

Successful risk management and compliance leaders will respond to the demands for better risk intelligence by revamping their programs to support traditional compliance and audit-related activities and enable business decision-making with ongoing risk intelligence.

Fortunately, many of the basic processes are already in place, including frameworks that provide best practices guidance; ISO 31000 provides strategy and business-oriented guidance for IRM initiatives. Compliance leaders looking for a framework that already aligns with their controls-oriented activities can complement ISO 31000 with the COSO Enterprise Risk Management framework.

Collaborating with strategic planners is a good place to start with IRM. But don’t stop there. Risk management principles advance and secure many areas of business: new product development, third-party risk management, and even help companies avoid reputational damage and the impact of political upheaval.

Now that integrated risk management is mainstream, make 2021 the year to start or expand your IRM initiatives.

---

**Activities Supported by Risk Intelligence**

<table>
<thead>
<tr>
<th>Activity</th>
<th>0%</th>
<th>10%</th>
<th>20%</th>
<th>30%</th>
<th>40%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>78%</strong></td>
<td>80%</td>
</tr>
<tr>
<td>Strategy Execution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>63%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investment Decision Making</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>47%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Portfolio Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>46%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Performance Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>57%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Party Performance Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>52%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>45%</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>7%</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Source: FCInsight and RMA*

---

**About the Author**

French Caldwell is a managing partner and co-founder of The Analyst Syndicate. He has been a naval officer and submariner, a liaison to NATO for a congressional commission, a consultant with the Central Intelligence Agency and Department of Defense, a Gartner Fellow and analyst, and an executive on the leadership team of a Silicon Valley tech company.
A single, comprehensive approach to data privacy may be the better and most risk-averse approach.
When it comes to data privacy law, change is the only constant. The global pandemic unleashed a new set of risks related to data privacy that companies will have to confront in 2021. But despite the COVID chaos, data privacy regulations around the world are becoming more strict, more prolific, and more stringently enforced.

In the coming year, we predict that organizations, especially those with global operations, may find that a single, comprehensive approach to data privacy in order to operate in this increasingly complex environment, the better and most risk-averse approach.

What are the biggest questions being asked in the privacy community? What else does the future hold? Dr. Tobias Schelinski, German partner at the international law firm Taylor-Wessing, and Jessica Wilburn, Data Privacy Officer and Senior Counsel at NAVEX Global, offer global perspectives and bold predictions around the trend toward complexity around data privacy laws.

**“What is the Biggest Threat to Organizations?”**

- **Tobias:** In the European Union, we will see many more consumers making use of their data protection rights granted under the GDPR and local data protection laws. This will include an increase in damage compensation claims. You could say that privacy law will be the new consumer protection law.

- **Jessica:** I expect this to be a global trend. California residents under the newly passed CPRA (amending and expanding the current CCPA), and Brazilians under the new General Data Protection Law, are just two recent examples of newly established data subject rights.

**2021 PREDICTION**

Data privacy regulations around the world are becoming more strict, more prolific, and more stringently enforced. Organizations will need to establish a single, one-size-fits-all approach to data privacy, in order to operate in an increasingly complex environment.
Jessica cont’d: Data privacy is in place to protect people. It's fair to want to know the biggest threats and tools to combat them; but if you implement privacy principles (transparency and accountability are key principles) across your organization and make it a critical part of your culture, the rest follows easily. Managing data subject rights should be at the forefront of your privacy program.

Consumers will demand transparency and start exercising their access rights. Spikes in data subject requests have already increased over the last several months.

Tobias: There are several reasons why privacy law has become more popular for consumers lately and will continue to be. The 2020 Schrems II decision of the Court of Justice of the European Union caused significant privacy awareness. Consumers are beginning to realize that they just need to send a GDPR-related request to the company via email, and the company must “obey,” and respond to their requests in time. On the other hand, disputes based on consumer protection law are complicated, usually require a lawyer, and often are not justified from a legal perspective.

Jessica: I agree! Privacy in the news, new laws in the United States, and global tension created by the Schrems II decision have merged to form a privacy awareness campaign.

“What Will 2021 Bring for Data Subject Requests?”

Tobias: Companies with a large consumer customer base in the European Union should be prepared for a second wave of GDPR-related requests, particularly damage compensation claims. More than ever, it will be important to have and maintain appropriate internal processes and have technology in place to handle such requests and claims.

Jessica: Responding to data subject requests can be very complicated. Thus, it’s critical to have streamlined processes and procedures in place to the extent possible.

To implement and leverage processes and technologies, it will be necessary to become a master of the personal-data process. I expect we will continue to see a rise in data subject request tools and automation, such as the use of contact centers and secure web portals with backend software, to manage these requests.
“How Do You Align Privacy Approaches to Ensure Global Compliance?”

