



RiskBusiness Key Business Concerns Report 2023



Welcome to the annual *RiskBusiness Key Business Concerns Report, 2023*. Each year, we analyse the industry's biggest risk surveys to identify the most pressing issues impacting financial institutions in the year ahead, from a non-financial risk perspective. Every year brings new challenges for those responsible for risk management, compliance and related roles. This year is no different, with the aftermath of Covid colliding with growing political and economic turmoil, set against the backdrop of the largest war on European soil since WW2.

The key business concerns listed in this report are done so in no particular order, but comprise the issues most highlighted across key industry surveys. The RiskBusiness newsletter readership is largely individuals who work in non-financial risk management roles and so the report tries to look at these risks from this particular perspective.

DEALING WITH THE UNEXPECTED: IMPACT OF GLOBAL EVENTS

If the past three years have taught us anything, it is to expect the unexpected. Low-probability, high-impact events have highlighted the vulnerability of the delicate systems our world relies upon to operate. The risks associated with Covid have now declined as it reaches its endemic state - but the after-effects are still being felt. In September 2022, many global banks began lifting Covid restrictions on office-based working, with Wall Street largely abolishing testing and mask-wearing requirements. In China, Covid travel restrictions were only lifted in January 2023, and a negative test is still required for those entering the country. But in December, domestic lockdowns that had lasted far beyond any other country's measures were beginning to take their toll on operations within China's financial sector, with some institutions reportedly rushing traders and

other key members of staff back into the office in December 2022 as remote working impacted productivity. According to Bloomberg, during a spike in cases in China in late December, nearly 80% of traders at one bank were either off sick or working from home, making arrangements such as split teams or routing trades through those still working at the office nearly impossible.


However, in general, Covid is no longer at the forefront of risk management as we enter 2023. "This year's results confirmed that the financial services industry has moved on from Covid, at least in most parts of the world," says Protiviti's [Executive Perspectives on Top Risks report](#). "Concerns about government mandates and restrictions, ability to protect the health and safety of employees, and the possibility that the pandemic would drive negative shifts in customer spending patterns all fell significantly, and collectively accounted for three of the eight lowest-rated risks in this year's survey," it said.

A return to near-pre-Covid operations elsewhere around the globe was abruptly interrupted by the Russian invasion of Ukraine in February 2022. Europe's energy crisis - a direct impact of the Russia-Ukraine conflict - has only just begun to materialise. How this might impact day-to-day operations within the financial sector is still unknown. In September 2022, banks in Europe began preparations for potential winter blackouts as Russia cut off gas supplies to the region. "The banking

system is part of other systems," Gianluca Pescaroli, professor in operational continuity and disaster resilience at University College London, told Reuters. "My main concern is the cascading effects on society of failures to ATMs or cashless transactions. Similarly, the dependencies banks have on other services such as the internet." In the summer of 2022, JPMorgan confirmed that the bank would be stress testing power cut scenarios, including the use of generators to ensure the ATM network remained functional for customers. Deutsche Bank said it was implementing energy-saving measures across its network of 1,400 buildings in Germany, including limiting the use of hot water and ensuring all lighting was switched off overnight. And Unicredit, based in Italy, also confirmed it had reassessed its operational resilience plans, highlighting its reliance on data centres which are supplied by two independent power stations.

Thanks to unseasonably warm weather this winter, Europe has managed to avert a complete energy apocalypse so far, but experts warn the crisis is not over and high energy prices will remain for the foreseeable future. "There will be no return to a pre-2022 stability," says Control Risks' [RiskMap 2023](#). "Energy risks will continue to disrupt supply chains. Companies need to evaluate their upstream and downstream exposures to energy disruption. Think about diversifying suppliers, self-insuring through backup power provision, and relocating supply chain operations to energy-secure locations. Understanding local political and regulatory factors affecting power supplies will be vital."

