CYBSERSECURITY AND DIGITAL OPERATIONAL RESILIENCE

GERRY CROSS
Director Financial Regulation, Policy and Risk – Central Bank of Ireland

DORA – The final countdown to implementation

The details of the DORA framework – the so-called "Level 2" regulation – are currently being finalised ready for implementation on January 17 2025. The European Supervisory Authorities, together with more than 50 competent authorities and others, completed this work taking into account the close to 900 comments received during public consultations.

A key theme from the received comments is the need for proportionality given the wide range of firms, across all financial sectors that are subject to DORA and the consequential need for the DORA framework to be fit for application to firms of all types, sizes, shapes, and levels of complexity.

Proportionality therefore has been a guiding principle of the work to develop the DORA framework and has been built into the foundational architecture of DORA as key concepts. For example a strong emphasis on proportionality can be seen in DORA's ICT risk management framework that should be consistent with the size and nature of a firms' activities and which is further supported in the RTS on ICT Risk Management, where Article 1 requires financial entities and their supervisors to take into account elements of increased or reduced complexity and risk.

Furthermore, DORA frequently uses concepts such as "criticality", "major", and "systemic" throughout the framework when setting requirements and contains specific proportionate requirements such as the simplified risk management framework for non-complex firms. Similar examples of strong proportionality can be seen in DORA's RTS on incident reporting, where values have been set purposely high to reduce the burden on smaller entities and in DORA RTS on TLPT where selection criteria have been tested to ensure only the biggest and most appropriate financial entities will become subject to TLPT requirements. As regards the monitoring of outsourced activities, while financial firms remain responsible for their activities, regardless of whether or not they have been outsourced, the level 2 regulations should embed a fully proportionate approach.

The practical implementation of the DORA requirements is of course centre stage, both from financial entities' perspectives but also from that of competent authorities. Financial firms should by now be advancing well in their implementation work, including completing gap analyses between their existing controls, policies and procedures and the requirements of DORA, towards a timely and high quality implementation of those requirements.

Financial firms should by now be advancing well in their implementation work.

With regard to critical third-party providers of ICT services to financial entities, the new oversight regime reflects the important role that these technology firms have in the functioning of the financial system. At the same time it recognises that these technology firms are not providers of financial services but rather the providers of outsourced activities.

Over recent months, the ESAs and national competent authorities have established a High-Level Group on Oversight that is helping oversee the establishment of the operational aspects of the new oversight regime. One key aspect will be the designation of those third party ICT service providers which should be considered critical in accordance with the delegated published in the Official Journal of the Commission end of May. The designation of these "CTPPs" is dependent on the collection and analysis of the registers of information on ICT outsourced services based on the ITS on the Register of Information. Work is ongoing to have the new registers of outsourcing arrangements up and running in good time and the ESAs and competent authorities have been collaborating in a dry run exercise to assist financial entities to become familiar with the operation of the new templates.

FRANÇOIS-LOUIS MICHAUD

Executive Director – European Banking Authority (EBA)

EBA-EIOPA-ESMA joint preparations for the fast-approaching application of DORA

Policy

The Digital Operational Resilience Act (DORA) was adopted to enhance the digital operational resilience of the EU financial sector. It addresses the key vulnerabilities, like cyber risk, and dependencies of the financial sector towards technology, with a view to fostering a smooth, continuous, and safe provision of financial services to customers.

As requested by DORA, the EBA, EIOPA and ESMA (the ESAs) published in 2024 a series of standards and guidelines in the areas of ICT risk management, ICT incident classification and reporting, testing of ICT systems, management of ICT third party risks and oversight. A guiding principle was to devise requirements which are proportionate, pragmatic, harmonised for all entities across the financial sector, while also consistent with existing legal acts.

With the legal framework now almost completed, financial entities can accelerate their preparations for DORA's application in January 2025. Adjustments are in particular expected in the areas of ICT risk management, incident reporting processes, and contractual arrangements with third party providers, including the related registers of information.

One of the priorities the EBA just set for EU banking supervisors in 2025 (as part of its European Supervisory Examination Programme) relates precisely to checking on the adequacy of institutions' risk management frameworks, of their classification and timely reporting of major incidents, threat-lead penetration testing and reporting of the registers of information.

To help financial entities prepare to submit their DORA registers of information in 2025, the ESAs are also carrying out a voluntary "dry-run" exercise. More than 1 000 firms plan to participate. They would thus receive specific feedback in the autumn, in addition to the wider take-aways which will be shared with the entire industry.

