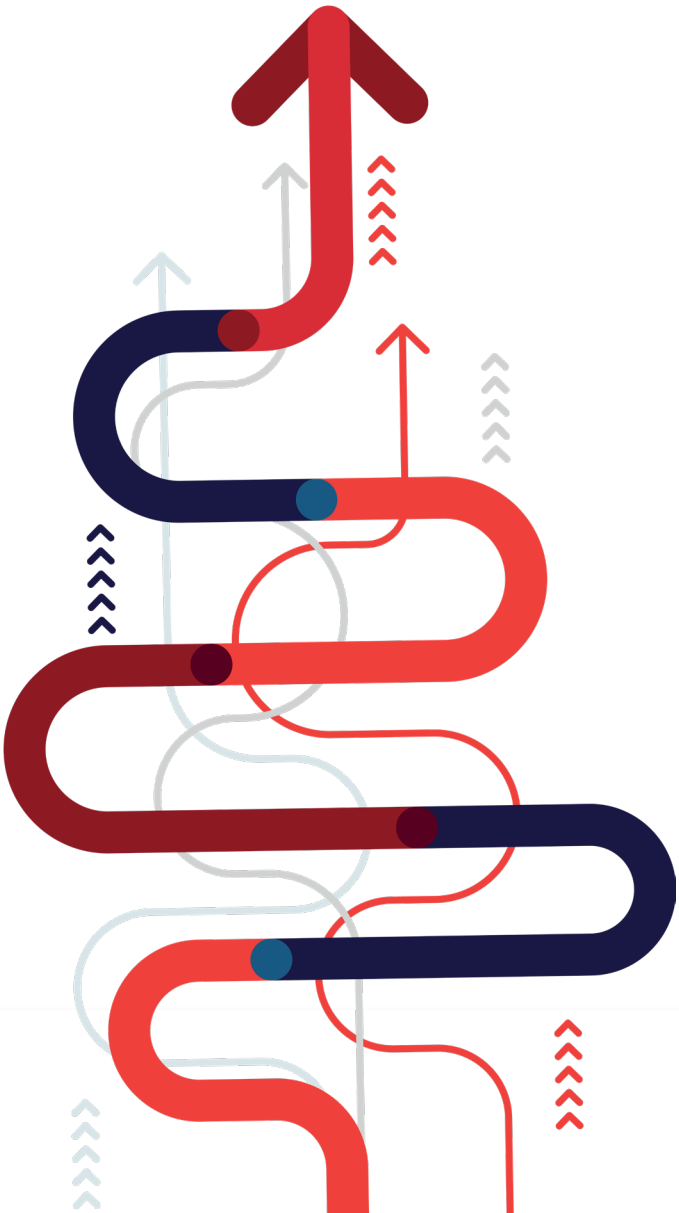
Diligent

Outlook 2023:

Navigating New Threats & Emerging Opportunities



For those overseeing governance, risk and compliance in today's world, there hasn't been one dull moment over the past year. If companies and their boards found themselves navigating a confluence of cyberthreats, geopolitical volatility and evolving technologies in 2022, what can they expect in 2023?

In one word: risk. To paraphrase the title of a popular 2022 movie, risk will be everywhere, all at once, in the new year. This means that ESG and compliance teams will need to expand their roles to include risk management. Audit teams will need to escalate new priorities, like macroeconomic risk and geopolitical uncertainty, in their day-to-day work. Finally, effective governance will require comprehensive visibility of risk, in all its facets, by the board and by management.

Here's a high-level overview, followed by deeper dives into governance, risk, audit, compliance and ESG.

Attack Surfaces Keep Expanding

In the digital realm, watch for even more complexity, uncertainty and intensity. Increasing interconnectedness across cloud environments, social media channels, open-source code and more are expanding companies' digital footprints and **criminals' attack surfaces**. Meanwhile, immersive technologies like augmented and virtual reality trigger even more risks, such as privacy issues, identity theft, data breaches and exposure to malware.