Jessica: I expect many companies will start taking a single, comprehensive approach to data subject rights. In my opinion, the countries (and states) that have data subject rights in their legislation are all similar. If you operate a global business, it may be best to provide rights to everyone, rather than trying to work out the requirements on a case-by-case basis. New local data-privacy laws are emerging on a fast-paced and consistent basis.

Generally, global compliance with privacy laws is always the burning question. If you are subject to GDPR (or even if you’re not), the E.U. requirements are a leader in this space and a good starting point.

Tobias: Yes, the advantage of an E.U.-driven approach is that you can rely on best practices and high standards that are accepted around the world. At some point, however, fast-growing or multinational companies will have to comply with different local privacy laws.

“What’s the Outlook on Future New Regulations?”

Tobias: The challenge for companies to comply with different privacy law regimes will increase in 2021, as new privacy laws will come into force in several countries, for example in Switzerland.

Jessica: 2020 brought us California’s CPRA (CCPA 2.0), Brazil’s General Data Protection Law, the Schrems II decision impacting international transfers, and the list goes on. We expect 2021 to be no different. It will be interesting to see what happens in the United States. Will the CPRA push along federal privacy legislation? Will other states pass comprehensive privacy laws in line with California? Having a “patchwork” of requirements across the states is likely to counteract what privacy laws are designed to protect (people).

Tobias: In the European Union, we will have to deal with privacy issues relating to Brexit; the question is whether the UK will be recognized as having a privacy law regime that is adequate to GDPR. New regulations from China are coming as well. It will also be interesting to see how companies implement the new Standard Contractual Clauses for data transfer to recipients outside the European Union. And who knows ... maybe the ePrivacy Regulation will finally come into force (with more than three years’ delay!).
3. Use GDPR as a Starting Point for a Universal Data Privacy Program

Leverage the GDPR, as the leader in the space, as a helpful starting point. You’ll find you may not have to reinvent the wheel for your operations in other countries. Regulators will appreciate a comprehensive approach to respecting individuals’ rights to their personal data, especially if you do business in different countries.

Organizations should focus on minimizing risk and limiting exposure. To do this, you need to create living and breathing data inventories with policies and procedures formalized throughout the organization.

Continuous assessments of new and existing data processing activities will be critical when managing privacy in your business on a global scale in 2021 and beyond.

Steps for Organizations to Take

1. Establish Efficient, Automated Processes for Responding to Data Requests

Individuals are becoming more aware of their rights and are exercising them. Depending on the context, the employment context by way of example, fulfilling and responding to requests can be complex and chaotic. This will increase in the coming months. We expect to continue to see a rise in technology solutions and automation in this space.

2. Consider Local and Global Data Privacy Regulations

Legal and compliance professionals have been focused on the E.U., but there are many other laws around the world. Shifting your privacy program to a global outlook, versus focusing on individual country compliance, will better prepare organizations in the long run. It may be easier to treat everyone the same (individuals and countries) to the extent possible, which will track back to your data inventory and records of data processing activities.

About the Authors

Dr. Tobias Schelinski is a specialist lawyer for information technology law and heads up the industry group Logistics & Transport. Based in Germany, Tobias is highly experienced in IT projects, including digitization, outsourcing, e-commerce, and data protection and Tobias supports his clients with strong negotiating skills in national and international technology projects. His clients praise his distinctive commercial and technical understanding and his extensive international network. In the games industry, he is regarded as one of the leading lawyers in Europe.

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.
It is unacceptable and ineffective to compartmentalize diversity and inclusion efforts - or to expect diverse employees to be responsible for advancing DEI.
Diversity, Equity, and Inclusion: More Transparency and Accountability

By: Chai Feldblum
Partner and Director of Workplace Culture Consulting, Morgan, Lewis, & Blockius LLP

Emily Cuneo DeSmedt
Associate, Morgan, Lewis, & Blockius LLP

Perhaps no year has forced employers to re-examine their work environments more than 2020. While COVID-19 has thrust upon us a workplace that is physically amorphous, the Black Lives Matter movement has also created an unprecedented urgency for a more genuinely diverse and inclusive workforce.

Of course, most employers have long accepted the benefits of diversity in the workplace, and many have devoted significant resources to diversity, equity, and inclusion (DEI) initiatives. But, because employers risk liability under Title VII when they take race, gender, and other protected characteristics into account in employment decisions, employers have historically tiptoed around more aggressive DEI approaches and designed their DEI programs around indirect strategies.

Only this year, under the spotlight of the #BLM movement, have employers collectively acknowledged that their existing methods have simply failed to produce sufficient representation and inclusion of Black employees, women, and other underrepresented minorities throughout their organizations.

