THE RISK REGISTER

Scanning the risk radar

In a volatile world fraught with geopolitical tensions, environmental concerns and financial crises, the role of the chief risk officer has never been more pivotal.

When the midnight bells ring out the old year and herald the new, it is traditional to look forward to the opportunities and new adventures that lie ahead. Inviting chief risk officers (CROs) to the party might dampen the optimistic mood – after all, they get paid to anticipate dangers and threats. There were plenty of those in 2023: the continued conflict in Ukraine, the escalation of the Israel-Palestine conflict, adverse weather events due to climate change, and economic uncertainty.

The World Economic Forum (WEF) released a survey last July identifying other factors such as supply chain and pricing disruption, regulatory changes and enforcement and even ethical risks from the adoption of AI that could "threaten economic growth, destabilise global markets and disrupt business operations". The WEF described these risks as a "polycrisis", whereby several global risks have a compounding effect on each other.

So, where do CROs in the banking sector see the greatest risks? What is jumping off the pages of their risk registers for 2024?

No room for complacency

As outlined in the WEF survey, CROs are concerned that geopolitical events such as the Russian invasion of Ukraine could lead to a new energy crisis, increased control over critical industrial inputs and further disruption to supply chains and prices for commodities such as fuel. The survey also highlighted risks from strikes and riots within domestic borders.

"CROs in major international banks will be worrying about and planning around risks such as an escalation in China/Taiwan tensions and the resilience of US commercial real estate given the scale of debt in that market," predicts James Royle, Chief Risk Officer, Recognise Bank, a UK-based challenger bank.

"We are more focused on the UK economy and the outlook for our domestic SME customers. Those global risks would clearly have an impact, such as disrupting supply chains and prices, so it is something we have to keep an eye on. But they are less of a direct exposure risk."

> **"In periods of global conflict like this, we get waves of inflation. It may be easing now, but it has not passed us yet because there is so much uncertainty around the direction of those conflicts."**
>
> Nigel Williams,
> CRO, Commonwealth Bank of Australia

Royle also highlights credit risk in the current tough economic climate. "Because we have been through such a benign economic cycle with low interest rates and levels of defaults, it is easy for some people to become complacent about lending," he says. "However, following the events last year [increased inflation and interest rate hikes] it is certainly higher up on the agenda now."

Nigel Williams, CRO, Commonwealth Bank of Australia, warns that, although markets there are becoming more comfortable with inflation outlooks and domestic household budgets and spending are holding up well, people need to be aware of history.

"History tells us in periods of global conflict like this, we get waves of inflation. It may be easing now, but it has not passed us yet because there is so much uncertainty around the direction of those conflicts," he says. "In addition, there are major elections in the US, UK and India this year. The outcomes of those may surprise us resulting in new

policy changes and impacts on trade and supply chains. It is getting harder to predict where commodity markets will go."

Williams says that the bank is also increasingly focused on financial risks with expectations that a squeeze on Australian household spending may come this year. "We started looking [at this] about 18 months ago, with the rise in interest rates and potential impact on consumer spending. That impact in Australia is still to come through," he says. "Households have been very resilient by reducing their discretionary spend. That will flow through to the business sector this year."

Operational resilience

UK regulators – the Financial Conduct Authority and the Prudential Regulation Authority – have launched a consultation process on the risk of financial services firms using third-party services to support their operations. As per a 2023 report, regulators want to "manage risks to the stability of, or confidence in, the UK financial system that could arise from a failure in, or disruption to, a critical third party's services".

Royle continues: "For a small bank like us, this can be a challenge because one of our advantages is that we don't have the legacy infrastructure systems that our bigger rivals do. We don't have a big technology stack that we own. We tend to outsource and rely on third parties that provide great technology, agility and efficiency. But when we rely on third parties to provide services, such as payments, then we need to understand their risks, key vulnerabilities and single points of failure. CROs have to get comfortable with that."

Within that, Royle adds, there are risks around the use or misuse of data by banks and third parties when it comes to developing automated systems. "When we start using ML in areas such as financial crime screening, then we have less control and less visibility. What is going into the models? What is the governance around those? What are the assumptions they are built on? That becomes harder to understand," he says.

Indeed, the WEF also highlighted concerns among CROs about the ethical and social risks of AI development and deployment. CROs believed that AI was 'outpacing' management of these risks and there was a lack of understanding about the pace of change and the implications of it.

"AI is a sexy subject that many people talk about but don't really understand how it works or whether it will be a risk or a support to banks," says Christian Garcia, CRO, Gibraltar-based Trusted Novus Bank. "We haven't incorporated any AI solutions, but some of the bigger banks are already counting on it operationally in some areas. Managing these technologies in the future and not jumping into them too quickly will be important."

Donna Francioni, CRO, Kroo, also has maintaining operational resilience high up on her risk register. "FIs rely on their network of partners and third-party operators to make sure their services are running smoothly, any disruption in their services could have a cascading impact on the overall customer experience," she says. "Our focus should lie on reducing and preventing serious harm, setting and testing higher standards, and promoting competition and positive change."

Garcia says regulators believe that banks are not performing enough due diligence on their outsourcing partners. "They are expecting more focus on making sure that enough vendor research is being done upfront before suppliers are selected."

