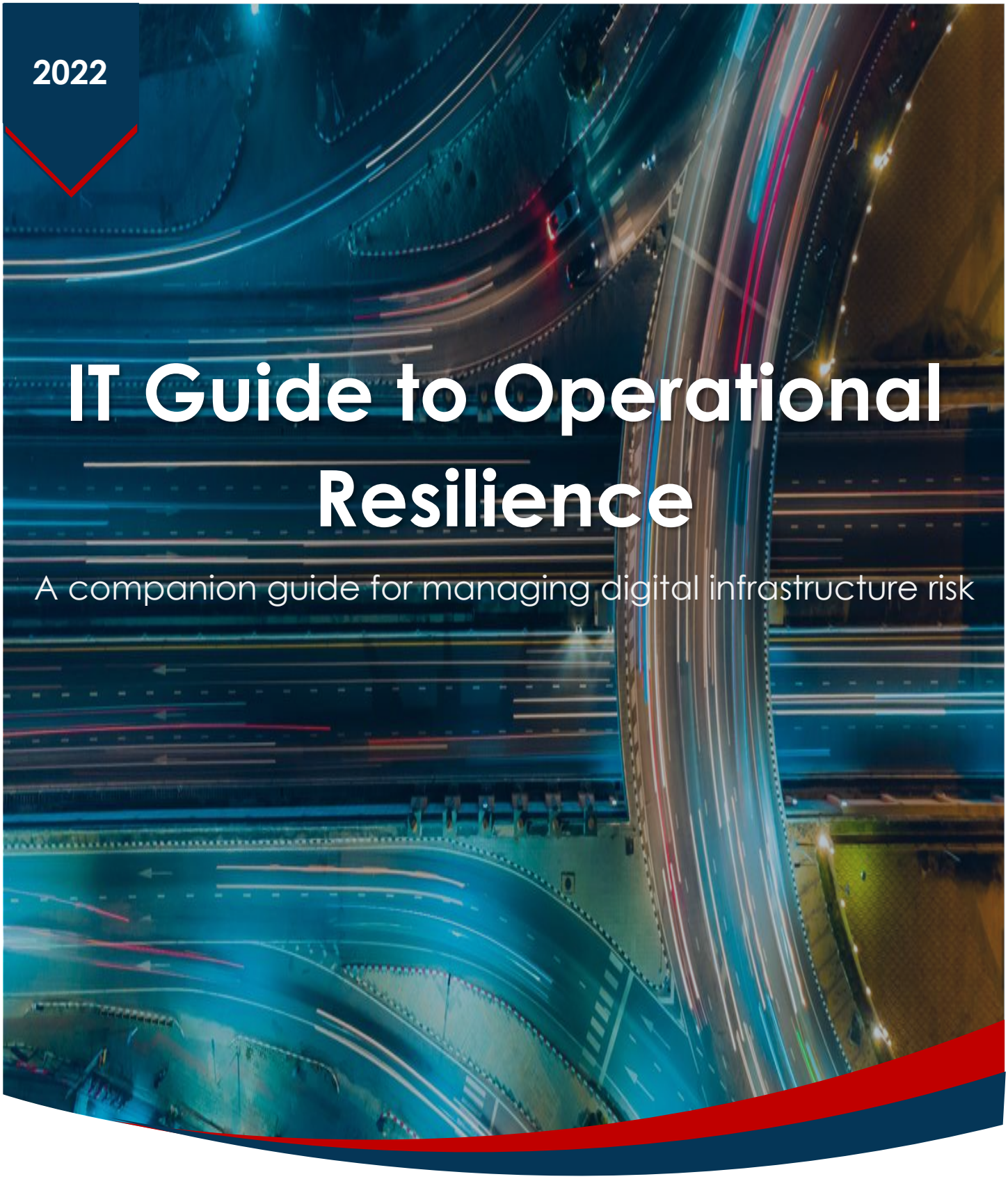
2022

IT Guide to Operational Resilience

A companion guide for managing digital infrastructure risk



Red Hat

JWG

Global regulatory intelligence through collaboration

Contents

I. Executive summary 2
II. New digital rules 3
Digital Operational Resilience 3
Third party risk management 4
New technology imperatives 4
III. The board's new risk dashboard 5
A new infrastructure risk dashboard 5
Board oversight of infrastructure risk 6
Firm: supplier: regulator engagement 7
V. Recommendations and Conclusion 7
Recommendations 7
Conclusion 8

About the research

This report is a companion guide to a larger research report, 'Managing Digital Infrastructure Risk: A collaborative path to financial services safety' produced by JWG. It is intended to help IT managers understand the implication of new regulatory demands on the IT supply chain.

