Risk publications

Risk

RISK MANAGEMENT • DERIVATIVES • REGULATION

Risk.net March 2021

Top 10 op risks 2021

Supported by

Baker McKenzie.

Contents

2 Introduction

Op risk managers could be Covid long haulers

New threats sprang from old sources in this year's Top 10 op risks, belying a big drop in losses

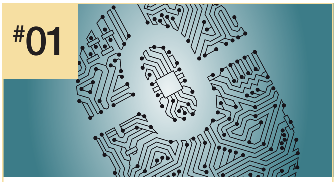
3 Sponsored feature

The importance of getting technology change right

Christoph Kurth, partner and member of the global financial institutions leadership team at Baker McKenzie, covers some of the rapid technological changes under way brought about by, and in the wake of, the Covid-19 pandemic

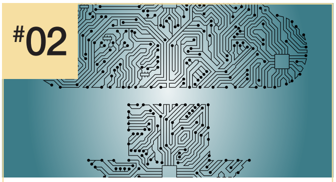
5 Top 10 op risks 2021

The biggest operational risks for 2021, as chosen by industry practitioners



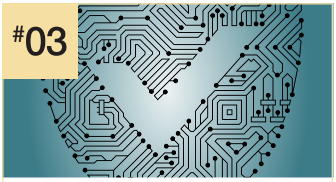
5 IT disruption

Integrity of core systems paramount as risk managers battle outages and hacks in work from home era



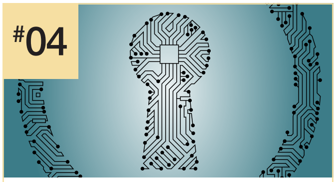
6 Data compromise

Remote working elevates fears of data theft, misuse and abuse



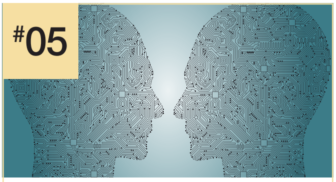
7 Resilience risk

Industry survives biggest real-world stress test, but challenges remain for firms and regulators



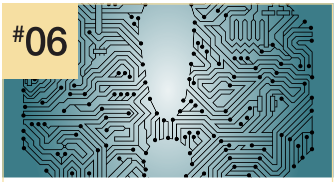
8 Theft and fraud

Changes in working practices since Covid shift angle of criminal attack on financial institutions



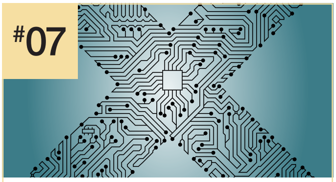
9 Third-party risk

Pandemic and shift to cloud computing inflame concerns for banks and regulators



10 Conduct risk

Remote working vastly complicates the job of conduct risk supervisors

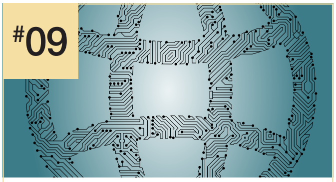


11 Regulatory risk

Big dip in fines belies lingering fears over Covid loan mis-selling and sanctions risk

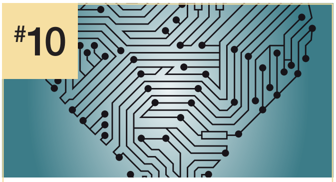
12 Organisational change

Change the sole constant as industry ponders its post-Covid future



13 Geopolitical risk

Stimulus unwind, Covid nationalism and regime changes spell volatile operating environment



14 Employee wellbeing

All-encompassing impact of Covid leaves employees with the feeling of 'living from work'

15 Sponsored feature

Heightened operational risks in a changing world

Christoph Kurth, partner and member of the global financial institutions leadership team at Baker McKenzie, discusses the growth of conduct and operational risks in the light of the pandemic, including those caused by mass home-working, the enhanced technological ability to address them, and why we should design a new type of workplace culture or risk losing one altogether

Illustration: Mark Long, nbillustration.co.uk

In depth

Monthly special features:
Top 10 operational risks 2021

Supported by:

Baker McKenzie.

Op risk managers could be Covid long haulers

Like many, operational risk managers were glad to see the back of 2020. Unlike most, their worries show few signs of easing. The giant sources of op risk engendered by the coronavirus – opportunistic cyber attacks, creative money laundering and vast new possibilities for internal fraud – aren't going anywhere, even as the world charts a course out of lockdown.

Among broad categories of concern, this year's Top 10 operational risks look superficially similar to previous years, with movement between them as expected: conduct and resilience risk have both risen up firms' agendas, with more esoteric concerns like organisational change and talent risk dropping. Employee wellbeing was the sole new entry – both a welcome sign that managers are taking the human element seriously, and a worrying one that the scale of the problem is big enough to be top of mind.

Yet within each category, risk profiles have changed dramatically in ways that are difficult to predict and impossible to fully track. The threat of IT disruption remains the top collective concern, for instance, but conversations suggest that owes as much to insider threats from disgruntled employees – those on notice or paid leave who still have access to systems and controls, for instance, or sensitive data – as it does longstanding worries over outages and overloads. And perhaps counterintuitively, the trend in op risk losses has been falling during the pandemic, along with attendant capital numbers – 2020 marked a post-crisis low in both frequency and severity of losses, according to data from ORX News.

When might the increased array of threats firms face in the work-from-home era crystallise as loss events? That all depends. When modelling losses, firms tend to divide events between those stemming from conduct related issues, and everything else. In part this is due to the difficulty of modelling the former, given it is skewed by infrequent, but catastrophically large losses.

But conduct losses are also a slow burn: fines for mis-selling, market manipulation and most forms of internal fraud take a long time to come to light, then hang around for far longer – perhaps forever, in reputational terms. "When we model, we assume most conduct losses will show a three-to-five year lag – whereas normal, transaction-style losses will appear within a one-year window. One year into Covid, we've not seen any transaction losses of any real note – so I don't know whether we will now. But who knows what conduct looks like," says the head of op risk capital at one European bank.

Covid has also exposed the limitations of point-in-time year-ahead forecasts, including our Top 10 op risks survey. Few risk managers reported pandemic risk among their top concerns last year – one honest bank admitted it drew up a pandemic scenario, before dismissing it as unrealistic. It last appeared in 2013's Top 10, in the wake of the Asian swine flu epidemic.

So, *Risk.net* is considering ways to shake up the format of the Top 10 op risks, to make it more dynamic and informative for readers. What might that look like? A quarterly poll, to see how the main areas of concern for op risk managers evolve over the course of a year? Or a free-form exercise designed to identify emerging risks?

Tom Osborn, Editor, Risk Management

Let us know your thoughts: send suggestions to tom.osborn@risk.net

"Quote me"

"The consequences of IT disruption are likely to be higher, because of our increasing dependency on technology"

Operational risk consultant

"Two years ago, resilience sounded like an academic concept: 'you're only as strong as your weakest link'. But it's so true – this year has proved that in spades"

Head of strategic risk, US asset manager

"By working in the office, you can pick up informal signals and signs that may point to issues"

Head of op risk at a large international bank

"I feel that we are seeing increased volatility in previously stable regions. This could, for example, be demonstrated by the recent storming of the US Capitol: an event in a country that I would have always considered to be among one of the most stable in the world"

Non-financial risk consultant

Baker McKenzie.

The importance of getting technology change right

Christoph Kurth, partner and member of the global financial institutions leadership team at Baker McKenzie, covers some of the rapid technological changes under way brought about by, and in the wake of, the Covid-19 pandemic

Key takeaways

- Covid-19-propelled digitisation is increasing the number of technology change projects.
- Failed technology changes are more serious than other change management failures and they are likely to impact customers.
- Identifying why projects fail, continuing investment and change, using cloud technology and having robust governance arrangements are all vital to reducing the number of incidents and their impact.
- Having in place a robust IT or cyber risk incident response plan, including required third-party support, is essential to mitigate fallout from failed IT change management or other IT and cyber risk incidents.

Technology change on steroids

Technology in financial services is no longer limited to fintechs. Its adoption is a vital component of every financial institution's business model in responding to disruptive competitors, meeting higher customer expectations and reducing costs. We have been living in the fourth industrial revolution for some time, but Covid-19 has further accelerated the digitisation of financial services – some commentators consider parts of the industry have advanced five years within the space of just one year – and, inevitably, installing new IT brings new opportunities, but also risks. Given the intensity of technology changes being put through at a fast pace with stretched resources, the usual risks may be elevated, particularly where there are new technologies. Operational risk managers must design and put in place effective processes to identify, manage and monitor them – during and after change. The increased expectations of financial institutions in this respect are growing, as reflected in an increasing number of regulatory requirements.

Technology change management review

The recent publication by the UK Financial Conduct Authority (FCA) of a cross-financial services review into technology change management is timely and welcome.[1] While the organisations surveyed are UK licensed, the findings are relevant to all financial institutions wherever they are regulated. The review considers how financial institutions manage IT change, the impact when changes fail, and how to reduce their number and seriousness. It aims to identify ways in which related operational risk can be reduced.

