

THE WEAKEST LINK?

Why supply chain oversight is key to reducing risk



INSIDE THIS ISSUE

Assessing the risks and opportunities in ESG

By Global Head of CIO, Deutsche Bank

The route to cyber resilience

Understanding concentration risk in the supply chain

How agile is your firm?

Why adaptability holds the key to mitigating vendor risk

In step with sanctions

Keeping pace with geopolitical change

Best in class supplier oversight: how-to guide

By Global Head of Strategic Supplier Oversight, LGIM

Securing data across suppliers

Views from industry experts

CONTENTS

TPRM Edition

- 3 FOREWORD**
Resilience through agility and stability
Codee Woo, Legal and General Investment Management (LGIM)
- 4 THE BIG CONVERSATION**
ESG: Understanding the risks and seizing the opportunities
Markus Müller, Deutsche Bank
- 6 RISK FOCUS**
Third-party transformation: Cutting costs without increasing risk
Alpa Inamdar, AIG
- 8 SANCTIONS**
Keeping ahead of sanctions risk in a volatile climate
Scotiabank, Morgan Stanley, Atlantic Union Bank, State Street, Sayari & Kaufman Rossin
- 10 INFOGRAPHIC**
Counting the cost of the supply chain crisis
- 12 INDUSTRY INSIGHT**
Top 3 vendor risks for 2023 for US and European firms
Alice Kelly, CeFPro
- 13 EVENT PREVIEW**
Non-Financial & Operational Risk USA
- 14 RISK FOCUS**
5 steps to best-in-class supplier oversight
Shamial Afzal, Legal & General Investment Management (LGIM)
- 16 Q&A**
The route to cyber resilience
Cyril Korenbeusser, BNP Paribas
- 18 RISK FOCUS**
The power of next-gen enterprise cybersecurity architecture
Ashesh Kupur, Bank of Montreal
- 20 ADVERTORIAL**
The overlooked pillar of trust
Monocle
- 21 EVENT PREVIEW**
Fraud & Financial Crime Europe
- 23 TALKING HEADS**
What are the key considerations in ensuring data security across suppliers?
- 24 ADVERTORIAL**
Getting comfortable with your CECL results through challenger models
SS&C Technologies
- 25 ESG**
4 ESG myths demystified: Why controls are key to ESG reporting
AuditBoard
- 27 Q&A**
Remaining agile to mitigate third-party risk
Anit Banerjee, TPRM SME

Written by the industry, for the industry

The views and opinions expressed in this publication are those of the thought leader as an individual, and are not attributed to CeFPro or any particular organization.

Resilience through agility and stability



Codee Woo
Strategic Supplier Risk Manager
Global Strategic Supplier Oversight (GSSO)
Legal and General Investment Management (LGIM)

As a member of the new CeFPro Third-Party Risk Advisory Board, I would like to welcome you to the eighth edition of iNFRont magazine, which focuses on third-party risk management.

Risk professionals would have hoped for a calm start to the year following the volatility of 2022, caused by events such as the war in Ukraine and the LDI pensions crisis. Instead, 2023 kicked off with a dynamic risk landscape and the threat of operational disruption becoming our new normal.

Supply chain resiliency was tested by a global banking crisis which saw the collapse of Silicon Valley Bank (SVB) and Signature Bank, emergency aid from 11 US banks to First Republic, as well as the takeover of Credit Suisse by rival UBS and the takeover of SVB's UK arm by HSBC. These events highlight the importance and value of agile risk management to maintain stability and mitigate systemic risk on a global level. They also remind us how threat actors seek to take advantage of such situations.

This edition sheds light on managing cyber security, data security, and cloud risks. Key risk indicators and associated thresholds support monitoring and mitigation of threats to financial stability, supplier performance, and control environment. They also influence the decision to mobilize business continuity or exit plans.

At CeFPro's Vendor & Third-Party Risk Europe conference last November, our Global Strategic Supplier Oversight team presented on how we have enhanced and embedded third-party risk culture in LGIM. This involved targeted training and awareness sessions and designing processes that create a positive user experience, to help third-party risk be better understood, received, and followed.

Sharing knowledge and insights within the non-financial risk community is highly valuable. CeFPro's recent Operational Risk Europe summit provided thought leadership on interpreting key regulations such as the Digital Operational Resilience Act (DORA) and Consumer Duty Act. With support from the Third-Party Risk Advisory Board, CeFPro has also launched its global survey on Third-Party Risk Management: Benchmarking the Industry and Building Resilient TPRM Teams. Your contribution to the survey will help inform the industry on best practice and provide an aide to decision making, so make sure your voice is heard. You can take part or download the report at www.cefpro.com/tprm/.

The third-party risk agenda is not only important for individual risk professionals and firms; it requires collective action from all business stakeholders within an institution, as well as industry collaboration, to protect the financial ecosystem.

We hope you enjoy this issue of iNFRont and find it useful. Please get in touch if you would like to feature in a future issue or join CeFPro's Third-Party Risk Advisory Board.

OUR MAGAZINE TEAM...

We welcome contributions. If you or your organization are interested in featuring in our next issue, please contact infront@cefpro.com

ADVERTISING & BUSINESS DEVELOPMENT

If you are interested in sponsorship and advertising opportunities, please contact: sales@cefpro.com

PUBLISHER

Alice Kelly
alice.kelly@cefpro.com

EDITORIAL ASSISTANT AND OUTREACH MANAGER

Ellie Dowsett
ellie.dowsett@cefpro.com

MANAGING EDITOR

Kate O'Reilly
infront@cefpro.com

HEAD OF DESIGN

Natasha Marino

www.cefpro.com

ESG: UNDERSTANDING THE RISKS AND SEIZING THE OPPORTUNITIES



Markus Müller
*Chief Investment Officer
ESG & Global Head of Chief
Investment Office*
Deutsche Bank

What is the importance of ESG within financial markets?

ESG is an overarching concept that broadens the horizon for economic decision-making processes and, as such, has become an increasingly important area within financial markets. A focus on ESG can help investors and financial institutions to better manage the economic risks associated with issues such as climate change, the loss of biodiversity, and the pollution of oceans, including:

- **Physical risk:** for example, if food production is affected by droughts and crop failures.
- **Transition risk:** such as being left behind in the competition for sustainable transformation.
- **Liability risk:** unexpected legal costs; for example, because a company has polluted a river.
- **Contagion risk:** such as issues in the supply chain.

ESG provides a framework to help investors know, understand, and ultimately quantify these risks, creating long-term value for investors. From a portfolio perspective, the ability of firms with ESG strategies to navigate a difficult environment may be valuable. Conversely, investing in firms without a coherent ESG strategy may result in a bumpy ride. Chopping and changing investments to replace non-performers will have cost implications for a portfolio, not least because 'market timing' mistakes in entering or exiting investments can be expensive.

ESG also offers opportunities for investors. In 58% of company studies on operational metrics such as ROE, ROA, or share price, there is a positive correlation between ESG and financial performance; 13% show neutral effects; 21% mixed results; and only 8%

demonstrate a negative correlation. The improvement in financial performance due to ESG becomes more evident over time. Corporate sustainability programs seem to improve financial performance due to mediating variables like better risk management and increased innovation.

ESG also paves the way for new markets and business models by helping firms to identify and then replace problematic economic activities, not just on the investment side, but also the financing side – after all, companies need money for sustainable transformation. In this area, there have been financial products under development for several years already and we can safely assume that demand for these will only increase with the transformation of our economy.

How is climate change affecting supply chains?

Extreme weather events, such as droughts, floods, and hurricanes are disrupting production and transportation, resulting in increased costs, stockouts, and delays. In addition, ports, rail lines, highways, and other transportation and supply infrastructure will be threatened by increases in sea levels of between an estimated two to six feet – perhaps more – by the year 2100. Around 90% of the world's freight moves by ship, and, according to Becker, inundations will eventually threaten most of the world's 2,738 coastal ports, whose wharves generally lie between just a few feet to 15 feet above sea level.

Research shows that raising 221 of the world's most active seaports by just two meters (6.5 feet) would

require 436 million cubic meters of construction materials, an amount large enough to create global shortages of some commodities. The estimated amount of cement alone – 49 million metric tons – would cost \$60 billion today.

Moreover, higher temperatures and changing weather patterns are also affecting crop yields, livestock productivity, and fisheries, threatening food security and increasing the price volatility of agricultural commodities. The WEF risk report found that six out of ten global risks, ranked by their short- and long-term severity, are related to the environment.

At the same time, there are indirect consequences for supply chains caused by climate change. Evolving consumer preferences and regulations are increasing demand for sustainable and low-carbon products, creating opportunities for companies that can adapt their supply chains accordingly. As such, businesses must proactively manage climate risks and opportunities in their supply chains to ensure resilience and long-term success. For those reasons, investors as well as companies are increasingly diving into CO2 exposure of their value chains, considering not just their own CO2 emissions but also those of their whole supply chain.

How relevant is ESG to the socio-economic system?

Firstly, it is imperative to acknowledge that the transformation of our current economic model towards sustainability is crucial – it is time to shift away from tradition and implement a nature-compliant approach. However, it is important to also recognize that over six billion



people are currently living in emerging markets and developing economies, striving for prosperity. These countries require substantial energy resources to achieve their goals, but their residents are also grappling with changes in incorporating sustainability into their daily lives. For instance, prices for sustainable products and services are increasing, leading to so-called 'greenflation'. Therefore, when developing a nature-compliant economic model, social aspects must also be considered.