JWG is an independent, pioneering market intelligence company who has been working with firms, technologists, and regulators since 2006, to help the industry comply with the ever-changing regulatory landscape.

This research report is based on a variety of global sources including intelligence gained from JWG's **Risk Control for a digitized financial sector report**, from analysis of the viewpoints presented at the **JWG November 2021 Annual RegTech Conference**, the **JWG RegCast** series, **survey results** and feedback from the **120+ institutions** that have attended **JWG workshops and events**. The report also includes global analysis from JWG's **RegDelta** system and **RegDelta Radar Services**.

For more information contact: Corrina.Stokes@jwg-it.eu

I. Executive summary

New regulation will **fundamentally change the landscape for the biggest tech companies** — particularly cloud providers — by demanding end-to-end controls.

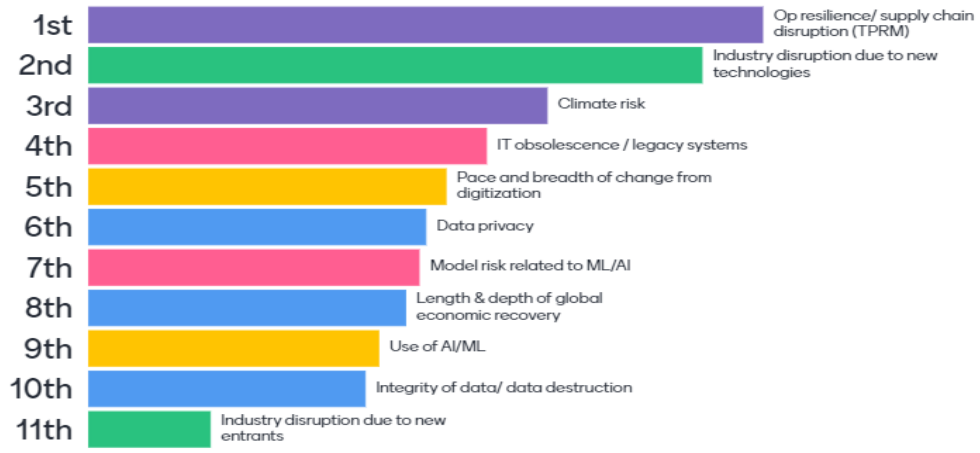
Firms will need to **upgrade current controls** with governance frameworks capable of mitigating AI and other technology risk but also comply with cyber secure data privacy laws that extend across the supply chain.

New supplier management strategies will be required to account for regulatory compliance requirements that demand **portability between providers**.

> This report is intended to help IT managers understand the implication of new regulatory demands on the IT supply chain. It is a companion guide to a larger research report, 'Managing Digital Infrastructure Risk: A collaborative path to financial services safety'

In November 2021, a JWG survey found that supply chain disruption and operational resilience was ranked top of the emerging risks list with disruption due to technology closely behind (see Exhibit 1).

Exhibit 1: Top RegTech risks by 2026



Source: 15 respondents asked to rank a modified EY risk survey at JWG's 11/21 RegTech conference

Overall, infrastructure risks dominate the top half of the league table. Infrastructure and supply chain disruption features just above risks from IT obsolescence and legacy systems.

JWG's analysis, which includes a review of 287,897 pages of new rules in Q122 shows that by 2025, overlapping requirements to mitigate **operational resilience** threats; control **third party services** and improved technology **governance** will **move technology risk management out of the back office and into the boardroom for financial services firms**.

The industry has a **window now to create a harmonised set of controls** for infrastructure risks which JWG research shows to sit squarely at the top the risk league table and be prone to fines.

II. New digital rules

Quick take:

- **Operational resilience** (UKPS6/21, DORA) recasts operational risks as threats
- **Third party outsourcing** and ESG increase transparency of services
- **Technology governance** rules demand oversight of AI, cyber, privacy, data risks
- **New supplier management strategies** will need to account for risks identified in these three sets of policies and require **common controls, metrics and measures**

Digital Operational Resilience

Today's financial services businesses are under pressure. On one front their customers are pushing the board toward ever more resultant and trusted digital infrastructures. On the another, regulators want firms to control the systemic technology risk upon which the business relies. Both these pressures are finding their way down the supply chain.

The UK and EU are taking the global lead in defining new standards to hold firms to account. In 2018, a UK Regulatory Discussion Paper on Operational Resilience placed the industry on a path toward new controls that look beyond the individual institution's operational risk and consider a broader range of non-financial risks across the supply chain. The first phase of the resulting policy outlined in Exhibit 2 concluded on March 31, 2022[i] when firms mapping exercise were expected to be completed.