One common target: access credentials for external remote services, remote desktops and virtual private networks, with criminals and "hacktivists" becoming even more sophisticated in their tactics. All in all, the severity of these attacks is expected **to grow in 2023,** as is their impact.

Much of this risk extends not only to third parties but their vendors and partners as well.

> "Across sectors, fourth parties have been responsible for much recent disruption," KPMG states in its 2022 Risk Management Outlook. "In manufacturing, that might result from shipping failures. More broadly, it could be a security vulnerability at a supplier's cloud provider that results in a cyber incident."

Gartner predicts that by 2025, nearly half (45%) of organizations will have experienced attacks on their supply chains — a threefold increase from 2021.

Economic Volatility Meets Regulatory Scrutiny

Supply chain woes overall are continuing to trigger a chain reaction of trouble for the global economy. As the cost of producing and transporting goods and services continue to rise, consumer sentiment falls. And this lower spending, augmented by inflation, weakens prospects for the world economy.

"The International Monetary Fund (IMF) has cut its global growth forecast for 2023 as economic pressures collide from the war in Ukraine, high energy and food prices and sharply higher interest rates," Al Jazeera reported in October.

In this environment, organizations have much to prepare themselves for in the year ahead: financial and legal risks for the company, potential health and safety hazards for employees, operational impacts in areas like oil supply and prices, the list goes on. Meanwhile, proposed or recently enacted regulations, such as the EU's **Corporate Sustainability Reporting Directive** (CSRD), are about to become reality in areas like carbon disclosure, net zero, board diversity and human rights, making life even more interesting not only for boards but also for audit, compliance and ESG teams.

How can boards and leadership teams gain the visibility they need to navigate these evolving trends? How can they translate data into insight to mitigate risk and seize opportunities for growth?

Knowledge is power. Read on for a look at the year ahead.

Governance and Risk in 2023

What to Expect

If you're wondering whether you should expect more pressure from investors and proxy advisors about ESG oversight in the new year, the answer is "yes" — on many fronts.

Institutional Shareholder Services (ISS) surveyed the landscape in its **October 2022 Global Benchmark Policy Survey**. If their findings are an indicator of what's ahead, much will be expected from directors at both the board and the committee levels, with significant consequences for inaction.

For example: Did the company exclude climate risk considerations from its Critical Audit Matters? If so, 42% of investors believe this is a good reason not to re-elect members of the audit committee to the board.

Should individual directors be held accountable for climate change disclosures and risk management? Only a small percentage (17%) of investors say "no."

Finally, half of investors (50%) say it's a material governance failure if the company hasn't set realistic targets for Scope 1 and Scope 2 emissions through 2035, with opinions trailing not far behind for relevant Scope 3 emissions. A slightly smaller percentage (47%) would consider failure to strive toward net-zero emissions by 2050 to be a material governance failure.

Heightened pressure around climate action dovetails with proposed Securities and Exchange Commission (SEC) rules about **cybersecurity oversight**. These rules — likely to become law in 2023 — require periodic disclosures about:

- Policies and procedures to identify and manage cybersecurity risks
- Management's role in implementing cybersecurity policies and procedures
- Directors' cybersecurity expertise, or lack thereof

Boards will need to take their cyber savviness to the next level, particularly in terms of viewing cybersecurity as a business financial risk and understanding its potential material impact on business.

Geopolitical instability continues to be a governance issue in 2023, particularly with the need to oversee third-party and supply chain risk. If new trade sanctions or customer preferences affect a region or supplier, does the company have alternatives in place to pivot as necessary?

According to **Diligent's September 2022 reading of director confidence**, optimism in the boardroom has fallen in recent months, from 5.9 to 5.5 on a scale from 1 to 10. Directors' ratings of current business conditions have also declined, from 6.1 to 5.6. To put these figures into context, this rating was 5.2 amid the U.S. presidential election turmoil of 2020.