ESG creates a link between ecology, society, and corporate economic governance, thereby connecting it to the financial world. By embracing ESG principles, we can pave the way towards a more sustainable and inclusive economic model that creates value for society, the environment, and businesses alike.

ESG is key to the socio-economic system in several ways:

- **Risk management:** ESG factors can have significant impacts on companies and their stakeholders. By integrating ESG considerations into decision-making processes, companies can better manage ESG risks and mitigate negative impacts.
- **Innovation and growth:** Companies that adopt sustainable and responsible practices can create new business opportunities and competitive advantages. This can lead to innovation and growth, which can benefit both the company and the broader socio-economic system.
- **Stakeholder engagement:** ESG considerations can help to build trust and credibility among stakeholders, including customers,

investors, and community groups. This can lead to stronger relationships and partnerships, which can contribute to the long-term sustainability of the socio-economic system.

- **Regulatory compliance:** ESG considerations are increasingly becoming a part of global regulatory frameworks. Companies that integrate ESG factors into their operations and decision-making processes can better comply with these regulations and avoid potential legal and reputational risks.
- **Social and environmental impact:** ESG factors can have significant social and environmental impacts, both positive and negative. Companies that prioritize ESG considerations can contribute to positive social and environmental outcomes, such as reducing greenhouse gas emissions, promoting social inclusions, and supporting legal communities.

How can financial institutions effectively manage the impacts of ESG requirements?

From our annual CIO ESG client survey, 75% of our clients expect their financial institution to be able to adequately protect their portfolio against natural risks. In addition, 61% of our clients say that their financial institution should provide them with the relevant expertise and solutions to successfully navigate the transformation.

Financial institutions may therefore face a double challenge. Firstly, they need to demonstrate their relevance and ability to 'align all financial flows to support the conservation and sustainable use of biodiversity' (as agreed in the Convention of Biological Diversity in 2021). And they also need to develop expertise and skills to measure and manage risks within portfolios. This must be supported by establishing a thorough and practical analytical framework and using it (with the support of central banks and regulators) to develop more comprehensive risk assessment tools and increased management oversight. This is a difficult task at a time of rapid economic and investment change, but an essential one.

Financial institutions can also help their business clients to better understand both the risks and the opportunities around ESG. For example, our survey found that almost 48% of business clients see the upcoming data and disclosure requirements as an opportunity. At the same time, 56% cannot say that biodiversity loss is considered in their company's sustainability/ESG strategy.

What is certain is that ESG will become a core part of financial institutions' activities. This is likely to be reflected in the relevant frameworks, policies, and organizational structures.

Delve into climate risk challenges and opportunities at our upcoming Climate Risk USA, October 4-5 in NYC. For full information visit www.cefpro.com/climate-risk-usa

THIRD-PARTY TRANSFORMATION: CUTTING COSTS WITHOUT INCREASING RISK



Alpa Inamdar
Transformation Leader
AIG

Over the last few months, there has been a trend among organizations of all types – financial services, manufacturing, technology companies, and more – of reducing headcount. Most mornings we awake to a press release or headline announcing that a significant number of people have been laid off. As a result, companies have less human capital and are being forced to rely more and more on technology and transformation, especially in the areas of procurement and third-party governance. With cost efficiencies driving so many organizations to downsize, the challenge is how to avoid inviting greater risk in exchange for cost savings. Organizations must therefore look at ways to drive

efficiencies and innovation in how they manage their third-party governance. Against this backdrop, it is important to understand the risk perspective and broader vendor ecosystem. Reviewing the whole ecosystem and understanding how best to manage it is a major challenge; when there is a layoff, there is a risk, so it is vital to understand the ripple effect. In the case of third-party governance, one risk is the loss of expertise. If you reduce the team by any percentage, workload typically increases for the remaining employees. It is imperative to balance this risk, as there is a likelihood for errors to increase with a heightened workload.

The impact of staffing cuts

From a vendor and third-party governance perspective, in the event of limited resources, shortcuts may be taken when completing risk assessments, due diligence, or on-site assessments. With limited bandwidth, if annual, bi-annual, or on-site assessments are not conducted effectively, additional risk is introduced. When teams are reduced, organizations may consolidate expertise across functions. Within the third-party governance example, this can impact direct contact with vendors – for instance, where one person was in direct contact with vendors on a daily, weekly, or monthly

basis, that connection and relationship may now be lost. Where individuals may have focused within a single silo or workstream function, they may now have a much broader purview covering multiple tasks.

Similarly, relationship managers may not be able to interact with vendors in a timely manner, instead relying on emails with limited follow-ups and potentially impacting the quality of the assessment. This in turn impacts documentation and ultimately audit, with diminishing communication and documentation trails.

Harnessing the power of technology

To combat this, organizations are leveraging the power of technology, investing in infrastructure to aid in managing risk, such as AI tools to support the review of the vendor ecosystem and risks across the supply chain. Other options include search engines that review information coming through social media, publications, press releases, etc. to flag any changes to vendors that require attention. Investing in continuous monitoring can help organizations to balance the cost challenges whilst managing risk effectively. Location and geographical monitoring can enhance governance over outsourced teams and may well reduce assessment costs.



Another approach is to rely on remaining team members to cover expanded workloads. However, this brings inherent risk. Take the area of cybersecurity as an example. This is an increasing concern, with recent case studies highlighting the challenges that reduced headcount and limited investment in infrastructure can bring. Oversight and monitoring of key areas such as IP addresses, phishing scams, training, etc. have been impacted as a direct result of fewer resources. Training budgets for IT teams have been reduced at the same time as hackers' tactics are becoming more sophisticated, and online training may not be enough to stay ahead. Organizations must consider these domino effects when determining the process for downsizing teams.

The ripple effect

Third-party governance does not operate in isolation; it is essential to day-to-day business, in particular those operations classified as 'critical'. Headcount reductions in procurement and third-party teams could have a fundamental impact on day-to-day functions, which in turn brings a risk implication and possible revenue impact. For example, the vendor may previously have had a dedicated team or function to support issues and escalations, but now no longer has a specific contact in place. The

ripple or domino effect can be seen at many levels – from the CRO not having a full view of the risk landscape; to how the risk is being managed across risk assessments, due diligence, surveys, and processes; to monitoring the overall health of vendors. There may also be legal or compliance implications as the contractual language may not have been updated to reflect any new contacts.

Another risk factor is that of media reports highlighting potential weaknesses to threat actors. As mentioned above, there has been an influx of press releases and statements of late around layoffs and reduction of teams, which could well serve those looking to exploit vulnerabilities, particularly if specific details as to where those cuts have occurred is revealed. One international bank recently announced they are hiring significant numbers of regulatory staff to address this increased risk.

Maintaining standards with outsourced teams

With the ever-increasing use of outsourced services to manage cost constraints, many firms do not offer 24/7 services as a result of different time zones, which brings increased risk around incident response. As organizations continue to outsource, they also continue to invite additional risk that must be managed alongside any cost-efficiency objectives. It is therefore imperative to carry out risk assessments to ensure high standards are being maintained, even with reduced in-house teams.

During Covid, supply chain risks were heightened, as was third-party governance and reliance on third parties. Organizations increased their headcount to manage these supply chain issues, but now, firms are looking to downsize. However, those disruptions and issues are still present. Organizations therefore need to learn to manage these continued risks while balancing the pressure to reduce their costs.

**CeFPro hosts a number of events focusing on third party risk management within financial services and across sectors. Visit www.cefpro.com/forthcoming-events for all information towards our upcoming events: Vendor & Third Party Risk USA, June 7-8, NYC
Vendor & Third Party Risk Europe, June 15-16, London
TPRM & Supply Chain Risk: Cross Sector, November 7-8, Nashville**



KEEPING AHEAD OF SANCTIONS RISK IN A VOLATILE CLIMATE



Andrew Jensen
Managing Director and
Global Head, Global
Sanctions & Screening
(GSS), Scotiabank



Julianne Susman
Executive Director and
Counsel, Global Financial
Crimes Legal
Morgan Stanley



Hunter Kreger
VP, FIU Deputy
OFAC Officer
Atlantic Union Bank



Erika Alders
Managing Director and
Managing Counsel, Head
of U.S. Regulatory Legal
State Street

The recent actions of Russia in regard to Ukraine have been met with unprecedented disapproval from nations across the globe. This has subsequently resulted in Russia receiving some of the most comprehensive sanctions ever levied against a nation. Sanctions have become the alternative to direct military intervention, and regimes have been evolving quickly in a rapidly changing environment. With the scope and complexity of sanctions regulation also increasing, multinational businesses are advised to regularly assess the regulatory standards to establish whether any sanctions are applicable to the business they intend to carry out.

At CeFPro's recent Fraud & Financial Crime USA Summit, an expert panel discussed the ever-evolving sanctions landscape and staying ahead of changes as volatility and uncertainty remain. Below are some of the key points discussed during the panel and key takeaways from the speakers...

The one-year anniversary of Russia's invasion of Ukraine occurred recently. How have sanctions requirements and expectations changed relative to, say, volumes, types, transactions, jurisdictions, and so forth?

Andrew Jensen: The control framework has largely stayed the same. The big change came back in 2014 with the introduction of sectoral sanctions and the addition of things like security screening. As a result, many of us were primed to deal with the Russian invasion of Ukraine from a broader control framework perspective.

What we weren't prepared for were the volumes, with vast backlogs of payments as a result of the analysis required to identify whether something was sanctioned. This was an incredibly complicated time with a lot of the burden being placed on customers who were trying to exit Russia and ensure their assets weren't compromised. With all of this in mind, I have a lot of confidence that the framework was working as intended. The proper controls were in place, it was just the volumes that made it far more complicated.