With increased dependency on digital services, even short-lived incidents, such as a denial of service, can cause significant disruption, reputational fallout and regulatory exposure. According to the FCA survey, failed IT changes are generally more serious than other change management failures, and even low-level incidents – especially when they are customer-facing – can trigger potential regulatory investigations and public enforcement action. Most financial institutions, other than fintechs, still rely on legacy infrastructures, and replacing them is associated with the highest failure rate in change management. It is for this reason many institutions are reluctant to migrate to new systems when, despite much planning and preparation, there are too many examples of problematic outcomes. On the other hand, more promisingly, cloud technology is being rapidly adopted. While it has advantages and disadvantages, it can reduce the risks involved with technology change.

The FCA review confirms that there is no one-size-fits-all solution to successful change management. Nevertheless, it confirms that robust governance arrangements and ongoing investment into technology beyond any given change life cycle are central to reducing the number of incidents and their impact.

Drivers of change

What are the drivers of change? The review found the most common reasons for technology change were maintenance and upkeep, satisfying regulatory and legal requirements, followed by improvements for customers – for example, to improve their experience of a service with new interfaces and additional functionality. Other drivers include costs and company growth, which is especially relevant for fintech entrants as they begin to scale up their operations and customer base.

Risk characteristics

Where should financial institutions focus their efforts to reduce the risks associated with change management projects? The evidence shows there are a number of key characteristics shared by all high-risk projects. Some of those identified by the FCA review are unsurprising. These are projects with external dependencies, where there are tight deadlines or poorly defined goals, as well as matters characterised as 'major' projects, where complexity and a failure to break them up into more manageably sized projects increases the risk profile. Of special interest are projects that involve replacing legacy technologies. These have been 'patched over' for many years and work alongside newer applications – a particular issue with traditional banks and insurers – and those involving unused technology within an organisation or employing emerging technologies, such as blockchain, artificial intelligence and machine learning.

Another category bearing elevated levels of risk are those projects with substantial numbers of staff located offshore. In this regard, the role of third parties is not always factored in sufficiently and clearer communication on their responsibilities is needed. Increasingly, and more so in sectors such as payments, reliance is on unregulated companies providing technology or technical services to the financial sector, another important risk factor.

Christoph Kurth

The importance of governance

Many financial institutions use governance bodies (change advisory boards) to support the assessment, prioritisation, authorisation and scheduling of changes. The use of change management by financial institutions is also not new. In fact, the review found that most entities surveyed actually had in place "rigorous governance arrangements". A key takeaway is that, while less than 2% of technology changes go wrong, due to their sheer number their impact is significant, with 14% of these resulting in customer impacts.

As organisations speed up digitisation to enable remote working, the shift of customer preferences to digital channels and investing to improve efficiency, boost productivity and profitability, senior management must plan the implementation and risk management of change projects with extra care. The effective use of project management is also critical to achieve a high rate of success with change management, not least in ensuring that strategic objectives are met, ensuring high standards of risk management and quality control.

Effective governance starts with senior managers who should take steps to secure an effective operational environment. Here, governance arrangements that have been in place longer tend to enjoy a higher rate of success. A caveat is that such arrangements should not be left to themselves. As opposed to *ad hoc* reviews, best practice means regular reviews to ensure they remain adequate for the task, which may itself evolve when technology and business models continue to adapt as quickly as they are currently. Besides senior management, non-executive directors should bolster governance by challenging change plans. While the board is ultimately responsible, the chief operating officer or another member of senior management should have direct and specific responsibility for managing technology change. Of course, some jurisdictions such as the UK impose prescribed responsibilities on senior management function holders, who will be liable when things go wrong if they have failed to take reasonable steps.

The importance of continued investment and change

The FCA review also reveals a direct correlation between lower levels of legacy infrastructure and the success rate when implementing technology change. Moreover, financial institutions with less legacy infrastructure are less likely to have to install IT changes in an emergency, and those changes tend to be more successful – a virtuous circle. By their nature, emergency changes are carried out with speed, increasing the margin for error and risk, exacerbating any existing weaknesses. Clearly, therefore, investment in renewing and deploying up-to-date technology brings advantages beyond its inherent efficiencies and capabilities. Hence, a reluctance to invest in IT is a false economy. The review data shows that financial institutions investing a high percentage of their IT budget in change activities tend to make fewer changes that give rise to issues. The principle of 'little but often' has its rewards. The concept of regular updates is a reminder that managing the risks of change as part of everyday project management is more likely to be successful in comparison to using risk management on a one-off basis.

Cloud-based infrastructure

Public cloud service providers are fast becoming part of the financial infrastructure. They provide on-demand computing services and infrastructure managed by third parties shared with multiple entities. Financial institutions are becoming progressively more dependent on cloud because of its ability to reduce costs, enable businesses to adopt and scale new technology on demand, accelerate digital transformation and facilitate mandatory data analytics. Although they can result in a lower level of oversight and direct control, an additional benefit of change management with cloud is that it allows for more frequent change cycles and greater automation, as in repetition and consistency. This not only reduces the need for 'big bang' changes and lowers the manual risks around technology change, but also improves the ability to respond when something goes wrong.

The importance of incident readiness

Even the best-managed change project does not guarantee frictionless implementation, and even frictionless implementation of change is no guarantee for ongoing operations without friction. Because of these realities and the ever-wider use of technology, it is recognised that the management of operational IT risk and its counterpart, operational IT resilience, are increasingly important. This is reflected by the emphasis regulators place on adequate systems and controls, management reporting and clarity over senior manager responsibilities. This is against a background of recent high-profile failures in technology change management that have led to significant levels of disruption and customer detriment. Accordingly, it is essential that, during the change process and beyond, financial institutions have robust IT and cyber incident response plans in place. As a starting point, financial institutions should identify their key business services, including people, processes, facilities, information and, in particular, the technology that support these services. They must have clear governance around each technology, a clear understanding of the data these technologies process and how the process can be controlled or control recovered. Part and parcel of a robust incident response plan are also unambiguous escalation and reporting procedures, a solid understanding of reporting obligations and the instantaneous availability of trusted partners that can be brought in to help manage an incident whenever and wherever it materialises, including forensic firms and law firms.

While customers might benefit from a stronger operating platform in the future, if technology change results in service disruption, or an increased technology risk profile post-change is not managed properly, regulatory and reputational fallout from technology failure or vulnerabilities will obscure the benefits to the business for some time. The opportunities that new technology brings requires improved operational risk management capabilities and practices. This is particularly true during this current time of rapid change.

---

[1] *FCA (February 2021),* Implementing technology change, *https://bit.ly/3upCCPW*

Top 10 op risks 2021

Welcome to *Risk.net*'s annual ranking of the top op risks for 2021, based on a survey of operational risk practitioners across the globe and in-depth interviews with respondents.

As in years past, there is no great secret to the methodology: *Risk.net*'s editorial 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.

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

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

A. Top 10 operational risks 2021

Position	Op risk	2020 position
1	IT disruption	1
2	Data compromise	2
3	Resilience risk	5
4	Theft and fraud	3
5	Third-party risk	4
6	Conduct risk	7
7	Regulatory risk	8
8	Organisational change	6
9	Geopolitical risk	9
10	Employee wellbeing	-

#1 IT disruption

Integrity of core systems paramount as risk managers battle outages and hacks in work from home era

Risk managers might look back on 2020 as the year in which the threat of IT disruption – an already broad remit encompassing everything from accidental systems blackouts to deliberate attacks by outside actors – exploded into millions of home offices around the globe.

The shift to remote working left financial firms more exposed than ever to cyber attacks by high-tech adversaries, backdoor threats introduced via newly critical third-party suppliers, or hackers intent on causing chaos.

Small wonder then that industry respondents ranked IT disruption their top concern once again in this year's Top 10 op risks, and by a greater margin than previously. While the industry surprised itself with its ability to function so effectively from home, some teething problems were inevitable. Housebound employees are intimately familiar with the turmoil created by dodgy Wi-Fi connections, a virtual private network going down at the worst possible time, or the system they are trying to remote into falling over under the sheer weight of traffic.

Meanwhile, threats such as ransomware attempts, which might be easy to manage together and dismiss in the office, took on a new, lethal credibility outside the office.

"The threat landscape from ransomware remains on the rise with threat actors looking for new ways to facilitate ransom payments, such as targeting senior management mail inboxes," says an operational risk head at one global bank.

Regulators are paying close attention. Last October, Nick Strange, senior technical adviser for operational risk and resilience at the Prudential Regulation Authority, said supervisors were considering whether "regularised" remote working would improve resilience or "increase technology risk as a single point of failure". The Bank of England is in the midst of putting together its long-awaited operational resilience framework, and recent events may factor into that equation.

Perhaps more surprisingly, there were fewer operational loss events attributable to outages in 2020 compared with previous years. But high-profile tech failures at a number of banks and technology vendors and trading platforms still led to chaos in key markets such as futures and foreign exchange trading during March's unprecedented cross-market volatility.