This is still a concern for financial institutions because of the large premises they operate in, but it should also be considered in the context of the wider



The crisis is not over and high energy prices will remain for the foreseeable future

Households face real financial hardship and they are more likely to default on loans and mortgages

cost-of-living crisis. As many households face real financial hardship, they are more likely to default on loans and miss mortgage repayments. From a regulatory compliance perspective, this places further pressure on financial institutions to ensure they are providing consumers with appropriate support and acting in their best interest. This is an area of particular interest for regulators, with new guidelines such as the [Consumer Duty](#) in the UK holding institutions increasingly accountable for the financial welfare of their customers.

The Russia-Ukraine conflict also created a new regulatory minefield for financial institutions to navigate as Western nations implemented a list of unparalleled sanctions in what was dubbed by many as a [new era of financial warfare](#). “The Ukraine conflict

triggered the imposition of sanctions, nationalisation of key players, and government appropriation of assets, such as Germany’s seizure of Russian energy companies’ stakes in local refineries last year,” says the World Economic Forum’s [The Global Risk Report 2023](#). Reputational and legal risk also grew for many multinational company operations as consumers put pressure on firms to break links with Russia. “Goeconomic confrontation was ranked the third-most severe risk over the next two years by GRPS [Global Risks Perception Survey] respondents,” says the WEF report. “Interstate confrontations were anticipated by both GRPS and EOS [Executive Opinion Survey] respondents to remain largely economic in nature over the short term. Goeconomic confrontation – including sanctions, trade wars and investment screening – was considered a top-five threat over the next two years among 42 countries surveyed by the EOS and featured as the top risk in many East and South-East Asian countries, among others.”

The conflict in Ukraine has also had a significant [impact on cyber risk](#) for financial firms, which we look at in greater detail below.

CYBER SECURITY

Cyber security will always feature prominently in global risk reports because of the growing threat placed by malicious actors - and also by simple human error. Control Risks’ *RiskMap 2023* ranked cyber risk as third in its top forecasted risks for businesses in 2023. “The cyber arms race will accelerate in 2023, enabled by an expanded attack surface and a significant increase in automation across the entire spectrum of cyber threats,” it says.



“Following the example of the Ukraine conflict, the fifth domain [cyber space] is now firmly anchored as a critical part of modern warfare.” A report released by FinCEN (the US Financial Crimes Enforcement Network) in November revealed a significant uptick in the number of ransomware attacks reported by financial institutions. FinCEN says Russia-related ransomware variants accounted for 69% of ransomware incident value, 75% of ransomware-related incidents, and 58% of unique ransomware variants reported in the second half of 2021, in the lead-up to Russia’s invasion of Ukraine. The results for 2022 will provide interesting reading.

The WEF report ranked “widespread cyber crime and cyber insecurity” eighth in its top 10 global risks by severity and reminded readers to consider not only malicious actors when thinking about cyber risk, but also the more complex push-and-pull of risk versus return in the context of adopting new technology: “The ever-increasing intertwining of technologies with the critical functioning of societies is exposing populations to direct domestic threats, including those that seek to shatter societal functioning. Alongside a rise in cybercrime, attempts to disrupt critical technology-enabled resources and services will become more common, with attacks anticipated against agriculture and water, financial systems, public security, transport, energy and domestic, space-based and undersea communication infrastructure. Technological risks are not solely limited to

rogue actors. Sophisticated analysis of larger data sets will enable the misuse of personal information through legitimate legal mechanisms, weakening individual digital sovereignty and the right to privacy, even in well-regulated, democratic regimes.”

The Economist Intelligence Unit (EIU) [Risk Outlook 2023](#) report presents 10 “risk scenarios that could reshape the global economy”, one of which is “Scenario six: inter-state cyberwar cripples state infrastructure in major economies.” The report suggests that high costs of direct military action and the ability of cyber criminals to escape prosecution is likely to see an increase in the use of cyber warfare as a weapon of choice from state actors. “This could be triggered by a complete diplomatic breakdown, leading to an escalating string of tit-for-tat cyber-attacks ultimately targeting software that controls state infrastructure. The shutdown of a national grid, for example, would severely disrupt business operations,” it says.

