Risk publications

Risk

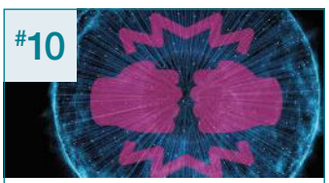
RISK MANAGEMENT • DERIVATIVES • REGULATION

Risk.net March 2020

Top 10 op risks 2020

Supported by

Baker McKenzie.



Top 10 op risks 2020

The biggest operational risks for 2020, as chosen by industry practitioners. By Tom Osborn

Supported by

Baker McKenzie.

Welcome to *Risk.net*'s annual ranking of the top op risks for 2020, based on a survey of operational risk practitioners across the globe and in-depth interviews with respondents.

As in years past, there's no great secret to the methodology: *Risk.net*'s team gets in touch with 100 chief risk officers, heads of operational risk and senior practitioners at financial services firms, including banks, insurers, asset managers and infrastructure providers, and asks them to list their five most pressing op risk concerns for the year ahead. The results are then weighted and aggregated, and are presented in brief below and analysed in depth in 10 accompanying articles.

As before, the survey focuses on broad categories of risk concern, rather than specific potential loss events. The survey 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.

For a note on the impact of the coronavirus, see the final chapter, geopolitical risk.

Risk.net invites feedback on the guide – please email tom.osborn@infopro-digital.com with any views.

Profiles by Costas Mourselas, Steve Marlin, James Ryder, Alexander Campbell and Aileen Chuang

A. Top 10 operational risks 2020

Operational risk	2019	Change
#1 IT disruption	2	↑
#2 Data compromise	1	↓
#3 Theft and fraud	5	↑
#4 Outsourcing & third-party risk	6	↑
#5 Resilience risk	–	New entry
#6 Organisational change	4	↓
#7 Conduct risk	10	↑
#8 Regulatory risk	7	↓
#9 Talent risk	–	Re-entry
#10 Geopolitical risk	–	Re-entry

#01 IT disruption

Risk of downed systems, from hack or outage, continues to make op risk managers fret

When bank customers are suddenly unable to access their money because of a paralysing cyber attack or a critical IT systems failure, the consequences for bank profitability and reputation are clear.

Respondents to this year's *Risk.net* survey of top op risks report a two-pronged risk to systems and IT operations. First, the threat from hostile hacking groups and even nation states laying siege to a bank's defences: breach attempts only have to be successful once to sow widespread chaos. Second, banks must upgrade or patch ageing IT systems to stay competitive, and in doing so they can expose themselves to cyber attacks or good old-fashioned outages.

"Whenever I talk to my cyber guys, they say the threats are evolving, becoming more clear about where they target," says the group head of operational risk at a European bank.

"Cyber attacks lead to significant reputational damage, particularly from retail customers," says the head of operational risk at another European bank.

In this year's survey, IT failure has been considered alongside IT disruption, where last year the categories were considered separately. Although the drivers and risk management of the issues are very different, the consequences – the loss of critical services leading to parts or all of an organisation being unable to function – end up looking much the same.

Both concerns also feed into resilience risk, which considers the consequences of an outage or failure in the context of changing regulatory expectations around how and when a firm can return to operations, as well as the consequences of that outage for other firms that depend upon its services, and the role it plays within the financial system as a whole. IT failure specifically addresses the opportunity cost of failing to do business and the consequences, including permanent damage to a firm's reputation, which can last well into the future.

In the US, the FBI's internet crime complaint centre recorded 467,361 complaints in 2019 leading to losses of $3.5 billion, up from 351,937 complaints in 2018 for losses of $2.7 billion.

"It's no longer just how long the outage is, but also very much how the public perceives the outage. Banks have to respond very quickly, and in a way that does not open them up to liability"

Shresti Bijou, FirstRand

The hacking of retail foreign exchange services provider Travelex in December highlighted the grave risks posed by well-executed cyber attacks. The firm was forced to shut down its online currency services for several weeks, with client services by HSBC, Royal Bank of Scotland, Lloyds and Barclays all affected.

The Travelex incident shows how an outage at one firm can affect business operations at others. A bigger fear is for a cyber attack to spread to the IT systems of multiple connected banks, as a February report by the European Systemic Risk Board shows.

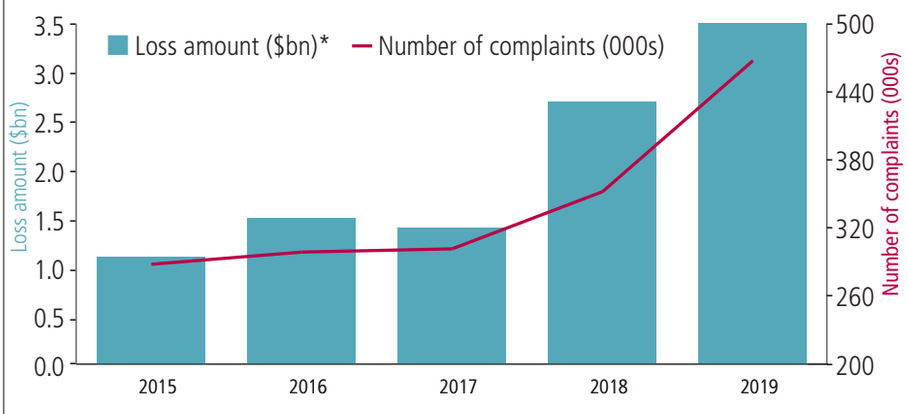
The ESRB, like the Federal Reserve Bank of New York, argues that systemic risk can emerge when an outage turns into a liquidity crisis, shattering confidence in the financial system. A smaller-scale but carefully targeted cyber attack could therefore have widespread implications for markets. For example, if a global systemically important bank was unable to process outgoing payments, other banks would fall below their normal reserve levels.

Another target could be systemically important financial market infrastructure providers (FMIs) such as clearing houses and settlement providers, on which the functioning of many markets depends. The chief risk officer of one of the largest FMIs tells *Risk.net* he spends most of his time worrying about non-default risks, and that he's "particularly worried" about risks stemming from cyber attacks.

Several survey respondents linked geopolitical instability to the heightened risk of cyber attack. For example, the US administration's sanctions regime has spurred target countries to respond with cyber crime, says Richard Jacobs, the assistant special agent in charge of the counterintelligence cyber division at the FBI.

"There are countries that are very strapped financially as a result of sanctions," he said during

1. Internet crime reports received by FBI



*Rounded to nearest million.

Source: FBI

#01 IT disruption continued...

a speech at the Risk USA conference in November. "And they are literally engaging in massive cyber crime similar to any financially motivated criminal: for money, and that is to fund their coffers. We're dealing with a lot of very sophisticated actors conducting cyber crime on behalf of government entities for that purpose."

IT failure

However, systems collapses don't have to come from cyber criminals: human error and outmoded hardware and software can pose as great a threat.

Hong Kong Exchange had to freeze futures trading in September from 2pm until the following day because of a software bug. The inability to continue supplying data related to futures meant issuers struggled to price its most popular retail derivatives contracts, significantly impeding hedging activity.

Several clearing houses last year suffered minor operational failures, but critics point out that there isn't a standardised framework for recording these outages. As a result, certain failures may not be reported and known by the market.

Research published in the *Journal of Operational Risk* last year argued that cyber risk modelling needed significant improvement. Of 341 loss events from 2009 to 2017 recorded by ORX News, only 103 provided data on the size of the loss.

Separately, respondents refer to ongoing digitalisation efforts by many large banks, and highlight that the process of change can result in outages or expose critical flaws. These changes can include adapting to artificial intelligence and blockchain solutions, or overhauling the retail-facing online business of the bank.

One former chief information security officer at a large financial institution says challenger banks have a significant advantage over modern ones when it comes to IT disruption risk, as they have been able to construct the bank on more modern, robust systems.

"Our outward-facing platform for retail customers, including the mobile app, looks great," says the head of operational risk at the European bank. "However, there is a lot of underlying legacy infrastructure that is a work in progress. There are vulnerabilities there, and that's our main concern."

Social media, too, can amplify issues in the eyes of customers and turn a minor outage into a PR nightmare.

