Risk publications

Risk

RISK MANAGEMENT • DERIVATIVES • REGULATION

Risk.net April 2022

Top 10 op risks 2022

Supported by

Baker McKenzie.

The top 10 op risks, reloaded

Survey to be expanded into semi-annual benchmarking exercise, writes *Tom Osborn*

You can plan a pretty picnic, but you can't predict the weather, as the Outkast song has it.

It's an often-heard frustration among operational risk managers that trying to anticipate when and how large losses will occur is extremely difficult.

In recent years, the industry has been encouraged to consider esoteric risks that might previously have been assigned a low or near-zero probability as part of routine stress-testing, including regulator-set exams – in other words, knowing what your exposures are and thinking about what losses would occur if there were a significant changes to your operating environment. (Or packing an umbrella or scoping out a nearby café, to torture the picnic metaphor in ways that Outkast's André 3000 and Big Boi never imagined).

Of course, whether firms choose to act on the outputs these exercises throw up – like the bank that built a stress scenario for a global pandemic two years before Covid-19 struck, before tearing it up, dismissing it as unrealistic – is another matter.

For more than a decade, *Risk.net* has tried to help guide op risk managers pool their collective insights as a list of shared concerns over broad categories of risk in the form of the Top 10 Op Risks.

The analysis that results is consistently the most popular piece of content *Risk.net* produces all year. Many of the world's largest banks say they spend time debating the survey as part of so-called external perspectives exercises, puzzling over the ranking of a particular category, asking whether they're paying enough attention to it and have enough internal expertise to respond appropriately if threats are realised.

But – as was the case with the advent of Covid – Russia's invasion of Ukraine, while not wholly unexpected, has also exposed the inherent limitations of the Top 10 as a static, point-in-time exercise. So the survey needs to evolve, too.

Later this year, we'll be getting in touch with respondents and asking for your input. How regularly should we run the survey: a semi-annual poll, to see how broad areas of concern to managers have evolved over the course of the year? Or a free-form exercise designed to identify emerging risks? What time horizon should we be thinking along?

Our ambition is to produce a more granular survey that provides a detailed breakdown of perceived threats, and discussions with op risk chiefs about how they're responding accordingly.

As with this year's Top 10 report, the analysis of the survey will be exclusively produced for *Risk.net* subscribers.

Read this year's top 10 operational risks on pages 4–10.

Baker McKenzie.

Emerging trends in op risk

Karen Man, partner and member of the global financial institutions leadership team at Baker McKenzie, discusses emerging op risks in the wake of the Covid-19 pandemic, a rise in cyber attacks, concerns around conduct and culture, and the complexities of geopolitical risk

What are the main regulatory trends and priorities we should expect as economies and markets emerge from Covid-19 pandemic-related restrictions?

Karen Man: The digitisation, sustainability, and environmental, social and governance megatrends have already been shaping the future regulatory environment prior to the pandemic, but the pandemic has accelerated them – the former by increasing regulators' expectations around the need for resilient systems and controls in the face of a faster adoption of digitised solutions. And the latter around new obligations concerning reporting, disclosures and governance on all aspects of sustainability, where the pandemic has been a catalyst for the awareness of the importance of sustainable – or resilient – operations.

In both cases, institutions are exposed to enforcement and litigation risk. There have been signs of an uptake in action, for example as a result of misconduct during the pandemic. However, we would expect that, in the short term, the extent of such actions is likely to be lower than after the global financial criss that began in 2007–08. This is because the expanded regulatory architecture put in place after this financial crisis has been successful in spite of stressed markets and the financial strain on the economy caused by Covid-19. However, we expect this endorsement will see regulators continue their current expansive approach over digitisation and sustainability megatrends, which is already translating into a tighter web of hard regulatory requirements – requirements that regulators will enforce and that clients will use as a launching pad for civil action.

What challenges do changing working practices present for firms in how they manage and monitor conduct and culture?

Karen Man: With the onset of Covid-19, there was concern that financial institutions might lose sight of the importance of culture as they were dazzled by stressed market conditions. This, against a backdrop of emerging conduct risks resulting from widespread home and remote working, gave rise to practical challenges of supervising staff.

In fact, a more complex and varied picture has emerged. On the one hand, many businesses have doubled down on facilitating healthy cultures out of a need to help their staff cope with the crisis, keep them operative and to reduce conduct risk. On the other, regulators have been concerned that extended homeworking has led to fewer 'watercooler moments' – informal social settings that facilitate the exchange of ideas and views among employees and, through this exchange, promote good grassroots culture.

Karen Man

What does it mean when regulators emphasise not just the 'tone from the top' but the 'tone from within' – referencing each individual's mind-set, preferences, beliefs, habits and predispositions? What we said last year still holds true: either you design a culture or you have one. This is especially relevant as businesses respond to the need to embrace diversity and inclusion (D&I) in their working practices and culture. D&I across firms is a key constituent of the tone from within and tends to pre-empt unhealthy subcultures.