Artificial intelligence (AI) is being increasingly relied upon by financial institutions to provide more streamlined services, recommend appropriate financial products and identify suspicious activity. The benefits of this technology are vast, but what about the risks? “Companies in every sector will contend with new reputational risks when key executives or accounts are impersonated with malicious intent, triggering public relations scandals and even stock selloffs,” suggests [Eurasia Group’s 2023 Top Risks Report](#). “Generative AI will make it difficult for businesses and investors to distinguish between genuine engagement and sentiment on the one hand, and sabotage attempts by hackers, activist investors, or corporate rivals on the other, with material implications for their bottom lines. Citizen activists, trolls, and anyone in-between will be able to cause corporate crises by generating large

Artificial intelligence (AI) is being increasingly relied upon by financial institutions

Each new generation entering the workforce has created a sea change in societal constructs

enough volumes of high-quality tweets, product reviews, online comments, and letters to executives to simulate mass movements in public opinion. AI-generated content amplified by social media will overwhelm high-frequency trading and sentiment-driven investment strategies, with market-moving effects.”

CLIMATE CHANGE AND NATURAL DISASTERS

Climate change and the impact of extreme weather events is high on the agenda for business leaders, with several reports highlighting it as a key risk for 2023. “Failure to mitigate climate change” and “Failure of climate change adaptation” were two of the top 10 risks identified by the WEF. “Climate and environmental risks are

the core focus of global risks perceptions over the next decade – and are the risks for which we are seen to be the least prepared,” it says. “As floods, heatwaves, droughts and other extreme weather events become more severe and frequent, a wider set of populations will be affected.” The WEF report also addresses how corporations and governments are choosing to act on climate change: the mitigation versus adaptation debate: “Although climate mitigation [prevention/reduction of greenhouse gases] has been overwhelmingly favoured over adaptation [adjusting to the immediate and future effects of climate change] in terms of financing to date, particularly in the private sector, EOS results indicate that climate adaptation may now be seen as a more immediate concern in the short term by business.”

In July 2022, the European Central Bank published the results of its climate change stress test. It showed that most banks did not have robust climate risk stress-testing frameworks and lacked relevant data on the risks presented by climate change. “Euro area banks must urgently step-up efforts to measure and manage climate risk, closing the current data gaps and adopting good practices that are already present in the sector,” said Andrea Enria, Chair of the ECB’s Supervisory Board. In November 2022, the regulator published its [thematic review](#) of these stress tests, which increased pressure on banks to take action and warned of higher capital requirements and hefty fines if they did not implement necessary changes identified in the review by a 2024 deadline. “We detected blind spots at 96% of banks in their identification of climate-related and environmental risks



in terms of key sectors, regions and risk drivers,” said Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board. “Banks are certainly keen on new forms of sustainable business, and have plans to allocate more funds to them soon. Many are also phasing out specific activities, such as thermal coal power generation, and have started discussing the transition with their most carbon-intensive clients. However, it is too often still unclear how these initial steps shelter banks’ business models from the consequences of climate change and environmental degradation in the years to come.” The ECB will be launching its 2023 climate risk stress test at the end of January.

FINDING AND RETAINING TALENT AND THE TECHNOLOGY SKILLS GAP

Covid’s lasting impact on how we choose to work, a greater reliance on technologies such as AI, plus ‘Generation Z’ (the so-called TikTok generation) entering the workforce, has all contributed towards a major shift in recruitment requirements for firms. As a result, “ability to attract and retain talent” moved up two places to no.2 on Protiviti’s top risks this year, and “access to IT talent and digital knowledge” moved five places up the list to no.7.

“Risks related to the transition to hybrid work and ongoing increases in the cost of labour also increased significantly year over year,” said Protiviti. “We would expect this set of risks to decline by the time of our

2024 survey, as the crypto implosion and layoffs and hiring freezes across the technology industry reduce a source of competition for FSI [financial services industry] talent. Meanwhile, headcount reductions in areas like mortgage lending and investment banking increase the supply of available candidates.”