Oversight

To address third-party and concentration risk, DORA entrusts the EBA, EIOPA and ESMA with the responsibility of ensuring an oversight of Critical Third-Party Providers (CTPPs) providing ICT services to EU financial entities. Four aspects deserve particular attention.

Firstly, the oversight of CTPPs will rely on an intrinsic cooperation between the the ESAs and competent authorities. In particular, Joint Examination Teams will be assembled bringing skills, experience, and competences on ICT risk supervision and operational resilience from the ESAs and other sectoral supervisory authorities. These authorities will also take part in an Oversight Forum, which is tasked to promote a consistent approach in monitoring ICT risks, to coordinate measures to increase digital operational resilience and to play a role in the designation of CTPPs. In addition, national supervisors and the ESAs will coordinate their actions and share information to ensure effective management of risks posed by CTPPs to financial entities. The ESAs will be able to issue recommendations to address issues at CTPPs, which national authorities can follow-up through supervisory actions to their financial entities. On the other hand, the supervisory findings related to the services of CTPPs will also feed into the ongoing oversight activities.

Secondly, to ensure an efficient oversight maximising limited resources and building an oversight culture, the ESAs have decided to create a truly joint function, pooling the oversight resources envisaged for them by DORA, to carry out the day-to-day oversight tasks. This "joint oversight venture" will maximise synergies and ensure a fully consistent cross-sector approach when overseeing CTPPs. This joint function will be headed by a director placed under the direct responsibility of senior managers from the three ESAs gathered in a Joint Oversight Network.

Thirdly, the ESAs, working closely with a dedicated high-level group on DORA oversight, are currently developing the methodologies, arrangements and processes for the DORA oversight. This includes risk assessment methodologies, processes for onsite and off-site activities, but also processes for issuing recommendations. potential penalties, and for collecting oversight fees.

EBA, EIOPA and ESMA make good progress on their joint setting-up of the DORA oversight framework.

Finally, a lot of attention is currently paid on preparing for the CTPP identification and designation in 2025. Here, financial entities' registers of information about their contractual arrangements with third-party provides will play a key role. Data will need to be available timely in a good quality, so that it can be provided by financial entities to their direct supervisors and then to the ESAs' joint oversight function so that they could designate CTPPs in 2025 on the basis of the criticality criteria set out in DORA and the related Delegated Regulation.

All in all, preparation for DORA are progressing well. DORA is a game changer which will benefit both ICT users and providers and should result in a safer environment for all. The global ICT disruption experienced at the end of July was yet another reminder of the criticality of the ICT chain in our economies.

FRANCESCO MAZZAFERRO
Director General of Secretariat – European Systemic Risk Board (ESRB)

Systemic cyber risk is a continuously moving target

The ESRB has been working on the systemic nature of cyber risk and its threat to financial stability for a significant portion of its existence. Growing digitalisation, the financial sector's heavy reliance on ICT (information and communication technology) services and cyberattacks on financial entities have sparked concerns over its potentially systemic nature. Cyber risk has also continuously been cited as top priority by financial entities, regulators and supervisors alike.

Systemic cyber risk is a cross cutting risk that transcends sectors and therefore often requires staff from vastly different backgrounds to work together and assess its potential impact. When a threat crystalises, it is called an event and if the event is severe enough to cause negative effects, it is called an incident. It is therefore critical to assess if an incident is an isolated event or may escalate from an operational level to the financial and confidence realms. For the latter to happen, either critical functions that underlie the real economy must be incapacitated or financial losses need to reach levels that the ensuing shock cannot be absorbed by the system. For this purpose, the ESRB developed conceptual frameworks to assess at which points or thresholds cyber incidents can become systemic and pose risk to financial stability. We call them Systemic Impact Tolerance Objectives. These SITOs are conservative measures and should help authorities inform their policy response.

It is also important to understand which ICT services the financial sector most heavily relies on and in the event of a severe incident, how the economy would be affected by an outage of these services. These critical functions are often provided by entities (known as critical third party service providers) that are seldomly known outside the world of IT. Certain services are only provided by few companies and concentration risk and non-substitutability of services can have detrimental knock-on effects. Though without systemic consequences, this can be seen in recent incidents affecting large financial entities. Albeit having invested considerably in cybersecurity they are not immune to exploits and cyberattacks. Significant investment in cybersecurity is therefore a necessary but not sufficient condition for cyber resilience.