Cyber risk and data breaches continue to appear regularly as one of the most costly sources of op risk losses. What measures can firms put in place to mitigate the impact?

Karen Man: Mitigate is the right word. Given the amount and value of the data firms hold, the number and sophistication of attacks will not recede. And, given the ever-increasing transferability of data across the extended enterprise, the 'outer skin' of financial firms and their inherent vulnerability will remain vulnerable. Accordingly, you will never stop all incidents, all the time. This means the response can only be to maximise resilience by identifying critical data and key vulnerabilities, setting tolerance levels and scenarios for disruption and, within those parameters, ensuring continued operability to the extent possible or ensuring a quick recovery. Prior to breaches, regulators will scrutinise your risk management framework where requirements have become tighter. After an incident, regulators will investigate whether firms responded efficiently and effectively. Key measures to ensure resilience include:

1. Mapping where data is held, what is outsourced to the cloud and who is responsible for it
2. Investing in security information management and event software
3. Having proper governance, reporting and supervision up to board level
4. Assuring third-party IT and data hygiene
5. Most importantly, fostering a compliance culture
6. Putting in place an effective incident response team, including forensic experts and legal counsel.

Where the response is a critical part of your resilience and mitigates your regulatory and financial exposure, the importance of this last point cannot be underestimated. It means early identification and assessment, promptly bringing the response team into operation. Legal requirements may mean notifying regulators, law enforcement and data subjects. Outside counsel will advise on the most effective ways to manage regulatory risks and help preserve privilege in the face of increasing civil litigation and threats of regulatory fines.

Increasing reliance on digital channels has placed pressure on legacy IT systems and infrastructure. What risks should firms pay most attention to as part of longer-term digital transformation projects?

Karen Man: Many institutions have found that replacing legacy infrastructures is associated with the highest failure rates. Unsurprisingly, they are reluctant to migrate to new systems when, despite much planning and preparation, there are so many problematic outcomes. However, there is no escape, as further patching over legacy infrastructures, alongside emerging technologies such as blockchain, artificial intelligence and machine learning, to deliver on cost reduction targets and client expectations on their digital journey will only exacerbate the propensity of the IT environment to costly failures.

Common risks to projects include external dependencies, tight deadlines or poorly defined goals, a lack of the right level of focus on legal and regulatory requirements around dataflows, and failure to break projects up into more manageable ones, not least to ensure proper implementation – particularly regarding data transfers into new systems.

What is the solution? Effective governance by senior managers, robust business continuity planning and, best of all, an emphasis on the importance of continuous investment and updating or replacing systems based on sound legal and regulatory advice paired with the right focus on implementation.

Decentralised finance and cryptocurrencies offer new opportunities for market players but have been associated with high-profile cases of fraud and money laundering. How can regulators strike the balance between innovation, protection and prudence in emerging technology?

Karen Man: When it comes to emerging technology, the US Securities and Exchange Commission recently said that the question for regulators was how to achieve their core public policy goals. Concerns around blockchain include consumer protection, financial stability and the risk of financial crime leading to market restrictions, if not outright bans. For a better balance, we need quicker and better regulatory catch-up that accommodates new technologies and facilitates business activity. We can see the positive effect of anti-money laundering controls on promoting market confidence. Regulators also need to revisit their mantras – as expressed by the UK Financial Conduct Authority: "Same risk, same regulation".

Applying existing requirements to new technologies, without making sufficient allowance for their difference in nature, can lead to an unintentionally tougher approach as many innovative products do not easily fit into existing regulation. This needs to change. We must get past the halo effect, which sees regulators fearful that regulation may confer a form of legitimacy and a false sense of confidence with the public. Nonetheless, when it comes to decentralised finance and crypto assets, the approach of authorities in certain financial centres is one of caution, rather than balance, and this is unlikely to change in the near future.

> "Diversity and inclusion across firms is a key constituent of the tone from within and tends to pre-empt unhealthy subcultures"

Which other op risks should financial firms have on their radar in 2022?

Karen Man: It's not surprising that, in current circumstances, geopolitical risk is identified as an emerging op risk for financial institutions, as of course it is for the wider economy. Both political and economic rivalry is increasing, as are disputes over sovereignty that risk impacting trade and investment. There are no easy answers to managing such uncertainties, but financial institutions must identify their vulnerabilities and assess the likely impact on their business models.

At the same time, we see sanctions being weaponised by states as instruments of policy. Businesses need to have the right systems and controls to effectively screen against sanctions lists and asset-freeze targets, as well as to identify when licences are required to permit activity otherwise prohibited. There are also obligations on firms to report known or suspected breaches of sanctions or asset freezes. Training needs to be put in place to facilitate this. Whether or not prohibited activity has taken place, firms and their management are at risk of legal and regulatory action when their procedures and processes are inadequate. We can be sure that regulators will have high expectations around compliance.