Over the past year, employers have largely answered the call to reexamine their pursuit of diversity, equity, and inclusion and embraced the introspection that is necessary for meaningful change. In 2021, we expect a trend toward a more comprehensive approach to DEI to include input and collaboration of their Human Resources, legal, ethics, and compliance teams. We anticipate trends in the coming year around increased transparency, better leadership buy-in, and increased accountability and enforcement for managers.

Increased Transparency

While employers have historically collected and maintained varying degrees of demographic data about their employees, many have shied away from sharing that information with their workforce or the public.

2021 PREDICTION

We expect a more comprehensive approach to DEI that includes HR, legal, ethics, and compliance teams. We anticipate increased transparency, leadership buy-in, and increased accountability and enforcement.
More recently, however, some employers have published descriptive demographic data about their workforce to make their commitment to DEI more transparent. While employers should work with counsel to understand the risks associated with publishing data, when done carefully, publishing descriptive demographic data can encourage employee dialogue about DEI efforts and identify root causes of underrepresentation in the employer’s workforce.

**Leader Buy-in and Employee Engagement**

Employers are acknowledging that it is unacceptable and ineffective to compartmentalize their DEI efforts - or to expect their diverse employees to shoulder the responsibility of advancing DEI. It is critical that the employer’s most senior executives demonstrate their personal commitment to moving the needle on diversity. Employers will implement mechanisms to engage a range of employees, develop ideas for greater DEI, and implement those ideas across the entire enterprise.

To do so, we encourage employers to create an employee-driven DEI council, as well as an executive-led DEI council, with clear communication lines between the two groups. This can ensure that DEI is implemented into the annual targets of each component of the enterprise.

**Increased Accountability**

As employers embed DEI initiatives across their organizations, many are also implementing new mechanisms to hold employees, and particularly managers, accountable for diversity and inclusion. Those mechanisms include:

- Performance reviews that require managers to provide concrete examples of their efforts, to make their teams more equitable and inclusive, and develop diverse members.
- Policies that demand civility, ensure consistent consequences for uncivil behavior, and empower bystander engagement and reporting.
- Programs that require managers to regularly review and hold each other accountable for their respective DEI efforts.
**Steps You Can Take**

Most employers were already seeking diverse slates of candidates for their open positions and promotions, but many still need to implement more thoughtful and intentional diverse recruiting. Some strategies that we are encouraging employers to implement include:

1. Examine the schools or groups with which you advertise your positions. Do those schools include Historically Black Colleges and Universities (HBCUs)? Is your organization attending recruiting events held by diverse organizations and affinity groups?

2. Review your job descriptions to make sure a commitment to diversity and inclusion is an essential requirement of every position. Do your job requisitions make clear that you expect all employees to promote a diverse and inclusive work environment?

3. Reconsider your referral sources. Are your organization’s female and Black employees referring their contacts and colleagues for open positions at the same rate that their male and/or White employees are referring them?

4. Train your hiring managers on strategies to check implicit biases. If your hiring managers believe particular candidates do not demonstrate the skills or commitment for particular roles, are they trained to question whether they would come to the same conclusion if the candidates were of a different race, or gender, or age?

5. Ensure that your hiring and interviewing team is as diverse as possible. Does the slate of interviewers and decision-makers for each role convey to candidates that the team takes diversity seriously?

These are only a few examples of the many new strategies employers are implementing as they re-examine their existing DEI efforts and acknowledge that simply prohibiting employers from considering race, gender, and other protected characteristics is not enough to achieve meaningful diversity and inclusion in the workplace. While some of the changes to the work environment that we have seen in 2020 might be temporary, we are optimistic that employers’ collective effort to improve diversity, equity, and inclusion will only grow in 2021.

---

**About the Authors**

Chai Feldblum, partner at Morgan, Lewis & Bockius, LLP, helps companies and organizations create safe, respectful, diverse, and inclusive workplaces. Chai served as a commissioner of the Equal Employment Opportunity Commission (EEOC) from 2010 to 2019 and is co-director of Morgan Lewis’s Workplace Culture Consulting.

Emily Cuneo DeSmedt, associate at Morgan, Lewis & Blockius, LLP, assists in the representation of employers in a wide variety of employment-related matters, including the defense of wrongful termination, harassment, discrimination, and retaliation claims.
Should employers call for a return to the office at all?
COVID-19 introduced a bevy of changes to the workforce – from increased use of video communications technology to widespread remote work. Across industries and company structures, the virus forced employees to work from home. As they begin to return to the office in 2021, employers will each have to tailor their own best strategy for safely transitioning back. How they proceed may prove vital to their success in the current shifting market.