In a prescient report published in January 2020, the BoE found that the largest banks and insurers were highly reliant on the two largest cloud providers. In late 2020, the Federal Reserve Bank of New York warned that problems at one of the large cloud providers could "plague multiple institutions at once", causing a large-scale shock that "wouldn't be possible if we had a more diverse ecosystem".

Regulators weren't immune to high-profile tech failures last year: the European Central Bank suffered an outage of nearly 10 hours on October 23, 2020 to its Target2 real-time gross settlement system caused by a software defect on a device used in the internal network of the central banks operating the service on behalf of the Eurosystem. A review by the ECB, the findings of which will be released in the second quarter of 2021, is investigating this incident as well as others that took place during 2020, including those affecting Target2-Securities, the Eurosystem's securities settlement platform.

The introduction of new systems and platforms products always carries risks, some of them harder to quantify than others. Fines for systems outages are getting bigger, though – and are a clear driver of regulators’ recent operational resilience efforts.

“If we put a new system, and it doesn’t work, regulators will come down on us like a ton of bricks. But the biggest damage will be reputational damage. And that is difficult to put a dollar value on. [But] there will be an economic loss financially as well,” says a senior risk manager at one financial market intermediary.

Keeping cyber security up to date is a constant battle, and some industry figures see breaches as an inevitability. Systems revamps remain a critical – and familiar – source of IT risk; the same individual points to the potential for outages during tech overhauls, adding that, “reliance” on old or legacy systems, “developed using outdated coding language [and] combined with a shortage of knowledgeable IT staff” is a continued problem.

“Legacy systems are particularly prone to issues arising from change management, due to the bespoke way they have been adapted over a number of years,” the op risk head says.

Of course, clients and other stakeholders rarely care what causes an outage, meaning any operational failure can also have serious reputational consequences, particularly where customer-facing systems – like banking apps or payments services – are affected.

“Say we’re putting in a bug or enhancement and it goes wrong, and as a result your systems go down. We experienced that when we implemented a new online platform a couple of years ago where it was up and down the first couple of days. You have to understand the criticality and the customer impact of any type of service disruption, whether it is fraud or cyber related or normal change management,” says an operational risk executive at a North American bank.

An operational risk consultant shares those concerns, adding that “burnout” of key employees tasked with maintaining and upgrading systems caused by the long-term uncertainties of Covid-19 could compound the legacy problem.

“There is also the exposure aspect: the consequences of IT disruption are likely to be higher, because of our increasing dependency on technology,” they add.

While the risk of IT disruption during legacy tech overhauls predates Covid-19, the consultant points out that, as firms grow ever larger – which in itself boosts concentration risk – the likelihood of such mistakes also increases; more systems requiring adjustment means more labour, and a greater chance that mistakes will be made in the process.

“The older and bigger firms I work with have more problems,” the consultant says. “Firms that grow by acquisitions often have unintegrated and fragmented systems; they need to be updated and modified.” ■

#2 Data compromise

Remote working elevates fears of data theft, misuse and abuse

For those tasked with keeping track of their organisations’ sensitive data, 2021 is shaping up to be a tough year. Large numbers of staff at financial firms are working remotely, due to the lingering effects of the coronavirus pandemic. Many users are having to access systems via VPN, often over home Wi-Fi networks, which increases the opportunity for cyber breaches. With staff scattered to the four winds, managers also lack physical oversight of potential bad actors.

Throw in a steep rise in ransomware attacks and phishing reported by most respondents to this year’s survey, and it’s not hard to see why threats to information security rank a narrow second in the Top 10 op risks 2021, behind only the basic functioning of systems.

“Information security is one area where requests and demands on proving our capability is taking far more work than I thought. The rapid adoption of cloud because of Covid means you have to double down on governance and monitoring,” says the head of cyber risk at a large US bank.

At the root of most data compromise events are faulty processes and procedures. Human error can also be a factor – or, in an era when many staff are at risk of job cuts or placed on reduced hours, malfeasance.

While financial firms publicly reported fewer losses from breaches than in previous years, 2020 brought some high-profile examples. Many firms say they are closely monitoring the ongoing fallout of the 2020 hack of SolarWinds, fearing they haven’t heard the last of the giant breach at the US software company.

At the advent of the Covid crisis last March, SolarWinds’ Orion software – employed somewhat ironically by a number of US government agencies for network outage monitoring, as well as other companies – was breached. SolarWinds’ general clients list, which has recently been removed from the firm’s website, included companies like Credit Suisse, MasterCard, and Ameritrade. Various US officials have stated that a hacking group backed by Russia is behind the attack.

On February 1, 2021, the Office of the Washington State Auditor revealed that personal information from about 1.6 million unemployment claims made in 2020 may have been exposed to unauthorised access. The compromise took place at a third-party software services provider, Accellion, when records were in temporary storage awaiting file transfer.

Bank of America suffered a data breach on April 22, 2020, while it was uploading client loan application data to the Small Business Administration’s test application platform for the Paycheck Protection Program, the bank revealed in a regulatory filing. It became apparent that other lenders and their vendors may have been able to view applicant information, such as business address and tax identification number, as well as personal information.

Breaches such as these have a range of effects on financial institutions, including legal costs, payments for customer redress and regulatory penalties. There is a potentially longer-lasting impact from reputational damage, in loss of business.

A typical breach involves a perpetrator finding weaknesses in an institution’s IT infrastructure in order to gain access to confidential information. This can be accomplished by using malware via tactics such as phishing. However, breaches can also occur from the inside, for example when firms install faulty software.

A further area of weakness can be at the point of contact with third-party service providers. The increasing reliance of many banks on cloud providers is a concern for many IT risk professionals.

“When you’re utilising cloud providers, you’re at their mercy. One small hiccup and it’s a headline risk,” says the head of cyber risk at the US bank.

The country-level chief risk officer at an international bank sees it differently. In his eyes, while increased use of cloud providers does limit a bank's surveillance capabilities versus using internal systems, this is partially mitigated by increased resilience from more sophisticated cloud providers' defence systems.

"You will have an attack, and they're going to get everything they want. All you have to do is check the phishing results, to realise there's always 1%–5% of your staff that are going to give their password, their code name, their email, everything," he says.

"But the cloud is a lot more resilient than an in-house system, because you can have multiple copies of your overall environment ready to be rolled out. As soon as one of them gets hacked, you can have teams monitoring the network for instability," he adds.

A joint statement on sound cyber security risk practices issued by US regulators in 2020 highlights three critical areas: response and resilience capabilities, authentication and system configuration.

Identity and access management are important controls in securing the IT environment, regulators noted. Institutions should establish authentication controls such as multifactor authentication, and implement controls that limit user privileges to enter and change critical business data, and regularly review levels of assigned access.

Institutions are urged to practice good "cyber hygiene" by securely configuring networks, documenting security standards, performing vulnerability scans of all network and hardware components, and rolling out anti-malware software.

Education is also a key part of an institution's defences. Firms should implement ongoing training on recognising cyber threats, phishing and suspicious links. ■

#3 Resilience risk

Industry survives biggest real-world stress test, but challenges remain for firms and regulators

Two years ago, in the course of routine business continuity planning, one of the world's largest banks drew up a scenario in which a third of its global workforce was locked out of their offices without warning due to a pandemic.

It tore it up, dismissing it as unrealistic.

"Our planning wasn't good enough," says a senior executive at the bank, reflecting on the real-world stress test of the financial industry's resilience that was 2020. "I'll be candid: we never thought about the global non-availability of staff to anything like this degree. We talked about it – we even looked at pandemic modelling based on World Health Organization data – but we said 'this couldn't happen'. We only considered the impact in very localised contexts."

He is far from alone, of course: financial firms of all stripes and in every corner of the globe have weathered coronavirus-related tumult this year, testing their capacity to deal with challenges such as unprecedented market volatility, back-office bottlenecks and trade breaks, all while rushing to properly equip employees for long-term remote working.

Risk managers cited threats to their operational resilience so frequently, in fact, that it appears at third place in this year's Top 10, behind only risks specifically threatening the basic functioning of systems and the security of data.

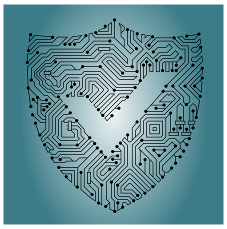
Resilience planning – which the head of strategic risk at one large US asset manager distinguishes from operational risk management as the ability to bounce back from failures, rather than trying to prevent them from happening – was a new entrant in last year's Top 10, sitting awkwardly among more familiar threat categories like technological disruption, fraud and conduct risk. Back then, its appearance owed more to a renewed regulatory focus on both sides of the Atlantic; this year, as the op risk head puts it, it has become a daily reality.

"Two years ago, resilience sounded like an academic concept: 'you're only as strong as your weakest link'. But it's so true – this year has proved that in spades," he says.

Interconnectivity and concentration risk are familiar to the financial sector; third-party concentration risk was foregrounded sharply over 2020, with numerous industry voices calling attention to the increasing reliance of financial firms on a small group of cloud providers. The resilience of such entities is critical, regulators said, with systemic implications; while cloud platform behemoths Amazon, Google and Microsoft have enabled employees to keep working as offices closed, even a short outage at any one of them could have huge consequences for the sector at large.