"We have seen some banking platforms go down for an hour, and retail clients are very quick to revert to social media without going straight to the bank," says Shresti Bijou, group head of operational risk management at South Africa's FirstRand. "It's no longer just how long the outage is, but also very much how the public perceives the outage. Banks have to respond very quickly, and in a way that does not open them up to liability."

In the face of increasingly sophisticated cyber attacks, the US Federal Reserve is mulling whether to compel financial firms to submit data on cyber incidents. Banks have traditionally been nervous about sharing information about cyber threats, and sources worry that information could leak out, painting a bullseye on other firms.

"If you are part of a closed group and nothing leaks out, that would be hugely beneficial," says Andrew Sheen, a consultant and former operational risk executive at Credit Suisse. When information leaks, "cyber criminals just move on to someone else".

But one senior op risk manager suggests that sharing as much information as possible is the right approach.

"We have constant discussions with other banks on industry committees because we really believe that to mitigate cyber risk, there is no point taking a siloed approach," the manager says. "It's a severe risk that the industry as a whole faces."

#02 Data compromise

Hackers, thieves and wobbly in-house data management keep this category near the top of the list

Sitting atop a trove of personal data, banks make tempting targets for hackers looking to make mischief, criminal rings out to collar data for cash, even cyber terrorists bent on holding banks to ransom.

While the operations and reputation of any bank hinge on accurate and secure data, the possibility of breaches, disclosure or destruction of information seems to be growing. A handful of expensive and embarrassing incidents in the past year highlight the threat, with assailants relentlessly probing for chinks in bank cyber defences.

"The threats continue to evolve. You have an increased need to be in front of it," says an operational risk executive at a large North American bank. "We saw the big Capital One breach, so it's certainly not going away."

Last July, Capital One, the US credit card giant, said a hacker had penetrated the bank's firewall and got hold of the personal data of 100 million credit card applicants as well as 140,000 social security numbers and 80,000 bank account numbers of existing credit card customers. The incident would cost Capital One as much as $150 million in customer notifications, legal fees and technology upgrades, it said.

In this year's Top 10, data management, a discrete category in previous top 10 lists, has been folded into data compromise to form a single topic. Although the causes and preventions are different – one requires protecting a firm's data from external malicious attack, the other the risks of mismanaging or mislaying data internally – the financial and reputational harm can be the same. Last year, data management was eighth on the list.

Banks face an uphill battle in protecting their data. In a March 2019 report, cloud security provider Carbon Black said 67% of surveyed financial institutions had reported an increase in cyber attacks in the previous 12 months, and 26% had been targeted by "destructive" cyber incidents, that is, intrusions that destroyed data.

Several factors are at play. The sophistication of attackers is on the rise. Some may be part of state-sponsored cyber terrorism rings, which can become more volatile in uncertain global times. Others are ordinary criminals seeking to peddle the information for profit.

#02 Data compromise continued...

"What I really worry about is someone taking critical customer data and putting it on the dark web," says an operational risk executive at a North American bank. Some banks have proactively sent ethical hackers on to the dark web to detect attacks and assess threats.

At the North American bank, the approach to preventing breaches is twofold: it has put in place advanced controls on the most sensitive data and is educating employees on good practices, some as basic as how to recognise phishing to keeping up with the latest software patches. The bank has also begun monitoring employees with access to critical data, including IT teams.

> "What I really worry about is someone taking critical customer data and putting it on the dark web"
>
> Operational risk executive at a North American bank

Not all intrusions are virtual, and some are inside jobs. Just last month, Fifth Third Bank said several former employees had manually stolen the information of around 100 customers and shared it with a fraud ring. The bank underscored that the theft was not a cyber breach, "but rather an orchestrated effort by a small group of employees to steal personal information".

In yet another old-school theft, last September Allianz Global Assistance, the travel insurance arm of Allianz, said a safe containing backup magnetic tapes was stolen. Initially, the insurer said 260,000 customers who had purchased roadside assistance had been affected, but it later emerged that more than 2 million customers who had purchased assistance indirectly through car manufacturers were also exposed.

The other side of data compromise is in-house management. Last year, UK authorities fined Goldman Sachs and UBS millions for transaction reporting lapses, while Citi was penalised in the US for prudential reporting lapses. Data mismanagement underpinned all these cases.

"Fines tend to be imposed for repeated and systemic failures. To avoid being fined, banks need to periodically test that their reporting logic is correct and that trades are correctly flagged and that all relevant trades are flowing into their reporting engines," says an op risk executive at a global bank.

The fines for UBS and Goldman were for legacy issues under Mifid I, which was supplanted in 2018 by Mifid II, which banks claim is unduly burdensome. They are lobbying for revisions in the European Union's targeted review, such as altering the scope of transparency for over-the-counter derivatives and addressing the delays applied to some types of trade reporting.

"Trade and transaction reporting is one of our biggest risks," says an operational risk executive at a North American brokerage. "It's something we actively manage through the RCSA [risk control self-assessment] process. We've invested to beef up that process."

Yet another aspect of data management is adherence to the Basel Committee's principles on risk data aggregation and risk reporting, BCBS 239. Originally conceived as a framework for internal reporting, BCBS 239 is increasingly being applied by regulators to assess the adequacy of regulatory reporting, and in some cases they have fined banks for lapses.

The financial industry appears to be getting the message, with companies investing heavily in cleaning up data that is likely to be modified over the course of time.

"We are maintaining our vigilance around data quality, ensuring clear data elements owners, lineage and data tracing," says the head of operational risk at a financial markets utility. "Historical data on legacy systems or in central hubs can increase the risk of cyber threats or data compromise."

Banks are still struggling with technical aspects of BCBS 239 though, according to a study in the *Journal of Risk Model Validation*. Surveying 29 banks, the study concluded that banks need to make improvements in four areas: master data management, audit trail, metadata management and data validation. It also found that external contractors working on model development, backtesting or any other projects that require the use of data were the primary source of problems in the audit trail.

#03 Theft and fraud

From mega loan fraud to canteen theft, the danger is ever present

Theft and fraud jumps to third in this year's survey – a sign of both its ubiquity for financial institutions of all types, from the largest global lenders to eight-person hedge funds, and likely a function of its role in five of the 10 largest reported operational risk losses of 2019.

Professionals surveyed by *Risk.net* this year highlighted a wide range of factors behind the rise: technological innovation, fast-changing regulatory expectations and rising institutional complexity. The category is also a broad one, encompassing a variety of crimes.

Many of the most severe frauds reported last year, particularly in emerging markets, bore a similar characteristic: namely, the help of an inside operative working for a bank. That leads one respondent to dub this simply "insider risk". It was also the case for 2018's biggest fraud loss – an eye-watering $12 billion hit for Chinese insurer Anbang.

Internal fraud incidents can also have a long tail. Wells Fargo's legacy losses relating to its 'ghost account' fraud scandal also increased throughout 2019, with the total bill for settlements and restitutions already topping several billion dollars and counting – not to mention the long-term impact on the bank's op risk capital requirements.

While the march of progress may produce all sorts of convoluted, tech-centric crime, naturally theft and fraud can still take place in a more mundane fashion. Earlier this month, Citi was widely reported to have suspended a senior bond trader after he was accused of stealing food from the firm's canteen in London.

#03 Theft and fraud continued...

The increasing ease with which low-level crimes can be orchestrated is helping to keep the category firmly on the radar of risk professionals. One senior op risk professional cited concerns over the profusion of "information available to fraudsters from ongoing data breaches" amid the "rapid pace of digital innovation and instant money movement". Data theft is a reliably high-ranking risk in itself, and a serious breach can lead to spiralling losses as financial criminals put the stolen information to use. Often, the theft of data is just the beginning.

"[We're seeing] more sophisticated fraud," says an operational risk manager at a US bank. "What I really worry about is people taking critical customer data and putting it on the dark web. I don't worry about a hold-up."

Theft and fraud losses are also closely linked to the drive to automate processes and systems. A senior risk manager at a global bank points out that automation of customer authentication, for example, gives criminals the chance to use stolen data to fool robot gatekeepers.