THE RISK REGISTER

Hot topics

Regulatory pressures were highlighted as a key risk by Garcia. "Since Brexit, from a regulatory perspective, there has been a lot of repatriation from the EU into our own local regulations," he says. "That transition, and associated risk, is still happening."

He also raises the "continuous motion" of the Basel framework including Basel 3.1 which will "change how various aspects of risk will be calculated and monitored both internally and by the regulators".

He adds that the FCA's Consumer Duty rules are also a very hot topic in the UK and in Gibraltar where it is relevant to firms which provide financial products or services to retail customers in the UK. He says: "Banks need to consider how they approach and treat customers in certain situations. They also need to be well prepared to provide services to vulnerable clients and ensure that they are not impaired. That is a huge topic for 2024."

Although not new, Garcia is also keen to keep an eye on anti-money laundering (AML) trends and activity. "Gibraltar is at the entrance of Europe geographically. If we are not well protected, it could be a soft spot for activity such as smuggling. The Gibraltar government is always at the forefront of regulatory initiatives around AML, fines and deterrents," he says. "So, keeping on top of sanctions lists and ensuring they and lists of high-risk countries are kept up to date is crucial. It is also important to keep a tab on politically exposed persons. These risks are always hot for us."

Cybersecurity innovations

According to the 2023 IBM *Cost of a Data Breach* report, the losses incurred by financial organisations amount to approximately US$5.9m per cyber incident. The cost includes paying ransoms to criminals to unlock systems and restoring infrastructure after an attack. Only the healthcare industry suffers higher losses.

High-profile cyber incidents in 2023 included a ransomware attack on the US financial services division of Chinese banking giant ICBC and the European Investment Bank.

"As fraudsters continue to adapt and leverage new technologies, regulators and FIs need to remain vigilant to stay one step ahead of these evolving threats. Strengthening cybersecurity measures and investing in advanced fraud detection technologies will be essential in ensuring customers' money remains safe," says Francioni.

For Williams, cybersecurity and financial scams is number one on his risk list. "Cyberattacks run the risk of undermining trust in institutions," he states. "In addition, I am concerned about the impact of financial scams on our customers, so helping customers to avoid them is an incredibly important issue for us."

Williams says financial scams are becoming more significant and sophisticated, such as social media messaging with the extraction of the proceeds from these schemes going through both bank and non-bank payment companies.

"To disrupt the impact of scams we need to take a whole-of-eco-system approach, including all of the participants in the financial system, social media firms and telcos. We've worked with telcos, for example, to utilise their fraud detection data to shut down scams more quickly," he explains. "We have also used AI over the past 12 months to improve our scam detection. In addition, we are sharing some software with smaller banks to help them disrupt scams and prevent customer harm."

Garcia also puts cybersecurity in his 'top three' of risks, namely managing and mitigating threats from phishing attacks, unauthorised access or data breaches. "The PR repercussions for the bank are huge," he admits. "It can also be an expensive risk to mitigate because of the technology required and cyber insurance. It is important that the insurance is tailored to the risks you are facing or exposed to given your geography, type of business and technology you offer. The more technological an organisation, the more exposed it is. The perpetrators learn quickly, and it is always a race to keep at the forefront of the technology and skills."

Many CROs come through traditional routes such as credit and operational risk roles. However, they are increasingly having to add these new skill sets around digital technology and security. "You can have the best systems in the world, but you need to educate and train yourself and colleagues throughout the whole organisation on how to effectively use them to prevent cyberattacks," says Royle. "The weakest part of IT security is people. The reputational impact, the time and the cost of a cyberattack could far outweigh typical credit losses."

From climate change to diversity

Risks from continuing climate change include the impact adverse weather events are having on food and water supply and security. Banks and their clients also face increased scrutiny on their ESG impact, reporting, services, products and policies.

"In Australia, given the risk of bushfires, cyclones and flooding, we are very focused on the impact on our consumers, both the practical effects and the cost of insurance," explains Williams. "Consumers are really seeing the cost of climate change now through higher premiums or higher energy costs to fund the transition."

Royle of Recognise is keen to highlight the often-overlooked social and governance elements of the ESG term. A particular focus is on diversity and inclusion (D&I) in a bank's leadership team both in gender and ethnicity. "That is a big challenge for the banking sector," he says. "Without it, the diversity of thought and approach gained from people from different backgrounds are lost. Customers also want to see themselves reflected in the companies they deal with."

Garcia adds: "Investors in the future will not only be interested in knowing typical yields but carbon-credit scores of individual securities. It means banks have to provide that new information and research to investors."

A matter of balance

Securing skills and talent is, Williams says, often seen as a risk by banks but not, it seems, at Commonwealth Bank of Australia. "Organisations that invest in skills, data and AI – as we have done – continue to attract talent. It is not a negative risk for us.

"It is important to look at the opportunities that can emerge from risks. For example, with AI it is not about putting on a black hat and saying it is risky. It is how can we use it in an effective way that can set boundaries on risks and is good for our customers. The CRO needs to provide that balance." CB

“The more technological an organisation, the more exposed it is. The perpetrators learn quickly, and it is always a race to keep at the forefront of the technology and skills.”

Christian Garcia,
CRO, Trusted Novus Bank