E-BOOK

riskonnect

BUILDING OPERATIONAL RESILIENCE IN FINANCIAL SERVICES

CONTENTS

RESILIENCE FOR A NEW ERA

Business continuity plans and risk management play a crucial role in any financial services company's objective of achieving operational resilience. The disruption caused by the coronavirus pandemic has made this even more important

WRITER: GEORDIE CLARKE

Risk is familiar territory in financial services. Loan books, insurance underwriting and investment portfolios all require careful financial risk management. Along with this, banks and financial services companies face a litany of operational risks that have the potential to threaten business continuity and, in the event of an unforeseen crisis, result in insolvency.

Corporate leaders are navigating a world that is changing at a brisk pace, bringing with it increased automation, shifting consumer behaviour and tighter regulations. On top of this, concerns around climate change and geopolitics are ever-present. While most companies have disaster recovery plans in place, the disruption brought on by the coronavirus pandemic is putting their operational resilience to the test.

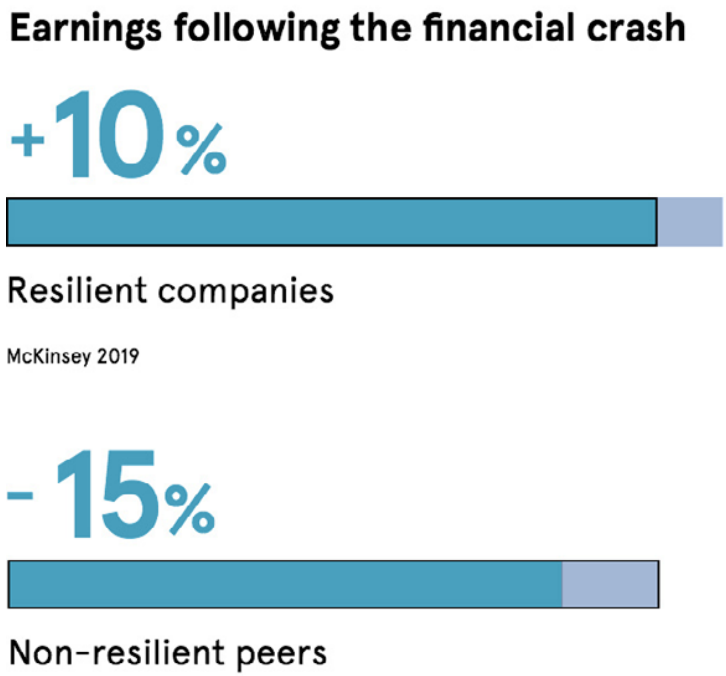
"Threats to organisations come in many forms, from unforeseen pandemics to sophisticated cyber-attacks," says Alan Calder, founder and executive chairman of GRCI Group. "Strong operational resilience accepts there is a risk that any attack or threat to your business could be successful, no matter how well prepared your defences are."

Those threats have widened as a result of technological innovation in a more digitally connected world, says Jason Edelboim, chief operating officer at Dataminr. He says this creates a greater number of opportunities and challenges for business continuity teams.

“More than ever, it’s important for risk management and business continuity to work in tandem, united under one integrated, holistic framework that takes into consideration multiple decision-makers across an enterprise and co-ordinates processes and roles to produce a unified, agile system and approach,” he says.

To their credit, financial services companies know a thing or two about volatility. While the global financial crisis took place more than a decade ago, its memory is unlikely to fade. During that 18-month period in 2007 and 2008, global economic growth plummeted by 1.9 per cent, then the biggest contraction in the modern era. Industrial activity and trade dried up, while unemployment levels skyrocketed.

“Strong operational resilience accepts there is a risk that any attack or threat to your business could be successful”



GREATER RESILIENCE

Some companies managed to survive that challenging period, but others struggled. According to research by McKinsey & Company, some companies proved to have a greater degree of resilience than others, and this allowed them to ride out the turbulence and deliver above-average growth to shareholders.

For David Poole, chief executive of Emergence Partners, risk management needs to be agile and adaptive so the teams responsible for guiding the business through a crisis are able to adapt to new circumstances.

“Indeed, the key to effective risk management is being agile and adaptable as new risks and situations emerge,” he says.