Top 10 operational risks for 2022

The biggest op risks for the year ahead, as chosen by senior industry practitioners

Welcome to *Risk.net*'s annual ranking of the top operational risks facing the financial industry, drawn from votes by heads of op risk, chief risk officers and senior practitioners.

Although the survey was run in the advent of Russia's devastating invasion of Ukraine, in a climate of rapidly deteriorating relations, many of the in-depth interviews with risk managers that follow were conducted once the invasion had begun – as reflected in the write-ups below.

The methodology remains unchanged: respondents are asked to list their five most pressing op risk concerns for the year ahead, which are then weighted and aggregated – but the results produced might not match many firms' risk taxonomies. The survey deliberately focuses on broad categories of risk concern, rather than specific potential loss events. It is inherently qualitative and subjective: the weighted list of concerns it produces should be read as an industrywide attempt to relay and share worries anonymously, not as a how-to guide.

As ever, *Risk.net* invites feedback on the guide and its contents – please send views to: *tom.osborn@risk.net*. ■

Profiles by Steve Marlin, James Ryder, Tom Osborn and Costas Mourselas.

A. Top 10 op risks 2022

	2022	2021	Change
IT disruption	1	1	←
Theft and fraud	2	4	↑
Talent risk	3	–	↑
Geopolitical risk	4	9	↑
Information security	5	2	↓
Resilience risk	6	3	↓
Third-party risk	7	5	↓
Conduct risk	8	6	↓
Climate risk	9	–	↑
Regulatory risk	10	7	↓

#1: IT disruption

Along with the human toll, the invasion of Ukraine is a salient reminder of the omnipresent danger of state-sponsored cyber attacks that aim to disrupt and disable IT systems.

As banks brace for an escalation in hacking attempts from Russia-linked groups, op risk managers have never been more aware of the hazards posed to their institutional infrastructure by malevolent actors.

Last year marked the first anniversary of the devastating Russian hack of SolarWinds, which is thought to have compromised US government servers as well as banks and other financial institutions.

Among respondents to this year's *Risk.net* survey of top op risks, an op risk manager at a Japanese bank says the thought of business disruption due to successful cyber attacks on financial market infrastructures or domestic internet service providers keeps him awake at night.

The head of cyber risk at a European bank says he also fears IT disruption from extreme cyber attacks or outages beyond his control. And his views echo those of the largest US banks, which voiced their fears to Congress in May.

Perhaps the danger of disruption is perennially top of mind for risk managers precisely because potential threats come from such a vast, amorphous number of sources. Concerns expressed this year range from faulty cables and backdoor threats in the Internet of Things through to runaway algorithms inflicting losses as banks explore ever more complex forms of machine learning in internal modelling.

Hardware failures can have unexpected ramifications, as those affected take desperate remedial action. In January, *Risk.net* blew the lid on a dispute that emerged over vendor strategy at DBS after it suffered a critical outage on its trading systems at the height of the Covid market panic.

New dangers on the horizon include the prospect that quantum computing could decode the current cryptography protecting data and other assets.

On top of that, the pandemic and trend towards hybrid working practices have only

B. Five IT failures in 2021

Date	Outage	Business line	Country
March 2021	Mizuho Bank data glitch, which closed about 80% of the bank's cash machines and lasted over 24 hours, originated from a failed data migration.	Retail banking	Japan
May 2021	Santander customers in Scotland experienced difficulty carrying out online and in-store card payment and were unable to use cash machines and online banking.	Retail banking	UK
September 2021	BBVA México system failure left more than 20 million users without access to cash machines and mobile app.	Retail banking	Mexico
October 2021	The Hong Kong Monetary Authority experienced business disruption after its Faster Payment System crashed and real-time fund transfers and registration of account proxy were unavailable for approximately five hours.	Retail banking	Hong Kong
November 2021	DBS Bank Singapore customers experienced a three-day outage, unable to access the bank's digital services.	Retail banking	Singapore

Source: ORX News

exacerbated the risk of IT disruption by providing more access points for failure or breach. With a majority of bank employees working from home, experts say the number of entry points for hackers has increased.

The head of op risk at a US financial services group tells *Risk.net* the failure of legacy systems and infrastructure can lead to downtime causing reputational and/or financial loss. Any changes to systems can have long lead times and be costly, she says – but if left unaddressed, the cost could be significantly higher in the long term.

"As companies look to decommission disaster recovery sites and transfer to hybrid models, have companies really considered all potential risks?" she asks.

In some senses, says the head of enterprise risk at a broker, IT system failures are the bread and butter of operational risk. "But what has made it bigger is remote working. There is more dependence on infrastructure. Remote working puts more pressure on our systems," he adds, rather than less. "What does that mean in terms of dependency on key systems?"

It is also noteworthy that technology and infrastructure failure represented the smallest subset of losses by broad category, according to ORX News's ranking of the largest publicly reported op risk losses of 2021.

