SCHEME RESILIENCE

The resilience shield

European pension funds are redefining resilience as geopolitical instability, climate risk and digital dependence reshape the landscape. Beyond funding and investment risk, regulators are now focused on operational vulnerabilities – from cyber threats to reliance on non-European IT providers – raising new questions about the role of pensions as critical financial infrastructure. Ellie Carric **reports**

As the 2020s continue to unfold, it's clear the post-war, rules-based global order is over, replaced with a more fragmented, unstable and uncertain world. At the same time, climate change is already affecting people and the environment, and from a technological perspective, increasing digitalisation, cyber risk and artificial intelligence (AI) are presenting new challenges.

Against this backdrop, European pension funds are being forced to rethink what resilience means. Long defined in terms of funding levels, asset-liability risk, and sponsor covenant, resilience is now taking on a broader and more complex dimension.

Recent warnings from De Nederlandsche Bank (DNB) president, Olaf Sleijpen, highlighted how vulnerabilities such as reliance on non-European IT providers and exposure to cyber threats are pushing pension systems into the realm of critical infrastructure.

As a result, funds across Europe are facing the dual challenge of safeguarding long-term returns while ensuring their operations can withstand an unpredictable world.

Old risks, new pressures

Even the way pension funds assess and manage traditional risks is evolving. According to research by Nuveen, investors worldwide are recalibrating their investment approaches as three powerful megatrends – AI, energy transition and deglobalisation – reshape the global economic landscape.

While the majority of European investors who responded to the survey remain "anchored to longer-term strategic investments," they are placing more importance on "diversification and taking a more selective approach to geographical exposure," Nuveen head of UK institutional, Sophie Ballard, said in the report.

The research found that almost two-thirds of European investors made regional adjustments to their portfolios with Europe being the beneficiary of this, and the majority already consider, or plan to consider, energy transition (87 per cent) and climate risk (81 per cent), in their investment decisions.

New dimension of resilience

But a new avenue of risk – that of operational capacity – is also emerging. Speaking earlier this year at the Netspar Pensions and Science Conference, Sleijpen told delegates that pensions must become "more resilient".

"DRIVEN BY THE FINANCIAL SECTOR'S GROWING DEPENDENCE ON DIGITAL INFRASTRUCTURE, OPERATIONAL RESILIENCE HAS MOVED FROM THE PERIPHERY TO THE CENTRE OF THE REGULATORY AGENDA"

"In a world where power politics are increasing, Europe must reduce its dependencies," including in "financial infrastructure," he said.

His thoughts were based on a joint publication by DNB and the Dutch Authority for the Financial Markets (AFM), warning that the Dutch financial sector faces increasing systemic risks stemming from its growing reliance on a limited number of non-European IT service providers.

The numbers back this up. A European Insurance and Occupational Pensions Authority (EIOPA) spokesperson says "the vast majority of Institutions for Occupational Retirement Provision (Iorps) outsource part – if not all of – their services to third-party providers".

And a report commissioned by the Committee on Industry, Research and Energy (ITRE) of the European Parliament, stated: "The pervasive dominance of US-based technology giants, especially in cloud computing, AI platforms, operating systems, and enterprise software, often reaches market shares exceeding 70 per cent."

The joint DNB/AFM paper looked at what action can be taken in the short and longer term.

In the short term, preparation is key. Financial institutions must accept their continued reliance on non-European technology providers while actively preparing for disruption by stress-testing their operations and collaborating more closely with peers, vendors and authorities.

This includes developing realistic threat scenarios, sharing intelligence on emerging risks, and running end-to-end simulations of IT supply chains, alongside practical steps to strengthen control over data and reduce dependency through more flexible, multi-vendor technology strategies.

Over the longer term, the paper continued, the focus shifts to reducing this dependency altogether by building a stronger and more autonomous European technology ecosystem.

Achieving this will require coordinated action at EU level, including investment in home grown alternatives, collective adoption of European solutions where available, and structural reforms to support innovation and scale up – ultimately strengthening resilience while safeguarding European values such as data sovereignty and strategic independence.