Mitchee Chung, partner and European director at Mercer Sentinel Group, says business continuity plans are a critical part of a company’s approach to risk management.

“Effective planning requires a firm to undergo a thorough self-analysis of how it operates to identify what systems, functions and roles are critical on an immediate, short and medium-term basis in the event of a business disruption,” she says.

Crucially, companies need to strike a balance between the differing objectives of risk management and business continuity teams, and instead bring them into a collaboration, says Simon Bittlestone, chief executive of Metapraxis.

“The secret to a good response to a crisis is strong and continuous communication between these teams, but also with the finance function that is ultimately responsible for managing one of the largest risks organisations face: financial insolvency,” he says. “While it is often hard to predict crises, they can be mitigated and organisations can be ready to act.”

Although some may insist the COVID-19 outbreak was predictable, it's fair to say that few businesses could have been fully prepared for the way it unfolded. Nevertheless, those with effective and flexible risk management and business continuity plans may emerge from the health and economic crisis in a stronger position than those that buried their heads in the sand.

THE DIGITAL PARADOX

The coronavirus pandemic has forced companies and employees to change the way they operate and embrace remote working. Digital tools such as video conferencing and cloud computing are critical for making this possible, but they also bring with them their vulnerabilities. Here, experts discuss what companies need to do to prevent their systems from being compromised.

What have we learnt about business continuity from the coronavirus pandemic?

Mitchee Chung, partner and European director of Mercer Sentinel Group: "COVID-19 clearly stressed investment managers in a way not previously experienced. Typical arrangements such as having critical staff work from a secondary location from the primary office were not feasible. Firms needed to adapt plans quickly and those that had weak or no plans in place were caught out, facing a scramble to put in place measures to continue operating. Those that had a strong plan in place were able to focus on adapting existing practices, giving their staff much needed capacity to prioritise strategies around market volatility, investor demands and managing a remote workforce. We think the best plans are ones that are the result of collaboration across IT, business functions and risk management, with clear, accountable owners and oversight from a board-level committee."

How are banks and financial services companies addressing vulnerabilities?

Mark Hepsworth, chief executive of Asset Control: “In the past, financial services companies were cautious when it came to using cloud computing and open source technology. But around 18 months ago, a corner was turned and organisations are now embracing these because they offer significant cost-savings and productivity gains. As a result, we’re also seeing a lot of focus around cyber security; it’s one of the largest areas of focus of security for financial services at the moment.”

What are some of the techniques companies use to protect themselves?

Jason Edelboim, chief operating officer at Dataminr: “We are seeing an increasing number of modern financial services firms implement risk detection technologies, such as our real-time alerts, and placing it directly in the hands of the people responsible for evaluating and responding to potential threats, allowing them to quickly assign ownership of risk evaluation to the appropriate stakeholders across the enterprise. Through this framework, all decision-makers receive the same high-quality information as an event unfolds, and can best position themselves to confidently launch a co-ordinated response and be flexible in unpredictable situations.”

Many companies are still grappling with legacy systems and are not as digitally integrated. Does this mean they are less vulnerable to cyber-attacks?

Ed Gouldstone, chief operating officer for northern Europe asset management at Linedata: “Technology and increased digitalisation are seen as the saving grace for effective risk management, leading to widespread adoption. A surge in automation is helping to reduce the margin for human error, though automation should not be the only answer as not all errors are human. This crisis is the ultimate test of how financial institutions manage risk. Those that have adopted these technological solutions, and particularly moved more systems to the cloud, are faring better, while companies still reliant on more manual and fragmented systems may be exposed to a higher degree of risk.”

RESILIENCE IN PRACTICE: HOW FINANCIAL SERVICES FIRMS ARE COMBATING THE CORONAVIRUS

Prior to the pandemic, the Financial Conduct Authority set out guidelines for operational resilience. Specifically, financial services organisations should take appropriate steps to minimise the likelihood of disruptive events, but also reduce the impact on core business activities

WRITER: SALLY WHITTLE

In the financial services and banking sector, preparations for the coronavirus pandemic often started as early as January. During the early stages of the pandemic, we saw many banks shut down international travel and implement work-from-home policies. By the time of lockdown, companies had taken a range of steps to build resilience into operations, focusing on scenario testing, business continuity, employee wellbeing and information security.