Given global watchdogs are still drafting their supervisory frameworks around resilience, the regulatory context is still vitally important – and in a case of practice rapidly overtaking theory, watchdogs are amending their proposed requirements in response to the pandemic.

In October, Nick Strange, senior technical adviser for operational risk and resilience at the UK's Prudential Regulation Authority, told a *Risk.net* conference the UK could revisit its stance on hard-and-fast targets on minimum service provision after outages, to see whether they were "still appropriate" following the coronavirus – an issue global supervisors have not always seen eye to eye on.



On October 30, the US Federal Reserve published its own sound practices to strengthen operational resilience proposals, in a short discussion paper. Prior to publication, Fed deputy director for policy Arthur Lindo – who also leads the Basel Committee on Banking Supervision's working group on operational resilience issues – said that the Fed's stance had been strongly influenced by the responses of financial companies to the pandemic.

"The importance of design[ing] resilient systems and operations, along with incident response programmes, has been highlighted as banks have needed to respond to Covid-19 related impacts," says one US op risk supervisor. The individual adds that the prevalence of other threats, like natural disasters and the use of ransomware, also make the need for such resilience clear.

The Basel Committee also published its own high-level operational resilience proposals in 2020, issuing a consultation paper in August. The Basel paper takes the view that the work of resilience must be multidisciplinary, involving concerted efforts from a number of functions including continuity planners, risk management and governance – while leaving national supervisors a fair amount of latitude to tailor requirements for their own jurisdictions.

One senior risk manager at a large financial service firm, himself a former supervisor, points out that defining resilience is in practice difficult for some supervisors. Operational resilience is defined by the Bank of England and the Financial Conduct Authority (FCA) as the ability of firms to resist and respond to operational disruption.

"What do you define as, 'It's still working?'" the individual asks. "People have different standards, and tolerances are massively different… How do you capture the diverse topography of what people think works for them? That's conceptually very hard: it's easier for the Fed, the PRA and the SEC, because they deal with major banks; the FCA looks at 56,000 firms with all sorts of business models."

Industry professionals agree that operational resilience cannot be understood in a vacuum, given the sheer volume and variety of events that can put pressure on a firm's day-to-day performance. It is a meta-category of sorts, given almost all threats can, in their own way, upset the usual course of business at dense and highly interconnected financial companies.

"Business continuity and operational resilience [are] consequential, and pivot off from other operational risk types like information security, third-party and IT risk," says one op risk manager.

Some risk managers take a sunnier view of the cloud provision issue. One professional, a chief risk officer at a global bank, argues that while heightened use of such providers and outsourcing in general increases the risk of IT disruption, the potential danger of such practices is "partially mitigated" by the resilience of the cloud providers themselves.

The ex-regulator argues that supervisors themselves – subject to the same social distancing and remote working guidelines as financial companies – were equally ill-prepared for the coronavirus, and are also struggling to perform certain duties.

"They were nowhere near ready," the individual says. Having worked for a well-known regulator, they say that the body does have some equipment for remote operations, but that the "serious calculatory work" regulators conduct is not possible without a desktop or high-powered laptop. "You can basically write a few scathing letters and email people," they add – something which could explain the big drop in fines. ■

#4 Theft and fraud

Changes in working practices since Covid shift angle of criminal attack on financial institutions

Even in normal times, the risk of theft and fraud is high on the priority list for banks. In the post-Covid age, the risk has intensified as it morphs into new, dangerous forms.

Pandemic-related changes to business practices and consumer habits have opened or exacerbated at least four areas of vulnerability for banks.

Government stimulus programmes have dangled juicy morsels of cash for fraudsters to target. Banks' own fraud detection systems have been thrown off kilter by the sudden shift to online banking. Criminals are also taking advantage of the rise in home-working to trick consumers into transferring money to fake destinations. And with more bank staff themselves working remotely, the potential for internal misdeeds is growing.

As the head of operational risk at a North American dealer says: "The risk of internal fraud such as rogue trading is amplified by people working remotely."

US banking giant JP Morgan fell victim to its own, home-grown fraud when it discovered last September that staff had siphoned off funds intended for pandemic-hit businesses into their own accounts. The funds were provided by the US government under its Economic Injury Disaster Loan programme. A small number of staff were subsequently fired, according to media reports.

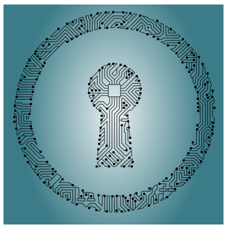
Brazil's Caixa Bank was forced to block thousands of accounts in July, after hackers attempted to steal coronavirus relief payments.

"Any time you have government handouts, there's always the possibility of fraud," says an operational risk executive at a North American bank. "You have another round of stimulus handouts so you may see fraud related to that." US lawmakers approved a third wave of stimulus payments to eligible individuals in late February.

A bulletin by the Financial Industry Regulatory Authority, issued last May, noted an increase in the use of stolen information to establish accounts to divert congressional stimulus funds and unemployment payments.

Op risk managers are right to be worried about fraud. Losses attributable to internal and external fraud made up the largest single loss category for banks and financial institutions in 2020, according to publicly reported loss data collected by ORX News, an op risk data service. Fraud losses totalled $17.9 billion last year, versus $13.8 billion for the second-largest category, 'clients, products and business practices'.

Another type of scam, according to Finra, involves impersonating firms and creating fake websites to trick customers into revealing personal information or transferring funds. Imposter websites typically mimic a firm's actual website by creating genuine-looking email domains and accounts to obtain personal



information or login credentials, which criminals can use for financial fraud. Finra noted that the prevalence of remote working may increase the likelihood of this type of activity.

Meanwhile, banks' own defences against fraud have been wrong-footed by changes in consumer habits since the onset of the pandemic. Artificial intelligence-based systems that were trained on past patterns of behaviour began churning out large numbers of false positives as online transactions soared. The bank bots, in effect, saw breaches when there were none, increasing the likelihood that real cases of fraud go undetected amid the noise.

In response, banks have had to supplement machine learning models with more traditional rules-based systems that classify transactions according to pre-set criteria such as age, occupation and income.

Changes in working patterns have affected bank staff too. With many employees either working from home or remote trading floors, financial institutions have seen an increased potential for internal fraud. As the head of a risk control firm described last year, it's not unusual for young traders to co-habit. How can firms guard against collusion by housemates who may work for rival institutions?

Banks have reacted by upping their surveillance. They are analysing voice communication records, trade data and employee behaviour to determine whether a transaction is suspicious. The head of op risk at the North American dealer says the firm is tightening controls over what people can receive and send in their email systems.

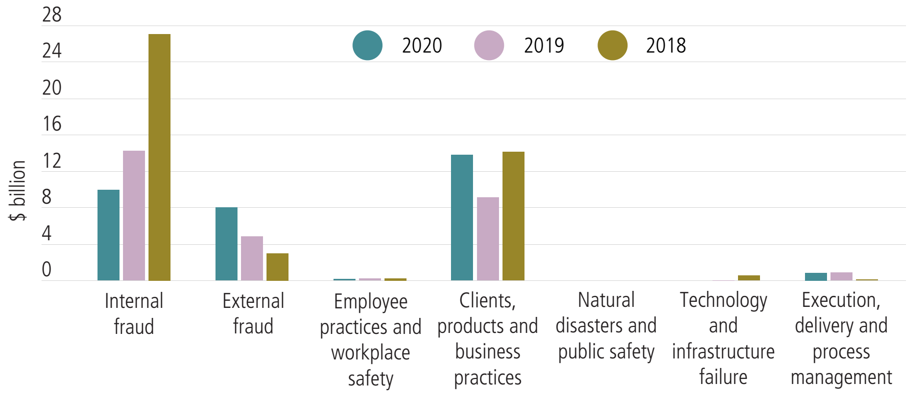
Fraud losses haven't yet trickled through into a material increase in operational risk capital, says the operational risk executive, but that could change once a full year's worth of data becomes available. "We are working on data which is six months old. So the actual effects of what has been happening recently aren't apparent yet."

Ransomware attacks also have seen an increase since the start of the pandemic. The number of ransomware attacks against the financial sector grew by nine times from the beginning of February 2020 to the end of April 2020, according to a survey of chief information security officers by tech vendor VMware Carbon Black.

The Financial Crimes Enforcement Network, a unit of the US Treasury, in 2020 warned of a sharp increase in the use of virtual currencies by cyber insurance companies, which could indicate that a business covered by cyber insurance has been targeted by ransomware. Any rise in the flow of criminal money through the financial system could leave banks at greater risk of breaching anti-money laundering rules.

Despite plummeting cash use in many countries facing strict lockdown, money laundering continues to be a major fraud concern.

1. Losses by event type



Source: ORX News

Under anti-money laundering rules in the US, Europe and elsewhere, banks must file suspicious activity reports (SARs) for questionable transactions. However, regulators only have the resources to investigate a small percentage of these reports.