Critical financial infrastructure

As pension schemes are increasingly treated as critical financial

infrastructure, regulators are placing greater emphasis on resilience and oversight, and expectations on continuity, governance, testing, and incident response are converging with those for banks and insurers.

Aon partner, Emmy Verbist, said: "Pension schemes can be more susceptible to infrastructure risk due to the often-fragmented profile of their operational framework – they outsource most services and multiple suppliers share data and assets between networks. This increases the likelihood of risk incidents occurring due to both human error and nefarious intent.

"Therefore, it is now of utmost importance that pension scheme managers understand the operational footprint of their schemes: where, when, and how member data and other sensitive information is being both stored and shared," she said.

At the pension provider APG, IT dependencies and cyber risks are a key focus, fully embedded in its risk management framework, with strict security policies, continuous monitoring and dedicated capabilities, APG spokesperson, Sanne Hofland, says.

APG actively manages third-party risks and regularly tests its resilience through "scenario-based testing and incident response exercises," she adds.

"We are conscious of the fact that the world is changing fast and global investors must take account of many more risks than even a few years ago. Managing risk is the bread and butter of investing, but you must have an overview of the probability and impact of different things that can happen, if you want to manage them.

"Our biggest concern right now is to keep our list of possible risks complete and up to date, making sure we look at regular as well as 'previously inconceivable' risks," she says.

Scanning the horizon

In April, EIOPA published its quarterly risk dashboard. It revealed that digitalisation and cyber risks remain at a medium level, with the materiality of these risks for Iorps increasing in the first quarter of 2026, amid ongoing concerns related to geopolitical tensions and uncertainty.

Market and asset return risks increased to a high level, with equity and bond market volatility spiking at end-March, reflecting heightened concerns on the evolution of the war in Iran and overall geopolitical instability.

"PENSION SCHEMES CAN BE MORE SUSCEPTIBLE TO INFRASTRUCTURE RISK DUE TO THE OFTEN-FRAGMENTED PROFILE OF THEIR OPERATIONAL FRAMEWORK"

These findings highlight "the need for IORPs to maintain a strong focus on both investment strategy and operational capacity to ensure their long-term resilience," an EIOPA spokesperson says.

The European Commission has published a proposal for a review of the IORP II Directive seeking, among other things, to improve the consistent EU-wide application of forward-looking and risk-based supervision of Iorps' operational resilience, the EIOPA spokesperson adds.

DORA

The EU has also introduced the Digital Operational Resilience Act (DORA) – a regulation to ensure that financial institutions, including pension funds, can withstand, respond to, and recover from information and communication technology (ICT) disruptions, such as cyber-attacks or system failures.

"Driven by the financial sector's growing dependence on digital infrastructure, operational resilience has moved from the periphery to the centre of the regulatory agenda," comments Freshfields partner, Dr. Thomas Granetzny.

"DORA is the legislative response," he says. "A sector-wide framework that has generated significant compliance effort across the financial sector and continues to keep the industry occupied.

He explains that for Iorps specifically, this shift has "created a complex compliance picture".

"IORP II established the EU-wide governance and risk management framework for pension funds, but its focus was firmly financial – operational and technological risks were largely unaddressed at EU level, with isolated national rules in some member states. DORA was introduced to close that gap, and it sits alongside IORP II as an independent obligation rather than an extension of it," he says.

A dual challenge

As the definition of pension fund resilience continues to evolve, pension funds must have one eye on financial risks, and the other on operational vulnerability, notwithstanding that many of these risks are interconnected.

Looking ahead, EIOPA says its *Strategy towards 2030* signals a continued focus on risk-based supervision, digital operational resilience, and stronger supervisory convergence, supported by new tools and guidance. Greater cooperation between European regulators and industry, and perhaps greater autonomy, as Sleijpen suggested, will be key to managing emerging risks and underpinning a more resilient and sustainable financial system.