Santander, one of the largest banks in Europe, began building resilience into its operations by February, when it introduced a range of policies designed to protect employee wellbeing. This included avoiding unnecessary travel, postponing training, cancelling meetings involving large groups and requiring reporting of any potential contagion.

Additionally, corporate buildings were all assessed and split into zones so essential workers in company offices could be split into separate locations to ensure business continuity and social distancing.

To support employee wellbeing, the bank arranged free access for all employees to Thrive, a mental wellbeing app where they can ask for support. Also, the bank has extended its existing employee assistance programme so it can proactively contact colleagues identified as in need of additional support, including virtual counselling.

CONTINGENCY STRESS TESTING

In March, Lloyd's of London shut its underwriting floors for the first time in its history. This wasn't because the government lockdown was in effect. Instead, it was a stress test of the 333-year-old insurance market's COVID-19 contingency plans.

> ***"Please take the day to relax and enjoy time with your families. We need to take care of ourselves."***

This was an opportunity to test electronic trading measures ahead of lockdown, with traders completing trades and negotiations via email. The stress test was part of a range of measures completed before lockdown started. Lloyd's also conducted deep cleans of its underwriting rooms and ramped up its business continuity policies during March 2020. The company said the preparation was vital to ensure the 45,000 employees who use the underwriting room could continue to work under increased lockdown measures.

Citi was one of the first banks to offer support to employees to ensure they could continue working during the pandemic. In the United States, employees earning under $60,000 received a $1,000 stipend to help with the burden of working during the pandemic. Globally more than 75,000 employees received the award, which was adjusted to reflect local compensation levels.

The bank also took steps to help support employees' mental health by giving a bonus day off to 200,000 workers worldwide in May. The step was taken to avoid the risk of workers burning out during the pandemic and meant employees had a long weekend, which stretched to four days in the UK, due to a Bank Holiday Monday. The company's chief executive said in a memo: "Please take the day to relax and enjoy time with your families. We need to take care of ourselves."

The London Metal Exchange (LME) implemented its emergency plan, thereby allowing traders to switch from open-outcry trading floors to fully electronic trading. The LME, which operates the Ring in the Square Mile, said its contingency plans originally involved relocating the ring to a recovery site in Chelmsford, Essex. But with lockdown, it switched to a work-from-home policy for staff and changed from ring-based to electronic price discovery. "We continue to work with members regarding contingency plans, with focus on the trading ring, and we are ready to implement additional measures to ensure we can continue to operate," the LME says.

75,000

Citi employees globally received bonuses to help with the burden of working during the pandemic

Citigroup 2020

£250

extra per week for US frontline employees at Santander

Santander 2020

RISK AT THE HEART OF BUSINESS

The chief risk officer may be the face of a company's risk management strategy, but the job is bigger than one person alone

WRITER: GEORDIE CLARKE

The chief risk officer, or CRO, is at the centre of communications with other vital functions to build company-wide operational resilience.

To some it's one of the most important roles in a business, to other's it's an impossible job. There's little doubt, however, that the CRO's position in financial services has grown in importance in the past two decades, and following the 2008 global financial crisis in particular.

Following a raft of new regulations in the financial sector, those in senior management roles have more responsibilities and accountabilities than ever. A CRO is not only responsible for overseeing risk strategy and ensuring operational resilience, but also for making sure everyone in the company is working together to achieve those goals.

John Shiels, CRO at Hitachi Capital UK, says it's not just the CRO who is responsible for overseeing risk. Rather, it's a shared responsibility.

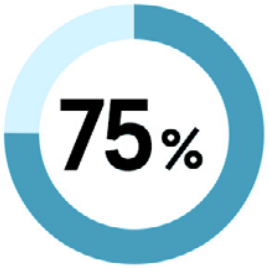
"All executive roles will have risk management responsibilities," says Shiels. "The executives who will be managing the most significant risks at any point in time will depend upon the strategy of the business, particular issues under management and ongoing developments in the external environment.

"All executive roles will have risk management responsibilities,"

"It should be a partnership between the two, the CRO should help the chief executive evaluate and mitigate risks inherent in decisions. A board-approved risk management framework should guide as to which executive is empowered to accept risks of various magnitudes, and where and when escalation is required."