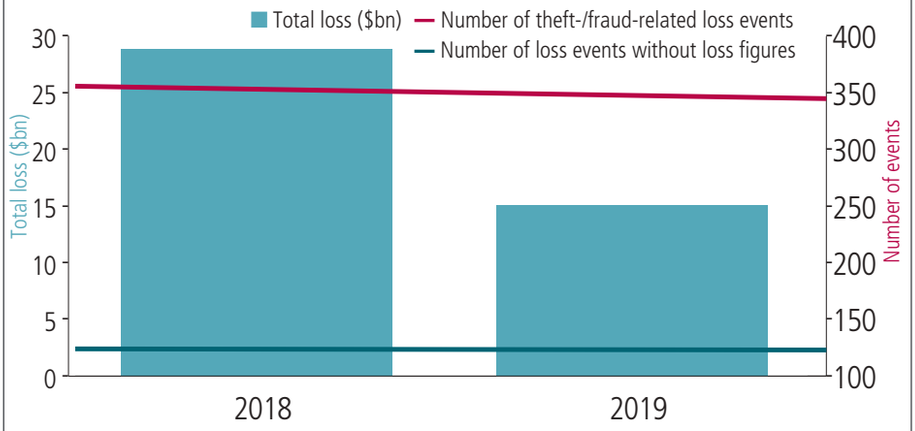
"The situation [with automation] is improving, but the threats are increasing. It's like the two sides are growing together," says the risk manager.

Institutional complexity may be a boon to fraudsters: super-intricate systems architecture can hinder a bank from understanding how and when a financial criminal has gained access. "It can make it more complex for the fraudster, of course, because they have to work with 10 systems instead of one. But it creates more points of failure, so I'm not able to say if it's a plus or a minus. A unique system is a unique, single point of failure – and 10 systems are 10 entry points," the risk manager says.

However, automation and digitisation are among the main tools in the fight against theft and fraud. Loan frauds may be easier to perpetuate online, but when a bank has a large digital dataset to parse, it can spot anomalies much quicker than in the days of paper-based fraud. "With big data and correlation tools, we try to find abnormal patterns in payment systems and trading systems," the senior risk manager says. "But it is not the panacea – it's a work in progress."

Regulation may be another factor in the ascent of theft and fraud in the rankings this year. Gaining access to the data used to commit theft and fraud, some argue, is becoming easier because of laws compelling financial institutions to collect larger quantities of information on customers.

2. Theft- and fraud-related loss events



Source: ORX Association

#04 Outsourcing & third-party risk

Respondents worry about risks stemming from an opaque web of vendors with poor controls

Big banks have decided there are many things it is not worth their while to do in-house. So they contract them out.

And that has birthed a whole new anxiety: third-party risk, or the possibility of getting body-slammed by problems at a vendor – cyber infiltrators, power failures and disreputable behaviour among the most common.

Then there are the vendor's own third-party vendors. At that point, third-party risk splits into fourth-, fifth-, etc, -party risk – a radiating pond of ever less visible odds.

On this year's top 10 op risk list, third-party came in fourth place, moving up from sixth last year.

Banks don't believe their thicket of vendors take risk management – particularly cyber security – nearly seriously enough, with one respondent to this year's survey calling them the "weakest link in the organisation".

Amit Lakhani, the global head of IT and third-party risks for corporate and institutional banking at BNP Paribas in London, notes that along with regulatory pressures, how one retains one's mission, or 'unique selling proposition', needs to be addressed.

"You could be in a situation where you are outsourcing so much that all you are is a vendor manager, not a bank," he says. "Customers trust us as risk managers to maintain and protect their data, and management has set certain outsourcing thresholds so we don't lose our USP."

Operational risk managers at Nedbank, headquartered in Johannesburg, South Africa, might agree. The personal details of 1.7 million of its customers may have been exposed after a breach at Computer Facilities, one of its vendors, the bank said last month. Computer Facilities carried out text messaging and email marketing for Nedbank, and had access to the

#04 Outsourcing & third-party risk continued...

names, addresses and government ID numbers of the bank's customers.

Power outages at vendors can also bring services to a standstill. Last August, an electrical failure at a data centre in Mexico City put the credit cards and cash machines of six banks out of commission for several hours. The banks included HSBC and Santander, as well as domestic lender Banorte and Banjército, Mexico's military bank.

Banks involved in these mishaps are flamed to varying degrees on social media. Respondents to this year's survey noted that a hit to the brand can be severe: even false reports can run amok online, leaving firms scrambling to undo the damage. But even if vendors were airtight on cyber security and company culture, what about their vendors?

"Fourth-party provider use is even less transparent and difficult to monitor, which increases exposure to additional avenues for cyber and fraud events," says another respondent.

The risk posed by fourth and fifth parties was much discussed by op risk managers last year, as the European Banking Authority set new guidelines that significantly raised the bar for scrutiny of vendors, as well as their suppliers of critical services. The EBA now expects banks to negotiate audit and access rights for fourth parties working with their vendors. European op risk managers privately say this is wishful thinking – getting even basic information to assess the security of those subcontractors is difficult.

Banks are increasingly turning to other vendors to watch their vendors. Cyber-risk rating agencies are being touted by banks and insurers as a cost-effective way to keep track of vendors. These agencies scour the deep web – content not indexed by search engines – for clues on companies' cyber security practices. But some observers say not all these services apply a standard high enough to be reliable, so some banks simply avoid them.

Cyber-risk rating agencies are being touted by banks and insurers as a cost-effective way to keep track of vendors. But some observers say not all these services apply a standard high enough to be reliable

"The level of much of the detail provided by these services is quite good," said Charles Forde, group head of op risk of Allied Irish Banks in Dublin. "I think the challenge is you can't use all these services in the same way. Some of the cyber risk ratings apply a very good layer of analysis to the data they gather, providing accurate conclusions. But the data analysis of some providers can be of low quality, so can't be used as a decision point in a risk assessment."

Besides third and fourth parties, financial institutions rely on a host of infrastructure providers such as clearing houses to execute and clear trades. William Moran, chief risk officer for technology at Bank of America, said that rarely is any information provided by clearing houses.

"They either won't participate at all – that is, they won't answer your questions – or they won't let you do an on-site [inspection], or they basically cherry-pick which questions they want to answer," he told a Risk USA conference in New York in November.

He similarly criticised regulators, saying they "don't tend to be very responsive about what they're doing in terms of cyber".

Another issue flagged in the new EBA guidelines is concentration risk. This is defined as the outsourcing of many services by one bank to a single provider, making them excessively dependent on that vendor, or as a convergence of business at just a handful of big companies. This could leave companies exposed if anything went wrong at those few heavyweights.

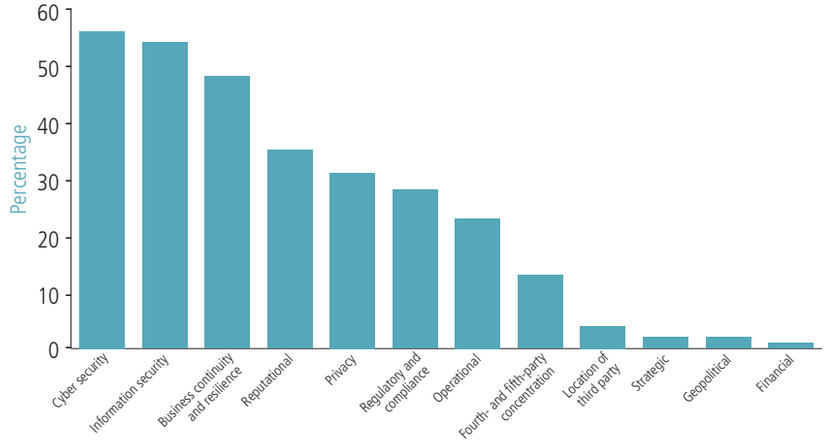
Respondents expressed concern that a few cloud providers have tightened their grip on the market, singling out Amazon Web Services and Microsoft Azure as particularly powerful. Spending on cloud infrastructure services was up 37% last year, according to research firm Canalys, with AWS, Azure and Google Cloud dominating the business. One source notes that the cloud companies are co-ordinating their lobbying efforts in Brussels, making themselves heard on a range of issues.

Their large market share – AWS and Azure alone have half the market – also means they can extract favourable terms from all but the brawniest financial services companies. Typically, cloud providers want firms to sign a standardised contract that retains most oversight for themselves and their own third-party auditors.

The chief executive officer of a systemically important financial institution recounts that he rejected the boilerplate contract pushed by one of the cloud providers, and then endured months of winding negotiations to get the guarantees he wanted before agreeing to move to the cloud.