Finally, if **crypto and blockchain** aren't already on the board's radar, it's time to add them to the 2023 agenda (even in the wake of FTX's collapse). Companies are increasingly recognizing the potential of digital assets and blockchain digital assets (BCDAs) to increase global competitiveness — and are increasingly adopting these assets. Yet are they ready for the compliance obligations?

According to a **June 2022 report** by the Diligent Institute and SVDX, which educates boards in Silicon Valley, 74% of directors believe that the SEC and similar regulatory bodies will continue to materially tighten the regulation of cryptocurrency in the next 1–2 years. Yet directors rated their boards' understanding of BCDAs at only a 4 on a 10-point scale.

New digital products like cryptocurrency and blockchain will affect a company's risk profile. Boards and management will need to understand these new assets' potential impact and align governance with their overall strategy for risk, growth and the business, asking questions like:

- What's the predicted operational, financial and reputational risk?
- What controls, policies and processes are currently in place to tackle this exposure?
- Are other tools and technologies in the works for building resilience?
- Can risk management for this asset be integrated into the company's broader risk management strategy?

Dan Siciliano, Co-Founder of the Rock Center for Corporate Governance and Chair of the SVDX, likened the normalization of cryptocurrency and blockchain to the normalization of e-commerce in an end-of-year **Diligent podcast**. "Directors have an opportunity to get ahead of this before we 'drop the preface.' It's incumbent on management to brief the board on how these technologies might disrupt long-term strategy."

UNIVERSAL PROXY BALLOT'S IMPACT ON BOARDS AND INDIVIDUAL DIRECTORS

In November 2021, the SEC adopted new rules giving shareholders the ability to vote by proxy for their preferred combination of board candidates, similar to voting in person. The **Harvard Law School Forum on Corporate Governance** called the new rules "nothing less than the most dramatic change in the U.S. proxy system in a generation" and "proxy access on steroids."

Boards can expect a significant increase in proxy contests and threats, and individual board members should have their guard up as well.

"The new rules will potentially make all incumbent directors on a board more vulnerable for replacement, whether they are specifically identified as a targeted director by the activist or not," wrote proxy advisory services company Glass Lewis. "We also expect there to be a greater emphasis on evaluating the respective skills and qualifications of each individual company and dissident nominee, not only for those nominees who are pitted against each other, but also in terms of the board composition as a whole."

How the Board and Management Can Prepare

- ☐ **Be intentional and proactive about oversight related to cyber resilience:** potential financial exposure, the amount of exposure the organization takes across the extended global/digital supply chain and the resilience of the company's digital plans.
- ☐ **Align the company's budget and business strategy with cyber resilience,** to mitigate and minimize exposure to cyber risk.
- ☐ **Work together inside and outside of the boardroom** to give high-impact cyberthreats the attention and resources they require.
- ☐ **Increase collaboration with risk and governance teams,** to further align efforts as the company prepares for expanding threats and disclosure requirements.
- ☐ **Strengthen oversight over third parties and the global supply chain** with predictive risk analytics and AI for real-time monitoring.
- ☐ **Use technology tools like dashboards to give leaders on-demand visibility** into enterprise-wide risk, as well as risk related to ESG, audit and compliance.

Integrated Risk Management in 2023

What to Expect

Leaders will increasingly use risk-informed decision-making to make their companies more resilient. But they won't just be looking at risk in terms of threat prevention. As digital landscapes and business models evolve, they'll see **risk as a driver of business performance and value** as well. Forward-looking companies will embed integrated risk management (IRM) into their business strategy, so they can better understand the risks associated with new strategic initiatives and be able to pivot as necessary.

IRM plans will need to account for ESG as well. As companies tout **sustainability** in their mission statements, many lag in putting these statements into action. Meeting ESG goals while mitigating risk requires real-time data and visibility across the supply chain. Look for companies to use technologies like AI to address this challenge, particularly as CIO performance metrics become increasingly linked to the IT organization's sustainability.