In 2021, we expect businesses across industries to make long-term changes to their remote work policies and in-office practices to meet employee needs and expectations, and support recruitment and retention efforts. These changes will have lasting impacts on the very nature of work and on employer-employee relations.

Manage a Strategic Return to Work

Much has been said about the hazard assessments that OSHA and the CDC recommend employers conduct for a safe return. Employers should make these assessments and implement changes accordingly, which may involve improving air filtration systems, providing masks and cleaning equipment to employees, and installing temperature checkpoints.

But thoughtful, strategic businesses should also consider other factors for a win-win return for both employer and employee: Should they restructure the office to address the safety concerns of returning? How has COVID affected their employees’ mental health? Should they require employees to get a COVID vaccine?

And perhaps the biggest question: Should employers call for a return to the office at all?

It is already apparent that one trend post-COVID will be a large-scale shift to remote work. Several noteworthy companies have already announced a permanent remote work plan going forward. In industries where this approach is widely adopted and employee-favored, flexibility will be much more important to recruit and retain top talent after COVID.
Because 77% of the workforce has indicated a preference for continuing to work from home at least part of every week, employers in every industry must decide how to best address both company and employee needs. To do this effectively, employers should weigh their particular in-office efficiencies against the potential retention of employees with new bargaining power to demand flexibility. They should also account for some employees with COVID-related anxiety not being comfortable returning to the office.

Employers will need to get ahead of these issues. They may find that the market has shifted, and their employees’ expectations with it.

**Steps for Organizations to Take**

1. **Assess How Successful Work-From-Home Has Been for Your Company**

Do you truly need your employees to return to the office? This analysis will depend on the specific needs of your company. For some, it may be necessary to adopt a flexible policy to recruit and retain top talent. This is especially true for roles that work well remotely and may expect remote work as the new norm. For others to work optimally, a physical return may be necessary.

To determine whether your company will benefit from a long-term change in work-from-home policy, evaluate employee productivity while working from home. Poll workers about their preferences to assess the risk of losing talent if you implement a strict return-to-work policy. Some may be craving a return to the office and human contact, while others may fear it.

If your business did not suffer from remote work, you will likely be able to continue working remotely or increase flexible work options for your workers without significant sacrifice. Most companies have already upgraded their technological capabilities for the months-long remote work that COVID has required. If your company has already integrated advanced technology or otherwise invested in remote work functionality, its use and value are worth noting.

2. **Address Employees’ Mental Health Needs**

Employers should already be addressing your employees’ mental health concerns, COVID-related and otherwise, you must also prepare to implement new support strategies when your employees return to the office.

COVID forced the majority of the workforce into many months of isolation. The lack of regular human interaction, coupled with fears of loss and infected loved ones, have necessarily taken a toll on many employees’ mental health. Your employees may be struggling to cope beyond what is visible in a video conference or phone call.

Some employees may crave a return to normalcy and human interaction, while others may have significant social anxiety related to relearning the social dynamics of the workplace after so long in isolation. Still others may have developed depression from the lack of human contact and worry for their loved ones.

To support your people and foster a supportive, productive environment, decide how best to address their concerns and discomforts about
returning to work. For example, this could mean allowing flexibility, offering your employees mental health support systems such as counseling or mindfulness trainings, or attempting to foster a non-judgmental, inclusive environment. Decide which approaches will most benefit your employees and company, and start implementing them now.

3. Consider How to Change the Physical Space

With many employers requiring fewer in-office full-time workers, large office spaces will no longer be the norm, and commercial real estate prices may drop. Whether you downsize or reconfigure your current space, consider: What should the office space of the future look like?

In a post-COVID world, offices big and small will be revamped for safety. The open floor plan office design was already long in the tooth (and unpopular among employees), and COVID will likely hammer the final nail in its coffin. Gone are the days of employee bullpens and stuffy cubicles. Instead, employees will likely expect more private or isolated offices. Although employees often enjoy open and edgy common areas, they may be reluctant to continue using such areas for fear of infection.

However you proceed, weigh the benefits of safety measures against the negative impact minimizing human contact could have on the culture. Human interaction and collaboration are key reasons to require in-office work, and employers should take measures to keep these benefits intact.

4. Decide Whether to Require a Vaccine

With the desperate desire for a cure for the virus and its attendant disruptions to our lives, employers who want their employees to return to the office face a new question: Should they require their employees to get the vaccine before returning?

The Equal Employment Opportunity Commission announced in its December 16, 2020 guidance that an employer may exclude an employee
from the office if that employee refuses to get vaccinated because of a disability or sincerely held religious belief for which there is no reasonable accommodation possible.