One characteristic of systemic cyber risk is its inherent level of uncertainty. It is impossible to predict when an incident will occur, but it is certain that incidents will occur. Businesses and authorities across the system need to employ an assume breach mentality and integrate it into corporate culture and business strategy. This will help employ sound business continuity, disaster and recovery, and crisis management plans to prepare for worst-case scenarios. Here we move from assessment and prevention to mitigation for increased resilience.

It is impossible to predict when an incident will occur, but it is certain that incidents will occur.

A technique that can help macroprudential authorities prepare for worst case scenarios is Cyber Resilience Scenario Testing in which system-wide operational stress tests are conducted. One difference between microprudential and macroprudential operational stress tests is that in a macroprudential setting, all dependencies should be tested, not just the firm's individual response. Therefore, a financial entity's response to stress needs to be considered in another financial entity's response and vice versa. This is a highly complex task but does not only inform the individual firm on their own cyber resilience, but it also helps authorities in their role to respond to and mitigate a systemic incident in the future.

Systemic cyber risk is a continuously moving target for which financial entities and macroprudential authorities alike need to embrace change. When a cyber crisis evolves into a full-scale financial crisis, traditional tools such as capital buffers may be effective. However, they may be largely ineffective if the system's operability itself is incapacitated. Thus, macroprudential authorities should consider tools outside of their traditional realm or develop new tools that meet the requirements of effectively responding to an evolving threat.

System-wide contingency options and backup solutions can help to ensure the sustained provision of critical economic functions. There may be systemic cyber incidents that cannot be solved by business continuity measures employed by individual financial entities alone. System-wide tools and backup systems are developed, tested and put in place in advance and can take effect immediately after an incident occurred. These can temporarily ensure the continued provision of vital services to the economy and maintain confidence in the financial system. Such tools can foster overall and system-wide resilience and safeguard financial stability in the long term.

DAVID BAILEY

Executive Director for Prudential Policy – Bank of England

An ecosystem approach to cyber and digital operational resilience

Introduction

1. The Prudential Regulation Authority (PRA), working with the Bank of England (BoE) and Financial Conduct Authority (FCA) define operational resilience as the ability of financial institutions (FIs) and the financial sector to prevent, adapt to, respond to, recover from, and learn from operational disruptions. Our operational resilience and third party risk management (TPRM) policies are technology-neutral, but with cyber resilience and digital operational resilience as key elements. Respondents to our Systemic Risk Survey repeatedly identify a cyber-attack as a key risk to the financial system. These concerns are backed by recent attacks which often involved third party service providers to FIs (TPSPs) (Capita and ION) and, in some cases impacted FIs' delivery of vital services (ICBC). The BoE Financial Policy Committee's 'Macroprudential approach to operational resilience' sets out how operational (including cyber) disruption could impact financial stability.

2. Compliance with regulations on operational resilience, TPRM and proposed regimes for Critical Third Parties (CTPs) is necessary to strengthen the financial sector's digital operational resilience. While FIs and CTPs are/will be individually responsible for complying with relevant regulations, in doing so, it is crucial that they take into account the financial ecosystem in which they operate and how they may impact it. A key theme is that, to strengthen the financial sector's digital operational resilience, we need to treat it as an ecosystem all parts of which must work individually and collaboratively towards shared goals.

Financial institutions

3. UK FIs collaborate to improve the resilience of the financial sector through collective action and sector response initiatives, including via the:

- Cross Market Operational Resilience Group (CMORG), co-chaired by the BoE and UK Finance, which aims to strengthen the resilience of the financial sector and its ability to respond to operational incidents through collective action. This allows FIs and regulators to collaborate outside of formal regulation and supervision;
- Sector Response Framework (SRF) which coordinates FIs' response to incidents affecting the financial sector; and
- sector exercises, such as SIMEX (the next of which will take place later this year).

Regulators

4. The role of regulators includes regulating and supervising the cyber resilience of FIs and the wider financial system. In the UK, we do so by:

- developing outcomes-focused, proportionate regulation on operational resilience, TPRM and CTPs;
- CBEST, which has been our flagship intelligence-led penetration testing programme since 2014. While CBEST focuses on systemic FIs, we publish thematic findings and have launched a similar programme for smaller FIs (STAR–FS); and
- FPC cyber stress tests, which we also follow up with thematic findings

5. Regulatory cooperation during incidents is key. In the UK, we have the Authorities' Response Framework for the regulators and HM Treasury to co-ordinate with each other, FIs and other authorities during incidents that could majorly disrupt financial services.