Companies will also need to figure out how to manage **data privacy** across multiple jurisdictions. By the end of 2023, modern data privacy laws will cover the personal information of 75% of the world's population, according to **Gartner's cybersecurity predictions** for 2023–2025. As companies juggle GDPR, Brazil's General Personal Data Protection Act, California's Consumer Privacy Act and more, look for companies to explore technology solutions like automation and data privacy management systems.

Finally, there's continued supply chain turmoil to consider. According to a May 2022 **report by Accenture**, supply chain challenges arising from the COVID-19 pandemic and Russia's invasion of Ukraine could result in a potential €920 billion cumulative loss to gross domestic product (GDP) across the Eurozone — or 7.7% of GDP — by 2023. Companies will be looking for sophisticated solutions for managing these risks — and turning them into a strategic advantage.

When **Diligent and Censuswide** surveyed over 450 risk and compliance professionals in the United States in 2022, supply chain issues, cyberattacks and market volatility ranked high among their concerns. Survey respondents also cited evolving legislation and regulations (36%) and social responsibility issues (35%).

How Risk Management Teams Can Prepare

- ☐ **Prioritize a big-picture view:** Because of the multipronged effect climate change or third-party risk can have on a company's reputation, finances and beyond, leaders need real-time oversight of evolving patterns, so they can put strategies and playbooks into action when needed.
- ☐ **Make sure security controls and risk management solutions scale:** This will be essential as the risk landscape grows and becomes increasingly complex.
- ☐ **Prioritize and refine communication:** Diligent's recent 2022 Risk Survey indicated that less than a fifth (18%) of Risk & Compliance professionals are very confident in their ability to clearly communicate risk to the board. Good and clear lines of communication are imperative when it comes to succeeding in the battle against risks.
- ☐ **Leverage AI and ML:** With these technologies as part of a risk management solution, boards and management are better equipped to continuously monitor, predict, prevent and mitigate complex risks in a timely manner.
- ☐ **Build a sustainable security culture:** Do employees believe a cybersecurity threat could affect them personally, feel empowered to report suspicious behavior and feel responsible for acting to prevent cybersecurity threats? These are the hallmarks of a **robust security culture** where multifaceted security programs consider employees part of a strong line of defense.
- ☐ **Leverage the CISO's role to bolster decentralized cyber decision-making:** "Those in charge of security and risk management are at a turning point as a company's digital footprint grows, rendering centralized cybersecurity control useless," **Eden Data** reports in its cyber trends for 2023. A CISO enables companies to set centralized policies for cybersecurity executives dispersed throughout the organization.
- ☐ **Renew investments in supply chain resilience:** Successfully recovering from and adapting to supply chain disruptions will require real-time risk identification and mitigation and analysis into strategic risks and opportunities.

Audit and Risk in 2023

What to Expect

Audit's role in corporate governance has been evolving. Where once internal audit teams were strictly focused on finance and compliance, now boards and executive management expect them to help identify, prioritize, manage and mitigate interconnected risks across the organization.

In 2023, these risks will run the gamut: **geopolitical volatility, talent management, DEI, ESG, IT security and business continuity** amid large-scale operational and utility interruptions, to name a few.

The timeframe of such risk monitoring has been expanding as well. While companies still require a short-term view of imminent threats, they also need insight over the next 5–10 years into evolving challenges such as recession, war and supply chain issues.

But the day-to-day activities of many audit teams don't yet align with the latest developments in the risk landscape. To illustrate, audit teams polled by the Chartered Institute of Internal Auditors ranked **macroeconomic and geopolitical uncertainty** as a high risk priority, but they put the same area low on the list for time and effort.