This guidance may first appear to lend credibility to employers’ requiring the vaccine, but it does not completely shield employers from risk. Employers still may not take any adverse action against an unvaccinated employee unless that employee poses a direct threat to the health and safety of the office and no reasonable accommodations, such as wearing a mask or social distancing, is possible.

In our current era, it’s going to be hard to argue that continued, paid work-from-home is not a reasonable accommodation, when the employee at issue or other similar employees have already been working from home successfully.

It may be tempting to allay some employees’ safety concerns by requiring a vaccine, but employers should carefully consider the risks before doing this; significant safety, morale, and legal concerns caution against requiring vaccines. The initial vaccine trials have been encouraging, but in this early stage, we cannot yet be sure of their long-term effects. These were the first licensed mRNA vaccines in the United States. Employers should hesitate to require their employees to take that risk.

Employers may face legal risks from mandating vaccines. Employees with religious or ADA objections could allege discrimination if their employers do not provide them reasonable accommodations, or at least attempt to, before excluding them from the office. Further, the federal EEOC guidance does not affect state law, so it does not immunize employers from potential state tort and discrimination litigation down the road for requiring vaccines. Absent clear rules establishing no liability for requiring employee vaccines, there will be litigation about it. Although the EEOC says employers may mandate the vaccine, employers still must consider ADA and religious accommodations, as well as state tort, privacy, and discrimination laws.

The best practice will be to let employees choose. This will ensure fair treatment and avoid a potential new wave of litigation down the road.

---

About the Authors

Scott Nelson is a partner, Labor & Employment, at Hunton Andrews Kurth, LLP. Scott has been recognized as a Texas Super Lawyer and a leading U.S. lawyer in Labor and Employment Litigation and Workplace and Employment Counseling. He is also Board Certified in Labor and Employment Law by the Texas Board of Legal Specialization.

Savannah Gibbs is an associate, Labor & Employment, at Hunton Andrews Kurth, LLP. Savannah represents corporate clients in substantial discrimination, trade secret misappropriation, and wage and hour litigation. She guides clients through all aspects and stages of labor and employment matters, with each client’s specific needs and long-term goals in mind.
Compliance professionals have an unparalleled opportunity to build a bridge to the supply chain team.
Third-Party Risk and Resiliency: Building a Bridge Between Compliance and Supply Chain Management

By: Josh Reid  
Principal, Crowe LLP

One of the most critical takeaways from the events of 2020 was the fragility of the supply chain for many businesses as well as the national emergency response. Almost every industry and business struggled with at least one of the following scenarios:

- The inability to obtain the raw materials needed to create products
- The inability to purchase or import products needed to support an emergency response
- A decrease in demand for products, which resulted in slow movement and capital being tied up in inventory

Whether it’s relying on suppliers in countries with political instability or sanctions; grappling with pandemic-disrupted logistics; ensuring that downstream suppliers are not creating environmental, social, and governance (ESG) risk to the organization; or addressing risk arising from new regulations impacting third-party data security, an organization’s supply chain is subject to, and creating risk – dare we say, now more than ever.

Risk to and from supply chains is underestimated, and our approach to managing these risks has been siloed between Compliance and Supply Chain teams. Compliance teams have often primarily focused on the risk of bribery and corruption in the supply chain and less so on the stability of it or the damage that a supplier could do to the organization’s reputation. The events of 2020 demonstrated that these issues are interconnected and the risks need to be addressed holistically.

In 2021, compliance professionals have an unparalleled opportunity to contribute their expertise to the overarching supplier risk management strategy and build a bridge to the supply chain team. These four steps can help organizations proactively identify a potential supply chain interruption and enable proactive decision-making.

2021 PREDICTION

In 2021, compliance professionals have an unparalleled opportunity to contribute their expertise to the overarching supplier risk management strategy and build a bridge to the supply chain team.
Steps Organizations Can Take

1. Build a Bridge Between Compliance and Supply Chain Management
   - Learn to speak the language of supply chain – logistics, redundancy, and business continuity.
   - Understanding supply chain management priorities.
   - Look for areas of overlap of third-party oversight responsibilities between functions.
   - Ensure that third-party risk-management technology can view and prioritize all risk areas, including compliance, ESG, geopolitical, and supply chain disruption risk.

2. Assess Opportunities for Disruption and Points of Failure
   - Segment and risk-rank your supplier base by considering key factors, including contributed revenue, country, and product line. Address compliance and reputational risks, including ESG risks in the segmentation and ranking.
   - Identify those suppliers that are affected by volume changes - both increases and decreases.
   - Develop risk mitigation plans and actions for working with high-risk suppliers.