Besides concentrations at cloud companies, the EBA guidelines spurred some soul searching on another subject: how much outsourcing is too much? The agency warned that an excess of contracted services could turn a bank into an "empty shell".

3. Top third-party risks



Survey of 94 firms across 43 countries, June–September 2019.
Source: EY and Institute of International Finance global bank risk management survey

#05 Resilience risk

In an entwined financial system, an outage at one bank can reverberate through many more

When a broker can't execute a trade because of a system meltdown, or a customer can't get money out of a cash machine, they don't ponder whether the bank in question has set its risk appetite correctly. They just want to know when they can get their trade done, or their cash in hand.

Resilience, the ability to get operations and services up and running after a disruption – IT snafus, cyber attack, bungled third-party supplies, cataclysmic weather or any other hazard – is a new entrant to the top 10 op risks, and makes its debut at fifth place.

Several forces are at work in elevating the topic. The growing complexity of banking and the interwoven nature of the financial system, both now rooted in technology, have combined to make resilience a subject of boardroom discussion.

"I definitely see it as a risk in its own right at the moment – and I think that will remain the case for the next three years at least," says a senior op risk manager at a large European bank.

Several incidents in the past year raised alarm. CI Banco in Mexico found ransomware on an employee's computer and restricted operations, taking down online banking services. Smoke in a Wells Fargo data centre shut off power, disrupting online and cash machine services for 14 hours. When hackers tried to steal millions from the Bank of Valletta in Malta, the bank closed all its branches, its cash machine and its website. It returned to normal service the next day.

Some banks have moved quickly on the issue: last year, HSBC hired Cameron 'Buck' Rogers, the Bank of England's cyber risk chief, as its first head of resilience risk, while LCH, the largest clearing house of over-the-counter derivatives, formed a dedicated resilience department. Fears have arisen in the banking world that a cyber attack on a clearing house, for instance, could reverberate throughout the industry.

Unlike business continuity and disaster recovery, which deal with individual systems, resilience looks at how quickly the entire organisation can resume its routine.

> "Resilience is an outcome, business continuity is a management tool. You are resilient if your banking system is available to the level you target"
>
> Senior op risk manager at a large European bank

"Resilience is an outcome, business continuity is a management tool," says the European bank's operational risk executive. "You are resilient if your banking system is available to the level you target."

Regulators are taking a closer look. The Basel Committee on Banking Supervision established a working group in 2018 with the aim of including a discussion of resilience metrics in an update of its principles on operational risk and, ultimately, to create a set of metrics for the industry. The Federal Reserve is also understood to be preparing a policy paper on the subject. A New York Fed study in January said a disruption at any of the five most active US banks would result in significant spillover to other banks, affecting 38% of the network on average.

At the US Treasury Department, network theory is now being used to identify which links in the financial system chain are most vulnerable, and defend them accordingly. In a targeted attack, the hub with the most direct connections to other nodes in the network is the most critical to protect; in a random attack, the hub that connects to the most nodes – directly or indirectly – is most critical.

A consultation by the Bank of England last December required companies to set timeframes on how quickly services would be restored following any outage. This is a subtle departure from business continuity, which focuses on how long it takes for systems to get back online. The former is about services, the latter about technology.

The consultation will require 'impact tolerances' as opposed to risk appetite – the losses a firm is willing to swallow following an outage. The rules, which the Bank of England plans to finalise in 2020, could include impact tolerances for vital services in the broader economy, like payment systems.

That has some companies worried.

"Setting blanket impact tolerances in terms of hours or days could be hugely unhelpful," says the European bank's op risk manager. "No two firms look the same, and even within the same operating model you have very different business mixes." An outage at a retail bank with a large card payment network, he adds, could be far more disruptive to the financial system than a disruption at a big high street bank.

Exactly what is meant by 'impact tolerance' is a matter of debate. Some practitioners say risk appetite already includes it.

"The paper talks about defining critical processes and, for each of those critical processes, defines the acceptable tolerance. Some of that work has already been done through risk appetite," says an op risk executive at a North American brokerage firm. "That might be an area where some examples from the regulator about what they mean would be beneficial. Setting the tolerance at a certain level has financial implications."

Given the digitalisation of financial services, third-party providers can be weak links in the system. The Bank of England also addressed third-party arrangements in a separate consultation in December. The central bank would require contracts with critical service providers to include provisions for data security, audit, sub-outsourcing and business continuity.

The concept of cyber resilience, in particular, is well-established in the industry. The Financial Stability Board's cyber lexicon defines it as "the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents".

Banks are extending this definition or variants thereof to operational resilience. "Resiliency is broader than disaster recovery," says an

#05 Resilience risk continued...

operational risk executive at a US bank that has set up a working group on operational resilience. "We're focusing on end-to-end services."

More costly than getting things going again can be the lasting reputational damage. Today, there is little cover. If the mainstream media does not report the disruption to service, social media almost certainly will.

"Interconnectivity and social engagement means you can no longer isolate your failures," says the European bank executive. "If you're down for a few seconds, it's amazing how many times on Twitter it will get picked up."

#06 Organisational change

New tech has created a perennial state of flux in banking, as other kinds of shake-ups continue

One large European bank simply calls it "change risk". It refers to the kinks that may arise as a bank or firm reshuffles its operations for any number of reasons. This year, the biggest of them is the need to keep up with the unstinting pace of technology.

The relentless lunge to the latest technology is being watched closely. However much they invest, firms cannot responsibly move as fast as tech companies – but they do have to move. An op risk manager at a US bank says rapid evolution has to be carefully controlled to avoid any sudden movements.

"Change management is a top risk for us," he says. "Agile methodologies are something we continue to monitor."

One financial market infrastructure provider, like many others, is facing significant upheaval in integrating "new technology platforms, new services avenues and new management", its chief risk officer says.

At a large US asset manager, numerous "transformation" efforts are under way, says one managing director, as the firm absorbs the purchase of a business software provider. The firm refers to this sort of overhaul as "process re-engineering".

"We completely rebuilt our front-to-back systems," says the head of op risk. "All the processes we execute manually are going to be rebuilt using new technology."

Plenty could go wrong. Conversions of this sort, new projects and procedures – such as the long-overdue overhaul of domain models, for example – and the hatching of new enterprises often mean more work for employees who are already under pressure.

"Banks are re-engineering many core processes and leveraging fintech solutions, but time to market is short," says an op risk head at an international bank. "Agile development makes it hard for risk [teams] to catch up and ensure that risks are being properly addressed."

But the organisational change category takes in more than the onrush of tech: changes in business strategy, teething issues with new management, shake-ups, onboardings and anything else that could send waves through a company. When a bank shrinks instead of expanding, that also requires attention. Downsizings that put multitudes of people on the street can hollow out morale and ramp up the workloads of those still at their desks. Recently, HSBC announced it would slash 15% of its global workforce – 35,000 people. Deutsche Bank, in its restructuring effort, announced it would cut 18,000 jobs by 2022. Cost-cutting, generally a sign of lower profits, can be accompanied by reputational risk, especially when accompanied by extensive job culls.

> "Banks are re-engineering many core processes and leveraging fintech solutions, but time to market is short. Agile development makes it hard for risk [teams] to catch up and ensure that risks are being properly addressed" Op risk head at an international bank

Organisational change risks can be more mundane. The chief risk officer at one clearing house, for example, is dealing with a good old-fashioned merger – "a challenge to our IT integration and unexpected regulatory requirements as well".

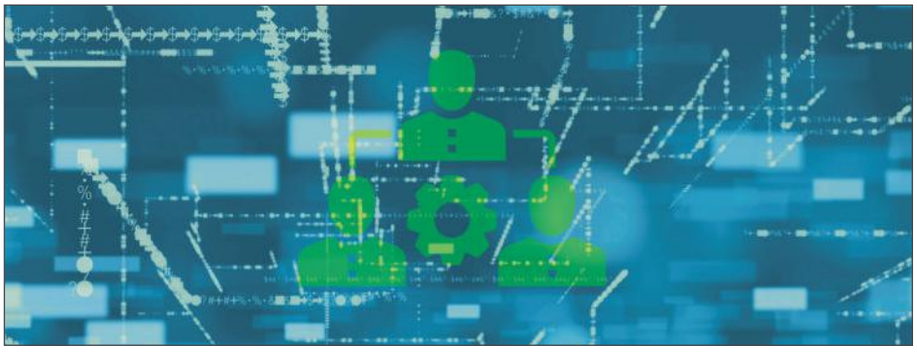
Brexit is no longer the anxiety it was a year ago. One senior risk manager at a leading European bank says the UK's rupture with Europe required shifts at his company, but that that work is now largely complete.