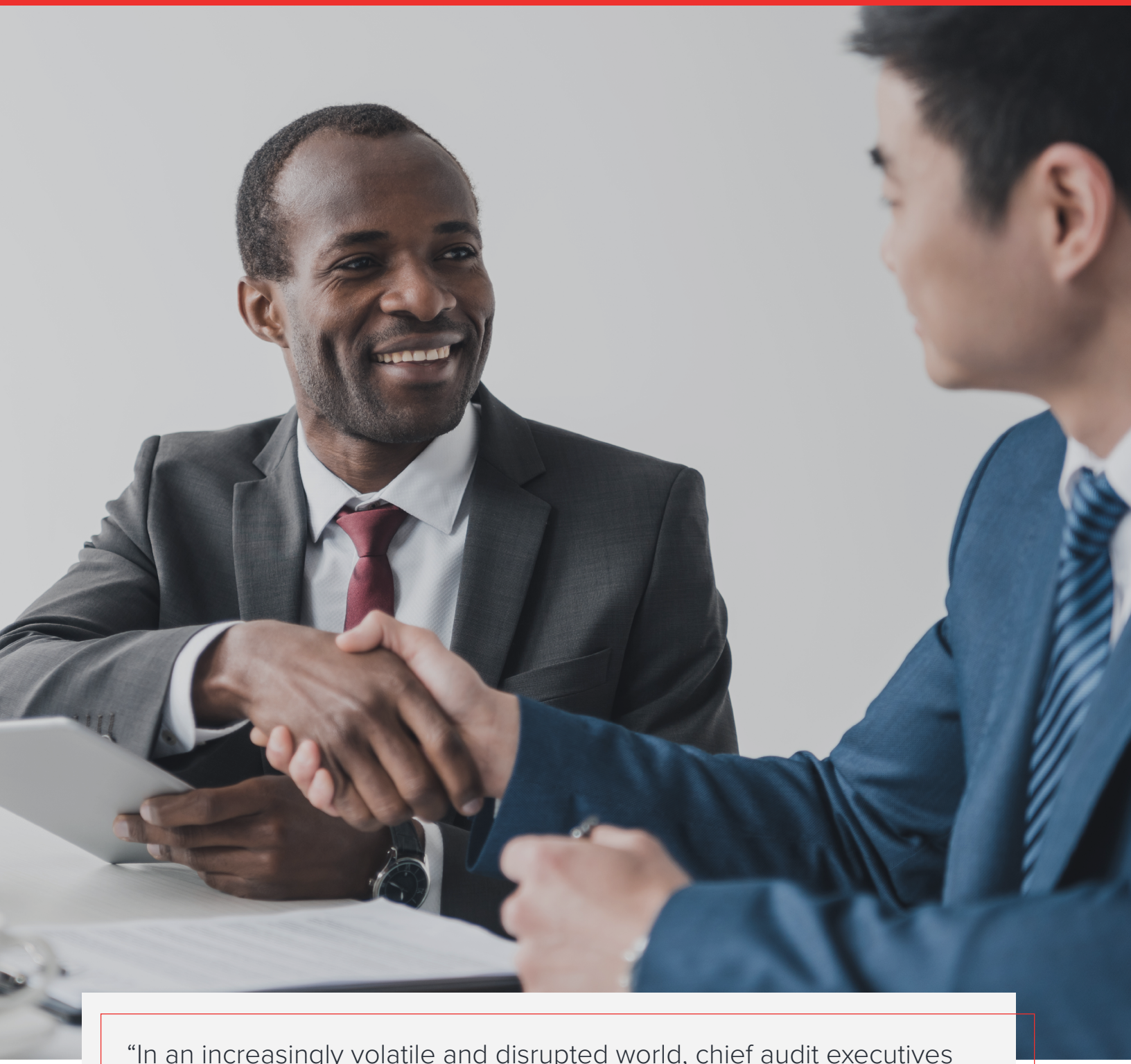
Bringing risks and audit activities into sync requires a reallocation of resources. Meanwhile, reacting quickly to disruptions and pivoting to changing demands requires agility. Here's where internal audit needs a fresh approach, with technology for automating tasks, analyzing data and presenting a three-dimensional snapshot to the board.