In a way, the CRO sits at the middle of all these roles, serving as manager, communicator and referee to ensure everyone is working together to achieve company-wide operational resilience.

This is not to say it's just the CRO who has to carry all the weight. "In financial services, the evolution of regulatory expectations has required all executives to allocate time and resource to the management of risk within their areas of control," says Shiels. "This includes an appropriate level of documentation and to evidence that they have adequately considered risks when making key decisions."



of CROs report directly to the CEO

of risk professionals cite collaboration between business units and risk function as high priority

Deloitte 2019

CHIEF RISK OFFICER

Sitting at the centre of a company's risk management strategy, the CRO occupies a leadership position that cuts through silos and often reports directly to the chief executive or the board of directors. This person must have the ability to work with managers across the business, while also being entirely focused on spotting threats and vulnerabilities, and how they will affect the organisation. Crucially, the CRO needs the power and ability to implement change in a company and ensure the right technological advancements are in place to adapt to a changing operating environment.

CHIEF EXECUTIVE

In many ways, the chief executive is ultimately responsible for a company's approach to risk management and business continuity. Risk is top of the agenda for financial services companies and chief executives are accountable to the board of directors and shareholders, where applicable, for how a company prepares for and manages a crisis. However, risk is not necessarily a core competence for a chief executive, which is why they must delegate this task to the CRO and other managers.

CHIEF OPERATING OFFICER

There's no one-size-fits-all description for a chief operating officer, but in general this person directs and controls all operations in a company in line with the plan agreed by the chief executive and the board. With a focus on ensuring objectives and goals are met, this also means working with the CRO to make sure risk management and business continuity plans are being implemented effectively.

CHIEF FINANCIAL OFFICER

The chief financial officer (CFO) is no longer just a number cruncher. In today's operating environment, they are expected to spearhead technological change, promote good governance and drive investment returns. On top of economics and profitability, the CFO also needs to ensure the business is sustainable and resilient. This means working in close collaboration with the CRO to make sure risk management is embedded in the business model as well as corporate culture.

HEAD OF COMMUNICATIONS

It may seem that a company's communications function has little involvement in risk management, but what a company says publicly can have serious consequences, both positive and negative. Crisis management is a critical component of any large company's approach to communications. From BP's Deepwater Horizon disaster to big banks in the wake of the global financial crash, it's clear that how a company communicates during a crisis can make all the difference in protecting its reputation.