"We had to reorganise in terms of legal entities, and who trades what," he explains. The "migration tasks" that do remain are well understood and thoroughly mapped out. "It doesn't add any value to us as a global bank, but it makes lawyers and consultants richer," he says of the effort.

One perennially predicted insurgency – distributed ledger technology – has not yet materialised. The probability that blockchain will one day bring seismic change to finance is high, but for now, it's somewhere out on the horizon, says the risk manager from the European bank, despite a surge of ledger-related work.

"I see some niche solutions in blockchain," the risk officer continues. "But at the end of the day, position-keeping for cash and securities will still be with a trusted third party – which is likely to be a regulated entity, rather than a cryptographic algorithm."

He adds: "Maybe it's because I'm old-school."



#07 Conduct risk

Root-and-branch reform of bank culture remains a work in progress

Conduct risk returns to this year's Top 10 Op Risks, although it's never really been away. The category is an aggregation of two key subsets of the risk – mis-selling and unauthorised trading – which have appeared repeatedly in previous years.

"We still have not moved away from the number one risk: conduct," says an op risk head at a UK bank, about the financial industry. "Conduct by its nature tends to take some time to be identified, and then often takes a long time to manifest itself in outflows from fines or restitution. You can't rest on your laurels."

Gauging the scale of the problem through risk modelling is notoriously hard: the seemingly sporadic nature of big conduct losses, with low levels of wearable losses punctuated by extreme instances of costly wrongdoing, makes it hard to parse datasets to deliver credible conduct value-at-risk figures.

In a recent high-profile loss, a rogue trader at a subsidiary of Mitsubishi Corporation placed a series of unauthorised trades in crude oil derivatives starting in January 2019. The trading firm discovered the positions in August – but too late. The bets had already racked up $320 million in losses.

Firms' focus on conduct has been sharpened by the implementation of a number of regulations, among them the UK's Senior Managers and Certification Regime, which was expanded in December to cover some 50,000 regulated firms. The UK Financial Conduct Authority disclosed in September it had a pipeline of investigations for "serious" breaches of the code.

The regime, which seeks to codify a culture of personal responsibility among bank leaders and risk managers, has helped spawn similar sets of rules in other jurisdictions – for example, Australia. Here, the Banking Executive Accountability Regime is set to expand in scope and penalty following a series of mis-selling scandals that have plagued the country's banking and insurance sector. The Australian Securities and Investments Commission has said it would not shy away from redoubling enforcement to punish misconduct.

The ultimate remedy cited by many practitioners remains an improvement in risk culture – "doing the right thing when no-one is looking" – rather than quick fixes.

"You need to have a culture which says that certain behaviours are inappropriate," says the UK bank's op risk head. "You achieve that in a number of ways. First, you create a tone at the top. Second, you ensure that you reward good behaviours and you put in measures to penalise bad behaviours."

One survey respondent says his firm, a bank in North America, has created a new dedicated conduct risk oversight committee, along with a sales and servicing committee to drive the tone from the top.

There are signs a stronger risk culture is starting to permeate: some banks in the Asia-Pacific region have revised their conduct scorecards to reward good behaviour over hard sales. Malaysia's largest lender, Maybank, has overhauled its individual compensation model by incorporating client satisfaction and ethical behaviour alongside financial targets. ANZ has abolished sales targets for its branch staff while Commonwealth Bank of Australia has capped the weightings of financial metrics at 30%.

Mis-selling itself has an evolving definition tied to regulatory risk, as watchdogs and customer expectation change over time, which adds to the complexity of managing such risk. An op risk manager points to the notorious selling of payment protection insurance in the UK as an example.

While the product itself wasn't deemed wholly inappropriate at the time, the cut-throat sales culture led to mis-selling of insurance on loans, credit cards and mortgages. The two-decade-long practice resulted in payouts exceeding £50 billion ($64.1 billion) by UK banks and credit card companies. Of this, more than £37 billion was returned to complainants, according to official data. The remainder was paid in fines and other costs.

Costly settlements on misconduct-related lawsuits can linger for years. Litigation and misconduct charges reported by large UK banks – Barclays, HSBC, Lloyds, Nationwide, RBS, Santander UK and Standard Chartered – increased 20% to £6.5 billion in 2018, according to their annual reports.

Senior op risk managers recognise that a comprehensive framework could be the key to the changing nature of conducts.

"Culture change can sometimes lead to not being compliant with policies, and that needs to be managed," says one op risk head at an EU bank. "It's not always intentional. But if you don't have a framework around it, you have a laidback attitude where people ask for exceptions."

#08 Regulatory risk

New technology and reams of red tape make non-compliance fines more likely

Regulatory risk slips back a few places to rank at eighth in this year's Top 10 – a function, perhaps, of a slowdown in the printing press of rulemakings that have reshaped the post-crisis financial landscape. The bedding down of reforms to derivatives markets, financial accounting practices, regulatory reporting and stress-testing requirements – the list goes on – doesn't make compliance with them easy, however. Given the breadth and volume of new sets of rules, the potential for mis-steps and misinterpretation is manifest. "Increasing regulatory and compliance requirements – in the form of both new rules and amendments to existing rulesets – as well as intense regulatory scrutiny, is a perennial challenge," says the head of op risk at one globa bank.

A time-honoured way of staying on top of such headaches is to poach those who wrote the rules: UBS hired the head of banking supervision at Switzerland's Finma, the bank's primary supervisor, as its head of regulatory affairs last year. Others have hired with the new regulatory compliance topic du jour, resilience risk, in mind: HSBC hired the Bank of England's Cameron 'Buck' Rogers as its first global head of resilience risk.

In many areas, differing global interpretations of supranational rules, particularly where they butt up against national-level requirements, can make compliance a nightmare. Take, for instance, the compliance risks involved in new data protection regulations. The European Union's General Data Protection Regulation (GDPR) came into force in 2018, followed in short order by a sometimes conflicting rule from the US state of California that inevitably binds many firms doing business with anyone in the US's most populous state.

One respondent warned: "Many countries have their own data protection laws, making the exchange of data between units of a group operating on five continents like a walk in a minefield, especially when the rules are not clear or fully articulated, or data protection authorities have not yet provided the required guidance."

Meanwhile, the potential cost of a failure – whether under GDPR with its 4%-of-revenue penalty cap, or from penalties and lawsuits in non-GDPR nations – remains high. Fears of infringing privacy regulations are even undermining efforts to encourage the sharing of cyber threat information, despite efforts by regulators to reassure institutions. With data compromise high on the list of op risks for another year, the instinct to clamp down on data flows is strong in 2020.

And the problems worsen when outsourcing and offshoring relationships are involved, other respondents point out: home regulators still demand high levels of supervision, which can be more difficult to achieve and verify for external providers. Some companies, one respondent said, have already reached the "tipping points of offshoring, where supervision is harder to continue to prove to home regulators".

That was in evidence from regulatory fines for data reporting breaches this year. The Bank of England fined Citi £44 million ($56.3 million) in November for submitting incomplete and inaccurate capital and liquidity metrics, a job that was offshored to teams in Budapest and Mumbai. The watchdog's report was a damning list of failings: the teams were under-resourced; the returns were not sufficiently challenged; and the bank was found not to have spent enough time on interpretation of UK rules.

With Brexit looming, it seems likely that, once the UK's exit conditions from the EU are finally confirmed later this year, they will include some degree of regulatory divergence for the financial sector – meaning two sets of reporting requirements for derivatives trades, as well as greater difficulty in cross-checking trade reports. Keeping up to date with the details of rapidly changing regulatory requirements represents a significant resource drain by itself, even without the additional cost of meeting the requirements.

Efforts to introduce common standards for trade data reporting have been, so far, only

partially successful – full success will require considerably more effort from banks. Slow adoption of the BCBS 239 risk data standard has led European regulators to resort to unannounced 'fire drill' inspections of the banks they supervise – effective, but onerous.