Audit teams are recognizing the transformation of their roles. According to the **Chartered Institute of Internal Auditors**, they've prioritized the following top five areas for the years ahead:

1. **Cybersecurity**
2. **Digital disruption**
3. **Business continuity**
4. **Environmental sustainability**
5. **Changing laws and regulations**

How Chief Audit Executives and Internal Audit Teams Can Prepare

- **Approach audit activities from a risk-driven perspective:** Focus your internal audit strategy on enterprise risk and use audit data and insights to drive integrated risk assurance across the organization.
- **Evolve the role of the Chief Audit Executive:** At and during board meetings, keep the Audit Committee regularly apprised on what's new and on what the company can do in areas like digital disruption and the ongoing talent war. In continuous monitoring efforts, partner more closely with compliance, risk and governance teams, to build stronger enterprise resilience. Finally, assume a key role in cyber resilience by using robust frameworks like the NIST Cyber Security Framework to assess the veracity of cyber controls.
- **Elevate and differentiate audit as a strategic partner:** Demonstrate your role's business value by predicting risks and opportunities before they materialize.
- **Get ready to audit ESG:** According to a 2021 survey, ESG and sustainability-related engagements currently make up **roughly 1% of internal audit plans**. Make your team the outlier and front-runner in this area. Evaluate the organization's ESG maturity, roles, responsibilities and goals. Make sure ESG policies and procedures are documented. Plan meaningful audits to identify gaps or material weaknesses in key controls, and work with legal and compliance teams to validate ESG reporting disclosures.
- **Help manage geopolitical issues:** Identify risk for the first and second lines and third-party suppliers, identify compliance gaps related to international sanctions, and keep an eye on developments related to financial strategy, including capital planning and management, net interest margins, credit/default risk, debt recovery, claims management and businesses cases for future investment.
- **Keep up with the audit committee's expectations: "Stand in the shoes of the audit chair"** to deliver what the board needs. Understand where internal and external stakeholders stand on key issues, assess and articulate the company's capacity to handle risks, and align audit with the company's broader strategic priorities.
- **Keep leadership apprised:** Elevate audit's role as a trusted advisor by delivering robust reports with insights around risk to the board, management and other key executives.



"In an increasingly volatile and disrupted world, chief audit executives and internal audit teams must remain agile in the context of a rapidly changing risk landscape."

Internal Audit in Focus FY23 by KPMG

Compliance in 2023

What to Expect

As regulations often respond to threats and vulnerabilities in the marketplace, risk is an inherent part of compliance. In the year ahead, compliance and risk will intersect even more as the regulatory landscape covers more areas, with greater complexity, making falling behind on reporting obligations a real possibility. Indeed, as reflected in Diligent's recent 2022 Risk Survey, regulatory compliance is a top risk for businesses in 2023, with 73% of risk professionals concerned about meeting demands.

Privacy and data protection are the big story for compliance officers in the new year. According to **Gartner**, changing government regulations through 2023 will require organizations to ensure the privacy rights of 5 billion citizens — a scope of more than 70% of the global gross domestic product (GDP).

In the United States, these regulations include the **Connecticut Data Privacy Act (CTDPA)**. Coming into effect on July 1, the CTDPA is the latest state privacy framework emerging in the absence of federal legislation, following in the footsteps of similar legislation in California, Colorado, Virginia and Utah.

But there are some marked nuances and differences. "Connecticut's privacy bill goes beyond existing state privacy laws by directly limiting the use of facial recognition technology, establishing default protections for adolescent data, and strengthening consumer choice, including through requiring recognition of many global opt-out signals," notes **Keir Lamont, senior counsel with the Future of Privacy Forum**.

BEYOND DATA PRIVACY, COMPLIANCE OFFICERS SHOULD KEEP THEIR EYE ON:

- **A heightened need to oversee third-party risk:** The German Supply Chain Act and EU Supply Chain Directive, for example, impose fines of up to €8 million, or 2% of the average annual turnover for companies making €400 million or more annually.
- **New regulations for corporate misconduct:** This includes "one of **the U.S. Department of Justice's** most elaborate overhauls of corporate enforcement in recent years, with greater credit to be given to companies that self-report, cooperate and remediate corporate wrongdoing."
- **More calls for ESG-related disclosures:** Investors and regulators want to see what companies are doing to fight modern slavery, greenwashing and human rights violations.