But even where fines for outages aren't issued, the opportunity cost in terms of lost business and man-hours spent on repairs – not to mention the often severe damage inflicted in reputational risk – can be impossible to quantify. The table above shows five high-profile public tech failures from the last 12 months, compiled by ORX News.

#2: Theft and fraud

Theft and fraud risk jumps several places this year, to second – perhaps owing as much to the bulk of last year's largest op risk losses emanating from huge external frauds (see table C) as to the current state of roiling markets and their propensity to drive episodes of internal fraud.

Banks have good reason to fear a wave of ransomware attacks emanating from Russian state-sponsored cyber criminals targeting the theft of funds from banks and their clients. The FBI notes a strong correlation between economic sanctions and an increase in cyber theft with the aim of replenishing national coffers.

"The events in Ukraine have increased the likelihood of a sovereign state [cyber] attack, in retaliation for our retaliations," says one veteran op risk practitioner.

"Clearly, firms are constantly under cyber attack: there are nation states and criminal gangs trying to breach firms' cyber security, with stealing information or stealing funds in mind."

The single largest loss in 2021 occurred in a commodities market that Russia's invasion has sent into a tailspin – but the source of the loss was more mundane. It featured an alleged elaborate investment fraud centred on nickel trading in Singapore. In March 2021, the Monetary Authority of Singapore cited firms in the Envy Group – Envy Asset Management and Envy Global Trading – for their part in an investment fraud that amounted to $1.23 billion.

What banks and asset managers fear most in such cases is malicious external actors benefiting from inside help – something new hybrid working models make more likely, senior practitioners fear.

"We don't know some of the impacts on behaviours when massive organisations adopted a work-from-home model," says a senior op risk manager at one UK bank. "It's not so much that fraud is [more likely] during homeworking, it's more when people work from home, your controls may not be as effective as having people in the office."

C. Top five publicly reported fraud losses 2021

	Firm	Loss amount (US$)	Business line	Description
1	Envy Group	1.23 billion	Asset management	Defrauded of $1.23 billion by former director, involving fake nickel deals and forged contracts.
2	Westpac	255 million	Commercial banking	Exposed to A$341 million loss through Forum Finance leasing invoice fraud.
3	Sberbank	108.2 million	Commercial banking	Defrauded of 8 billion rubles through commercial loans to supermarket chain.
4	Sumitomo Mitsui	73.9 million	Commercial banking	Exposed to A$98.9 million loss through Forum Finance leasing invoice fraud.
5	Mercuria	36 million	Commercial banking	Defrauded of $36 million after purchasing warrants for copper replaced with painted paving stones.

Source: ORX News

#2: Theft and fraud

Lots of industry reports show losses were not materially higher during the pandemic, he adds, but "the expectation is the gestation period for transaction-style losses is relatively short": "But I think the experience of the industry is [that], for conduct-style losses, the gestational period is longer. It would be silly to claim victory too soon."

Other threats loomed closer to home: the largest op risk losses of 2021 occurred within the hinterland of institutional finance – the world of cryptocurrency trading – in which two mega-heists of more than $2 billion each at US-based BitConnect and Turkish platform Thodex topped the charts. Both thefts were allegedly perpetrated by the platforms' proprietors.

The pandemic has raised the risk of internal fraud. The Monetary Authority of Singapore has warned of the increased risks created by remote working, including lack of physical oversight, circumventing controls, collusion with insiders or external parties, and inappropriate communications with customers. MAS recommended banks conduct periodic reviews of remote-access activities – especially for staff in higher-risk functions, such as trading and client investment advisory – to identify any suspicious incidents and trends. It also recommended enhanced surveillance of trades, to ensure they were transacted in accordance with established procedures, and monitoring of keystroke logging.

#3: Talent risk

Talent risk re-enters the top 10 op risk list this year in explosive fashion, rocketing all the way to third place amid a fight for talent on Wall Street that's driving up pay and bonuses, against a backdrop of roiling markets, record profits, fears of burnout, and a need to attract and retain staff with wanderlust.

In a period when several of the world's largest banks and fund managers have seen veteran chief risk officers hang up their spurs, it's small wonder that the head of op risk at one large US buy-side firm says "human capital" is now one of his shop's biggest concerns for the year ahead. Failure to manage it appropriately could leave firms exposed at times of crisis, or widespread staff shortages due to Covid, he adds.

"The competitive environment for talent has never been greater: the 'great resignation' means many organisations are being challenged with retention, attraction and compensation of employees," he tells *Risk.net*.

The trend also extends to quant finance graduates, where starting pay among the top schools is rocketing amid a fight for the best and

brightest – something one master's programme director attributed to Goldman Sachs's move to offer students a higher starting salaries, which other dealers, including Morgan Stanley, were then forced to match.