We can see an alliance developing between Russia and China. What are some of the lessons learned from the sanctions on Russia in 2022 and how might they help prepare for potential sanctions on China?

Julianne Susman: I should start by saying that Russia and China are like apples and oranges. The importance of China's economy is several magnitudes greater to the global economy. Therefore, I would not expect OFAC or other regulators to take exactly the same approach as they did with Russia.

One of the many lessons learned over the past year is that no entity or person is too big to sanction – few of us could have predicted that OFAC would come right out with such a broad spectrum of sanctions against Russia, including the major Russian banks. So, when we're preparing for sanctions on China, it's important to look not only at those companies that have already been designated as being part of the Chinese military industrial complex, but also at large, state-owned entities, the big banks, even the central bank, to get a holistic picture of sanctions risk.

We also learned that resource constraints can happen fast when sanctions hit with the speed and the scope that they did with Russia. If that were to be repeated with China, it really would be all hands on deck, so maybe now is the time to invest in some additional training.

A final lesson learned with Russia is that local countermeasures can and will complicate things. As firms struggled to comply with US, EU, and UK sanctions, Russia quickly issued its own countermeasures against so-called unfriendly nations, which restricted the movement of assets in and out of the country. While this was largely a business concern, it does also create potential conflict of law issues – this could affect companies with operations in China, if they were to impose similar measures. It's therefore important from a governance and escalation perspective to consider how your firm would handle potential conflict of law issues.

What lessons can be learned from the rapid changes to the sanctions environment during 2022, and what tools are available to help financial institutions prepare should a similar change occur in the future?

Hunter Kreger: One lesson learned from 2022 is that financial institutions have three options when it comes to keeping up with alerts generated due to rapid changes to the sanctions environment, and they should have a plan in place to be prepared for similar events in the future. Financial institutions can either leverage technology solutions, increase headcount, or reallocate existing staff. While reallocating staff or hiring new talent is sufficient, it is not necessarily efficient, and causes work/life balance

issues. In terms of technology there are a few different artificial intelligence (AI) and machine based learning (ML) solutions available in the marketplace that can perform level one reviews within your existing transaction monitoring system and dramatically reduce the volume of false positives that are closed by staff. These solutions are scalable in the event of sudden changes in the sanctions environment and are customizable based on the risk tolerance of the financial institution.

What are the biggest challenges you've encountered when working with clients exposed to Russia sanctions?

Erika Alders: We have to consider sanctions imposed by many jurisdictions, including the US, EU, UK, Australia, Singapore, Japan, Canada, and others. These sanctions and positions, while moving in a similar general direction, are not precisely the same. Different jurisdictions might have different sanctioned entities or categories of business, for example, so we always need to be aware of the overlap.

As a US entity, we will be subject to US sanctions, but some clients may not be subject to US sanctions independently. Thoughtful conversations discussing the intersection between US sanctions, regulatory expectations, and your own company's risk profile may be especially necessary when working with non-US clients.

My first piece of advice is to make friends with your lawyers. We're here to help, but firms need to have in place a robust training program so that everybody can be a financial crime professional. Governance procedures should also be implemented to escalate any risk up the chain for proper analysis.

Given the dynamic nature of sanctions requirements and expectations, how can financial institutions manage the cost of sanctions compliance while meeting regulatory expectations?

Andrew Jensen: Sanctions screening typically is conducted in real time, so managing the rapid regulatory developments in the current geopolitical environment can be quite challenging. Nevertheless, it is also an opportunity to demonstrate the value

that a well-established sanctions program can bring to an organization.

While adding resources may be one option to meet new regulatory demands, cross training existing resources in multiple risk areas is another option. If adding additional resources is unavoidable, we want to challenge the conventional perception of sanctions teams as just another compliance cost center. The sole purpose of the function is to avoid massive fines or penalties for not meeting obligations and so we see it as an asset that maintains the value of an organization.

How can financial institutions leverage sanctions, due diligence and their transaction monitoring systems to better position themselves to be prepared for future potential Russia events resulting in a rapid escalation or implementation of a sanctions program?

Hunter Kreger: Sanctions due diligence is incredibly important and must be treated as such. It should be upfront, ongoing, and provide you with tools, along with your sanctions and country risks assessments, to identify connections and risks across countries. This, in addition to de-siloing FIU and BSA teams, allows for more coordination and preparation. It is also imperative to collect data upfront to leverage the transaction monitoring system to identify potential sanctions evasions. If a customer formerly had frequent payments to Russia, and has since changed their payment destination, this could be a red flag. Collecting data can put organizations in a better position to be prepared for future changes.

"With the restrictions published by the Treasury's Office of Foreign Assets Control, the Department of State's Directorate of Defence Trade Controls, and the Department of Commerce's Bureau of Industry and Security, the stakes have never been higher."

Bryant Moravek, Director of AML & Sanctions Compliance, Risk Advisory Services, Kaufman Rossin

Fraud & Financial Crime, London, September 20-21 addresses key challenges within the Fraud & Financial Crime landscape. Providing a holistic oversight and delving into individual streams to divide fraud and financial crime. Visit www.cefpro.com/fraud-europe

Counting the cost of the supply chain crisis

Key figures around the impact of supply chain disruptions on global organizations

The global pandemic triggered an onslaught of supply chain disruptions and challenges. With countries effectively shutting down, supplies of basic goods and services were severely impacted. As we emerged from lockdowns, global supply chains were further rocked by the Russian invasion of Ukraine. This in turn had significant impacts on organizations globally and resulted in many paying more attention to their outsourcing activities. Organizations are now moving to restore resilience to their supply chains and begin implementing more sustainable networks. Many have had to pivot their business models to survive in a changing climate, adapting their outsourcing behaviors to accommodate onshore products and moving offerings in-house where possible. Global supply chains face extensive recovery across a range of sectors; the impacts of recent tensions and upheaval will affect activities for years to come...

FACTORS CONSIDERED MOST LIKELY TO IMPACT SUPPLY CHAINS IN THE NEXT FIVE YEARS

Source: [The Economist](#)



51%

Of suppliers are expected to be reshored or nearshored on average in the next three years
 Source: Interos Resilience survey

\$182M

The average annual cost to an organization of supply chain disruption
 Source: Interos Resilience survey

50%

Of companies lack end-to-end supply chain visibility
 Source: Opentext

83%

Of businesses demand that supply chains enhance the customer experience as a component of their digital business strategy
 Source: Gartner

\$20b

By 2023, the market for AI in supply chains is expected to reach USD 20 billion and grow 20.5% annually
 Source: McKinsey

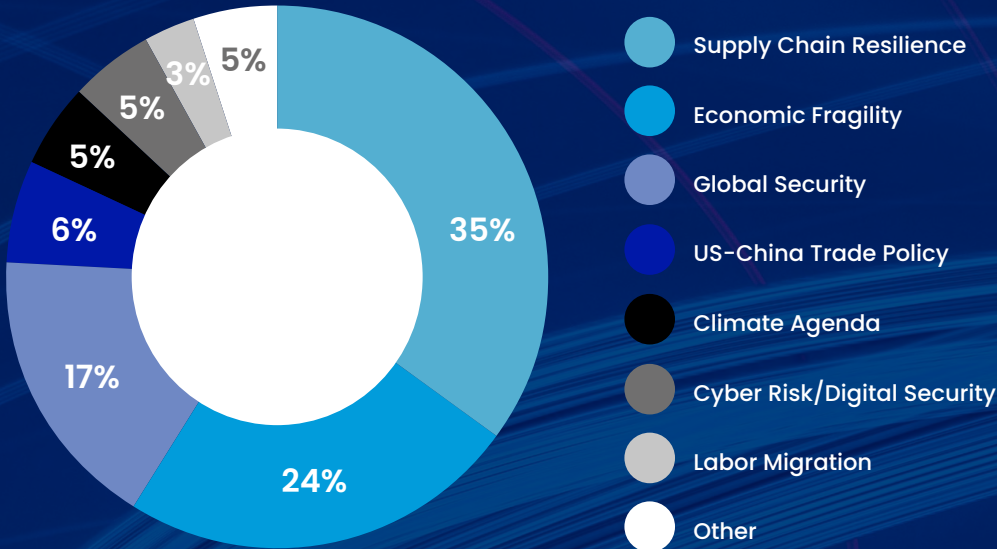
AVERAGE COST TO ORGANIZATION IN \$ MILLIONS

Source: Interos resilience survey



MOST PRESSING CHALLENGES

Source: IHS Markit



Market Intelligence Report:
 Global Third Party Risk Management: Benchmarking & Develop Resilience
 200+ industry responses & backed by CeFPro's Third Party Risk Advisory Board.
 Click [here](#) to download the report or visit www.cefpro.com/tprm

TOP 3 VENDOR RISKS FOR 2023 FOR US AND EUROPEAN FIRMS

Alice Kelly
Head of Content & Production
CeFPro



As the industry continues the trend of heightened reliance on outsourcing, risks of disruption to critical business services remain on the rise. Vendor and third-party risks permeate all organizations and industries, opening up firms to issues beyond the direct control of the traditional risk scope. To better understand the challenges at hand, CeFPro has conducted research annually into the key vendor and third-party risk challenges faced within financial services, with a primary focus on North America and Europe. Over the course of this research, the landscape has changed significantly; regulations globally continue to evolve, and technology is advancing to better monitor and manage risks. Here, we look at the shifting third-party risk landscape on both sides of the Atlantic and uncover the top three vendor-related challenges facing organizations today...