3. Strategize Supply-Chain Options
   - Understand any potential impacts on high-risk products, including supplier overlaps, the supplier’s financial viability, and country or political risk.
   - Define key risk performance measures to monitor for suppliers that are high risk or critical.
   - Determine which key contract and service-level agreements might be affected by changes in volume and demand.
   - Identify necessary action items during a disruption, making sure to consider different types and categories of disruptions.
   - Understand if technology could support risk monitoring and what supplier data is needed to implement that technology.
   - Implement the right technology to support risk monitoring.

4. Execute and Manage Change
   - Encourage organizational support of plans and needed changes. Support from leadership, as well as each department, is necessary to execute across the organization.
   - Drive the “heavy lifting” while managing unintended impacts. Although challenges might surface along the way, make sure they don’t derail the overall goal.
   - Implement processes with metrics to sustain benefits. The more it can be proved that the processes are working, the better the chance that the organization will continue to implement changes.
   - Deploy proactive processes for resiliency and visibility. It’s not enough to react to events; organizations need to go on the offensive and make sure they are prepared for any future disruptions. Organizations must know their downstream supply chain and where they are vulnerable.
5. Optimize for Future Supply-Chain Disruption

- Plan for future improvement, including identifying resources and developing strategies.
- Monitor and develop change management activities and procedures – updating them regularly based on current circumstances and past outcomes.
- Use supplier changes to develop or update a business continuity management plan.
- Provide visibility to the plan and consider the impact throughout the organization’s global supply chain.

Most organizations never could have predicted the scope of disruptions and speed of impact experienced during 2020. These events highlighted the importance of cross-functional relationships to ensure that organizations are identifying and holistically mitigating the most critical risks. Compliance should feel empowered to build a bridge with the supply chain team to better serve our organizations and most effectively use our limited resources in managing and overseeing our critical third parties.

About the Author

Josh Reid is a Principal in Crowe’s Risk Consulting Practice and serves as Crowe’s Governance, Risk and Compliance (GRC) Technologies solution leader. Mr. Reid has over 14 years of experience and focuses on leading GRC software implementation projects including operational risk management, cybersecurity, and regulatory compliance. His responsibilities include overseeing the strategic direction of Crowe’s GRC Technologies solution offerings, enhancing Crowe’s proprietary GRC SKILL implementation methodology, and bringing new GRC solution offerings to market.
Many sensitive issues are more about personal conduct and values than legal requirements.
Training: More Complex, More Important — and More Pushback

By: Ingrid Fredeen
Vice President and Senior Product Manager, NAVEX Global

In the last 5 years, ethics and compliance training programs have taken on a new life and focus. Organizations now recognize the critical role they play in an overall effective compliance program, and with increasing regulatory scrutiny, compliance programs have started to recognize training as an area of excellence and not just a task to be completed. As we move into 2021, the challenges that lay ahead will continue to test the effectiveness of the compliance function.

Issues are More Contentious

One of the more difficult challenges going into 2021 will be navigating our divided and heated workplace environment.

Compliance professionals will need to navigate the divides that exist while communicating their expectations of employees. Many sensitive issues are more about personal conduct and values than legal requirements; training a large, diverse group of employees will be a challenging task.

In previous years, compliance professionals faced little objection to training issues. Now there is the real possibility that significant numbers of employees will object to parts of a training. And since we have encouraged employees to speak up, they are doing so. Additionally, there are more avenues available to speak up through social media and internal business communication platforms.

Compliance officers should expect to encounter more resistance from employees who don’t like what they’re hearing or who feel empowered to present a challenge. Consider the following examples:

- Safety protocols for in-person work may require employees to wear masks or practice other safety measures, but many may be unwilling to follow such guidelines.

2021 PREDICTION

Employees may be resistant and push back against trainings on current divisive issues, such as getting a COVID vaccine, or diversity training - that are casting deep social divides today. In 2021, Compliance professionals will need to navigate these divides while communicating their expectations of employees. The most sensitive issues may be more about personal conduct and values than legal requirements.
• Your desire to advance issues of social justice or equity in your workplace may be met with strong internal resistance from those who hold very divergent views.

• The threat of climate change may cause corporations to alter practices in response to consumer, investor, board, and/or employee demand. These changes could be resisted by employees who see this challenge in a different light.

• Advancing equity and inclusion with gender-neutral language and accepting coworkers who identify as transgender or non-binary is a very important initiative, but employers should expect efforts to be met with resistance from those who do not acknowledge their need.

• Diversity training that encourages the advancement of programs for groups that have been historically subject to discrimination may experience significant resistance from others who deny that systemic discrimination exists. If employees interface with the public, this challenge is even more complex.

Organizations will need to think carefully about how they train on these topics, and how they address objections in the coming year. Meet objections with compassion and an open mind and thoughtfully consider them – but also be prepared to respond in a way that fits your organization’s values.

Your goal in 2021 is to find a way to reach all your employees.