"For me, the talent demand is inevitably a cost driver," says a senior op risk manager at a UK bank. "You clearly seek to be comparable from a compensation and benefits perspective, and put in place various plans for both retention and replacement – but every firm has [a] common management approach to recruiting and retaining talent."

But the risk is twofold: firms of all stripes say there simply aren't enough skilled employees to fill open vacancies in certain critical functions, particularly in first-line risk controls: that leaves open the danger that a "skills shortage leads to weak oversight of business operations, [particularly in] risk compliance personnel", says a senior risk manager at a Japanese bank.

Even the official sector is not immune: the *Financial Times* reported in December that the UK's Financial Conduct Authority was calling in consultants and external lawyers to fill staffing gaps, as it struggled to fill some 500 vacancies out of a total staff of 4,000.

Rapidly evolving regulatory and stakeholder pressures in areas such as climate risk can also create shortages amid pressure for specialised talent and the need to reassign staff from other functions.

One veteran op risk practitioner says turnover among key functions is their top op risk for the year ahead: "Demand for staff with specialised experience and technical expertise has required banks to increasingly focus on the recruitment, development and retention of key talent. Bank management teams should continue to monitor recruitment efforts and turnover of key staff positions."

#4: Geopolitical risk

Russia's invasion of Ukraine, with its unpredictable and far-reaching effects, poses a complex threat to the operations of financial firms. The chief risk officer at a large European asset manager succinctly sums up the impact of the conflict on his firm's operational risk profile: "We have [an invasion] in Europe. Not just small blips: things that move our business entirely."

The conflict propels geopolitical risk into the top five operational risks for the first time since 2017, when Donald Trump's presidential election victory and the UK's decision to leave the European Union brought politics to the forefront of risk managers' attention.

Geopolitical events pose direct and indirect risks for financial firms. Direct risks include the financial or physical consequences from nation state actors themselves. Indirect risks are the propensity for losses caused by mis-steps or malfeasance amid the economic chaos that follows.

In the case of the Russian invasion of Ukraine, concerns centre on supply chain failures and the effect on the global economy as energy and commodity prices spiral.

The headline risk of a rise in state-sponsored cyber attacks in response to sanctions is "a probability", says one head of cyber risk. Banks and other key financial institutions are among a range of natural targets for such activity. The day before Russia's invasion, Ukrainian companies were affected by malware believed to have originated from Russia.

However, the impact of global instability has wider potential ramifications for the threat profile of banks. "Geopolitical risk has a cyber element, but also supply chain and resilience elements too," the risk head says.

Within hours of Russia's invasion, the country was the subject of sweeping sanctions by the US, EU, UK, Japan and other countries.

Most painfully, Russia's central bank had most of its $600 billion in reserves frozen by the West, substantially limiting its ability to support the ruble, which has collapsed in value since the invasion.

Operational risk professionals also need to contend with the reputational risks associated with being seen as supporting the Russian state. In recent days, large companies from various industries have sought to sever connections with Russia. UK energy company BP hastily dumped its 20% stake in Rosneft, the Russian state-owned oil company, in a move that could cost the firm up to $25 billion. The decision indicates the lengths to which some companies will go to distance themselves from Russia.

Even if companies do not pull out of the country by choice, they could be the subject of severe retaliation by the Russian government. Societe Generale has said that it could be stripped of its Russian subsidiary, Rosbank, in tit-for-tat economic conflict, leading to a potential $15.4 billion hit to the bank.

#5: Information security

Information security risk slips to fifth place in this year's top 10 operational risk survey, having ranked second (as 'data compromise') in both the 2021 and 2020 editions.

Risks that were evident during the Covid-19 pandemic – including a rise in phishing attacks designed to exploit cyber vulnerabilities of home workers – have largely abated for financial firms. However, these tech-related risks have given way to another type of threat following Russia's invasion of Ukraine.

Respondents to this year's survey, speaking before the February 24 invasion, told *Risk.net* that a conflict would have significant implications for information security risk. Sanctions against Russia have raised the prospect of retaliatory hacking attempts by entities sympathetic to the Russian state.

Bank risk managers are focusing on how to protect the data that the institution holds, rather than plugging every possible entry point for attackers. Any data that is compromised must be quickly reinstated.

"We tend to think of cyber as intrusions and vulnerability. But the greater impact is how we deal with data that's been compromised and how we restore it," says an op risk executive at a large US financial institution.

Companies that experience data breaches usually see long-lasting impact. Hackers often try to install programs that allow backdoor access long after the initial breach has occurred. Firms need to detect and patch such vulnerabilities in the infrastructure.

As the head of cyber risk at one of the world's largest banks puts it, the focus is on making sure that the firm's "defence mechanisms" are up to scratch, and that its risk and control frameworks are joined up enough to catch any attempted breaches.

Firms must also consider the damage to their reputation from a cyber intrusion and subsequent loss of data. By far the biggest "risk factor and concern is on reputational impacts", says the head of cyber risk.