Banks have been seeking more clarity on what information to include in SARs in the hopes of cutting down on needless paperwork and being able to focus on truly fraudulent activity. Forthcoming rule changes in the US and Europe will introduce what's hoped to be a more targeted approach to detecting dirty money. Firms will be required to identify specific risks and address them directly, instead of the current approach that leaves authorities swamped with reports, many of which are not an enforcement priority.

A proposed rulemaking in the US would encourage banks to boil down the content of SARs so that the reports only contain information with a "high degree of usefulness" for enforcement agencies. In other words, the onus shifts from the regulator to the bank in deciding what is or isn't relevant.

In general, experts say institutions can help combat the threat of fraud by maintaining good cyber hygiene, which is network management and configuration and strong authentication, combined with effective security monitoring. ■

#5 Third-party risk

Pandemic and shift to cloud computing inflame concerns for banks and regulators

Creaking middleware vendors; the inability to pen-test data centres; critical support locations locked shut without warning: 2020 stress-tested organisations' reliance on outsourcing beyond any op risks manager's worst nightmares.

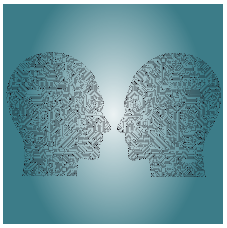
And with multinationals facing another year of uncertainty, in which employees and suppliers are part-exiled from their offices – another year in which most firms will be dependent on a handful of vendors to provide video conferencing, remote access to servers, or cloud storage – third-party risk is set to remain top of mind for many managers through 2021.

Among the concerns of financial institutions is to assess security weaknesses of their critical service providers – or for smaller outsourced firms, even their basic financial viability.

"It has never been more crucial for operational risk managers to take account of their company's critical and core third-party service providers," says an operational risk executive at a North American bank. "The risk they can expose to a company and its potential impact to daily business operations has never been greater."

Once the pandemic took hold, financial institutions carried out evaluations of critical processes to determine whether they were being handled internally or by third parties. With many third-party vendors located in far-flung locations such as the Philippines, India, Mexico and eastern Europe, users have extended their oversight of key suppliers. Potential disruption to the third party's business from Covid has reinforced the need for extra scrutiny.

"During Covid, we knew this was a big dependency and we looked at critical processes. Are they being supported domestically or by a vendor? If so, we had to go to service providers and manage them," says another operational risk executive.



Firms have also been fielding enquiries from regulators, who have expressed keen interest in the resilience of organisations. The pandemic has spurred banks to investigate the controls their vendors have put in place for managing sensitive data, given the possibility of hackers or rogue employees exploiting network vulnerabilities.

Lapses in third-party risk management were a factor in several high-profile legal settlements during 2020. Deutsche Bank, in settling a case involving the Foreign Corrupt Practices Act, was flagged for inadequate due diligence over the risks posed by third-party partners, such as the partner's reputation and relationships with foreign officials.

As part of the settlement, Deutsche must take steps to ensure the third party is performing the work described in the contract, and that its compensation is commensurate with the work being provided. The bank must also monitor third-party relationships through updated due diligence, training, audits and compliance certifications by the third party.

In January 2021, ORX News reported that the Australian Securities and Investments Commission and the Reserve Bank of New Zealand experienced data breaches in which a server used for file transfer was hacked. Access to the server was related to third-party file-sharing software that the two regulators were using.

Smaller banks that might have a greater reliance on outsourcing also found themselves exposed. In 2020 ORX News reported two cases of third-party IT suppliers experiencing issues with demand during the pandemic: Investitionsbank Berlin experienced a data breach caused by overcapacity in a third-party website processing grant applications, and Deutsche Kreditbank saw its externally hosted mobile banking app and brokerage website go down due to high demand.

Financial firms are keeping a close eye on the financial stability of their critical service providers, including scrutinising audited statements to determine their credit standing, sources of liquidity and available capital.

And regulators are stepping up their oversight of third-party relationships, especially in the area of cloud computing. In a joint statement in April 2020, US regulators warned that firms need to be able to identify and control the risks associated with cloud computing, contracts between cloud service providers and financial institutions need to be carefully reviewed and appropriate controls implemented to prevent operational failures or breaches.

In general, regulators are neutral to the technology or to whether a bank operates in-house, outsources to a more traditional network service provider, or outsources to a cloud provider. Their focus is on whether the institution is engaging that third-party service in a safe and sound manner. The responsibility for the third-party operation falls to the bank.

One industry professional points out that cloud service provision is currently a triopoly, with Amazon Web Services, Microsoft Azure and Google Cloud sharing most of the market between them. An outage or failure for one of this trio would create "a mess of awesome proportions", the individual says.

As the pandemic has accelerated the move to the cloud, the work to assess the importance of applications being ported becomes more crucial.

"We have seen cases where processes associated with applications are incorrect. Do we know what we're putting into the cloud and making sure it's accurate," says the second operational risk executive.

Controls management is particularly tricky for hybrid cloud environments, say banks, in which public and private clouds are combined so that data can be shared between them. IT risk professionals note that hybrid clouds are more difficult to secure than private clouds, because it's harder to delineate data flows, which apps are talking to which, and who has access, especially for organisations with large legacy systems.

The UK Prudential Regulation Authority, in 2019 guidance on third-party risk management, noted that when testing exit strategies from cloud service providers, firms with hybrid cloud environments needed to take into account the back-up functions located in their private cloud. ■

#6 Conduct risk

Remote working vastly complicates the job of conduct risk supervisors

For operational risk managers, circling the trading floor, happening upon colleagues in corridors or at the coffee machine and going to meetings have long been vital ways to spot hidden behaviours.

"By working in the office, you can pick up informal signals and signs that may point to issues," says the head of op risk at a large international bank.

With many professionals confined to their homes since the early part of 2020, that source of intelligence has been lost. So it is not surprising that in the latest *Risk.net* ranking of Top 10 op risks, conduct risk has moved up from the seventh-most concerning risk for op risk managers to the sixth.

While informal controls on improper behaviour – such as rogue trading and mis-selling – have been eroded, at the same time the risk of misconduct has gone up, notes a regional chief risk officer at another large international bank.

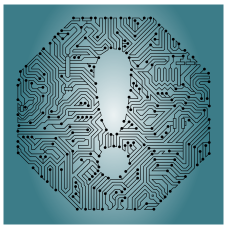
For instance, several sources have pointed to situations where young traders share a house with bankers from other organisations, raising the risk that proprietary information will be leaked, whether by accident or intentionally. Similarly, when working from home, it is much easier to make a call on a personal mobile phone – something that is prohibited on many trading floors – though working in the office is not a panacea either.

"There is nothing to stop staff from doing that when working from the office," says the head of op risk at the first bank. "They could just as easily walk out and have a coffee with a client."

Remote working may have also increased psychological pressures on traders. But, without regularly seeing them in the office, it is much harder to identify those who are not in the right state of mind to be taking big risks and making a market for clients.

In response, some banks have enhanced formal controls on employees. One example is the introduction of 24-hour monitoring of the computers of traders who work from home.

The regional chief risk officer at the international bank adds that goals for staff need to be clearly defined to improve oversight. "[These] are even more important when you don't see staff members every day," he says.



In other cases, traders police themselves – by keeping open through the day a video chat with other traders at their firm, according to a source at a large Asian investment bank.

But op risk managers also have to simply trust staff more than they used to and rely on a good corporate culture, sources say. Although culture is a nebulous concept and proved challenging to maintain even in the pre-Covid era, the consequences of an unhealthy culture can be painful and long-lasting.

For example, in January 2021, Deutsche Bank agreed to pay US authorities almost $125 million to settle charges related to actions that took place during 2008–17. And in one of the largest recent fines for misconduct, Goldman Sachs shelled out a combined $5 billion in fines and settlements to various parties for its involvement in extensive fraud at Malaysian sovereign wealth fund 1MDB.

Before a corporate culture can be improved, its quality and weak spots need to be pinned down.

A novel way of doing that was proposed in November by a senior executive at HSBC. Georges Elhedery said firms could draw on the vast amounts of employee surveillance data, currently being gathered by dealers, to capture positive signals as well as negative on the bank's culture. The data could be analysed by machine learning algorithms, he suggested. HSBC already makes use of machine learning bots across various channels of staff communication, to identify untoward activities.

But establishing a good culture is not enough. Firms then need to make sure it is resilient in the face of unexpected pressures and temptations.

One such test came during the early stage of the Covid-19 pandemic, when the US government launched sweeping economic support measures, including loans to be routed to businesses through banks. The emergency package provided ample opportunity for fraud. For instance, in September, JP Morgan said in a memo to staff that it was investigating some employees for misuse of the Paycheck Protection Program loans and other government programmes.

With or without the pandemic, ensuring good conduct by staff is a perennial job for op risk managers. The danger is that the distance from colleagues and the potential feeling of alienation as many workers remain at home have made that job even harder. ■

#7 Regulatory risk

Big dip in fines belies lingering fears over Covid loan mis-selling and sanctions risk

When supervisors intervened in markets over the past 12 months, it was more often to protect lenders than slap firms with fines: with a couple of notable exceptions, regulatory penalties in 2020 plummeted as Covid-19 spread across the globe.