Understanding context: US and European approaches to date

Historically, our US research has revealed an industry that is more advanced and better equipped to manage the risks associated with suppliers. With multiple large-scale case studies, regulators have enforced stringent requirements to get a full grasp of the supplier landscape. This is continuing to evolve with oversight now reaching beyond third parties and interacting with numerous privacy and security requirements. However, we are now starting to observe UK and EU-based teams also developing strong practices and implementing greater oversight of their supply chains.

Historically, much of the research in both geographies has been focused around understanding the ecosystem and identifying vendors and third parties. The discussions have since escalated towards a greater understanding of supply chains more broadly, with a focus on fourth and nth parties, to better understand the risks. As technology has advanced, much attention has been paid to effective management and oversight of cloud providers, including how to manage concentration risks given the limited supplier options. Alongside this technology evolution has come the treatment of fintechs as a third party and their position within the scope of a third-party risk management framework.

#1: Exit planning

For 2023, the focus turns firmly towards exit planning and stressed scenarios. With such global turmoil over the last three years, stability and resilience are key priorities. Covid-19 shook the industry and continues to have repercussions on supply chains today, from both a supplier and a geographical perspective. Many locations are still suffering from the fallout of the pandemic – continued lockdowns in some regions are impacting ability to deliver services.

Geopolitical tensions continue to rock the industry and the war in Ukraine is having a lasting impact on organizations worldwide. As a result, exit planning has risen in importance for both US and European firms. Companies are developing programs to enable them to update their exit plan tests,

with a particular focus on stressed exits. With the trend of prioritizing material and high-risk third parties continuing, managing the practicalities of running exit tests is an area that sits front and center in 2023.

Understanding supply chain vulnerabilities and testing plans for an orderly exit are critical in the current environment of uncertainty. Changes in the landscape globally have also increased the importance of understanding aspects such as the financial stability of vendors. Financial health risks rise with uncertainty, so ensuring that organizations understand the finances and stability of each supplier is critical. Tying into exit planning, it is also vital to understand where the tipping point may be when a supplier is deemed too risky and a move to exit is decided.

#2: Cyber

Another area maintaining its prominence across both geographies in 2023 is cyber risk. Cybersecurity is a key consideration in ensuring that data is protected internally and across vendors and represents an area where understanding supply chains end to end becomes increasingly important. Understanding the full chain and every data touchpoint within it allows for increased scrutiny and monitoring across vendors, requiring access to data as well as firewalls and systems. A timeless case study remains the Target breach, where a seemingly safe HVAC vendor enabled an infiltration of Target's firewall. Cybersecurity applies not just to critical third parties, but all aspects of the supply chain.

#3: ESG

The final area driving engagement across both geographies in 2023 is ESG. Regulators on both sides of the Atlantic are reviewing considerations from a third-party perspective and implementing new requirements.

ESG is quickly becoming a minefield, with many organizations and jurisdictions politicizing the topic. Much attention is being paid to reducing companies' carbon footprints, with many making substantial pledges. Supply chains play into an organization's direct footprint and therefore must be considered. However, understanding carbon footprint and its practical measurement and quantification remain a challenge; with service-driven supply chains, quantifying an intangible is problematic. Engaging third parties in ESG requirements is also an

important consideration. If a supplier does not conform to an organization's requirements, what is the future of that relationship? The industry must therefore find ways to engage third parties to drive a sustainable agenda, not just from a climate or environmental perspective, but also regarding issues that have been at the fore for many years, including social and ethical aspects such as human trafficking and modern slavery in supply chains. Predominantly associated with more tangible or product driven industries, the ethical actions of an organization's supply chain can have untold ramifications to its reputation.



As part of our research, CeFPro collates detailed agendas to share insight and knowledge with industry experts in both geographies. The results of these can be found at www.cefpro.com

CeFPro® Events

NON-FINANCIAL & OPERATIONAL RISK USA

8th Annual | Oct 4-5, 2023



Developing best practices to mitigate non-financial & operational risks in an ever-changing financial landscape

Featuring insight from leading industry figures including:

Amy Butler
Chief Risk Officer
Legal and General

Madiha Fatima
Executive Director
Operational &
Outsourcing Risk
J.P. Morgan

Sabeena Liconte
Chief of Compliance
ICBC

Michael Steinhofel
Director, Operational
Risk Management
Barclays

Zhi Chung
Director, Non-Financial
Risk Management
Credit Suisse

Philip Masquelette
Chief Risk Officer
Ulster Savings Bank

NEW for 2023: Interactive cyber security work stream

This new break out allows for increased engagement and interaction with the session leaders, featuring insight on key topics including:

Vendor Security - Managing cyber risks across supply chains.

Cloud - Monitoring security controls with cloud providers.

Technology - Reviewing the regulations around AI and machine learning.

Key topics include:

REGULATION
Managing disparities in an ever-changing landscape.

CLOUD
Monitoring security controls with cloud providers.

RSCA
Leveraging benefits and developing tangible outcomes.

RESILIENCE
Capturing risks with an overarching framework.

For more information visit:
www.cefpro.com/oprisk-usa

5 STEPS TO BEST-IN-CLASS SUPPLIER OVERSIGHT



Shamial Afzal
Global Head of Strategic Supplier Oversight
Legal & General Investment Management (LGIM)

We interviewed Shamial Afzal to discuss his journey towards implementing an effective third-party risk management framework within LGIM. Here are his five steps to achieving best in class supplier oversight...

Step 1: Understand the environment and supply chain

Having worked for various firms, my first step was to understand the organization by immersing myself in the new LGIM environment. This included looking at the supply chain to explore material relationships, critical services provided, and how they are managed, plus familiarize myself with the appropriate contacts. I then delved deeper into the oversight processes and supplier risk profile of relationships, before starting to map out the supply chain.

My next task was to conduct a desktop gap analysis against policies within the organization, as well as against regulation with upcoming changes. This identified areas to prioritize as a firm, and within our Global Chief Operating Office.

Step 2: Build an engaged interdepartmental community with C-suite buy-in

Armed with key information from step one, I began to focus on communication and transparent messaging to build a community that would begin to trust the idea of developing the program, whilst also gaining relevant support and intel. Being more familiar with the firm, this community provided insight into how things had been conducted previously and where change may be required. We listened to views and came together to discuss ideas, often virtually as this was at the height of the pandemic.

A key takeaway from this stage is to keep the messaging on point and identify the right stakeholders early on. I worked with second line

colleagues and compliance before ultimately sharing the outputs and recommendations with the C-suite. Securing engagement from the get-go across different teams was critical to ensuring a good level of C-suite engagement, especially during the gap analysis and recommendations phase.

Step 3: Develop and communicate a clear Vision and long-term roadmap

Looking to the longer term, I wanted to set out a three to five-year vision that would include establishing the baseline of where we were currently as a firm, conducting the gap analysis, developing a roadmap, and ultimately having the ambition to be best in class. I used parts of the initial desktop gap analysis to create the roadmap and then looked to identify key team figures to help develop it. Critical to this was determining how to turn each item in a milestone across the three-year plan, and what this would look like quarter by quarter. Identifying the right people to engage with and bring in during the planning phase to ensure they understood the vision was very important. Giving them then the opportunity to work within the community that we had built was also vital.

I then wanted to test the plan to ensure it was meeting regulations as well as our own appetite, to ensure we were on the right path and working at the right pace. With that proving successful, we began to breathe life into the roadmap.

Next was utilizing engagements across the firm, including the Risk,

Compliance and legal teams. We were transparent in what we were building and ensured that senior management and the supplier management community were comfortable that we were moving in the right direction. Engagement with the CRO's teams around compliance, risk, information security, and resilience was vital. With that secure, we were able to build a robust roadmap with clear milestones and a strong delivery plan. In parallel, we identified any resource limitations and extra support required.

By this point, we had shared the vision, developed the milestones, and set clear communication pathways. We had established cadence with relationship managers, second line, global COO, CRO, and appropriate senior management. We next needed to ensure that our function would be complementary to other functions rather than disruptive. We conducted a number of awareness sessions across the business to maintain transparency, listening to other business lines and stakeholders to help us determine how we could work with supplier relationship managers to improve certain areas. In particular, we wanted to identify relationships that might not have been managed well in the past, for any number of reasons.

A key deliverable was a Supplier Risk Management (SRM) playbook. This is a practical guide, designed to cover all components of a supplier life cycle, covering everything from planning, evaluating and selecting, right through to managing, monitoring and exiting of a supplier.

Step 4: Designing and launching a Global Outsourcing & Third Party Management Framework

Bringing a set of standards and oversight model together in the one framework was a key stage in our development of TPRM Program. We made a conscious effort to ensure the framework was practical and met global regulatory changes whilst also meeting our group standards and requirements.

The framework was designed and broken down into key stages:

1. Risk appetite: Board approved statement that highlights the importance outsourcing and third parties provide to the firm.
2. Governance: Showing the formal governance and escalation process including various committees and how they are structured.
3. TPRM lifecycle: Demonstrating the different stages of the TPRM cycle including the minimum standards at each stage so that the business can easily follow and adopt.
4. Record keeping and reporting: Pointing to the group wide tools and technology used for storage and management of outsourcers and third parties.
5. Training and awareness: Showcasing the plethora of support, training and templates available to meet the different components of the framework.

We conducted a firm wide global launch event that was recorded, this took us through the different stages of the framework. This was well received and continues to be a good source of awareness of the framework. By establishing a framework, we could actively deploy and begin to address and mitigate our exposure. A clear and accountable escalation processes

was identified in the framework which supported the operationalization on a global platform. Our continued focus has been on supporting business lines in the compliance of the framework and how the firm can demonstrate that.