In-Person Training May Not be Possible, but Adaption Is

The delivery of training has become more complicated as the pandemic forced millions to work remotely or avoid close proximity. It was a massive challenge when eLearning suddenly became one of the only feasible options, and that will continue into 2021.

For organizations with employees who have little or no access to technology or company email, this is the year to start planning for the next inevitable disruption. Consider new approaches that simulate live delivery methods: Host a live video conference call or develop pre-recorded video resources that employees can access.

If we fail to respond to the lessons of 2020, our employees may go another year without critical training.

Steps a Company Can Take

1. Map Out Your Organization’s Needs and Make a Plan for 2021

Many plans were set aside in 2020, and many employees did not get all the training they needed. Now is the time to look at risks, the gaps, and employee needs, then make a plan. Build out a curriculum and identify how to deliver critical messages to your employees. You’ll need to rely more heavily on eLearning, and innovate training formats that may be new. Start your planning with an open mind. It's an opportunity to reinvent the function and approach learners in this new, virtual environment.
2. Align with Leadership on an Approach to Controversial Topics

Identify topic areas that may be controversial or challenging for your organization. For example, in 2020 we heard from many organizations that wanted to advance issues of social justice with training. In 2021, training for charged topics like social justice requires a strong message from the top, so make sure executive leadership is fully committed. Then let employees hear directly from leadership about your organization’s position and expectations.

3. Expand Your Definition of Training

To make your training program more effective and resilient, consider expanding your definition of training. It is not limited to an eLearning course or live event. Training is like a marketing program: you want to get information and messaging out to your audience, and you want the audience to take some action as a result, such as to follow rules or policies or model certain behaviors.

And like marketing, don’t rely on a single mode of communication; 2021 is the year to expand beyond traditional training. Use a variety of tools and communication methods to reach employees who find themselves in very different work environments.

4. Ask Executives to Model and Articulate Company Values

In 2021, it will be more important than ever for employees to see ethical leadership in action. With a transformed workplace (and many working remotely) this will be a daunting challenge.
Leaders will need to be connected to employees. They will also need help from the compliance department to effectively share important messages across the workforce. Employees need, and expect, to hear from executives and managers about how they and others are demonstrating ethical values.

**5. Be Prepared to Handle Objections**

In 2021, you will need a plan for handling employee objections. Whether it is to science-based protocols, diversity initiatives, social justice messaging, or efforts to reduce your organization’s negative impact on the climate, employees are likely to speak up. Some may express opinions that are wildly different from those of the organization, and different from your own.

Be patient and listen. Your job is to reach all employees with important compliance and ethics messages. Be thoughtful in your response, share views with vendors who provide training, and seek the most effective way to get all employees to understand and meet expectations.

Finally, be prepared to hold everyone accountable for a successful training program in 2021: management, employees, third parties, and especially yourself. Patience and cooperation will be necessary for everyone’s success in the coming year.

**About the Author**

Ingrid Fredeen, J.D., Vice President, Online Learning Content, has been specializing in ethics and legal compliance training for more than 15 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.
Look for the rise of the ‘whistleblowing hero’.
In 2021, whistleblowers will come into their own in ways previously unseen. While the United States has had whistleblower protections for two decades, Europe and the Asia-Pacific region are setting new standards in requirements for whistleblower solutions and whistleblower protection. In 2021, we expect to see an explosion of whistleblower requirements in organizations, responding to a massive change in regulation, as well as a shift in the perception of whistleblowers.

In Europe: From Sceptic to Protector

Europe is in the midst of a regulatory leap forward for whistleblower protection. The EU Directive on Whistleblower Protection is a significant new piece of legislation that will shake up the European business landscape starting in 2021. The new laws will elevate the status of whistleblowers, as well as the role organizations play in bringing unethical behavior and criminal activities to light. It will also drive professionalization and standardization for whistleblowing systems and the management of whistleblower reports.

The Directive sets minimum requirements that can affect organizations significantly. For instance, the Directive requires organizations with 50 or more employees, or with an annual turnover or total assets of more than €10 million (about $11.1 million USD), to have a secure and confidential internal reporting channel. Additionally, whistleblowers must be protected against retaliation; the burden of proof lies on the organization that retaliation has not occurred. These requirements will inevitably shine the spotlight on whistleblower systems in the coming year.

In addition to compliance with the new laws, organizations will (or should) ensure their internal reporting systems are professionally run, to encourage internal reporting. Consequently, in 2021, we expect to see an expansion of the compliance function and related services in Europe, benefitting the profession as a whole.