Still, regulatory risk – the fear that changes to rulesets and supervisory expectations create openings for operational mis-steps, disclosure challenges, restrictions on activity or straightforward financial penalties – is never far from thought for banks, stung by fines and penalties totalling almost $1 trillion over the last decade.

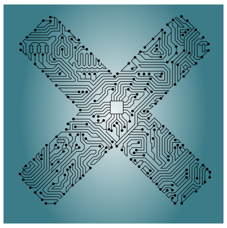
Those changes do not have to take the form of regulators wielding a big stick, or even be aimed at banks themselves; last year's huge government intervention programmes are a case in point. Like many official sector initiatives put together in a hurry, lenders fear the government support packages could become a major source of operational risk.

Any rapid deviation from stated regulatory policy carries its own risks, many argued at the time: "We were having to implement new government programmes at lightning speed," says a senior op risk executive at a large North American bank.

Regulators' swift attempts during the springtime to help banks free up liquidity to support the economy created difficulties from a nuts-and-bolts modelling perspective – as well as a potential source of reputational risk for those firms that rapidly became seen as outliers. Deutsche Bank, for instance, attracted scrutiny for its decision to extend the economic forecast horizon on its loan-loss provisioning model out to three years – even though it argued its move was designed to free up liquidity provision to the real economy in line with official sector requests – a decision that was subsequently vindicated.

The speed with which emergency loans to stricken businesses were rolled out meant banks were forced to expedite some of the usual key processes that safeguard against accusations of mis-selling by failing to rigorously assess whether new loan products meet client suitability criteria – chiefly, whether a customer actually needs the product, can afford it and that it is offered on a non-discriminatory basis.

In the US, the Paycheck Protection Program, designed to provide financial assistance to small businesses, resulted in allegations that large banks employed deceptive lending practices that favoured large clients by providing forgiveness of



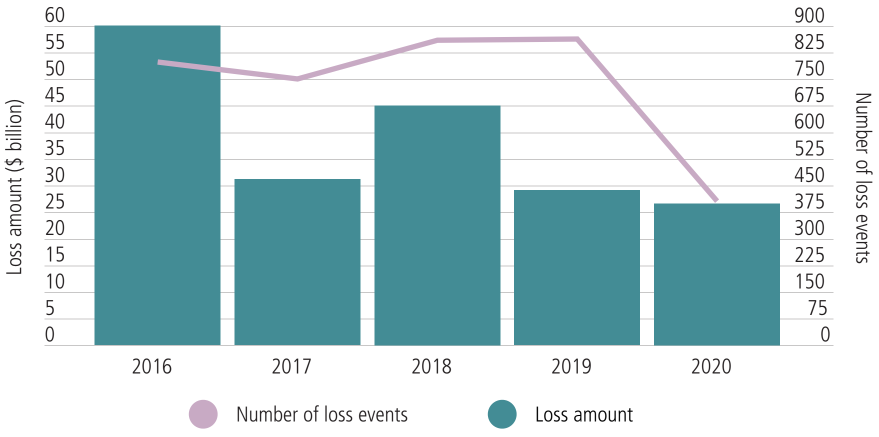
loan proceeds for up to two-and-a-half times an owner's monthly payroll.

As the speed of change accelerates, organisations need to have appropriate processes in place to manage the changes. Covid has clearly pushed the pace of change to the limit.

"As an example, when we implemented the PPP programme, the rules came out on a Friday and we were up and running on a Monday. That doesn't happen normally," the senior op risk executive says, grimacing with understatement. "We were never [before] forced to operate at such speed."

Another senior op risk manager at a large European bank says the dynamic holds true for their country's Covid loan programme rollout too – and foresees trouble down the line if the

2. Annual loss summary



Data refers to financial services firms only. ORX maintains running totals of historical loss events, which it updates periodically – to take account of fines or settlement amounts subsequently increasing or decreasing, for instance, and to add previously unreported losses to its database. This means the loss totals reported here may differ from static prior year totals reported by *Risk.net*.

Source: ORX News

political landscape shifts decisively against banks, as it did after the financial crisis.

"I think everybody's a bit nervous. We were asked to essentially execute against a government mandate at a speed that wasn't consistent with normal processes. We weren't asked to do much about checking affordability, and those sort of elements. You're taking a leap of faith you got things right, and that the regulators and politicians won't change [their attitude]. Because in five years' time, if we have a government that says 'no, we won't [honour] any of the loan guarantees – the whole thing was your fault' – then everyone is sitting on billions in unprotected credit risk. I don't think that'll happen – but there's bound to be some ugly things that crawl out from under the woodwork, because it was so hard to do," he says.

While 2020 brought fewer losses overall from fines and penalties, there were notable exceptions: Goldman Sachs' mega $5 billion in penalties, settlements and disgorgements for its role in the 1MDB fraud being by far the largest of these. Citi was also fined over control failures that led to the bank inadvertently wiring more than $900 million to a group of hedge funds it was involved in a lending dispute with. The bank's chief risk officer, Brad Hu, subsequently departed.

Sea-changes in the political landscape can also lead to shifting supervisory attitudes to areas of emerging risk too – and plenty of opportunities for compliance mis-steps. In the US, for instance, regulators have thus far moved with far less speed on climate change. But recent signals suggest that this could change in the near term. In an interview in February, acting Commodity Futures Trading Commission chair Rostin Behnam indicated a more interventionist attitude to climate-financial risk within the Biden administration.

Though government policy can be slow moving, professionals in the financial sector know where their industry is heading. One country-level chief risk officer says that the "most impactful" impetus for regulatory change is increasing awareness among supervisors of environmental risk factors.

"We're entering a new phase for [the category], which is the quantification of environmental risks," the CRO says. "Regulators have been kind, in a way, and the market is still being kind" – but the industry knows.

The CRO argues that, in the coming years, financial companies will need to tread cautiously when it comes to investment. "I expect you will have to be very careful [about] which types of exposures you put on; you'll want to think twice about lending to a client with a negative environmental profile."

That is certainly true for European asset managers, who will be required to comply with the 'level one' requirements of the European Union's flagship Sustainable Finance Disclosure Regulation (SFDR) from next month, a painstaking new set of disclosure requirements for ESG-labelled investments. Full implementation of the regulatory technical standards will be required in January next year.

Finally, the insidious influence of Brexit continues to pull attention towards diverging regulatory frameworks. Earlier this year *Risk.net* reported on swaps trading drifting to the US, as a result of the lack of equivalence arrangements between the UK and EU; more recently, the UK Treasury has suggested it may walk away from the 'open access' Mifid II rule, with some commentators asserting that the move will allow exchanges to extract higher profits from customers. ■

#8 Organisational change

Change the sole constant as industry ponders its post-Covid future

When HSBC, Europe's largest bank, announced late last month that it planned to reduce office space by 40%, it encapsulated what the long months since the start of the coronavirus crisis have driven home to many banks: plenty of the changes to operating environments wrought by Covid will be permanent.

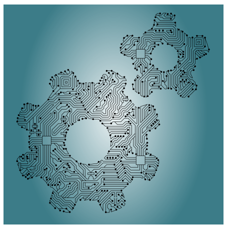
In an era when many customers have learned to live without being able to visit their lender's branches, many are openly contemplating a future in which the idea of a bank looks very different – one in which it could be leaner, cheaper and more resilient. That's the plan, anyway: getting there will mean an immense amount of upheaval – and plenty of opportunities for mis-steps.

Op risk managers were fretting over their firms' responses to epochal changes impacting their operating environments well before the pandemic struck: climate change, the Libor transition, Brexit, and digitalisation, to name a few. But Covid has accelerated the pace of change while proving that large organisations can be surprisingly nimble at weathering crises.

The rapid shift from on-site to work from home is an example of the need for effective change management for processes and services if it is to become permanent.

"Although the impact of Covid on operations has been well managed to date, there are risks associated with working practices over the coming year," says an operational risk executive at a large global bank, pointing to changes in firms' control environments that have only been patched so far as one area needing attention.

Still, as the pandemic enters its second year, companies will need to adapt to further changes down the road. Survey respondents cite change management as a perennial concern: the volume of change, ensuring appropriate budget prioritisation and executing shifting organisational mandates are raised frequently by firms of all stripes. Responses to the macro environment – such as Brexit, credit stress and changing regulator, investor and client attitudes to emerging risks such as climate change – are also cited as factors driving organisational change.



"Our industry and infrastructures are changing how we do things. All the banks are dealing with negative [real interest] rates, and how are they are going to change from a Libor perspective," says an operational risk executive at a large North American bank.

The speed of change and the need to innovate has spurred the introduction of technologies whose deployment needs careful management: machine learning, for instance, and robotic process automation. Banks need to have effective change management programmes to implement those in a safe and sound manner. Risks associated with organisational change can also take the form of mandatory regulatory requirements, project and programme management, legacy processes and systems and new third-party suppliers.

Managing change, and the potential overlap and interplay of these changes, can lead to a compounding of the impact of organisational change risk.

"Significant levels of change aimed at transforming and restructuring our organisational operating model are planned in 2021, alongside managing a demanding regulatory and risk agenda in a challenging economic environment," says an operational risk executive at a large European bank.