Advances in artificial intelligence represent another source of regulatory risk. Risk managers highlighted the vital importance of ensuring transparency as AI systems become more widely used. While AI involvement in decision-making increases, whether for trading or in customer-facing roles, the pressure to prove that its decisions are unbiased and well founded grows, too – even as the software, and therefore the task of explaining it, becomes more complex.

Privacy concerns abound with AI: investment managers are wary of the privacy risks around alternative data and worries about data protection are restricting the use of AI in internal surveillance. Fear of regulatory penalties, and of reputational loss and damages awarded in civil suits, makes this an area of particular risk.

Other respondents noted that internal pressures were also responsible for significant regulatory risk – the launch of innovative products increased the danger of missing reporting deadlines or failing to meet other regulatory requirements, which in turn could lead to penalties, intrusive inspections or reputational damage.

B. Regulatory fines

	Frequency		Severity ($ million)	
Region	2018	2019	2018	2018
Africa	10	11	110.6	10.3
Asia-Pacific	41	20	843.5	509.4
Eastern Europe	3	4	5.0	5.2
Latin America and Caribbean	12	7	78.6	82.5
North America	91	76	6,904.7	2,531.5
Western Europe	45	64	2,257.6	1,837.6
Total	**202**	**182**	**10,200.0**	**4,976.6**

Source: ORX Association

#09 Talent risk

Firms struggle to reduce headcount and fill gaps without cutting corners

Talent risk appears in the top 10 for the second time in three years – unwelcome evidence for banks and other financial firms of the struggle to recruit and retain the right calibre of staff and deploy them where they're needed, in an era of dramatic headcount reductions.

As banks shed jobs, it forces them to think more about how they manage talent risk, says a global op risk head at a US bank. Operating with a leaner business model has forced his firm to recognise more quickly where it does or doesn't have specific skill sets and juggle resources accordingly, he says. At the same time, a shift in its business mix or change in regulatory priorities can leave the firm exposed.

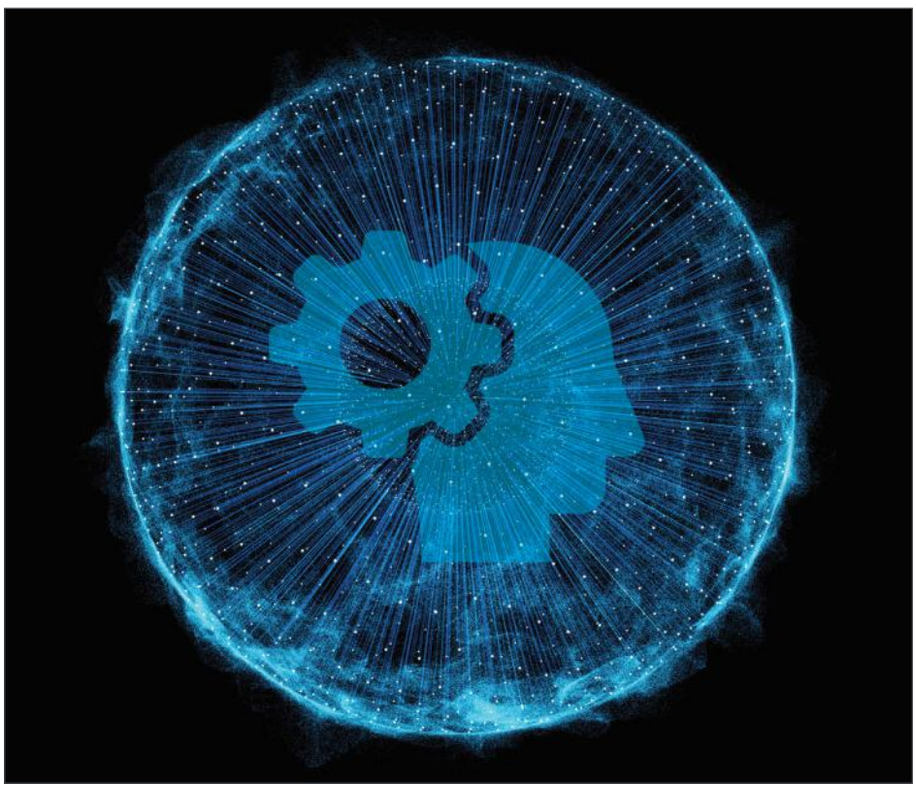
The emergence of new technologies such as machine learning is pushing financial institutions to adapt their business models in areas such as anti-money-laundering checks, credit decisioning, trading automation and improving customer experience.

An efficient organisational structure is especially important for the growing number of virtual banks around the world. As digital-only banks enter the market with more responsive customer services and product offerings, they are bound to face intense regulatory scrutiny on their risk management. Chief risk officers, chief compliance officers and other senior staff need risk management know-how as well as basic technical understanding of their products.

Many of those jobs require quants – and in some markets experienced hands are in short supply, notably pricing quants in Asia-Pacific on both buy and sell side. If the proliferation of specialist quant finance master's programmes is anything to go by, the future looks brighter – though banks may have to watch for their best quants being lured back into roles in academia.

With the era of rock star front-office quants charged with creating and pricing hot new derivatives long since over, banks worry that the attraction of the profession over the lure of Silicon Valley and other career paths is waning; making sure a model behaves itself within certain known parameters is not as fun as building one from scratch.

Banks worry the attraction of the quant profession over the lure of Silicon Valley and other career paths is waning; making sure a model behaves itself within certain known parameters is not as fun as building one from scratch



Banks have tried to raise the profile of some new hires: for example, UBS has vowed to raise the profile of the quants responsible for overseeing and validating machine learning-based models the bank is increasingly looking to deploy.

A dearth of staff can also morph into organisational change risk: delaying automation and digitisation projects can lead to banks' "inability to attract, manage, motivate, develop and retain competent resources", says Evans Kasai, head of op risk at South Africa's Nedbank. This can have a "negative impact on the achievement of strategic group objectives", he adds.

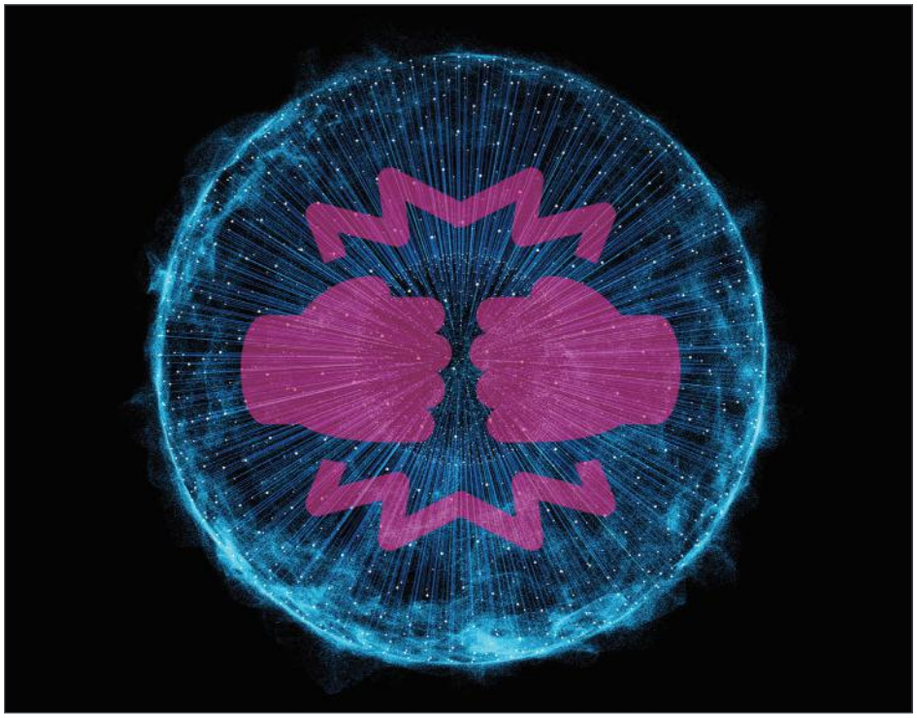
Within the risk function itself, the IT skills to keep up with digitalisation are in short supply, hiking the risk to banks, says one op risk head at a global bank. "Traditional ways of managing operational risk need to change, and the skills to identify and manage digital risk are still in development, but business is digitalising at a great speed," he says.