Step 5: Focus on Outcomes and producing meaningful TPRM intelligence and value to the business

A major step forward was to bring all of the above into one place. We established the Global Strategic Supplier Oversight function (GSSO), which has four key pillars:

Supplier management and oversight:

Looking into key relationships and how to manage them in accordance with framework, policy, and standards. Level of oversight is applied to each relationship

Third-party risk management:

Responsible for embedding third-party risk management culture across the firm whilst also identifying from a first-line perspective the key supplier risks and issues.

Strategic Relationship Management:

Identifying strategic partners of the organization and maintaining those relationships. Looking at different projects and innovations, and working with partners on a regular basis to identify known issues or areas of focus, dependent on external factors.

Supplier data and analytics:

Bringing data into one place and producing a standard reporting suite inclusive of who the relationships are with, history of reviews, scorecards, performance metrics, risk profile, and commercials.

To enhance the supplier data and analytics, we developed and built an app that is available to senior managers of these relationships at any time. It provides instant performance scores and risk issues associated with any given suppliers, and also includes their spend profile and other relevant data. We developed standardized reporting templates and conducted attestation and conformance testing to keep supplier relationships honest. We take a sample of their work and apply analytics to show how they are performing at any given time across the relationship. Getting that data is no longer painful – we have the mechanisms in place to collate it and we have secured the resources to support the app and build it out further.

The work that we've done at LGIM is shared across the company and has been utilized at a group level, so we can start to report our data in a meaningful way. My role now is to provide the intelligence around that, identifying where we need senior management and C-suite attestation and highlighting areas where we can better support the firm in relation to managing third parties and outsourced services.

My journey continues, always learning and adapting along the way whilst keeping our ambition to become best-in-class!

For more articles like this, sign up to CeFPro Connect for free and gain access to weekly news, articles, reports, videos, insights and much more...

Visit www.cefpro.com/connect for all information and to create a free account.



Cyril Korenbeusser
*Chief Operational Resilience
 Officer, Americas*
BNP Paribas

THE ROUTE TO CYBER RESILIENCE

What are some of the key cyber and operational resilience trends across the industry today?

There is definitely a growing risk on the cyber front. This is especially visible within the financial industry because it is very mature in regard to digital transformation, which makes it a good playground for cyber activity. From a landscape of unstructured, random hackers, we have now moved into a structured cyber industry with higher services available for people trying to push attacks. On top of that, financial institutions are increasingly relying on digital processes, which are a good target for those players. It's therefore a growing risk.

In addition, we are seeing a reduction in the number of trusted parties. Third-party providers can rapidly move from trusted to not trusted – the status of a team in Russia could have altered within a day as a result of government decisions, for example. And small players that were historically not the direct target of cyber events can now disrupt an entire industry, as witnessed with the recent ION hack.

How does operational resilience connect with cyber resilience?

Operational resilience is a recent introduction from a regulatory perspective, although the concept is

of course not new. In short, resilience is the ability of an organization to anticipate, prevent, detect, withstand, and recover from any disruption that could impact its vital business services. It is important to keep in mind that we are talking about vital activities, including all the steps from anticipation, through to withstanding and recovery. We want to prevent an attack, fight it if needed, and recover from it.

We focus on vital activity because operational risk aims to save an organization. In order to achieve that, we need to look at different areas: IT resilience and operational resilience strengthen processes from the inside;

third-party resilience looks externally; and then there is the cyber resilience pillar. Those are the four key pillars that contribute to the protection of vital services.

What is the role of cyber resilience under the broader resilience context?

As above, cyber is one of the big pillars that supports operational resilience. If you look at some of the key deployed frameworks such as NIST on cyber resilience or cybersecurity, they highlight the identification, protection, detection, response, and recovery of a cyber event. There are direct parallels between those avenues and the structure of operational resilience programs.

It can be interesting to look at the impact of an incident on an organization and not just focus on the root cause. Cyber is an area that could have a drastic impact, not least because it has no physical or country boundaries. Location of resources is no longer a consideration, given the global nature of cyber risks.

The key element regarding cyber resilience is to look in detail at concentration risk. Since there are no boundaries, there is no limit to the reach of a potential cyberattack – it represents a local impact with a potentially global threat. The challenge is therefore being able to provide a solution that can address the numerous local needs as well as the wider global threat.

Looking at the concentration risk within technology is a good starting point. The second concentration is around people and localization. If all the activity for a vital service is being supported and executed from one location, the risk level is increased. The third area to consider is around third parties, i.e., understanding the connection and risk concentration of third parties around a vital business service. If a firm depends entirely on one third party for a vital service and does not have an alternative option in case of a cyber event, that service is at risk.

Organizations depend on third parties, but those third parties depend on fourth and fifth parties, and so on. Therefore, they will each in turn have the same type of concentration risk. We cannot stop at the boundaries of our company, or our third parties. Cyber resilience requires a recurring effort that should reach the end of the chain, which by its very nature

“The key element regarding cyber resilience is to look in detail at concentration risk. Since there are no boundaries, there is no limit to the reach of a potential cyberattack – it represents a local impact with a potentially global threat. The challenge is therefore being able to provide a solution that can address the numerous local needs as well as the wider global threat.”

becomes extremely complicated. We can already see across the industry concentrations of tech players, with the main example being cloud providers. As there are only three or four major players, most third parties will host at least part of their services on one of those platforms. That in itself is a big risk, so it is important to understand the level of exposure.

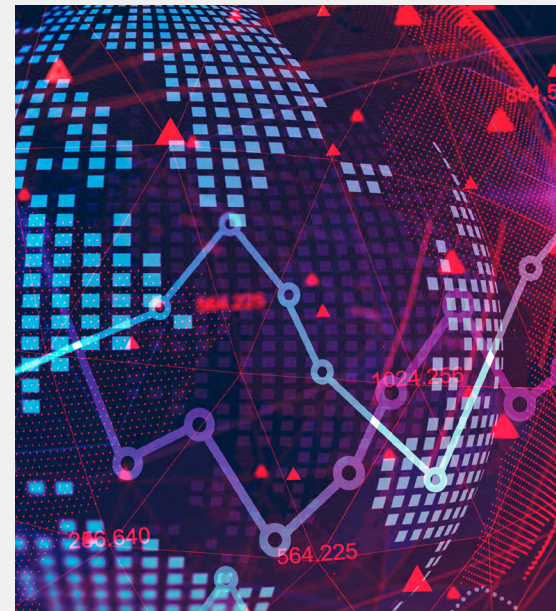
How has digital transformation impacted cyber resilience?

The financial industry started its digital transformation a long time ago with the objective of improving and accelerating client services, enabling both retail and investment banks to facilitate offerings such as real-time transactions and global coverage of business. The pace of what is possible continues to escalate – what used to take weeks can now be done in days or hours, even down to milliseconds. But that level of acceleration is also increasing risk. If an organization has days to react to a request, it can take steps to review its decision; if things are actioned in milliseconds there is no room for consideration.

The second factor is the scale of the impact caused by cyberattacks on the financial sector. The world of digital finance is continuously being

challenged by new and disruptive technologies. If quantum technology becomes a reality, it is not just the benefits that will be great – so will the risk to security and therefore the stability of the industry. From the day the technology becomes available, the previous historical models of protection, encryption, etc., will instantly be made obsolete. AI evolution is also something to consider, both from the point of view of its potential benefits as well as the growing risk exposure. There are a number of use cases that can be leveraged with the support of AI as an accelerator of a cyberattack, from analysis of the weaknesses to generation of the code to use and exploit.

In conclusion, we need a cyber resilience strategy not just at a corporate level, but also at a national level. A national strategy framework will enhance cross-sector collaboration. Regulation is one route to achieving this but the ultimate way to ensure it is effective and efficient is to make sure testing is in place. The financial industry has experience of this, with the stress tests it has put in place over time following different crises. What is now needed is something similar on the cyber front, to enable us to test an industry, or even a country. That will be the ultimate validation of our cyber resilience.



**Continue the discussion at Non-Financial & Operational Risk USA.
Taking place in NYC on October 4-5.
Featuring main event and breakout room focusing on cyber
security including strengthening cyber resilience.
www.cefpro.com/oprisk-usa**



Ashesh Kapur
VP Digital Product Management
Bank of Montreal

THE POWER OF NEXT-GEN ENTERPRISE CYBERSECURITY ARCHITECTURE

Traditionally, organizations have focused on defending their perimeter. But as cyberattacks become more sophisticated and data breaches more common, traditional measures are no longer enough. Enterprises are having to adopt new measures to protect and grow their business, leveraging today's technological advances. Going forward, cybersecurity must be integral, holistic, and automated from the outset rather than pieced together over time.

Why do we need a new security framework?

- **Social integration:** Defending operations against phishing attacks and scams, fake profiles/news, and malware attacks.
- **Business mobility:** Protecting devices from theft and accidental loss – developing a secure, mobile-first strategy is critical for any business.
- **Cloud migration:** Deploying policies, technologies, and controls to safeguard data, applications, and infrastructure.

- **Digital transformation:** Adding digital security to transformation plans to achieve dependable customer insights, high operational efficiencies, and reliable market growth.
- **Threat detection and response:** Detecting anomalies, analyzing threat level, and determining what mitigative action(s) may be required, including the use of big data analytics to secure enterprises.
- **Data security:** Protecting data across all applications and platforms from unauthorized access, ransomware, and corruption. Using Zero Trust design, data encryption, early intrusion techniques, etc. to secure data.
- **Compliance management:** Meeting regulatory or contractual requirements that a business is obliged to follow.
- **Brand protection:** Avoiding brand infringement, revenue loss, and reputational damage.