The past year has taught the industry that it should not take anything for granted given fluctuating markets and an uncertain and changing customer base. Lack of strategic anticipation to address structural changes and maintain a sustainable business model, such as dependency on a few key products or markets, will mark the laggards.

Perhaps the biggest source of organisational change is idiosyncratic to each firm: mergers and acquisitions carry their own set of risks, including the integration of disparate systems, redrawing of organisational charts and turf battles.

The 2019 merger of SunTrust and BB&T to create Truist Financial Corp was expected to usher in a wave of mergers among small and medium banks. While the pandemic has put a damper on mergers during 2020, M&A activity is expected to resume once Covid ends.

"Business transformation risks, including the impact of recent major integrations and divestments, has downstream impacts on technology, operations, resiliency, third party and people risks," says an operational risk executive at a large financial market infrastructure. ■

#9 Geopolitical risk

Stimulus unwind, Covid nationalism and regime changes spell volatile operating environment

Covid-19 erupted across the globe just as last year's Top 10 operational risks survey was going to press – a pandemic few predicted the severity of, nor its long-lasting insidious effects. What followed from governments was equally unprecedented: an attempt to counteract the virus by shuttering entire economies almost overnight, and to tourniquet markets rapidly pricing in the impact with massive fiscal and monetary stimulus.

In the advent, it took a Herculean effort from banks and financial firms just to keep pace with and adapt to these seismic changes to their operating environments. But perhaps greater risks lie in weaning markets off the medicine; in seeing which jurisdictions will move first to unlock their economies, following successful mass vaccination programmes; which will allow unrestricted international travel to resume – and how they'll set out plans to unwind stimulus measures, and start paying for them in the painful years to come.

All of that seemed far off in March 2020, as central banks rushed to shore up markets that were reeling from the fallout. The US Federal Reserve, for instance, offered trillions in stimulus and monetary easing measures – but only after markets had endured a couple of weeks of unprecedented volatility, and the US Treasury market had flirted with disaster. Stimulus has also had a deeply distorting effect on price valuations: although the S&P fell 33% in March, by September it had risen even higher than pre-Covid levels.

"What is particularly troubling is that we've pretty much exhausted the governmental tools that we could use to solve this crisis," says a regional chief risk officer of one Asian bank. "We can't lower rates more – they're at the bottom – and we can't inject more liquidity, as that will go straight into the stock market again."

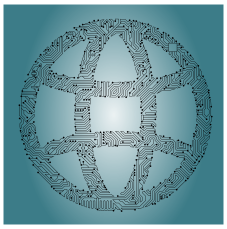
Moreover, while central governments appeared to act in a co-ordinated way going into this crisis, it is far from certain that such a unified approach can be maintained, as the liquidity life support is switched off – raising the spectre of further market disruption and policy fragmentation. Any difference in approaches taken could potentially place an additional compliance burden on financial firms operating across multiple jurisdictions.

Changeable attitudes to Covid lockdowns have also made it harder for firms to recruit and organise staff when they need to, both in-house and with contractors. Sweeping stay-at-home restrictions in countries like India, a key back-office jurisdiction for many banks, saw staff shut out of their offices almost overnight in March 2020, with some unable to adapt quickly to homeworking, cramping dealers' ability to pull key data and produce key reports close to quarter-end reporting dates.

Unable to send staff abroad, some firms say they have been forced to reassess the viability of projects that they outsourced overseas, bringing some of these projects onshore. This has placed even higher demand on the local job market, increasing the cost of human labour, at the very time that many expatriate workers are returning home.

"If you get senior project people who were leaving for other jobs or better-paid jobs, that puts pressure on the projects and everyone else. This overall pressure is driving costs up," says a risk manager at a securities exchange in Asia.

While Covid-19 is still very much at the forefront of everyone's minds, the geopolitical pressures that persisted before the upheaval of 2020 – most crucially national protectionism – have not gone away.



Rising nationalism and deepening trade wars, most notably between the US and China, were again flagged by many respondents to this year's survey.

Political sea-changes can also spell sudden shifts in the regulatory environment – both in terms of policy frameworks and broader attitudes to supervising financial firms. Although there is now a new commander-in-chief in the White House, many of the policies that former US president Donald Trump instigated remain.

While Joe Biden has made it clear that he is keen to rebuild bridges to the rest of the world, rapid unwinding of legislative programmes can create uncertainty in legal and operating environments for financial firms. Climate change is a case in point, with regulators under the Biden administration publicly pledging to make up for lost time when it comes to adopting policies the previous administration repealed, sat on or actively resisted.

The departure of the UK from the European Union, which formally took place at the end of the past year, has also been creating its own uncertainty, with many firms having to decide how much staff on trading infrastructure to retain in the country and how much to shift elsewhere – all of it creating room for operational missteps and the risk of upsetting new supervisors.

This is true even on issues banks and financial firms had reason to consider settled, like the trading and clearing of euro-denominated derivatives: delays over equivalence decisions have heightened the risk of swaps trading shifting away from the UK, but any sudden decision over this carries with it the risk of getting things wrong.

Financial institutions also expressed worry about regional social unrest in developed markets, with many firms exploring ways of stress-testing the impact on portfolios.

At the beginning of the year, a group of protestors supporting Donald Trump broke into the Capitol building, where the US Congress meets, in a failed attempt to overturn the results of the election. Last year, riots erupted across the US following the killing of an unarmed black man by police officers in Minneapolis. Similar unrest was seen in the UK and parts of Europe.

"I feel that we are seeing increased volatility in previously stable regions. This could, for example, be demonstrated by the recent storming of the US Capitol: an event in a country that I would have always considered to be among one of the most stable in the world. My concerns have also been heightened by the pandemic which seems to have resulted in, and highlighted, rising inequality, a factor that can result in increased volatility," says a non-financial risk consultant based in London.

In Hong Kong, the emergence of a new social unrest, raised by a contentious extradition law allowing the extraction of suspected criminals to mainland China, has developed into a national security issue, with financial institutions expressing concern about being targeted by protestors.

"We are sort of a natural target to [protestors], so we are in communication with Hong Kong Exchange about how they were dealing with it," says the general manager of enterprise risk of another exchange. ■

#10 Employee wellbeing

All-encompassing impact of Covid leaves employees with the feeling of 'living from work'

Stress. Burnout. Running on empty. Call it what you will – the financial industry faced an equally grave mental health crisis in 2020, to go with the humanitarian one playing out all around it.

The industry might have showcased its resilience with its ability to continue functioning with tens of millions of employees working from home, sometimes in makeshift offices, often competing for space and attention with children and loved ones. But for many employees, the early days and weeks of the pandemic – when markets were in freefall, control environments were being redrawn overnight and processes upended – probably felt more like a grim feat of endurance.

"Think about people working in a remote environment getting through more than two times their day job in a fairly seamless way – they did that by working longer hours," Deutsche Bank's then-head of non-financial risk, Balbir Bakhshi told *Risk.net* in the aftermath. "The mental health hotspots to watch, from an inherent risk perspective, are in areas like that."

It's not a working life any employer would wish on their staff. Covid anxiety has resulted in an "unravelling" of productivity, focus and morale at times, says the regional chief risk officer of one global lender – all of which can lead to employees making mistakes. The physical and mental wellbeing of his staff has become his top concern for the year ahead, he says.

"This is a risk that we need to take into account: the fact that our staff haven't been able to go on holiday, our staff haven't been able to meet their extended family, some of them have been through a loss – whether they've lost someone actually from Covid, or someone in their family has lost their job."

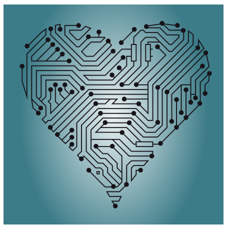
The management challenge for firms stems from the lack of universal remedy for staff, adds the CRO, as everyone could be facing very different, idiosyncratic problems.

"As a company, we are limited as to what we can do to mitigate this risk, which is why I think it's even a bigger risk than others, because we have limited powers to [manage] this. I can't go to the government and say, 'please reopen the borders, because my staff needs to get out there and travel, they need to meet their family'."

Banks and financial firms have good reason to fear from employees they fail to look after: threats from disgruntled employees, perhaps placed on part-paid leave, threatened with redundancy, or given a gruelling stay of execution in struggling firms all increase the insider risks a company faces, from aiding and abetting cyber attackers to vanilla theft and fraud.

The scale of the risk is likely impossible to quantify – but even before the pandemic, research suggested the biggest cause of business disruption across industries globally is poor health, outstripping other operational risks such as cyber attacks and IT outages.

Mental health-related absence can also be more costly for a company than absence from physical illness or injury. Employees who are absent for sickness such as stress, anxiety and depression are off work for 40% longer on average than those absent due to all types of illness and injury, according to recent UK government statistics.



A senior operational risk manager at one large European bank says supporting employees is one of their top priorities for 2021 – but adds that, with most staff and many managers stuck at home, it "remains a challenge".