Critical third parties and other TPSPs

6. As we saw with events involving CrowdStrike, FIs' reliance on TPSPs is increasingly important due to digitalisation and technologies such as cloud and artificial intelligence. TPSPs that support FIs' delivery of important business services must understand and facilitate their compliance with regulatory obligations.

7. A small number of TPSPs, known as 'CTPs' in the UK, could cause risks to financial stability if their services to FIs fail or experience disruption. To address this systemic risk, we are introducing a CTP Regime whereby HM Treasury will designate CTPs. We will directly oversee the resilience of CTP's services to FIs. Among other requirements CTPs, will have to document and validate their processes for coordinating with the regulators and their FI customers during incidents.

All parts of the financial services ecosystem need to collaborate to strengthen digital Op-Res.

Standard-setting bodies (SSBs) and international fora

8. As cyber-attacks do not respect national borders, SSBs are seeking to address regulatory fragmentation through global standards. For instance, the Financial Stability Board (FSB) has published guidance on cyber-incident response & recovery, third-party risk management, cyber-incident reporting and a cyber lexicon. The G7 has sought to facilitate cross-border cooperation through cross-border exercises.

9. However, cross-border regulatory and supervisory cooperation in this area could be enhanced. Regulators and FIs would benefit from exploring how existing or new bilateral and multilateral cooperation structures, such as colleges and crisis management groups, can improve coordination in areas such the management of cross-border incidents; oversight of CTPs; and exercises and tests.

TULSI NARAYAN

Senior Vice President, Security Solutions and Processing, APEMEA – Mastercard

Cybersecurity across the supply chain

In an increasingly digital world, cybersecurity is climbing the priority list for business leaders. While the excitement around evolving technologies is palpable, the boardroom is becoming increasingly aware of the risks that come with it. The impact of a cybercrime can be debilitating. Globally, the average data breach cost victims $4.45 million in 2023.

In response to this growing threat, cybersecurity has quickly developed from an IT challenge to a C-Suite priority; it's now the top digital risk businesses face today.

The best way to fight cybercrime is to understand the risk. What does it look like? Why does it happen? How can it be stopped? These are vital questions that both cyber leaders and their vendors need to know if they are going to address the risks effectively. Cybersecurity and operational resilience are now an integral part of any organisational strategy. The ability to identify vulnerabilities, detect threats and mitigate risks can be the difference between success and failure.

While enhancing consumer convenience, the increased reliance on third parties has led to greater complexity in payments acceptance and processing. An explosion of digital players, applications and devices is continually infused into the payments ecosystem, creating infinitely more undefined, and often inadequately protected web of connections between networks.

The ecosystem is under perpetual threat of widespread attack as a lack of proper third-party or supply chain risk management leave networks vulnerable. Criminal groups and indeed nation states are exploiting the weak links in that supply chain, targeting applications and providers that neglect to utilize network, regulatory and security standards and protocols.

Over the last few years alone, attacks such as SolarWinds Orion, Apache Log4J and MoveIT have all highlighted the entities' vulnerability to supply chain cyber-attacks. As a result, stakeholders are at risk of attack—even those with strong individual cyber and fraud protections in place.

Yet, it is important to underline how some players have tended to lack either the understanding about how these disruptions are impacting them – or the capabilities to mitigate the risks.

Organizations are not always able to look across third-party business relationships because of the lack of systems and processes available. Of course, the entity you're doing direct business with is important – but what about who these entities are doing business with? For example, if a business that you're heavily reliant on is working with a sanctioned organization or suffers a major cyber breach due to one of their own suppliers – that's a risk that you might not have visibility into.

In addition, risk monitoring practices are outdated if they involve fragmented teams of people, antiquated manual surveys and a large dependency on other organizations' inputs/disclosures.

To keep pace with the threat requires automation. It's imperative to proactively identify risk before disruption can occur.

At Mastercard, we continually invest in cyber security and network protection to address evolving widespread threats to the ecosystem. In fact, we have invested more than $7 billion over the past five years.