Still reeling from last year's multi-billion dollar losses following the default of a fund client, last month an anonymous whistle-blower provided data pertaining to some 30,000 Credit Suisse private bank customers to the German newspaper Süddeutsche Zeitung, including

evidence of alleged due diligence failures that allowed convicted fraudsters and criminals to store wealth with the bank.

Hacking attempts linked to Russian groups have recently affected financial firms. In October 2021, *Risk.net* reported on the ongoing impacts of the SolarWinds breach, which was attributed to the hacking group Cozy Bear, thought to be associated with Russian intelligence services. Financial companies insist that the attack has not compromised their systems over the long term. Cyber-security experts disagree, however, describing sophisticated re-entry methods employed by the hackers. A report by the New York State Department of Financial Services stated that almost 100 supervised companies had such entryways installed in their respective infrastructures.

Separately, the US Federal Reserve warned in October 2021 that looming changes in technology would produce new ways for information to be stolen from financial companies. Arthur Lindo, deputy director for policy in the board's supervision and regulation division, described the rapid growth of high-speed, internet-enabled mobile devices as an emerging source of risk for banks, providing cyber criminals with ever more options for ingress. Regulators would expect firms to be resilient to the changing terrain, he added, suggesting that artificial intelligence could be used to assist with breach monitoring.

For the chief risk officer at a European asset manager, an exponential rise in data volumes runs the risk of an unstable IT environment: "The sheer amount of data that is coming in puts requirements on what kind of systems we develop technology on, both in terms of hardware or cloud, but also for programming or accessing data. If this becomes unstable, we are sitting ducks."

#6: Resilience risk

Operational resilience – the ability to maintain critical business activities during a disruption – has been sorely tested since the start of the pandemic. Now, it is being put to the test once again, as the world nervously watches the unfolding horror in eastern Europe. Large-scale cyber attacks – or very real ones – are among the threats keeping resilience teams awake at night.

"It's moving so quickly," says the head of enterprise risk at a US investment firm. "Ukraine has crystallised resilience risk. With all the sanctions in place, we must take risk-based decisions on that basis. We're having to manage that risk as we speak."

The invasion of Ukraine has underlined the importance of maintaining resilient systems, but also the people and processes that maintain them, one senior market data manager at a European banknotes.

"As a result of nearshoring efforts, a significant number of banks have a lot of their back offices in places adjacent to Ukraine: Poland, Estonia, Romania, Hungary. It's something you don't [usually] pay attention to," he adds nervously.

Prudential Regulation Authority, London

The UK Prudential Regulation Authority's operational resilience principles require businesses to identify their key services and set impact tolerances – the maximum disruption the service could withstand without causing "intolerable harm" to clients or, in the case of larger firms, without posing systemic financial risk. The deadline for setting impact tolerances is March 31. Businesses will then have exactly three years to show the regulator that they can remain within those tolerances.

"The PRA is very proactive," says the head of enterprise risk. "Operational resilience in the UK is likely to spread to the rest of the world. You're losing staff, and meanwhile there's regulatory pressure to do more. That puts pressure on resources."

The US Federal Reserve's own resilience principles require firms to identify risks pertaining to business continuity, as well as recovery and resilience planning. The firms then have to incorporate these risks into "severe but plausible" scenarios outlining the impact of risk events on their critical operations and core business lines. Rather than prescribing scenarios, the Fed expects each firm to design its own scenarios that can then be used to test the business's tolerance for disruption.

"We need to increase tabletop exercises and rethink continuity management," says an operations executive at a US bank. "We need to create better connectivity to bring alignment with respect to critical applications and critical third parties."

Photo: James Oxley/Bank of England

Prudential Regulation Authority, London

The impact of the moves by the UK and US regulators is being felt throughout the financial services industry, where business continuity teams are making the transition into becoming resilience teams. These new teams are being challenged to think more broadly and to come up with precise measures of resilience, such as the time needed to get systems up and running after an outage and the maximum level of acceptable data loss. The ability of businesses – and perhaps the financial system as a whole – to continue functioning will depend on their success in doing so.

#7: Third-party risk

Universal banks are the equivalent of the Swiss army knife, offering something to everyone. But even the largest rely on outside help to provide some of their services. In fact, the bigger the bank, the more third-party relationships it tends to have. And third parties bring extra risks.

European Union regulators have stressed the importance of third-party risk management to a company's operational resilience. They note that it is hard for a firm to demonstrate thorough and proportionate risk management when it has outsourced a large number of operational tasks.

New guidance proposed by US prudential regulators also makes it clear that although banks can outsource administration of their operations, they cannot outsource the risks. Instead, they need to establish sound risk management practices for overseeing external providers. These should be commensurate with the criticality of the services provided by the third parties.

However, the proposed guidance does not distinguish between different types of third-party services. As an example, cyber-security experts say the use of cloud providers presents unique risks, including disruption from key supply chain entities and potential concentrations with individual providers.