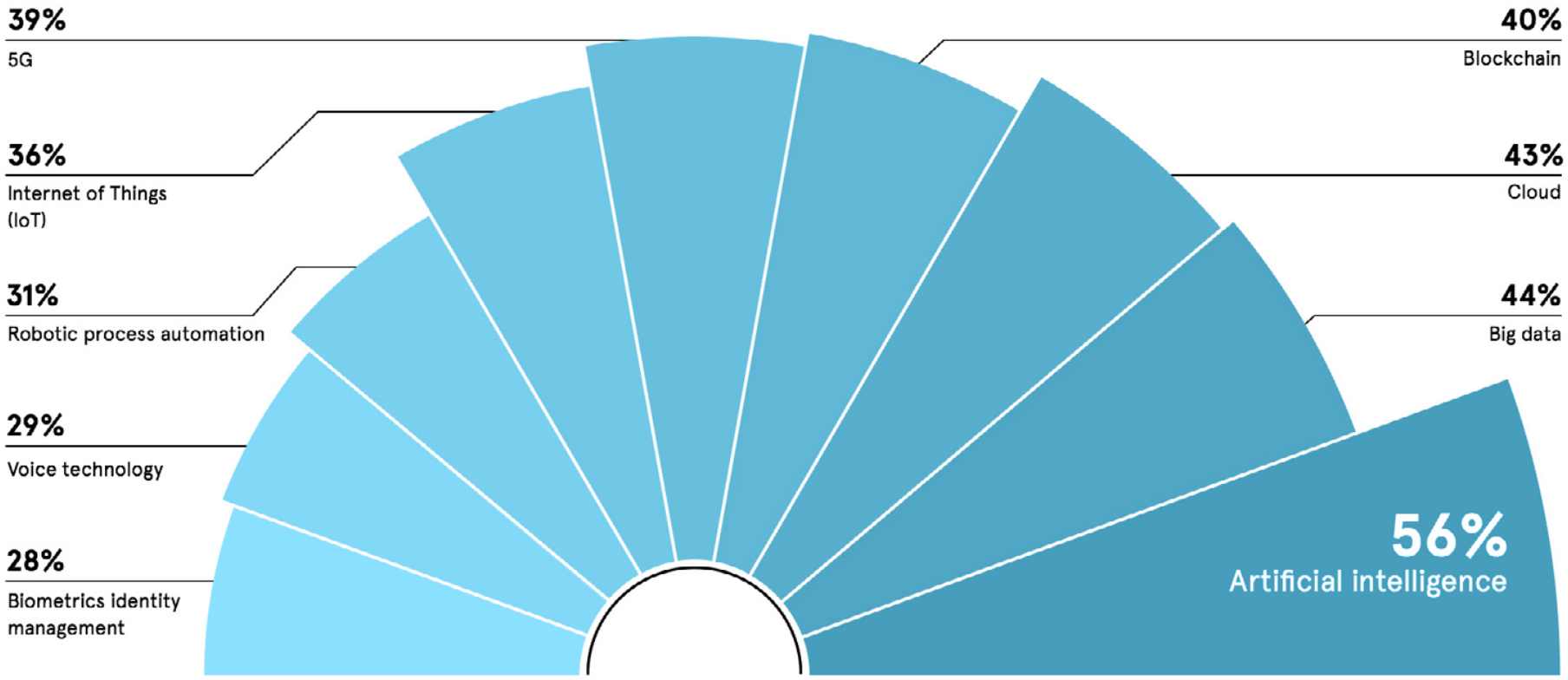
CHIEF INFORMATION SECURITY OFFICER

Responsible for a company's information and data security, the chief information security officer (CISO) has wide-ranging duties across security operations, cyber-intelligence, data loss and fraud prevention, security architecture and overall governance of a company's security measures. A CISO needs to have deep technical knowledge, while having strong management skills and an ability to work with a company's leadership, including the CRO.

DATA DASH - THE PERCEPTION GAP: AI IN RISK MANAGEMENT

There is a clear lack of confidence in financial services firms about their ability to get the most out of AI technology

Of all the new technology available to financial services, AI is expected to be an essential business driver
Which technologies will transform the way financial services are delivered within the next 2 years?



PwC 2019

77%

of FS execs anticipate AI will have a significant strategic importance to their business within 2 years

WEF 2020

91%

expect to see AI implemented in three or more areas of their business within 2 years

WEF 2020

There is appetite for the use of AI to manage risk, but a lack of confidence persists

already use AI in risk management

WEF 2020

of risk managers described themselves as 'fully capable' of assessing AI-related risks

Accenture 2019

categorised themselves 'at the forefront' of AI implementation

PwC 2019

FS firms know that leveraging data is crucial for harnessing the benefits of AI

63%

are actively improving their data collection ability

Accenture 2019

66%

are sharpening their enterprise-wide data analytics skills

Accenture 2019

63%

are attempting to utilise new or alternative forms of data in AI applications

WEF 2020

But

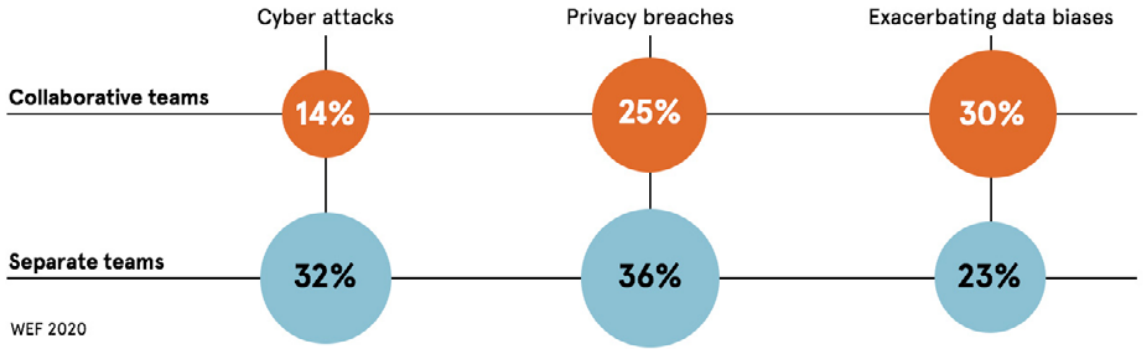
39%

are not confident they can gain insights from new data sources at the pace needed to respond to new risks