The Eurasia Group report highlights how each new generation entering the workforce has created a sea change in societal constructs and expectations from employers - and this generation is no different. Rapid changes in the use of technology, the wide-reaching potential of data and the proliferation of social media require a workforce that is very different to the mostly white, middle-aged male boards of directors currently sitting at the top of most financial institutions. “Generational transitions often require corporations and governments to make significant institutional, strategic, and policy changes,” says the report. “When women entered the workforce during World War II, businesses were required to develop new workplace conditions better suited to childcare and family obligations...Gen Z is redefining the workplace by pushing companies to incorporate fundamental changes in how they recruit, organise, retain, and develop talent; embrace new career paths and opportunities; foster genuine diversity and inclusion; and re-evaluate their social, political, and environmental impact. As a result, corporations will feel unprecedented pressure to take sides in political and geopolitical debates, whether they like it or not.”

POLITICAL RISK/ POLITICAL DIVISION

The Russian invasion of Ukraine provided a sinister, ever-present undercurrent to most areas of business activity in 2022. When Russian tanks crossed the border into



Euro area banks must urgently step-up efforts to measure and manage climate risk

US-China relations also pose a real risk to business as US firms look to decouple critical supply chains

Ukraine on 24th February, it exposed the whole world - but especially Europe - to the risks associated with political unrest and military conflict. It impacted global supply chains, increasing the price of several commodities and resulted in unprecedented sanctions on Russian banks, companies and individuals. The Eurasia Group report - which focuses specifically on political risk - highlights "Rogue Russia" as its key global threat for the year ahead and warns of further disruption: "Kremlin-affiliated hackers will ramp up cyberattacks on Western firms and governments," it says. "Pipelines, as well as LNG [liquified natural gas] terminals, will be attractive targets for Russian sabotage. Russian officials have credibly threatened retaliation against American and European satellites that play

a role in the war. Fibre is vulnerable too: cables in Europe and under the Atlantic will be targets, probably in a fingerprint-free way as with the Nord Stream pipeline attack in September (where there's still no evidence of responsibility)."

US-China relations also pose a real risk to business as US firms look to decouple critical supply chains. "With a raft of industrial policies and international initiatives, the US is making good on its pledges to re-shore and 'friend-shore' strategic industries, like semiconductors, EV batteries, and critical minerals," says Control Risks. "It is restricting China's access to technology, capital markets and investment opportunities, as well as US companies' ability to invest in advanced technology in China. Other Western countries are joining in more intensive scrutiny of China-based suppliers. Cross-border data protection laws are not far behind." Chinese investment in the US will also likely be deterred by policy restrictions and strained political relations, according to the report. "The emergence of regulatory and compliance dilemmas for companies trying to do business in both countries seems closer than ever," it adds.

Eurasia Group points to a "Divided States of America" as an environment it says will become increasingly challenging for firms that have been used to relying upon the US as a place with a coherent market and predictable regulatory regime. "States traditionally have competed for corporate investment through incentive packages. But now, conservative politicians are differentiating themselves by picking fights with major employers over issues such as environmental, social, and governance (ESG) regulations, while left-leaning



politicians are pursuing more pro-worker, consumer, and environmental policies that increase the cost of doing business in their states.” This political divide will have a marked impact on long-term investment for firms based both in the US and elsewhere, as an understanding of state-level politics becomes increasingly crucial to business.

Japan and India reportedly began joint air drills outside of Tokyo on 16th January 2023 amidst rising tensions with China. Ahead of the drills, Japan’s Defence Ministry released a statement saying the exercise, titled “Veer Guardian-2023,” would “promote air defence cooperation between the countries,” and would take place at Hyakuri Air Base.