What should an enterprise security approach and framework encompass?

A business needs to build a holistic framework to identify and respond to threats across all areas of enterprise IT and associated systems. This will allow end-to-end visibility and protection across all events and help businesses to continuously detect and remediate anomalous behavior.

Key components of the framework include:

- **Balanced security:** Building a balanced security and trust inference model that allows a business to consider resource constraints, operations, and regulations to handle real-world threats and manage evolving complexities.
- **Zero Trust design:** Exploring interesting architectural possibilities beyond traditional perimeter security, with verification of each request based on a deeper understanding of all software layers.

- **Secure data flows:**
Enabling a holistic enterprise view by visualizing all processes and data flows and how they are being accessed.
- **Incident response:**
Rapidly isolating and responding to attacks by ensuring adequate levels of business continuity.
- **Automated monitoring:**
Real-time monitoring, log analysis, and alerts on all aspects of enterprise IT including networks, devices, databases, and on-premises/cloud applications.
- **Enterprise security:**
Analyzing critical events and data breaches in enterprise applications such as CRM, inventory management, order and fulfillment, etc.
- **Cybersecurity risk:**
Organizations are becoming more vulnerable to cyber threats due to increasing global reliance on computers, networks, programs, social media, and data. Data breaches, a common type of cyberattack, have significant negative business impact and often arise from insufficiently protected data. As well as the risk of loss resulting from a cyberattack or data breach, they can also result in impact to the IT infrastructure and reputational damage.
- **Secure business operations:**
Assessing the risk management processes to protect company sensitive information.
- **Digital transformation:**
Companies are incorporating digital technologies to drive efficiency and lower the cost of their operations. It is imperative that organizational data is equally secure in rest, motion, and when it is used as a part of digital transformation initiatives.

Cybersecurity architecture

A successful enterprise cybersecurity program requires broad foundations and architectural context. Cybersecurity architecture aims to facilitate secure business operations using Zero Trust and other innovations.

The first step in developing cybersecurity architecture is to estimate and prioritize security requirements, attack surfaces, known and unknown risks, implementation tasks, and incremental improvements to achieve an effective cybersecurity design and a manageable roadmap specific to your business operations.

The main components of cybersecurity architecture are:

- **Data mesh architecture:**
A decentralized data architecture that organizes data by a specific business domain – for example, marketing, sales, customer service, etc. – providing greater ownership to the producers of a given dataset.
- **Asset control:**
Inventory of an organization's IT assets and the potential security risks or gaps that affect each one.

- **Intrusion detection system:**
Can monitor networks for intrusions and help infer unknown attack types (i.e., zero-day attacks).
- **End-point security software:**
In addition to protecting user devices, this can be used to mitigate business disruptions.

Data governance and fraud detection

Being compliant does not mean being secure. Being cybersecure does not mean being fraud proof or well governed. In reality, this means complementing your cybersecurity architecture with data governance and fraud detection programs.

It is important to prioritize risks and incrementally improve business operations, at the same time as managing cybersecurity requirements in a thoughtful and balanced manner. Maintaining focus on next-generation big ideas such as data mesh architecture and Web3 opportunities will help to define and visualize business operation improvements, as well as prioritizing and balancing enterprise cybersecurity requirements. But remember that data governance is a business function – it is about getting marketing, finance, and other teams on the same page.

Ultimately, the goal of data governance is to create a new business capability, which is synonymous with creating a new data (mesh) capability or, more precisely, a new data API or NFT. Going one step further, cybersecurity analytics and workflows that encompass data governance and fraud detection areas are also required. The digital inventory and security manager (or application) plays an even more important role with its integrated cybersecurity analytics and workflows.

To conclude, a new security architecture can help organizations transform and secure their business operations using Zero Trust, data catalog, and machine learning, among other innovations.

Choosing the right solution

When choosing a cybersecurity solution, it is important to maintain sight of NIST-CSF's breadth and guidelines. When building an optimal cybersecurity solution, including ransomware protection, it is important to use an integrated suite of products, ideally incorporating the following areas:

- **Digital inventory & security manager:**
Used to manage inventory and incidents, as well as automate security operations and access control, through integrated analytics, workflows, and other support.
- **Software defined perimeter:**
Provides Zero Trust security to enterprise deployments, cloud infrastructure, business applications, and data estate.

**Read where cybersecurity ranked in CeFPro's global NFR Leaders report for 2023.
Read the full report at www.cefpro.com/connect for free
or visit www.nfr-leaders.com for more information, including top 10 ranking
of non-financial risks and extensive deep dive into key areas.**

MONOCLE

The overlooked pillar of trust



Wiehann Weerts
Consulting Director
– Europe
Monocle Solutions

In the past few decades, the banking industry has undergone a significant transformation. Due to technological advancements, banks are now offering services that were unthinkable even a few years ago. Innovations such as fully digital banking, open banking, blockchain-based transactions, advanced analytics, and artificial intelligence (AI) have become commonplace in the pursuit of advancing and expanding the services that banks provide to their clients. However, in the race to embrace these new technologies, many banks have seemingly forgotten the importance of the building blocks for decision making and strategy execution – their defensive data strategies.

The aims of defensive data strategies are to minimize negative outcomes and risks, including, at a minimum, compliance with regulatory and fiduciary requirements. While these strategies may seem mundane and unexciting compared to the novelty of technologies such as AI, they are nevertheless the building blocks upon which trust in the system ultimately rests. Defensive data strategy serves as the stable base – as in the case of a building's foundation – on which an offensive data strategy can be built,

paving the way for future innovation. Yet, without trust, the value that these exciting new innovations may bring are ultimately nullified.

Maintaining trust

Banking is a complex industry that involves a wide range of financial activities, including lending, borrowing, investing, and managing financial assets. At the core of all these activities, however, is the concept of trust. Banks function as the intermediaries between savers and borrowers. Savers trust banks to safeguard their money, provide secure and convenient access to their funds, and offer competitive returns on their deposits.

Borrowers, in turn, trust banks to provide them with access to credit, manage their financial risks, and help them achieve their financial goals. In addition to upholding fundamental principles, banks have a responsibility to ensure that regulators, shareholders, and their own employees can trust the information they provide about their activities.

Banks must ensure they comply with a raft of regulations, including Basel III/IV, MiFID II, AMLD, and many others. These regulations require banks to collect, store, and report a vast amount of data to regulatory bodies. Implementing and maintaining robust and trusted statutory and regulatory reporting platforms can be challenging, largely due to the

complexity of regulatory requirements, data quality and integrity, and legacy infrastructure. Despite these obstacles, however, non-compliance is simply not an option.

Consequences of non-compliance

Failure to comply with regulations can lead to severe consequences, including substantial fines, reputational damage, and in the most severe cases, the revocation of banking licenses. Therefore, both senior executives as well as regulators must always have access to accurate and reliable data to make well-informed decisions and manage risks in an effective and timely manner. Recent examples at large and mid-sized banks – where poor decision making has resulted in catastrophic consequences – has only served to further highlight the critical importance of accurate and reliable data in the effective management of these financial institutions.

While defensive data strategies are crucial, it does not mean that banks are unable to innovate. Defensive and offensive data strategies are not mutually exclusive; in fact, they are mutually beneficial. An effective balance between the two, where a tested defensive strategy serves as the foundation for an innovative offensive strategy is the ideal scenario.

Monocle Solutions assists clients with the implementation of data products that prioritize defensive measures, such as completeness, accuracy, and timeliness, but also enable users to confidently identify new opportunities, enhance products, and provide superior customer service. This not only gives banks the assuredness that their regulatory requirements are met but can also provide them with a competitive edge in an increasingly difficult banking landscape.

<http://www.monoclesolutions.com/>

LAUNCH RATE
FROM £499*
Valid until June 23

6th Annual
September 20–21, 2023
London

CeFPro® Events

FRAUD & FINANCIAL CRIME

Reviewing the current fraud and financial crime landscape and leveraging advances in technology to mitigate risk.

info@cefpro.com
+44 (0)207 164 658
www.cefpro.com/fraud-europe



Key information

Fraud & Financial Crime Europe returns to London this September for its sixth edition. This year, CeFPro has incorporated new features into the event allowing for more content to be covered, as well as more speakers.

NEW for 2023: Two streams

After much demand, this year's event will feature two streams, plus opening keynote sessions. The content will be divided across the areas of fraud and financial crime to enable a deeper dive into each topic.