Compliance related to **cryptocurrency and other digital assets** is also expected to be a big challenge as regulatory requirements evolve and ambiguity around them remains. While more and more crypto compliance professionals expect compliance to be a rising priority — increasing from **53% to 86% from 2021** to 2022 — a full 20% of them don't yet have a policy.

One area to watch: regulations to prevent the use of digital assets for money laundering and terrorism financing. These "crypto travel rules" are in different stages of implementation, with some countries like the U.S. already having such rules in place and others, like the UK, expected to launch **them in 2023**.

How Compliance Teams Can Prepare

- ☐ **Equip your team to minimize regulatory risk:** Prioritize and stay ahead of regulatory requirements with a rigorous and structured risk assessment methodology, a centralized and data-driven approach to compliance, and tools like automation and AI to capture activities and deliver insights in a timely manner.
- ☐ **Take a holistic approach to ESG compliance:** With a strong foundation of technology, people, processes and data insights, you can manage and monitor ESG risks across the organization and meet external requirements for ESG disclosures.
- ☐ **Build your tech competence:** As digitization grows and the intersection between technology and regulatory requirements continues to increase, compliance leaders must get comfortable dealing with AI, machine learning, big data, cloud tech, cybersecurity, digital assets and more.
- ☐ **Have systems — and verifiable data — in place for monitoring and managing third-party risk:** Compliance plays an important role in supply chain management. Make sure your team has the technology and tools to stay ahead of evolving regulations and threats.
- ☐ **Diversify your skill sets:** As compliance increasingly involves complex areas like cybersecurity, climate change, supply chain threats, digital transformation, cryptocurrencies and more, you'll need to swiftly address any skills gaps.
- ☐ **Highlight the business value of compliance:** Limited resources and budget constraints have always been a major concern for compliance teams. In 2023, it's more important than ever for compliance leaders to highlight the business value of their work, so they can demand increased investments for automation, for recruiting the right talent, and for building, streaming and scaling the necessary infrastructure.

ESG and Risk in 2023

What to Expect

Sustainability leaders will continue to have much on their plate in the year ahead. As the **Russia-Ukraine war** spurs a turning point for ESG, with countries and companies shifting from Russian oil and gas to green energy solutions, the regulatory landscape will bring much to keep up with as well. **And the SEC's proposed rules for cybersecurity are just the beginning.** As CSRD becomes law, companies will need to start applying double materiality standards to their businesses' ESG impact. They'll need to be ready to comply with the European Sustainability Reporting Standards (ESRS) expected next summer and to obtain a third-party, certified audit of the information they report.

Keeping up — or failing to keep up — with all these evolving expectations and regulations poses a bigger risk than ever.

FOR THE **EU** IN **2023**

The European Securities and Markets Authority (ESMA) has gotten serious about disclosures and greenwashing, making sustainable finance a **top priority for 2023**.

ESMA's 2023 Annual Work Programme will focus on sustainable finance, technological change and data usage.

ESMA also plans to develop technical standards, guidelines and best practices related to new digital finance regulations, including the **Digital Operational Resilience Act (DORA)**, the **Regulation on Markets in Crypto-Assets (MiCA)** and the **DLT Pilot Regime**.

FOR THE **UK** IN **2023**

Look for ESG reporting to be further formalized through the **Sustainability Disclosure Requirements (SDRs)**, which incorporate the **UK Green Taxonomy** for verifying which activities can be considered "green." Also be prepared to meet the **Financial Conduct Authority's (FCA's) new requirements** to report information and disclose against targets on the representation of women and ethnic minorities on their boards and executive management.

FOR THE **EU** IN **2024**

Look for remaining technical standards for the **Sustainable Finance Disclosure Regulation (SFDR)** to be completed and for the European Commission's proposed **Corporate Sustainability Reporting Directive (CSRD)** to become the standard for reporting requirements.