China-Taiwan relations are also an ever-present risk. *The Economist’s* EIU report suggests the following as its third potential scenario that could reshape the global economy: “Direct conflict erupts between China and Taiwan, forcing US to intervene”. The EIU says direct conflict between China and Taiwan is unlikely, but tension has been mounting since China’s targeted military operations after Nancy Pelosi, speaker of the House of Representatives in the US, paid a visit to Taiwan in August 2022. “Recent military exercises by China and a more aggressive Taiwanese response raise the risk of a miscalculation, which could spiral into a wider conflict. Such a conflict would wipe out Taiwan’s economy, including its semiconductor industry, on which global supply chains rely. It would also risk

drawing in the US, Australia and Japan, starting a catastrophic global conflict.”

REGULATORY CHANGE

This area of risk is wide sweeping and is really a side effect of the other, aforementioned risks. Developments in technology, climate change risk, political unrest and the resultant economic stress have combined to create a potent regulatory cocktail for firms to stomach in 2023.

Increased use of artificial intelligence and machine learning in financial services has piqued the interest of regulators, leading to a swathe of new regulation focussed in this area. Several jurisdictions are making moves to address gaps in regulation for the use of AI in the financial sector, but the EU is the first major regulatory body to actually propose a law on the use of AI. Like the GDPR (General Data Protection Regulation) before it, the [EU AI Act](#) is likely to become a global standard, and so firms in all jurisdictions should pay close attention to its progress. Proposed fines for non-compliance with the final law will be similar in size to those issued in relation to GDPR non-compliance: up to a maximum of 6% of the firm’s global annual turnover. The law will impact not just providers of AI systems, but also any organisation that makes use of them.

Sanctions against Russian firms and individuals will be an ongoing challenge for compliance teams as the conflict continues. A recent [survey](#) of UK financial institutions by Comply Advantage found 45% of UK financial institutions changed their business model in response to Russia’s invasion of Ukraine, with 57% implementing a freeze on Russian assets and 54% implementing an onboarding shutdown in the country.

“It’s clear that compliance and sanctions teams realise how significantly the war in Ukraine can - and will - impact their businesses,” said Vatsa Narasimha, CEO at

Sanctions against Russian firms and individuals will be an ongoing challenge

The influence of crypto currency on the wider banking sector is also something to consider

Comply Advantage. “This will continue in 2023 with further changes to the lists of Russian sanctions designations. But the sanctions landscape is larger than Russia, so firms must prepare for measures that may arise in response to geopolitical events occurring in other countries. As western governments focus on improving private sector implementation and taking enforcement action, a laser focus on sanctions in the year ahead will be critical.”

Whilst staying on top of new and proposed regulation, firms should also be mindful of the impact of deregulation as governments scramble to boost growth and avoid a global economic downturn in 2023. In the UK, Chancellor of the Exchequer, Jeremy Hunt, has proposed a potential rollback of City regulations implemented in

the wake of the 2008 financial crisis, including ring-fencing rules designed to protect ordinary customers by separating their deposits from high-risk investment banking operations. The reforms could also prompt a discussion about the Senior Managers Regime, which currently holds senior executives of banks personally responsible for issues that happen under their supervision. Critics of Hunt’s so-called “Edinburgh Reforms” package say he is potentially putting everyday people at risk for the benefit of big business. Sir John Vickers, a senior economist who led a review into the 2008 financial crisis told *The Guardian*: “We want safe and sound institutions, we want well-functioning financial markets. What I think would be a great mistake would be to put the financial services sector on some kind of pedestal, warranting...special light-touch regulatory treatment, when we all need that sector to be safe and sound for the competitiveness of the economy as a whole.”

The influence of crypto currency on the wider banking sector is also something to consider from a regulatory risk perspective as we head into 2023. US regulators have recently warned financial institutions of the potential risks of fraud, legal uncertainty and inaccurate or misleading disclosures when dealing with crypto-related business – and 2023 is predicted by some in the industry to be the year of “the great crypto implosion.”