Accenture 2019

Risk experts worry about the impact of AI on a mass scale, but judge their own organisations to be less vulnerable. They are navigating AI risks much more effectively than their groupthink suggests

Percentage of respondents who report an increase in risks, due to AI adoption

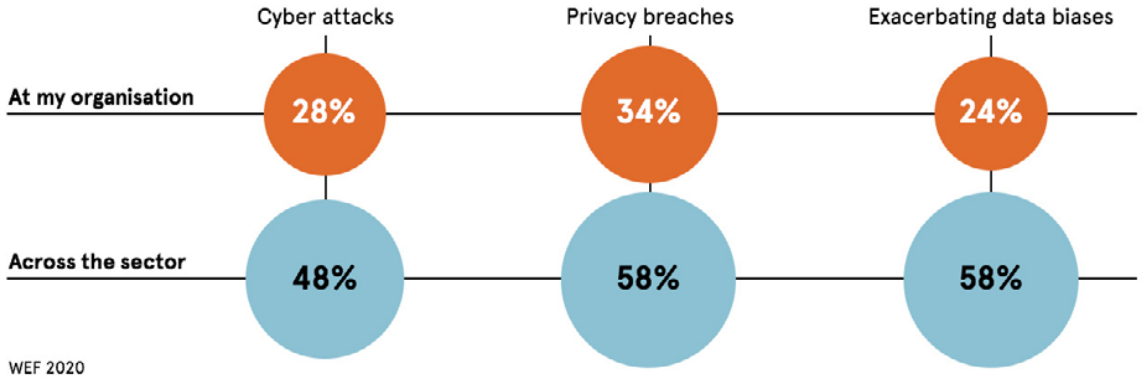


WEF 2020

Collaboration between Risk teams and Tech Innovation teams is crucial to overcoming the confidence crisis in AI-based Programmes and skills

AI implementation teams that include risk professionals report fewer negative impacts from their AI programmes. But conversely, these collaborative AI teams are more likely to be aware of biased data and algorithms as a longer term risk of AI programmes.

Percentage of respondents who expected an increase in risks, due to AI adoption



WEF 2020

A RISKY PICTURE FOR MERGERS AND ACQUISITIONS?

The coronavirus pandemic has halted M&A activity, but it could prove positive for longer-term risk management practices

WRITER: SALLY WHITTLE

The coronavirus crisis has presented organisations with many challenges around mergers and acquisitions but, in the long term, perhaps the lessons of 2020 could reduce risk in M&A.

M&A activity started to slow at the beginning of 2020, before coming to a virtual halt in March with the UK in lockdown.

A good company in 2019 would expect to see several interested buyers, but now organisations are having to work harder to get deals off the ground. “We’ve seen many deals paused or cancelled, and we’re seeing far less cookie-cutter deals,” says Phil Adams, chief executive of GCA Altium investment group. “What this means is we’re having to work harder and use our initiative to create deals and navigate bilateral agreement.”

GREATER RELIANCE ON DATA

The vast majority of M&A negotiations are now happening remotely, which means the personality of a management team is less of a factor in transactions. When buyers and sellers get around a table, the charisma of a company founder can be a critical part of the negotiating process.

In a COVID-19 world, however, we're seeing more focus on cold numbers, and requests for much more, and more detailed data. "I don't think this is a bad thing because we are seeing organisations doing better risk assessment because of this trend," says Andrea Brody, CMO of Riskonnect.

The flip side of this is sellers are weeding out what Adams calls "tyre kickers", companies that speculatively engage in M&A negotiations without the senior buy-in to complete a transaction.

"Our role is to prove the buyer is real as there is a far higher risk at the moment of a deal not happening. So we need to see evidence that someone has senior buy-in for the transaction and that's a key part of our risk assessment," continues Adams.

VIRTUAL MEETINGS

Lockdown put the brakes on many site visits, management roundtables and face-to-face negotiations. Where meetings are taking place, they are often on a smaller scale, with teams meeting in open spaces or with one or two visitors on a carefully managed site visit.