"Concentration risk and the ability to transfer at short notice to another provider are a major concern," says a senior operational risk executive at a European bank.

A key problem with shifting services to the cloud is that a grey area often exists in the functions that banks will continue to perform in-house and those that are outsourced to the cloud provider. Any uncertainty in the delineation of responsibilities between bank and vendor can lead to costly mistakes in how systems are set up. It can also spark lengthy contract renegotiations.

"Concentration risk and the ability to transfer at short notice to another provider are a major concern" *Senior operational risk executive at a European bank*

A typical area of confusion is in the shared-services model. Here, the cloud vendor is responsible for security of the underlying architecture, while the customer must ensure that its own systems are configured securely within the cloud. Customers often misunderstand this dynamic, vendors complain. Cracks in the relationship between bank and vendor can open the way for cyber breaches and expensive losses of data.

Banks are asking US regulators to provide more detailed guidance on the risks posed by these providers, including 'the big three': Amazon Web Services, Google Cloud and Microsoft Azure. The Federal Reserve has

previously voiced concern that overreliance on tech giants could place the financial system at risk in the event of an outage or service disruption. However, the regulator is understood to want the banks themselves to identify and manage the risks inherent in these relationships.

There is also a widespread acceptance that cloud services have to be fully integrated across the whole of a firm, including its subdivisions. "We are entirely dependent on these things working together," says the chief risk officer at a European investment firm.

#8: Conduct risk

Conduct risk falls a few places in this year's top 10 – perhaps owing to a lack of mega fines making it top of mind for respondents. Publicly reported op risk losses stemming from failings related to clients, products and business practices halved to €5.7 billion ($6.3 billion) last year, and, while losses from internal fraud held steady at €4.8 billion, that tally remains a fraction of the ugly multi-billion-dollar losses from fines and settlements for wrongdoing witnessed in years past.

But op risk managers warily eyeing the global economy's slow recovery from Covid and the invasion of Ukraine have seen this movie before. Times of great economic disruption and physical upheaval are breeding grounds for misconduct – ones that invariably take time to come to light, before the perpetrators can be brought to book.

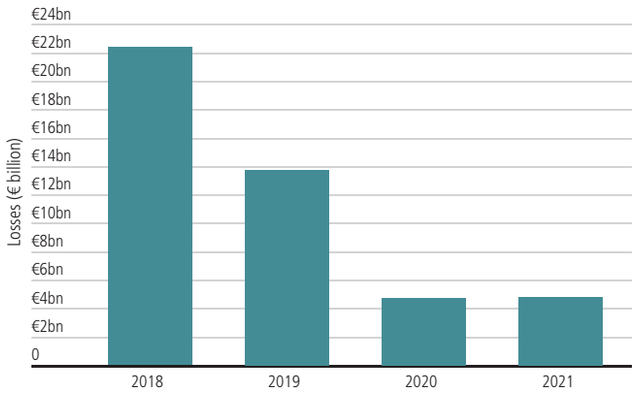
"We've had the pandemic: we've had two years of people working from home, doing God knows what – doing what they might not have been able to do in an open-plan office," says one veteran op risk executive. "So, I think there is potential for conduct risk events taking a while to crystallise. If there has been mis-selling, for example, that is unlikely to crystallise in the next 12 months. If it's something big, we will see that in two or three years' time."

The big fear talked of quietly among banks since the early days of the pandemic is a mis-selling scandal concerning hastily written Covid loans – something many warned regulators about in the advent.

The UK's bounceback loan scheme alone extended nearly £50 billion ($66.7 billion) to borrowers – as much as a 10th of which may have gone to fraudulent applicants, government auditors estimate. Banks blame the speed at which they were forced to roll out the loans, with many insisting privately that promises of indemnity made when concerns were aired must now be honoured.

Other Covid-era losses are likely to follow a familiar pattern: rogue trading stemming from front-office staff finding it far easier to collude with one another outside the normal working environment remains a risk, as do desperate decisions made by people to cover losses amid whipsawing markets. US regulators are understood to be probing the conduct of banks during their exit of positions from Archegos, the family office that blew up spectacularly a year ago.

1. Publicly reported internal fraud losses 2018–21



Source: ORX News

The long legacy of the Libor scandal and the ongoing shift to new rate benchmarks continue to pose a risk for banks. Dealers freely admit they are reliant on clients to self-police when it comes to observing US regulators' ban on trading most instruments that reference legacy dollar Libor.

Elsewhere in markets, heated debates over the practice of pre-hedging during 2021, in which financial firms attempt to create offset positions for client trades before the trade is actually executed, described by critics as akin to frontrunning.