Key Speakers



Paul Cain
Global Head of Research Analytics –
Financial Crime
HSBC



Raj Shah
Head of Financial Crime Screening,
Transaction Monitoring, Risk
Assessment Model and Analytics
Santander UK



Patrick Killeen
Unit Chief – International Corruption
Unit
FBI



Dr Liliya Gelemerova
Head of UK Financial Security
Crédit Agricole Corporate and
Investment Bank (CACIB)



Chloe Cina
Head of Global Sanctions Advisory
Deutsche Bank



Igor Sumkovski
Head of Financial Crime
China Construction Bank Corporation
London Branch

Keynotes and plenary sessions

→ Regulation

Reviewing the regulatory landscape and changes on the horizon to prepare for

→ Sanctions

Reviewing the sanctions landscape and keeping up with continued and upcoming change

→ Metaverse

Understanding uses of the metaverse as a risk and opportunity

→ Identification & Verification

Developing controls to enhance identification and verification with increased digitalization

Plus two individual work streams

Fraud

APP Fraud
Collaboration
KYC & Due Diligence
Legislation

Financial Crime

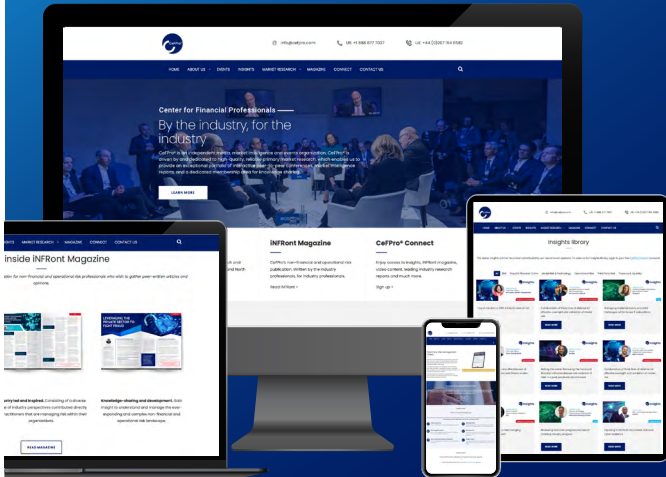
Trade Based Money Laundering
Technology
Ransomware
Financial Crime Models

CeFPro® is excited to announce the launch of our new website

By the industry, for the industry.

- ✓ Discover our wide range of risk, tech and innovation events across Europe and North America.
- ✓ Find out more about iNFRont Magazine, CeFPro's non-financial and operational risk publication. Written by the industry for the industry.
- ✓ Browse our global research Fintech Leaders, Non-Financial Risk (NFR) Leaders, Third Party Risk Management (TPRM), and our collection of bespoke industry reports.

Visit us on: www.cefpro.com



SHARED ASSESSMENTS

Third-Party Risk Management Education and Certification

Our certification programmes include the Certified Third-Party Risk Professional (CTPRP) and the Certified Third-Party Risk Assessor (CTPRA). These certifications provide professional credibility, recognition and marketability in third-party risk.

Third-Party Risk Fundamentals is a certificate-based learning course designed for individuals with limited or no third-party risk experience.

SIG Fundamentals is for novice users of the SIG questionnaire providing step-by-step instructions on how to create truly custom questionnaires to fit the needs of your vendor assessments.

3,000 professionals trained on TPRM best practices by Shared Assessments

96% would recommend Shared Assessments certifications to a colleague or friend

89% certificate holders report training improved ability to fulfill job duties



Learn More: www.sharedassessments.org/certification
Discount: 10% off any course with code "7TPRM_EDU"



A WORD FROM THE INDUSTRY...

What are the key considerations in ensuring data security across suppliers?

As supply chains evolve across the sector, the risk of a data breach caused by a third, fourth, or nth party is ever present. Keeping your company's and your customers' data secure is therefore an ongoing effort for today's financial institutions. Here, we ask some of the industry's leading figures for their insight into how to ensure data security across the supply chain...

Brian Shaw
Head of Financial Services
Mirato



"To ensure data security across suppliers, there are several fundamentals to prevent unauthorized access, data breaches, and loss. First, assess the suppliers' security practices to confirm compliance with industry standards and regulations. Second, encryption should protect data during transmission and storage. Third, limit access to data only to authorized personnel. Fourth, regularly audit and assess suppliers' security practices to certify ongoing compliance. Finally, implement contingency plans to address any potential data breaches or losses. Usually, the most significant practical challenges are too few resources to effectively manage large volumes of information across too many suppliers."

Kishan Majitha
Executive Director, Cyber
and Technology Controls
JP Morgan Chase



"As an industry, we need to get much better at assessing vendors at the time of engagement and then at a regular cadence afterwards. The shifting regulatory landscape means the days of 'trust most vendors and only verify the most critical' are gone if we are serious about data security and compliance with laws. Thankfully, there are more ways to gain assurance than just testing with audit reports (e.g., SOC2Type2) and cyber subscription vendors performing continuous monitoring on vendors to help reduce data security concerns. However, assessment is just the start, and in order for the approach to be effective, we also need robust mechanisms that oblige vendors to remediate in a timely fashion."

Madiha Fatima
Executive Director – Operational & Outsourcing Risk
JP Morgan



"Heightened incidents and data breaches have been an emerging trend in the supplier management space over the last 5-7 years. Ensuring data security across your suppliers in this interconnected and complex outsourcing era calls for a holistic and proactive approach to risk management for effective and robust oversight. This starts with understanding your risk appetite and exposure. The organizations can then focus on designing mitigation controls and strategies aligned to their appetite."

Hannah Macdonald
Head of Procurement & Third Party Risk
Monzo



"We need to recognise that data security is the responsibility of everyone. There needs to be appropriate methods to test and assess the strength of suppliers' security environments during selection, and organizations need to implement appropriate ongoing oversight methods to manage the risk during the supplier lifecycle. It's just as important to have robust processes to select as it is to exit. Clear policies and procedures should form part of day-to-day data management, and best practice should be followed. By limiting staff or supplier access to data, setting up tooling such as DLP, and educating your teams regularly, the aim should be to reduce the potential blast radius should a breach ever occur."

Maya Goethals
Director, Compliance and Risk Management
Bank of America Merrill Lynch



"In today's interconnected world, few suppliers do not have access to confidential data. Often, that's personal data of the client's customers; regulated data, protected by various privacy laws. Organizations should work with their suppliers to ensure that the promise they have made to their customers to protect their personal data is upheld. As much as imposing legal requirements and contractual clauses upon suppliers can help with that, firms first need to understand how their third parties treat customers' data. Conducting due diligence and reviewing the supplier's processes has become inevitable. As well as being required by regulators, customers expect to know how their data is being handled by the supplier network. Lack of awareness is no defence."

Shabbir Tahasildar
Operational Risk Oversight Lead for Technology, Cyber
and Third-party Risk Management
Handelsbanken plc. (UK)



"Designing robust data security measures and securing data transfers across the supply chain are vital to protect against cyber threats and data breaches. A data breach in the supply chain can have far-reaching consequences, including financial loss, reputational damage, and legal liabilities. Therefore, securing data at every touchpoint in the supply chain is crucial to maintain the integrity and resilience of the financial services industry. After all, safeguarding data is not just a compliance requirement, but a strategic imperative to protect customers, stakeholders, and the industry's reputation."

Getting comfortable with your CECL results through challenger models



Theresa Meawad
Head of Solutions
Consulting, EVOLV
SS&C Technologies

Current modeling challenges

As this period of unprecedented economic volatility continues, many institutions have found themselves in an economic environment that Chief Risk Officers have never seen. This will continue as the macro environment continues to be dislocated: Inflation, geo-political instability and war, technological disruption, remote work, governmental intervention, rising interest rates, disrupted labor markets and supply chains and changes in migration leading to changes in area demographics. In many ways the macro-economic environment today looks more like the 1980s than the 2020s. This has been coupled with:

- Hidden credit losses covered by governmental intervention and automatic modification.
- Fundamentally different loans coming into their portfolios due to rising interest rates and increasing acquisitions.

All of these create challenges for banks, putting stress on production models and model risk management teams as they work to validate their champion models as the recent historical performance of the portfolio was achieved in very different circumstances. Executives are staying up at night as they grapple with the adequacy of their CECL allowance and get comfortable with their production models.

Ongoing model risk management

The current environment has heightened the need for robust ongoing model validation. After a model has been developed, reviewed, tested and placed into production, then comes the need for ongoing model risk management to ensure that the model continues to be relevant and reliable. Model performance can deteriorate over time as institution-specific exposures, borrower behavior

and market conditions change from those embedded in model design. This happens much more quickly during times of economic volatility and broken banking relationships like those we have seen in recent history. To some degree, performance deterioration can be mitigated during the design phase; however, the more complex and granular a model is, the more of a liability it may become in times of sharp economic change. Executives, auditors, investors and regulators expect to see detective controls to identify performance deterioration in a timely manner, and there are many ways for an institution to implement these controls—but they are not all created equal.

Detective controls

Model stability monitoring, back-testing, benchmarking, and challenger models can all detect declines in performance. Each of these has its place—and limitations. Model stability monitoring ensures that the model continues to function as designed, but does little to ensure continued relevance and appropriateness. Back-testing goes beyond this by comparing model-predicted losses to actual results achieved. But back-testing has significant limitations, including:

- Short performance measurement window (e.g., quarterly) for models generating long-term, lifetime credit loss predictions.
- Loss measurement in counterfactual situations (e.g., CCAR/DFAST stress testing) is limited, as they are not intended to be realistic, and therefore, real results cannot be used to back-test these scenarios.
- Model error attribution/identifying root cause of performance deterioration can be challenging when models are complex, which is the case for many bank CECL models.

Challenger models and benchmarking can often help overcome some of these issues as they leverage a true CECL model, but management will need to ensure that the challenger model is reliable.

Finding the right challenger model

Model benchmarking or challenger models can address the limitations of back-testing and stability monitoring given that the right model is chosen. These models can be used:

- As verification of the accuracy or conservativeness of the production model.
- To compare loss predictions across models using same borrower/ macro-economic data inputs.
- To support attribution analysis of quarterly changes in production model predictions, especially if the model is more transparent than production models.

To achieve these results, an appropriate challenger model must be selected. Importantly, these models should be developed independently of an institution's champion model and:

- Include reasonable methodologies and assumptions.
- Leverage similar inputs to support "apples to apples" comparison.
- Be adequately documented and understood by management.
- Allow for deep insights into the key drivers of the allowance.