Any time compliance expectations change in specialised areas, it sparks a scramble among banks to find appropriate hires. That can be a particular problem in regions without deep talent pools. In Singapore, for instance, a shift in the way the local regulator expected banks to approach cyber risk management and counter cyber threats has forced firms to confront a dearth of IT talent. Salaries have risen as banks increasingly look to benchmark pay for technology risk and information hires to levels at tech firms, recruiters say.

As Basel III moves from rancorous rule-writing to full-on implementation, banks are hunting for experienced talents to lead their efforts. Bank of America, for example, recently hired one of Deutsche Bank's most prominent risk analytics executives to lead strategic market risk regulatory programmes, such as the Fundamental Review of the Trading Book.

#10 Geopolitical risk

Nationalism, trade wars and epidemics make for a heady cocktail



Surveys of this type are always in danger of being rapidly overtaken by events. In the category of geopolitical risk, that can happen before the ink is even dry.

As February drew to a close, the coronavirus left markets reeling from their worst paper losses since the crisis, with governments scrambling to formulate a cohesive response. When the survey was conducted in early January, the virus drew scarcely a mention from respondents, a handful of whom, based in the Asia-Pacific region, flagged it as a blip on the radar.

Epidemic diseases are a standalone operational risk, forcing authorities to respond with quarantining measures and blanket restrictions on travel – all of which play havoc with international firms' ability to do their jobs in a normal manner. However, the virus is here considered as a function of geopolitical risk.

With the virus likely to contribute to a global economic slowdown, this will trigger wider operational risks – making loan fraud more likely as credit markets deteriorate, for example, or increasing cases of internal fraud as front-office staff struggle to hit targets.

At the time of writing, no end to the coronavirus outbreak was in sight. The number of new cases in China is reported to be slowing, but news is emerging of fresh outbreaks and quarantines in Iran, Italy, the Gulf and elsewhere. As the prospect of large-scale remote working grows, organisations will be reviewing business continuity plans.

Global health officials have not yet classified coronavirus as a pandemic, though. And companies will be aware that as fast as global viruses spread, they can just as rapidly recede.

Another form of virus worrying op risk managers is the threat of state-sponsored cyber attack – one of many ways in which modern geopolitical conflicts play out, as its use by Russia, North Korea and the US has shown in recent years.

Cyber warfare is prone to overspill. Cyber weapons, once deployed, can spread rapidly, and the billions of dollars of damage done by the NotPetya attack in 2017 shows the potential scale of the consequences – which, regulators fear, could rise to the level of a systemic liquidity crisis.

Geopolitical risk manifests itself in other ways, too, such as regulatory uncertainty. Brexit, which also featured in the 2019 Top 10, continues to be an important concern for the financial sector. Almost four years after the UK voted to leave the European Union, there is still no EU-UK trade deal in place, meaning a lack of clarity on equivalence between UK and EU regulators, and on the ability of UK firms to trade in the EU after full separation at the end of 2020.

Many op risk managers regard the Brexit situation as more stable today than this time last year, with most financial institutions having established locally domiciled operations inside the EU.

Aside from whatever tariffs will eventually apply to a Brexited UK, the US government has imposed a raft of trade barriers on countries over the past three years. Survey respondents pointed out the increased compliance burden this involves, as well as the likelihood of sanctions-evading transactions. Fines for sanctions violations reached $19.9 billion between 2009 and 2019, stressing the need for effective know-your-customer procedures.

The link between geopolitical risk and financial impact, however, remains frustratingly indirect and uncertain. Nobel prize-winning economist Robert Engle, speaking at a *Risk* event in late 2019, pointed out that his 'Geovol' measure of geopolitical risk, derived from realised volatilities of multiple asset classes, rated the risk far lower than news-based measures like the Geopolitical Risk Index. Spikes in attention paid to geopolitical events are not always matched by market activity; in fact, 2017–19 was a period of abnormally low Geovol once the spike around the 2016 US election had subsided, Engle pointed out.

Another US election is due in November this year. The 2016 poll brought regulatory uncertainty as the two candidates differed significantly on financial regulation. And while Donald Trump is less of an unknown quantity this time around, November is likely again to present a choice between different regulatory and economic policies.

Climate change, leading the list of emerging global threats, does not appear on this year's list of top operational risks, but has ascended to the level of a strategic risk for many institutions. Many survey respondents cited disruption from climate change protests and the credit and reputational risks of association with legacy fossil-fuel industry as concerns. The model risk involved in adapting to the new threats to lending and mortgage businesses posed by climate-related disasters such as floods and wildfires is also a worry for banks.

Baker McKenzie.

Adapting to technological change in op risk management

Baker McKenzie's Jonathan Peddie explains how the role of operational risk manager has evolved in recent years, how financial firms are managing increasing demand for data privacy and transparency, and how technological advancements over the coming decade will change operational risk and its prevention

Jonathan Peddie, Partner and Chair, Financial Institutions Industry Group, Baker McKenzie
bakermckenzie.com

The scope and scale of operational risk managers' responsibilities has grown dramatically in recent years. How can managers keep pace and drive efficiency in their op risk management processes?

Jonathan Peddie: Whether outsourcing, data compliance or conduct issues such as mis-selling, risk managers need to design and implement effective processes to identify, manage and monitor op risks. A key element of this – as the UK Financial Conduct Authority (FCA) has made clear through enforcement notices – is to establish an appropriate, consistent risk appetite from board-level downwards. This will drive key decisions such as those around how much tolerance to allow and whether – and to what degree – substitutability and recoverability of systems and processes is required. For conduct issues, processes to monitor and promptly remediate non-compliant behaviours will be especially important. Critical to all of these activities is adequate resourcing – although technological solutions are of increasing relevance – and the ability for risk managers to raise issues when necessary at board-level, which the Senior Managers and Certified Persons Regime (SMCR) will facilitate.

Although 2019 op risk losses were down on previous years, theft, tax evasion and embezzlement remained prominent. Is regulation such as the SMCR the answer to tackling conduct risk?

Jonathan Peddie: Regulation can only go so far. Rather, culture has been an acknowledged key root cause of the major conduct failings across financial services in recent years. The SMCR, by clarifying responsibility and accountability at senior management level, is seen by regulators as an important tool in improving culture and therefore reducing conduct risk. In a foreword to the FCA's discussion paper on transforming culture in financial services, Jonathan Davidson, director of supervision at the FCA, said there is no single culture for firms to aspire to, but that "healthy cultures have some specific characteristics that reduce harm".[1] In his view, regulation has to hold the individual as well as the firm to account. In effect, regulatory penalties should not simply be the cost of doing business, and senior managers need to have clearly articulated what they are accountable for and their key responsibilities.

Data compromise is a perennial concern for op risk managers. How are financial firms coping with increasing demand for data privacy and transparency due to regulation such as the European Union's General Data Protection Regulation (GDPR)?

Jonathan Peddie: With the advent of GDPR, data compliance is now much more than a box-ticking exercise of having all the right policies in place. The best firms at managing risk have taken steps to see that compliance is embedded at a deeper level, ensuring that data protection has become part of the culture of their organisation. This reflects requirements under GDPR to 'bake in' data protection to business practices, from the design stage through the entire lifecycle of a project – "data protection by design and by default".[2] Data sharing – in the context of open banking, open finance and beyond – can complement or clash with individuals' rights under the GDPR, so firms must adopt a connected approach to navigate these potentially competing demands.

Customer demand and technological advances are putting pressure on financial firms to overhaul their creaking IT infrastructure. What can be learned from the market's experience about the risks involved?

Jonathan Peddie: Migrating or upgrading from various legacy systems to new IT platforms can be complex, requiring detailed planning and testing. Despite such preparations, some issues will invariably arise. Contingency planning is therefore essential on the basis that not everything will always go to plan. It is also important to ensure improvements to IT infrastructure are not too ambitious, and that those involved – including key IT contractors – are sufficiently experienced and ready. Attestations and supporting evidence should be sought in this regard. Depending on the scale of the project, management at an appropriately senior level must fully understand, consider and scrutinise key aspects of any project and, in particular, where relevant, non-executive directors must challenge it – all of which should be documented.