The consequences of such conduct can take a long time to crystallise. Citi, for instance, was struck with a $44.7 million fine by the Securities and Futures Commission of Hong Kong, which found that Citi staff had repeatedly misrepresented certain stocks to institutional clients to encourage trading activity as early as 2008, and highlighted "serious and systemic" lapses in the bank's controls frameworks. The regulator's chief executive officer, Ashley Alder, described the firm as home to "a culture of dishonesty", which "encouraged chasing revenue at the expense of basic standards of honesty".

#9: Climate risk

Climate risk appears in *Risk.net*'s annual survey for the first time this year, as regulators and financial firms alike attempt to grapple with a daunting gamut of potential op losses stemming from the physical and economic ramifications of anthropogenic climate change.

But while the former could take years or even decades to crystallise, plenty of the latter are already staring banks and fund managers in the face. One op risk manager rates the threat of climate litigation from investors and other stakeholders over claims of greenwashing as significant for his firm in the next 12 months.

The cornerstone of banks' first line of defence against such losses will be a strong controls framework. Goldman Sachs, among other banks, is working to hardwire climate risk controls into its framework – for instance, an otherwise healthy borrower's business model becoming challenged by emissions targets or divestment from shareholders – via integrated assessment modelling and scenario analyses.

Once the potential impacts are evaluated – an evolving process as more firms become subject to disclosures – the bank's risk teams set tolerances for key business areas such as lending and financing.

#9: Climate risk

Yet such actions remain difficult while the true scale of risk remains effectively unpriced by markets, risk managers argue. When it does, a reckoning will come. As surely as tock follows tick, economic shocks are heavily correlated with op risk losses – both their capacity to exacerbate existing losses as well as leading to the uncovering of historical failures and inappropriate responses, as Michael Grimwade, head of op risk at ICBC Standard Bank notes.

Delay and deferral of meaningful action among legislators also increases the regulatory risk of hasty or ill-thought-through action from policy-makers later on, finance professionals argue, pointing to key transitions such as the introduction of mandatory carbon pricing having the potential to cause significant price shocks across a range of asset types.

On the buy side, managers report confusion over how to designate their funds under the EU's Sustainable Finance Disclosure Regulation (SFDR), which came into force in 2021, and align compensation incentives with environmental, social and governance (ESG) objectives.

"We are hiring more people to follow what is being required under SFDR, and spending a lot of time to be compliant. We are struggling to incorporate this concept into our data, our limits, how we trade, how we report, which determines how we have done business," says the chief risk officer of a large European investment firm.

Still, this op risk's relatively low entry point on this year's leader board perhaps illustrates a widely held attitude among finance professionals: that climate risk proper has not yet 'arrived' in a tangible sense. Indeed, one operational risk manager describes climate risk as a serious concern – but one that wouldn't make it into their top five risks for the year, since they do not expect it to become a material concern for banks in 2022.

#10: Regulatory risk

Regulatory risk – the risk of noncompliance stemming from the magnitude of changes to rule sets and supervisory expectations – is a perennial feature of the Top 10. The potential to incur hefty fines and penalties, not to mention the enormous resources required to stay current with regulations, comes up in nearly every conversation with op risk managers.

European regulatory dissonance on everything from the supervision of central counterparties to the implementation of Basel III also increases the risk of noncompliance and makes for an overly complex, needlessly costly operating environment, banks complain. To say nothing of the seemingly permanent transatlantic schism in supervisors' attitudes towards internal modelling.

Risk managers also cite model risk as a continuing area of focus by regulators in the wake of the pandemic, when risk models for financial crime and credit risk were thrown off course because they were unable to anticipate sudden changes in consumer behaviour and the impact of government stimulus programmes. Managers are struggling to validate their models, especially those sourced from external providers.

"There's a lot coming from the regulatory front on model bias, with algorithms having to be documented. That presents challenges because models may be easy to identify, but are very hard to validate, especially when the product may not be yours," says the head of enterprise risk at a US financial services firm.

> "Models may be easy to identify, but are very hard to validate, especially when the product may not be yours"
> *Head of enterprise risk at a US financial services firm*

By its nature, regulatory risk is continually evolving: in a regulatory first in December, the UK's Financial Conduct Authority sued NatWest in a criminal court for £269.5 million ($360 million), including a fine of £264.8 million, over anti-money laundering oversight failings. The settlement was the fourth-largest loss of the year.

Compliance with a raft of new environmental, social and governance risk has been cited as one of the top regulatory risks this year (see *#8: Climate risk*).

On the buy side, the chief risk officer of a large European asset manager cites the EU's Investment Firm Regulation, which came into force in 2021, as a major headache. The rules could result in greater regulatory scrutiny of how firms manage various operational risks. Capital will be calculated using K-factors – business activity metrics designed to measure potential harm to clients, to markets, and to the firm itself. Larger managers say Pillar 2 capital – the firm's own assessment of capital needs – will still be the more significant demand, but firms holding greater amounts of client money could see a hike.

Baker McKenzie.

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 70 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

bakermckenzie.com/financialinstitutions