FOR **ASIA-PACIFIC** IN **2023 AND BEYOND**

ESG regulations are increasing in prominence throughout the region. Beginning in FY 2023, reporting under the Singapore Exchange's TCFD-aligned climate disclosure rules will become mandatory for companies in the financial, agriculture, food and forest products, and energy industries, with companies in the materials and buildings and transportation industries facing mandatory guidelines in 2024. In Thailand, the government is setting new carbon neutrality and net-zero timelines, with a climate change bill set to become law in 2023.

> "Fewer than two-thirds of directors say their board understands the company's climate risk/strategy or the internal processes and controls around data collection. And just more than half (56%) think they understand the company's carbon emissions."
>
> **PwC Annual Corporate Directors Survey for 2022**

How Chief Sustainability Officers and Their Teams Can Prepare

- ☐ **Have a robust ESG reporting infrastructure in place:** This is essential for overcoming any discrepancies in ESG measurements and data quality. Make sure that you're capturing granular data, as well as the macro-level details across the various aspects of your ESG reporting, such as climate risk vulnerability and diversity.
- ☐ **Standardize decision-making processes:** When assessing your ESG reporting infrastructure and framework, verify that the ESG data is reliable, verifiable and follows applicable guidelines.
- ☐ **Refine your data management processes:** Diligent's recent 2022 Risk Survey indicated that the two biggest challenges that ESG teams face are the analysis and embedding of ESG data into the organization's overall risk strategy (42%) and the standardization and management of such data according to various ESG frameworks (40%). Establishing a clearer picture of how ESG connects to your organization's broader risk strategy is crucial.
- ☐ **Optimize the collection and mining of supplier data:** As supply chain risks become increasingly complex and the pressure intensifies for timely supply chain insights, you'll need reliable and verified data from your suppliers and vendors.
- ☐ **Join forces with your colleagues in risk, compliance and audit:** This collaboration strengthens the accuracy of ESG reporting, drives alignment of ESG with broader business strategies, and helps create a consistent narrative for investors and other stakeholders.
- ☐ **Link sustainability with business value:** Showing how sustainability contributes to the bottom line, increases stakeholder buy-in and strengthens the company's brand positioning and revenue.
- ☐ **Integrate ESG reporting into traditional financial reporting efforts:** Working closely with the CFO to assess, quantify and report on ESG impacts helps elevate the role of CSO within the organization and make ESG goals and benchmarks a company priority.
- ☐ **Support strategy and informed decision-making:** Use dashboards and reporting to provide executives and the board visibility into ESG progress and benchmarking.

A Complicated 2023 Calls for a More Comprehensive View

As companies move into 2023 and beyond, boards and other key decision-makers will need real-time visibility into all of these internal and external factors. Diligent can help:

- Make it easier to produce essential reporting and share best practices.
- Bring third-party data to the board and management in a more streamlined way, with less time and effort.
- Standardize and simplify the creation of custom reports.

Diligent makes internal and external points of view easily accessible within a familiar board solution. It operationalizes data from across the organization — ESG, risk, audit, IT management and more — and combines it with proprietary intelligence to give directors, committees and leadership teams a comprehensive view of the risk landscape, so they can lead effectively in 2023 and beyond.

IN 2023, BE READY FOR ANYTHING WITH DILIGENT

Diligent commissioned Forrester to conduct Total Economic Impact (TEI) studies of the potential return on investment (ROI) organizations might achieve when deploying our digital solutions for increased visibility, centralized workflows and more informed decision-making. **Learn about these TEI studies for Boards, ESG and Entities today.**

About Diligent

Diligent is the global leader in modern governance, providing SaaS solutions across governance, risk, compliance, audit and ESG. Serving more than 1 million users from over 25,000 customers around the world, we empower transformational leaders with software, insights and confidence to drive greater impact and lead with purpose. Learn more at diligent.com.

To learn more about Diligent Compliance solutions or to request a demo, contact us today:
Email: info@diligent.com | Call: +1 877 434 5443 | Visit: diligent.com