Our cybersecurity solutions such as our third-party and supply chain risk management platform RiskRecon (https://www.riskrecon.com/solutions/riskrecon-by-mastercard) demonstrate Mastercard's commitment to investing and providing much needed capabilities to our customers and partners to drive operational resilience.

RiskRecon uses Mastercard's unique network view to protect customers by continuously monitoring 19 million entities to identify fraudulent trends. This data is then used to inform risk assessments against transactions, connections to third-parties, 4th parties and beyond, building trust across the ecosystem.

As the world changes Mastercard is evolving too, enhancing collaboration with partners, through our fusion centers, and, in Europe, through our recently inaugurated European Cyber Resilience Centre that allows us to bring together law enforcement, private and public sector and cyber security experts from across the region.

This collective approach sharpens our response and strengthens our ability to share intelligence about potential future threats. Strong alignment with policy makers, too, as illustrated in recently adopted legislation, such as DORA, and cross-sector legislation such as the NIS2 Directive and the Cyber Resilience Act are important steps in helping avoiding fragmentation.

Analysing the threats, sharpening intelligence, influencing the right regulatory approach and mitigating cyber risk all help us anticipate what the future may hold – and sharpen our collective defence.

THIÉBAUT MEYER
Director, Office of the CISO – Google Cloud

Navigating DORA compliance: a collaborative journey towards financial resilience

The Digital Operational Resilience Act (DORA) aims to bolster the European financial sector against ICT disruptions. While larger entities are generally ahead due to their existing risk management frameworks, the path to achieving compliance by January 2025 may be challenging for smaller entities, who may be grappling with resource constraints and the complexity of integrating DORA requirements into their operations.

One major pillar of the regulation is the effort towards robust Threat-Led Penetration Testing (TLPT). In this area, Google Cloud is providing thought leadership on approach and implementation of pooled testing. In November 2023, Google Cloud published a non-paper outlining a technical testing approach to address the "end to end" testing whilst accommodating the nuances of the Shared Responsibility Model. Google Cloud followed this with a further non-paper in June 2024 which provides our perspectives on principles that should underpin the creation of a customer pool to facilitate pooled testing. These proposals are supported by our experience as a leader in the security field to facilitate discussion amongst regulators and customers alike. We welcome the opportunity to continue shaping the development of guidance to address this key requirement.

While thinking about enhancing the resilience and the cybersecurity level of European financial entities, it is important to consider the impact of the coming AI revolution. First, AI will rapidly modify the threat landscape, enabling attackers to act faster, with sophisticated modus operandi that will be more challenging to detect. AI can be used by bad actors to gather intelligence, find and analyze vulnerabilities, and spread malicious software across organizations.

On the other hand, AI is also a highly valuable tool for the defenders. It enables the automation of repetitive and time-consuming tasks, allowing teams to focus on more complex activities. AI also offers the possibility to scale and analyze data more quickly to react more effectively to incidents and limit their impact. It is these types of features that we offer at Google Cloud in our tools.

Other regulations are currently being put in place in Europe with the aim to enhance the collective capacity of the European Union to detect, prepare for, and respond to large-scale cybersecurity incidents and attacks: the NIS2 directive, the AI Act, the Cyber Resilience Act, the Cyber Solidarity Act, PSD3 etc. Regulators need to maintain a focus on consistency between texts and avoid inconsistencies, particularly in more technical implementation acts.

To ensure a resilient financial ecosystem, DORA's implementation demands a collaborative effort to navigate evolving risks, compliance challenges and diverse interpretations.

In addition, one of DORA's significant challenges lies in the potential for divergent interpretations of DORA's requirements between supervisors and the industry. For instance, supervisors' interpretations of certain provisions may differ from how financial institutions understand them. This discrepancy can lead to confusion and delays in implementation, as organizations struggle with aligning their practices with evolving interpretations. We believe a better approach is to focus on the desired outcome rather than prescribing the methodology for achieving it. It is paramount to avoid overly prescriptive texts and guidance that may become outdated due to technological advances. A continuous cooperation between the European Supervisory Authorities and the financial national competent authorities will reinforce the harmonization and consistency of interpretation.

Google Cloud will play its role in this collective effort to strengthen the resilience of the European financial sector and has put in place a robust compliance readiness program. It focuses on key initiatives to prepare for the new direct oversight for critical ICT third-party providers under the Regulation and supports customer compliance. These initiatives span across DORA's five pillars - Digital Operational Resilience; Third Party Risk Management; Incident Reporting and Management; Risk Management and Governance; and Information and Intelligence Sharing. We have already announced updates to Google Cloud contracts to support our customers in ensuring their DORA compliance readiness and we will continue to support our customers with new resources that address the applicable DORA requirements.