SS&C EVOLV is a powerful solution leveraged by model risk management teams around the country to verify their models and to help gain comfort with their CECL results. To learn more about SS&C EVOLV's model risk management capabilities, visit ssctech.com/products/evolv.

4 ESG myths demystified: Why controls are key to ESG reporting

Environmental, social, and governance (ESG) disclosures in public company financial reports have been a constant topic of conversation for over a year. In the US, the Securities and Exchange Commission (SEC) has proposed requirements to standardize reporting metrics so investors and other stakeholders can compare companies and reduce the likelihood of fraudulent claims by corporations that exaggerate their ESG performance, a practice known as greenwashing.

As with any new topic, people are speculating about this requirement, and some misconceptions have arisen. In this article, we dispel a few of the most common myths related to ESG reporting and provide guidance on the best practices you should consider instead.

ESG myth #1: The published report is your finish line

Many companies think of ESG as a reporting exercise. In reality, the metrics included in the financial reports represent a snapshot of a robust ESG program. Each year, corporations should consider the data reported as the coming year's baseline. Management has an opportunity to set new targets, make improvements, and continuously work to meet their stakeholders' expectations. Without considering ways to make improvements, ESG reporting will require time and resources from the organization with little benefit.

ESG myth #2: Our existing sustainability reports are just fine

If your company is already publishing ESG results, you may assume that the proposed SEC rule is just business as usual. Some companies are already listed on an ESG index or may have published an annual sustainability report for many years, so they assume they will not need to make changes. In reality, they may once have been ahead of the market, but it is now time to revisit what information the new reporting rules are targeting. This could also be a good time to review the current SASB and other ESG frameworks, ESG risk factors, and the regulators' positions on specific risks. Finally, consider the format of your current reporting – the report should be dynamic and designed for all audiences.

ESG myth #3: Collecting data is the most important step

Accurate, reliable data is extremely important in ESG reporting. Data tells you the current status, progress made, and areas for improvement, and it must be scrutinized even when your data collection controls are in place. ESG information comes from various sources, and no individual is an expert in everything related to ESG. Having accurate, reliable data for ESG reporting requires governance programs around collecting, verifying, and aggregating the data. Ideally, the data should be managed in the same system of record as your ESG control framework. Using a consistent approach in the controls process allows you to tie together the ESG goals, data points, metrics, and controls for an integrated risk management approach.

ESG myth #4: A previous ESG materiality assessment is relevant

Materiality assessments performed more than a year ago are probably out of date. The company, metrics, and thresholds all change. Similar to the myth regarding prior experience with sustainability reporting, now is a good time to revisit and refresh your company's approach to establishing materiality. Some companies take on the assessment as a single, large-scale project, some outsource, and others spread the work into smaller initiatives. A good approach should balance the desired result with cost, effort, and stakeholder expectation.

[Click here for more information](#)




Claire Feeney
Senior Product
Marketing Manager
AuditBoard



Dylan Krieger
Business Value Architect
AuditBoard

ESG reporting requires action

The most common ESG myths have one theme: ESG reporting will be quick and easy. The truth is ESG reporting requires companies to take action by establishing a formal ESG program to set targets, choose a framework, establish metrics, identify risks, design and implement controls, aggregate data, and then test to verify the accuracy of the data in the report. Even those companies ahead of the game with sustainability reporting will quickly fall behind if they think they can continue without updating their current approach. Management will need to fully support the ESG data they present in an audit-ready format that will pass inspection from regulators, rating agencies, and external auditors. Take advantage of your time while the reporting rules are still in a proposed state to build a plan and explore solutions to streamline your ESG program.



Building trust in the digital economy.

Bitsight invented the security ratings industry in 2011. As the market leader, we are still the standard in how organizations quantify, manage, and monitor cyber risk.

With threats intensifying and CISOs working against growing cyber risk uncertainty, our mission has extended well beyond cyber risk ratings to enable integrated cyber risk management.

Over 3,000 global enterprises trust Bitsight's data and integrated applications to drive critical workflows across exposure, performance, and risk.

Discover how to grow your ecosystem with confidence.

BITSIGHT



NEW GLOBAL RESEARCH THIRD PARTY RISK MANAGEMENT

Benchmarking the industry and enable institutions to develop resilient TPRM teams in an ever-evolving environment.

What are we investigating?

- Team structures
- Scanning the horizon
- Use of cloud and security measures
- Defining TPRM
- Best practice
- Global events

For more information visit
www.cefpro.com/tprm



Anit Banerjee
TPRM SME

REMAINING AGILE TO MITIGATE THIRD-PARTY RISK



As global geopolitical challenges and the aftereffects of Covid-19 continue, which areas are currently the most challenging within supply chain and third-party risks?

Many of our challenges relate to suppliers in areas of concern, specifically China. Considerations range from child labor through to the slowdown of supply chains generally.

Across industries, many challenges revolve around manufacturers and their suppliers. We were fortunate to be able to act fast at the onset of the Ukraine invasion, meaning we had many contingencies in place ready to manage disruptions. During the Covid-19 pandemic, much of our focus was on cyber and privacy. We made changes to ensure that services could continue and had the option of secondary suppliers where needed. As a result, we can restrict conducting business in a risky country and transfer activities to other territories; we are able to move very fast to remediate geopolitical risks. Looking beyond our primary providers through to their providers has also become much more prominent over the last few years – it's important to look beyond third parties.

What has enabled you to remain agile and act fast amid changing geopolitical conditions?

From managing 55,000 suppliers, we had to have a plan in place to make certain shifts to allow us to act quickly. We are prepared not only for geopolitical risks, but also for a range of broad scenarios including upcoming regulatory changes in Europe and Asia, including India. We began around a year ago and were able to trace back all of the potential impacts in order to remediate the risks and develop a contingency. We took steps to potentially resolve any issues way before we needed to handle them; we acted first and fast.

How do you define 'critical' when reviewing remediation plans?

The events of the last few years have heightened our awareness of the overall importance of third-party risk management and the need to develop contingency programs and understand the interconnected nature of

our business. Criticality is described similarly across industries, with more or less emphasis on products, and rankings can typically be broken down into three areas:

- 1: Critical suppliers that would impact ability to provide goods and/or services.
- 2: Important suppliers with a significant impact that is slower to be felt.
- 3: Suppliers who are important but easily replaced.

We are able to move quickly from one supplier to another because of the way in which we have developed our program. For every critical provider, we aim for four or five contingencies to act as backup, allowing us to quickly shift from a supplier that may be vulnerable to geopolitical risks. If our core supplier fails, we are prepared for a relatively quick turnaround.

What are some best practices to monitor critical suppliers, as well as looking beyond to fourth and fifth parties?

Heavy reliance on AI. For example, using internal tools, we have created a range of roadmaps for organizations that we deem large institutions, which cuts down our SLA time. There are also institutions who fail to provide the correct documentation for due diligence. In these cases, we can leverage an alternative route with AI/publicly available tools to ascertain intel to help us gain a full security posture of the supplier. Without revealing too much, these third-party intel tools can provide us with not only third-party data, but also give us enhanced visibility into our significant potential fourth parties to advance our understanding of the associated risk.

Are there any unique areas you are seeing when managing third-party and supply chain risks?

On a very high level, one of the things that we are conscious of is certain changes coming out of primarily the EU, UK, and India. This could impact numerous areas when it comes to maintaining privacy policies. We are currently gauging what those changes may look like and how we could implement them, and planning accordingly.

For more information on third-party risk management across sectors, stay up to date on developments ahead of the launch of Third Party & Supply Chain Risk: Cross Sector at www.cefpro.com/tpm-usa



EVENTS CALENDAR

US Events

CeFPro® Events
RISK AMERICAS
12 Annual | May 23-24, 2023



www.risk-americas.com

CeFPro® Events
VENDOR & THIRD PARTY RISK USA
8th Annual | Jun 7-8, 2023



www.cefpro.com/vendor-usa

CeFPro® Events
DIGITAL BANKING USA
2nd Annual | Sept 28-29, 2023



www.cefpro.com/digital-banking-usa

CeFPro® Events
CLIMATE RISK USA
3rd Edition | Oct 4-5, 2023



www.cefpro.com/climate-risk-usa

CeFPro® Events
NON-FINANCIAL & OPERATIONAL RISK USA
8th Annual | Oct 4-5, 2023



www.cefpro.com/oprisk-usa

CeFPro® Events
BALANCE SHEET MANAGEMENT USA
Nov TBC, 2023



www.cefpro.com/balance-sheet-usa

CeFPro® Events
THIRD PARTY & SUPPLY CHAIN USA
Nov TBC, 2023



www.cefpro.com/third-party-usa

For more information, including agenda, speakers, location, and registration, visit www.cefpro.com/forthcoming-events

EMEA Events

CeFPro® Events
RISK EMEA
12 Annual | Jun 13-14, 2023



www.risk-emea.com

CeFPro® Events
VENDOR & THIRD PARTY RISK EUROPE
9th Edition | Jun 15-16, 2023



www.cefpro.com/vendor-europe

CeFPro® Events
FRAUD & FINANCIAL CRIME INTERNATIONAL
6th Annual | Sept 20-21, 2023



www.cefpro.com/fraud-europe

CeFPro® Events
BALANCE SHEET MANAGEMENT
Oct 17-18, 2023



www.cefpro.com/balance-sheet

CeFPro® Events
CUSTOMER EXPERIENCE EUROPE
Nov TBC, 2023



www.cefpro.com/cx-europe

For more information, including agenda, speakers, location, and registration, visit www.cefpro.com/forthcoming-events