"With the impact of lockdowns, accompanied by seasonal factors, [we're] likely to see some regression, with negative effects on mental health, fatigue and increased absence. Our HR function is focusing targeted support interventions to address increased pressure and potential burnout whilst being mindful of longer-term impacts on psychological [mental] wellbeing," they add.

A permanent move to more flexible working practices could help – working from home through choice is a world apart from doing so forcibly – but it will mean placing greater trust in employees, adds the CRO.

"That's hard. It's easy to do at the beginning, because you have this strong global movement towards it. But when the pandemic eases a bit, or more importantly, if your profits start to decline, [your firm] will want to get a stronger hold back on your staff members: 'guys, we're not meeting the target here, let's all go back to the office'."

A decline in mental health among individuals could open up banks to litigation risk as workers look to sue employers for stress-related illness. In 2019, JP Morgan faced a lawsuit from the family of a sales executive who committed suicide after suffering from depression. ■

Baker McKenzie.

Heightened operational risks in a changing world

Christoph Kurth, partner and member of the global financial institutions leadership team at Baker McKenzie, discusses the growth of conduct and operational risks in the light of the pandemic, including those caused by mass home-working, the enhanced technological ability to address them, and why we should design a new type of workplace culture or risk losing one altogether

The financial crisis that began in 2007–08 ushered in a wave of regulation that is still being rolled out today. How can regulators best support financial firms this time around as they emerge into a post-pandemic 'new normal'?

Christoph Kurth: The global financial crisis caught financial institutions unprepared and the regulatory system wanting. The international response saw the creation of the Financial Stability Board and commitments made to reform global financial architecture and to rein in excesses that had contributed to the crisis.

During the Covid-19 pandemic, regulators have responded sympathetically to businesses by pushing back consultations on new rules, with exceptions as required. This pragmatism should continue and previous reforms should be allowed time to bed in. That said, there is an important role for regulators to play in relation to the digitisation of the industry, including digital assets, and the transitioning of the economy to carbon neutral by 2050.

Financial institutions are conscious of their key roles as intermediaries in this transformation, which has been accelerated by Covid-19, yet there is a need for coherent, globally aligned frameworks and accompanying standards to allow them to play their parts effectively. Putting these in place and providing certainty will allow financial institutions to rise to the challenge more effectively, contribute positively to the transformation of the economy and to harness digitalisation for efficiency gains.

Christoph Kurth

What impact has the Senior Managers and Certification Regime (SMCR) had on the approach to conduct and culture in financial organisations? To what extent should we expect to see investigations and enforcement actions arising from pandemic-related stress and turmoil?

Christoph Kurth: It is still too early to assess the impact of individual managerial accountability regimes on conduct and culture. However, anecdotal evidence suggests senior managers are more engaged with compliance and conduct risk; no longer is it left to compliance officers or as the last item on the board's agenda. With Covid-19, there has been a real concern that a focus on stressed markets and widespread home-working, with its practical challenges of supervising client-facing staff, may translate into increased conduct risk. In fact, a more complex and varied picture has emerged. On the one hand, anecdotally, many businesses have doubled down on facilitating healthy cultures to reduce conduct risk. On the other, many businesses appreciate extended home-working leads to the loss of physical town halls, in-person bilaterals and team meetings as well as 'water-cooler moments' – all important in creating and maintaining culture.

Businesses must design new ways of building culture or risk losing it. As it was after 2008, as we return to the new normal we can expect to see investigations and enforcement activity rise as misconduct comes to light. However, given the reforms of the past decade, including the SMCR, this time around cases may be more modest. In any event, due to the long lead time for investigations, we will not know the full picture for a while.

Sophisticated analytics and a greater volume of available data have enhanced firms' ability to detect and monitor operational risks. What threat does this pose to customer/employee rights and data privacy?

Christoph Kurth: Rapid developments in advanced data analytics, artificial intelligence (AI) and data capture have created myriad new opportunities for our clients. We are partnering with a number of them to implement innovative technologies to boost productivity and mitigate op risk, while also managing customer and employee compliance and wellbeing. From an employment perspective, increased reliance on technology – and especially employee monitoring – can expose employers to risks of discrimination and breaches of the implied

The addition of employee wellbeing to the top 10 operational risks for 2021 reflects the heightened risk that has come with the surge of home-working during lockdown

duty of trust and confidence. From a data privacy perspective, many new technologies, if used to their full potential, may collide with concepts ingrained in the General Data Protection Regulation; regulators have shown they are alert to transgressions in this regard. Similarly, customer-facing technologies must be implemented carefully to mitigate against overreaching data processing that may present real regulatory risks. The sheer volume of data collected means technical and organisational security measures are of fundamental importance. Data breaches can cause considerable reputational and commercial harm, as well as exposure to regulatory action.

Covid-19 has had a profound and lasting effect on the world of work, placing greater reliance on digital channels and technology. What are the pitfalls financial firms face as they scramble to replace ageing IT infrastructure and systems?

Christoph Kurth: The fourth industrial revolution is well under way, but Covid-19 has further accelerated the digitalisation of financial services – some commentators consider parts of the industry to have advanced five years within the space of just one – and, inevitably, opportunities also bring risks. Given the intensity of technology changes being put through at such a fast pace with stretched resources, the usual risks may be elevated, particularly where there are new or emerging technologies. Most financial institutions, other than fintechs, still rely on legacy infrastructures, and replacing them is associated with the highest failure rate in change management. In fact, there is a direct link between lower levels of legacy infrastructure and the success rate when implementing technology change. Moreover, financial institutions that lack legacy infrastructure are less likely to have to install IT changes in an emergency, and those changes tend to be more successful – a virtuous circle. By their nature, emergency changes carried out with speed have an increased margin for error and risk, exacerbating any existing weaknesses.

New technologies such as AI, machine learning and blockchain bring equal measures of opportunity and risk. To what extent does regulation act as a drag on innovation, and how can regulators find the right balance going forward?

Christoph Kurth: Although regulation rarely keeps up with technological advances and changing market practice, this does not necessarily mean it holds back innovation. While it can impede new services and products, it is often a facilitator rather than an obstacle. A good example is payments, which today are synonymous with fintech. If the Revised Payment Services Directive had not required account providers to allow access and share customer data, we would not have seen such tremendous growth in new innovative third-party services. In contrast, the lack of legal and regulatory certainty, alongside political and other concerns, may hold back the development of digital assets – intangible assets supported by blockchain technology.

Clearly, regulation can be overprescriptive, stifling innovation and making compliance costly, but most regulators recognise the benefits of innovation and competition to the market and, besides regulatory sandboxes, seek to provide a technology-neutral framework within which the market may operate. Proof of this is in the approach of the Swiss Financial Market Supervisory Authority of enhancing client onboarding via digital channels and *The Kalifa review of UK fintech*,[1] the very welcome proposal for a new regulatory framework for emerging technology. Regulation should not regulate or hold back technology, but provide certainty on the regulatory treatment of technological innovation.

Given the increasing incidence of geopolitical risk facing the financial system, how should regulators and financial firms respond?

Christoph Kurth: Geopolitical risk is a fact of life with cross-border business. We have just come through Brexit, which has cut market access in Europe and where the extent of future equivalence-based access remains uncertain. Political and economic rivalry is increasing between the West and China, and with it possible protectionism. There are no easy answers to managing such uncertainties, but financial institutions must identify their vulnerabilities and assess the likely impact. Regulators will of course expect financial institutions operating in 'at risk' markets to be prepared, but supervisors can also help by liaising with counterparts, offering guidance and, where necessary, providing a degree of forbearance and flexibility to allow financial institutions time to adjust and adapt.

Which op risks should financial firms be most concerned about?

Christoph Kurth: IT disruption and data compromise are likely to be near the top of firms' agendas. The last year has seen accelerating digitalisation during the pandemic. With increased dependency on digital services, even short-lived incidents such as a denial of service can cause significant disruption, reputational fallout and regulatory exposure. Escalating cyber attacks that increase the risk of data compromise are an indirect consequence of greater interconnectedness in the banking and payments sphere, particularly when IT processes are built on a patched legacy infrastructure. Regulators, such as the Monetary Authority of Singapore, warn that, because large-scale remote working is a recent development, the risks may take time to fully emerge.

In recognition of such risks, countries are imposing tougher obligations on businesses over the collection, use, sharing, storage and disclosure of data. Whereas before, data protection regulators might not have brought enforcement action, now they just as likely to as financial services regulators, and can impose substantial fines based on turnover.

Another issue worth mentioning is the Covid-19-related impact on staff wellbeing. This reflects the heightened risks around home-working during lockdown, on the basis of which many employers have developed special programmes. As we move to the new normal, they should be careful not to overlook this duty.

---

[1] *R Kalifa (February 2021),* The Kalifa review of UK fintech, *Gov.uk policy paper, https://bit.ly/3kGNXGM*

Baker McKenzie.

COVID-19 represents one of the greatest challenges to the business models of financial institutions and the way they do business.

Finding Balance

Our series that maps the landscape for Financial Institutions as they shift to business renewal.

bakermckenzie.com/findingbalance

We are the New Lawyers.

Resilience
Recovery
Renewal