> ***"We are seeing organisations doing better risk assessment because of current trends"***

Replacing physical meetings with virtual tours and roundtables has been more successful than many people expected, says Riskonnect's Brody. As such, it seems likely the M&A sector will never return to the old "normal".

"When you're doing a deal these days, it's very focused on data and virtual conversations. I think as people become comfortable with that type of transaction, we will see a fall in the number of physical meetings, even as things go back to normal," she adds.

"I think we will see an accelerated trend towards more remote transactions, which is a good thing because you're spending less time flying, and I think people sometimes make better decisions when they're not swayed by the personalities of the management team."

Expect to see a greater adoption of analytics and data intelligence tools in the M&A sector as this trend continues and companies need intelligence to support strategic decisions that are made remotely.

NARROWING OF SECTOR ACTIVITY

The third trend COVID-19 has created in M&A is a narrowing of activity by sector. Over the coming 24 months, industry analysts expect to see different transaction volumes and types in different industry sectors.

"I think you will see more buyers and corporations using private funding to buy and build because of reduced interest rates and the availability of private equity. I think we will see lots of acquisitions as strong companies look to competitors and see more vulnerability," says Adams.

Some sectors have boomed during the pandemic and he expects to see interest in these sectors over the next couple of years. “Sectors like technology are doing very well, and specifically hosting, and any companies with contractual, monthly recurring revenue,” he says. “These businesses will command a premium because they will be in a better place to ride out the downturn.”

While the M&A landscape may look very different after the COVID-19 crisis passes, the key thing for organisations is to take the lessons of 2020 and use them to build resilience in a post-COVID world.

“The companies that are already planning how to come out of the crisis and deal with that new landscape will be the ones that survive and thrive,” says Brody. “This crisis has given many financial services companies the opportunity to really look at their risk management and assessment, and make positive changes.”

SPOTLIGHT ON SMCR: HELP OR HINDRANCE?

The accountability framework, designed to restore confidence in the financial services sector, has presented firms with a number of challenges

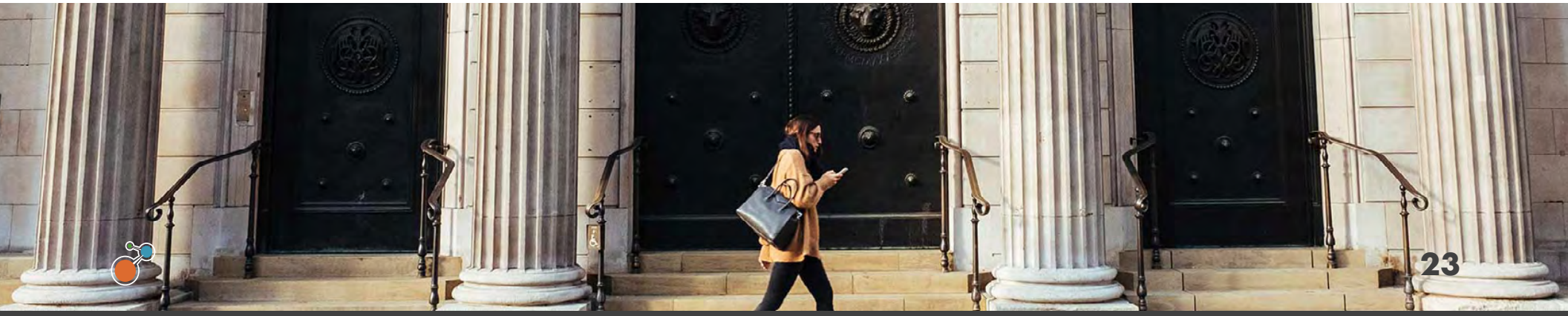
WRITER: SALLY WHITTLE

When the senior managers and certification regime (SMCR) was introduced, it covered more than 47,000 UK financial services organisations. The accountability framework was designed to restore trust in financial services and underpin a culture that works in the long-term interest of firms and their customers.

Two years on and most organisations are getting used to SMCR compliance, but many found the journey harder than anticipated.

SMCR requires firms to identify individuals as either subject to the senior managers regime or certification regime. Everyone in the first category must have a statement of responsibility, identifying what they are responsible and held accountable for. Those in the second category must be certified annually and trained on how conduct rules relate to their individual roles.