DORA's implementation journey necessitates a collaborative effort between regulators, financial institutions, and CSPs. Clear communication, consistent interpretation, and ongoing dialogue are essential to ensure smooth implementation and foster a resilient financial ecosystem. By embracing industry best practices, leveraging AI's potential, and proactively addressing emerging challenges, the financial sector can navigate the complexities of DORA and achieve its goal of robust operational resilience.

DIANA PAREDES
Chief Executive Officer &
Co-founder – Suade Labs

Balancing compliance and innovation: operational resilience challenges for SMEs

The global IT outage in July this year, described as one of the largest in history, highlighted vulnerabilities in our increasingly interconnected world. This incident saw 8.5 million systems affected by the faulty CrowdStrike update, causing widespread disruptions, including the infamous "blue screen of death" on Windows PCs. The disruption underscored the importance of operational resilience, demonstrating how a single point of failure can have far-reaching consequences for businesses and their stakeholders.

In an era of rising cyber threats and technological dependencies, strengthening operational stability and minimising systemic risks is a key priority for many, including the European Union. On 16 January 2023, The Digital Operational Resilience Act (DORA), approved by the European Union, came into force. DORA's primary aim is to bolster the operational resilience of financial entities by setting uniform requirements for managing information and communication technology (ICT) risks.

DORA is different from previous regulations because it is a regulation, not a directive, meaning it applies directly and consistently across all EU member states. This uniformity aims to ensure the security and confidentiality of IT systems and data across all financial entities. Before DORA, various guidelines existed but did not achieve full harmonisation. Now, the management body of each financial entity bears the ultimate responsibility for managing ICT risk, including setting policies for data availability, integrity, and confidentiality, and approving digital operational resilience strategies.

The implementation of DORA presents both opportunities and challenges. One of the critical considerations of DORA is its impact on innovation and third-party vendor management. While the regulation sets stringent requirements, it also seeks to encourage a more robust and transparent financial sector. The additional compliance measures are designed to enhance overall market stability and resilience, though they may also impose additional burdens on SMEs.

Small and medium-sized enterprises (SMEs) might encounter increased expenses related to compliance, as they may need to invest more in technology, train their staff, and possibly hire external consultants to meet the requirements of DORA. These expenditures can impact their limited financial resources, requiring careful budgeting and prioritisation. However, investing in these areas can also strengthen their overall resilience and competitiveness in the long term.

The detailed regulatory demands of DORA can be challenging for SMEs, which might not have the necessary expertise and experience in handling ICT risks. This can make it difficult for them to fully grasp and implement the regulations, increasing the risk of non-compliance and potential penalties. On the other hand, adhering to these regulations can enhance their risk management capabilities and prepare them for future disruptions.

DORA also aims to create a level playing field, ensuring that all market participants adhere to consistent standards. This could foster greater trust and stability within the financial ecosystem, potentially benefiting SMEs by providing a more secure operating environment. However, the uniform approach might not fully account for the unique challenges faced by smaller entities, which could impact their ability to innovate and compete effectively.

The proportionality principle within DORA, which scales requirements according to the size and complexity of the institution, aims to mitigate some of the burden on smaller entities. By enforcing a standardised approach to ICT risk management, DORA seeks to enhance overall market stability. However, it is important to monitor whether this approach sufficiently balances the need for security with the flexibility required for innovation.

In conclusion, DORA represents a significant step in safeguarding the operational resilience of the EU's financial sector, addressing current vulnerabilities and aiming to create a more secure financial ecosystem. While SMEs may face particular challenges in meeting DORA's requirements, the regulation's proportionality principle and its focus on consistent standards offer both potential benefits and drawbacks.

The regulatory demands may post challenges to SMEs, potentially impacting their ability to innovate.

The CrowdStrike incident exemplifies the critical need for robust operational risk management, underscoring that, despite the challenges, it remains imperative for organisations to strengthen their resilience against unexpected disruptions. As financial institutions work towards the January 2025 compliance deadline, the collective efforts to enhance operational resilience will be essential to fortify the sector against future disruptions and cyber threats, balancing security and innovation.