2021 PREDICTION

The E.U. Whistleblower Law will elevate the status of the whistleblower, increase the role organizations play in bringing unethical behavior to light, and drive standardization and professionalism.
In the upcoming year, the Directive will lead to a cultural shift on the continent for whistleblowers. Look for the rise of the “whistleblower hero!” Protections granted by the new law, clear data protection requirements, and the respect for professionals appointed to handle cases properly will create newfound respect for whistleblowers and improve their status.

**In the U.S.: Elevated Whistleblower Status**

In 2020, the U.S. Securities and Exchange Commission (SEC) published amendments to the rules governing its whistleblower program to provide greater clarity and transparency in the award determination process. Despite COVID, the SEC hit record highs in 2020 for the number of claims processed, the amount awarded, and the number of awards made to whistleblowers. Expect even higher record numbers for all of these metrics in 2021.

**In the Asia-Pacific Region: Increasing Regulation**

Until very recently, Asia-Pacific was thought of as a hostile environment for whistleblowers. That’s increasingly untrue. In 2020, Japan, Australia, and other countries implemented penalties for companies that do not have compliant whistleblower programs. Japan passed amendments to its Whistleblower Protection Act such that companies that fail (or fail to try) to establish a reporting system are subject to administrative action by the Consumer Affairs Agency. In Australia, the failure of an in-scope company to have a compliance whistleblowing policy can attract fines of over $125,000 AUD.

Protecting the identity of whistleblowers and maintaining confidential investigations ratcheted up in 2020 in Asia-Pacific. Amendments to a key anti-corruption law in Korea increased penalties for improperly revealing a whistleblower’s identity. In Japan, employees that disclose the identity of a whistleblower without a justifiable reason may be fined. And in Australia, new laws enhance the protection of whistleblowers during and following the reporting process.

A bill in New Zealand is working its way through the parliamentary process, replacing the Protected Disclosures Act of 2000. It clarifies the definition of “serious wrongdoing,” enables people to report directly to an appropriate authority at any time, and strengthens protections for disclosers. Like New Zealand, other countries are likely to either update or implement new whistleblower protections throughout Asia-Pacific in 2021.

**Global Trends in 2021**

Confidentiality is the hallmark of many new laws.

Failure to keep a whistleblower’s identity confidential may have financial, reputational, and even criminal penalties. We expect this trend to continue, with stronger protections for whistleblowers and fines for organizations and individuals that fail to protect their identities. We’ve even seen potential prison terms for disclosure of whistleblowers’ identities. The availability of stiffer penalties under the law is expected to escalate in 2021.
More countries are adopting a sympathetic and positive attitude toward anonymous reporting. Global data from NAVEX Global’s 2020 Risk & Compliance Hotline Benchmark Report shows that 59% of reporters choose to remain anonymous. We expect more countries, explicitly or implicitly, to endorse anonymous reporting and to remove the legal barriers that have previously existed, to encourage internal rather than external reporting.

Laws in Asia-Pacific and Europe will continue to expand the definition of whistleblowers. Once, it was only current employees; but the Directive in Europe, the amendments to the whistleblower laws in Australia, and the new Japanese law all extend protections and reporting capacity to others, including former and retired employees and directors. We expect the legal definition of who can be a whistleblower to continue expanding significantly in 2021.

Lastly, we expect laws will continue to allow larger fines and penalties against companies that engage in retaliation or fail to implement a compliant whistleblowing system.

In 2002, Time magazine named the Enron whistleblowers their persons of the year, earning them a cover story. In 2021, brave whistleblowers will be more revered globally, as laws and public policy strongly support their courage.

**Steps for an Organization to Take**

- Review and update your investigations protocol and strengthen the language relating to whistleblower confidentiality.
- Include a section about confidential and anonymous reporting in your onboarding and annual Code of Conduct refresher training to highlight their importance to employees.
- Review the security features in the technology system that manages your whistleblower complaints, cases, and the evidence you discover.
- Give specialist training to those who will be involved in investigations to reinforce the significance of confidentiality.

About the Authors

Kristy Grant-Hart is CEO of Spark Compliance Consulting and former professor at Delaware School of Law, Widener University, teaching Global Compliance and Ethics. She’s the author of the highly-acclaimed book, How to be a Wildly Effective Compliance Officer, and has been featured in the Wall Street Journal, Financial Times, Compliance Week, and on the cover of Compliance and Ethics Professional Magazine.

Karin Henriksson is an author, founder of WhistleB, and Vice President at NAVEX Global. Before founding WhistleB, Karin worked for European institutions in Brussels and advised European companies in her role as a business ethics consultant.
NAVEX Global is the worldwide leader in integrated risk and compliance management software and services. Our solutions are trusted by thousands of customers around the globe to help them manage risk, address complex regulatory requirements, build corporate ESG programs and foster ethical workplace cultures.