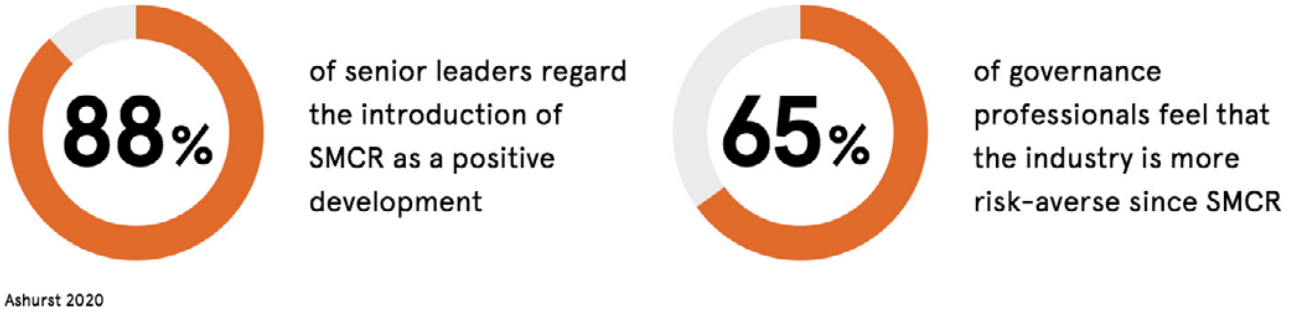
Meeting these requirements has presented firms with several challenges. For starters, creating statements of responsibility and certifying all other employees presents a huge commitment in terms of training and time.



“There are lots of factors to consider, including employment contracts, proper training and ensuring individual responsibilities are well documented so the individuals have a clear remit in terms of understanding when and where the buck stops with them,” says Jeanette Burgess, head of regulatory and compliance at Walker Morris.

TRAINING

Companies need to pay for consultants and lawyers, technology solutions and training providers to make sure certification is done correctly. “The SMCR rules don’t specify how training is to be delivered, so many firms have opted for e-learning. That has meant some firms adopting a ‘tick the box’ mentality using generic training packages,” says Sarah Ouarbya, partner at Mazars Financial Services. “The challenge is it’s unlikely to provide the level of interaction and discussion that is normally the most effective part of this type of training.”



Ashurst 2020

Monitoring ongoing compliance takes a lot of time and resources. This is especially true when the workforce is international and management roles span more than one country. “If you have an international business, especially with a matrix management structure, suddenly you have people in the United States being told they have to do things in a different way, and they’re pulled into being responsible and having training on a UK-specific framework,” says Douglas Cherry, partner in global dispute resolution at commercial law firm Reed Smith.

Finally, too many companies have approached SMCR as a box-ticking exercise rather than a broader cultural change, says Eleanor Malcolm, chief risk manager at Julius Bear International, a private bank.

“For us, SMCR has been quite smooth because we have a culture of clear ethics and accountability. If you don’t have that buy-in from the senior team, then it becomes much harder. I sit on the board and I know that culture comes from the top and moves down through the firm,” she says.

Despite the challenges, many in the industry believe SMCR is having a positive impact on financial services. “SMCR makes your organisation consider how it manages itself and, while the board is responsible for the bank [or financial services firm], now specific managers have responsibilities and are accountable for what they have done,” says Cherry.

“Culture comes from the top and moves down through the firm”

During the coronavirus pandemic, the benefits of SMCR may become even clearer. As part of the process of defining responsibilities, firms need to be introspective and present a clear map of the organisation and individual roles, says Malcolm. “SMCR means the chief operating officer knows what technology is needed to work from home, the human resources director knows who will be available and who may be shielding or coping with home schooling. That’s invaluable in a situation where speed is of the essence.”

ABOUT RISKONNECT

Riskonnect is the leading integrated risk management software solution provider that empowers organizations to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise. Through its unique risk correlation technology, over 900 customers across six continents are benefitting from actionable insights that have not been previously attainable to deliver better business outcomes.

Learn how **integrated risk management** can help your organization with data privacy law compliance and more.

VISIT US ONLINE AT WWW.RISKONNECT.COM

riskonnect.