In a joint statement, the US Federal Reserve, US Federal Deposit Insurance Corp (FDIC) and the US Office of the Comptroller of the Currency (OCC) said they would be keeping a close eye on firms with links to the crypto markets. “It is important that risks related to the crypto-



asset sector, that cannot be mitigated or controlled, do not migrate to the banking system,” said the statement. “The agencies are supervising banking organisations that may be exposed to risks stemming from the crypto-asset sector and carefully reviewing any proposals from banking organisations to engage in activities that involve crypto-assets.”

As a relatively new area of regulation and with recent high-profile crypto disasters such as the [collapse of FTX](#), the past 12 months have provided a steep learning curve for regulators. The three agencies go on to say they “continue to build knowledge, expertise, and understanding of the risks crypto-assets may pose to banking organisations, their customers, and the broader US financial system,” and warn firms to take a “careful and cautious approach.”

The fallout from the [SPACs crash](#) which began unravelling in late 2022, will continue to be felt in 2023. In simple terms, SPACs (special purpose acquisition companies) are shell companies, created with the purpose of raising capital to purchase (or merge with) another existing company. They peaked in popularity in the final quarter of 2021, going from a record high of 613 (according to EY data) to just a fraction of that number in 2022. SPACs were popular because they allowed a company to go public much more quickly than a traditional IPO and with far less red tape. In late 2022 however, many investors

were looking to divest from SPACs, with at least 80 SPACs meeting with shareholders looking to cash-out (according to [Bloomberg](#).)

This was in part due to new rules proposed in March 2022 by the US Securities and Exchange Commission. Designed to “strengthen disclosure, marketing standards and gatekeeper and issuer obligations by market participants in SPACs,” they are likely to bring the SPAC process more in line with a traditional IPO, from a regulatory perspective.

Another kick in the teeth for SPACs has been the apparent problems with compliance emerging towards the end of 2022. “Failures of internal controls and poor bookkeeping practices, disclosed in quarterly reports over the past month, add more evidence for critics of special purpose acquisition companies, who say the trend has resulted in a large number of immature and potentially risky new listings,” said the *Financial Times* in December. A more recent [article](#) in the *Financial Times* reported the average loss for SPAC founders from liquidation has been US\$9m - and many investors have also suffered “bone-crushing” losses. This, say the authors, will likely lead to plentiful lawsuits in the coming months and years. “Aggrieved investors claim that SPAC founders had a conflict of interest in pushing through a merger, and as a result skimped on due diligence, inflated forecasts and failed to disclose important business risks.”

REPORTS CITED IN THIS ARTICLE:

[Control Risks: RiskMap 2023](#)

[Economist Intelligence Unit \(EIU\) Risk Outlook 2023](#)

[Eurasia Group's Top Risk for 2023](#)

[Protiviti: Executive Perspectives on Top Risks for 2023 and 2032](#)

[The World Economic Forum Global Risks Report 2023](#)

About Risk Universe Newsletter

RiskBusiness Newsletter provides in-depth analysis, reviews and research on areas of interest within the broader governance, risk, audit and compliance landscape, designed to provide proactive, 360° intelligence for informed decision making across the enterprise.

About RiskBusiness

RiskBusiness is an international governance, risk, audit and compliance (GRAC) solution provider, delivering risk content, risk intelligence, risk tools and risk advisory services to its clients. It is an association of like-minded industry professionals, who have the aim of furthering the risk management discipline to enable better risk-reward decision making.

Risk management is an evolving discipline, which has developed in close partnership with the industry. RiskBusiness has, both as individuals and collectively, a depth of established relationships with leading players and regulators in the operational risk field. We are also active participants in industry working groups and contribute thought leadership through publications and education.

RiskBusiness was founded in 2003 and today has principal locations in Birmingham, London, Buenos Aries, Amsterdam, Hong Kong, New York, Singapore, Toronto, and Zurich. To learn more, visit www.riskbusiness.com

Contacts

Carrie Cook, Editor:
carrie.cook@riskbusiness.com

General enquiries:
info@riskbusiness.com

RiskBusiness

www.riskbusiness.com