As well as identifying significant risks to a project's success, management should ensure sufficiently robust contingency plans are in place to protect customers – and, if relevant, to safeguard market stability – should the risks crystallise. The appointment of independent advisers can provide both objective and expert review for managers as they scrutinise major projects. Larger firms with dedicated Prudential Regulation Authority (PRA)/FCA supervision teams should keep them updated on the progress of important projects.

Regulators have identified operational resilience as a key pillar in maintaining the stability of the financial system. What actions should firms prioritise in building resilience?

Jonathan Peddie: Firms should prioritise understanding the systems and processes that support their key services to customers, including those outsourced to third parties. It is vital to appreciate the impact of an individual system or process failing and how easily it can be substituted or speedily restored. Firms often wrongly assume interruptions will be of a short duration. Putting in place and regularly testing contingency and fallback plans – although potentially expensive – is essential and should form a key part of business continuity planning. Outsourcing technology, due to its very nature, is subject to only indirect control and therefore requires particular oversight and consideration. It is no coincidence the FCA has recently published a consultation on outsourcing and third-party risk management, which follows the European Banking Authority's (EBA's) updated guidelines on outsourcing arrangements that took effect in September 2019.[3,4]

Climate risk is scaling the op risk agenda, but is particularly complex for firms to measure and manage. How can firms improve their risk assessment and governance processes in this area?

Jonathan Peddie: To improve their processes, firms should integrate an assessment of climate change risks and opportunities into their business, risk and investment decisions. In doing so, they can also take advantage of climate-related disclosures, for example, from securities issuers in deciding whether to offer customers a specific product or service. A forward-looking and strategic approach is also required. This implies a move away from short-termism to take account of risks that could impact in the medium to long term. In this respect, following and sharing best practice is desirable. To this end, the Climate Financial Risk Forum, an industry group co-chaired by the FCA and PRA, has been established to reduce the obstacles firms face in devising such forward-looking approaches by developing practical tools and methodologies.

What will keep op risk managers awake at night in 2030?

Jonathan Peddie: Technological change is gathering pace. The use of artificial intelligence, machine learning, distributed ledger technology and other similar tools will be integral to the operation of most businesses and the provision of services to customers in the future. It is essential that boards, senior management and risk management fully understand these financial technology applications, or risk failing to effectively manage the operational and regulatory risks to which their businesses are exposed. An investment in the training and development of all staff is called for, as well as an understanding of the supervisory expectations of regulators, which face their own educational challenges in this regard, and whose rulebooks may inevitably be a little behind the curve.

Jonathan Peddie is a partner at Baker McKenzie and chair of its Financial Institutions Industry Group

jonathan.peddie@bakermckenzie.com
+44 20 7919 1222
bakermckenzie.com

[1] *FCA (March 2018),* Transforming culture in financial services, *https://bit.ly/2SKcrTm*
[2] *Intersoft Consulting,* GDPR – Data protection by design and by default, *https://bit.ly/2SJVHvm*
[3] *PRA (December 2019),* Outsourcing and third party risk management, *https://bit.ly/2SIGbQd*
[4] *EBA (February 2019),* EBA Guidelines on outsourcing arrangements, *https://bit.ly/3bW6IRG*

Baker McKenzie.

A growing focus on op risk

Operational risk and resilience have taken centre stage over the past year. While op risk concerns all systems and controls that deliver effective solutions against the risks financial services businesses regularly face, Jonathan Peddie, partner at Baker McKenzie and chair of its Financial Institutions industry group, explores those that concern IT and outsourcing-related failures

While business continuity planning has always been important, the growing number and impact of IT-related events – linked to increasing digitalisation and outsourcing in financial services – have changed priorities. Andrew Bailey, chief executive of the UK Financial Conduct Authority (FCA) and incoming governor of the Bank of England, told the UK Parliament's Treasury Select Committee last year (in evidence): "As we have hopefully mitigated some of the key risks of the financial crisis, the relative standing of operational risk – both growing as a risk in its own right, and as we have mitigated other things – has come up."[1]

The UK authorities are not alone in responding to op risk. The European Commission is consulting on harmonising European Union rules to make the financial sector more secure and resilient – with cyber attacks a particular concern. The upshot is that the authorities are giving heightened attention to op risk and the need for resilient systems and processes.

The consequences of failure

Last year's events exemplified this trend. Joint action was taken by the Prudential Regulation Authority (PRA) and the FCA against Raphaels Bank, a small retail bank offering prepaid cards and charge cards in Europe. Following a technology malfunction by the bank's outsourced card processor, there was a complete failure of IT services for more than eight hours, during which thousands of customers were unable to use their prepaid or charge cards.

Raphaels Bank was found to have lacked adequate processes to identify and monitor these arrangements, especially over how they would support their continued operation during such a disruptive event.[2] This resulted in a £1.9 million fine and probably an even larger dent in the bank's reputation.

Managerial accountability

Illustrative of the spotlight cast on op risk is the political pressure on regulators. The Treasury Select Committee's report last autumn into significant IT failures in financial services made recommendations to improve operational resilience, including ensuring accountability of individuals and firms.[3]

This reference to holding individuals to account is a reminder of the growing responsibilities on senior staff under the Senior Managers and Certified Persons Regime (SMCR). Regulators will, for example, look at the actions of the senior manager holding the chief operations function responsible for a firm's internal operations and technology. Individuals who fail to take reasonable steps – including training or appropriate oversight – to prevent or stop regulatory breaches in their area of responsibility will be identifiable and liable to disciplinary action.

The SMCR regime has applied to banks, insurers and large investment firms since 2016 and was extended to most of the sector last year. Although enforcement cases are slow in coming through the investigations pipeline, given the regulatory focus it can only be a matter of time before we see the first cases.

Building resilience

In December 2019, following a discussion paper, the PRA and FCA published a consultation paper entitled *Building operational resilience – Impact tolerances for important business services*.[4] With this publication, the UK's prudential and conduct regulators aim to strengthen the regulatory framework to improve operational resilience in financial institutions. The regulatory expectation is for the sector to identify its critical business services and then, crucially, to establish an 'impact tolerance' for each of them, setting maximum acceptable levels of disruption using severe but realistic scenarios. Where necessary, boards and senior managers must strengthen resilience for services likely to exceed their maximum tolerances, and this is where they should expect to be scrutinised and held to account by regulators.

What good looks like

What will firms resilient to op risk look like? According to the PRA and FCA, having identified their most important services, they should develop a comprehensive understanding of and map of the systems and processes that support them, including those that are outsourced. They need to understand the impact of an individual system or process should it fail, together with its substitutability or recoverability.

As with all business continuity preparation, regular testing of contingency plans is essential. Operational incidents are worsened by communication failures, so robust communication plans are vital to allow decision-makers to mobilise the resources necessary to resolve incidents and to manage the expectations of customers and business partners as relevant. A key element of any communication plan is compliance with regulatory notification requirements, for example, as required under the EU's General Data Protection Regulation and second Payment Services Directive.

Firms can expect to see new resilience proposals from the regulators in the second half of 2020.

Jonathan Peddie is a partner at Baker McKenzie and chair of its Financial Institutions Industry Group

jonathan.peddie@bakermckenzie.com
+44 (0)20 7919 1222
bakermckenzie.com

[1] *Parliament of the United Kingdom (October 2019),* IT failures in the financial services sector, *https://bit.ly/2SL5aIW*
[2] *FCA (May 2019),* Letter to R. Raphael & Sons, *https://bit.ly/2V6alyv*
[3] *House of Commons Treasury Committee (October 2019),* IT failures in the financial services sector – Second report of session 2019–20, *https://bit.ly/2SZ4oB0*
[4] *Bank of England and FCA (December 2019),* Building operational resilience – Impact tolerances for important business services, *https://bit.ly/32a1Cyg*

Baker McKenzie.

Financial institutions face a constantly changing regulatory landscape. Companies need a law firm that can navigate, adapt, and anticipate evolving market requirements.

We call it The New Lawyer.

Lawyers who embrace new ideas to help them navigate complex financial regulations seamlessly and effectively. Lawyers who understand where things are, and where things go from here.

We are The New Lawyers.
We are Baker McKenzie.

bakermckenzie.com/financialinstitutions