The EU Digital Operational Resilience Act (DORA)[ii] implementation is planned for 2023 and broadens regulatory focus to encompass operational sustainability. This more holistic obligation envisions an end state in which a firm weathers turbulence from unanticipated events in the system. Operational risks are threats to operational resilience and areas that must be at the centre of a company's operational resilience policy.

Exhibit 2: Key obligations of the EU's DORA and the UK's PS6/21

Digital Operational Resilience Act (DORA)	PS6/21 Operational Resilience: Impact tolerances
ICT **risk management** framework	Identify important **business services**
ICT-related **incident** management process	**Impact tolerance** for important business services
Risk-based digital operational resilience **scenario-based testing**	**Mapping exercise** & scenario testing with severe but plausible scenarios
Cyber **threat** intelligence **sharing**	Internal & external **communications strategy**
Third-party risk strategy	Conduct a "**lessons learned**" process to identify **shortcomings**, improve **reaction** times
Maintain a **register of contractual arrangements** with ICT third-party service providers.	Prepare **self-assessment** questionnaire on operational **resilience** and cyber **capabilities**

DORA's EU mandate extends beyond the UK to include both digital and ICT risks, with a clearer emphasis on cyber threats with the inclusion of cyber threat information sharing and an ICT incident management process.

It will also require contracts to include standard clauses which detail the services, the protections offered in delivering them and dedicated exit strategies. New technical standards on portability will specify how firms are to "identify alternative solutions and develop transition plans enabling them to remove the contracted functions and the relevant data from the ICT third-party service

provider and securely and integrally transfer them to alternative providers or reincorporate them in-house" as is stated in DORA's Article 25, section 9. Regulators will also specify what information on their contracts is reported to them.

Critically, ICT third-party service providers designated as critical (CTPPs) will be subject to a common oversight framework and direct oversight from EU regulators.

For third party risk management, the UK have created a separate supervisory statement (SS2/21)[iii] with similar obligations. See the following section for more detail.

Third party risk management

Supply chains in the financial sector are vast, encompassing technology, data, and infrastructure, and not traditionally an area of direct regulatory supervision.

UK and EU TPRM rules obligate firms to supply information on their outsourcing agreements to regulators. While US policy is still being formulated, early trans-Atlantic dialogue indicates a major upgrade to supply chain oversight is underway.

In line with updated EBA outsourcing guidelines which went into effect on the 31 December 2021, the ECB will collect 51 fields of data per outsourcing contract for "all existing outsourcing arrangements" in Q2 2022. The data will reside in a Centralised Submission Platform (CASPER), aligning with the effective date of the EBA's recent outsourcing guidelines.[iv]

This new EU reporting regime places the burden of supply chain transparency regimes on the regulator for the first time. Regimes like OSPAR in Singapore[v] placed the oversight burden on suppliers and their auditors, not regulators. Regulators will get a unique picture of the supply chain interdependencies and be able to identify concentration risks for the first time.

UK regulatory plans indicate that the UK is likely to follow suit in creating similar supply chain transparency obligations later this year, following implementation of the PRA's outsourcing and third-party risk management guidelines which went into effect on 31 March 2022. In June 2022, HM Treasury released a policy statement outlining its intentions to create a critical third party regime enabling regulators to create and enforce new resilience standards

Progress in the United States has been more limited. An interagency consultation on managing the risks associated with third parties was issued in July 2021.[vi] The consultation aligned closely with Singapore's third-party regime, however, there has been no further update since the comment period expired on 17 September 2021. However, the U.S.-EU Joint Financial Regulatory Forum meeting in March 2022 discussed mutual interests, including operational resilience and the regulatory cooperation on third-party providers.

New technology imperatives

In parallel with the push to digital operational resilience and third-party risk management, regulators have developed new obligations for the use of technology. Since 2018 many new technology risk controls have been introduced to address AI, APIs, Cyber Security, Data Privacy, and other technologies which are further detailed in JWG's broader paper, Managing Digital Infrastructure Risk.

These technology obligations vary in depth and breadth, with some, such as the cybersecurity framework creating holistic and deep needs, and others focused on individual points of control. Taken together, infrastructure managers need to navigate uneven terrain that starts with high level strategy, governance, process and moves into deep controls, metrics, measures, and proof points.

Some of the frameworks are still in their infancy (e.g., PET, Quantum) but have the potential for them to expand quickly to overlap with other obligations. Clearly, there is an opportunity for a more systemic approach to defining digital infrastructure controls for financial services.

III. The board's new risk dashboard

Quick take:

- Cloud-based connectivity means **infrastructure controls are core to the business**
- Boards can **no longer mitigate the effect** of losing their infrastructure
- **Firms need to take the lead** in defining best practices and holding suppliers to them

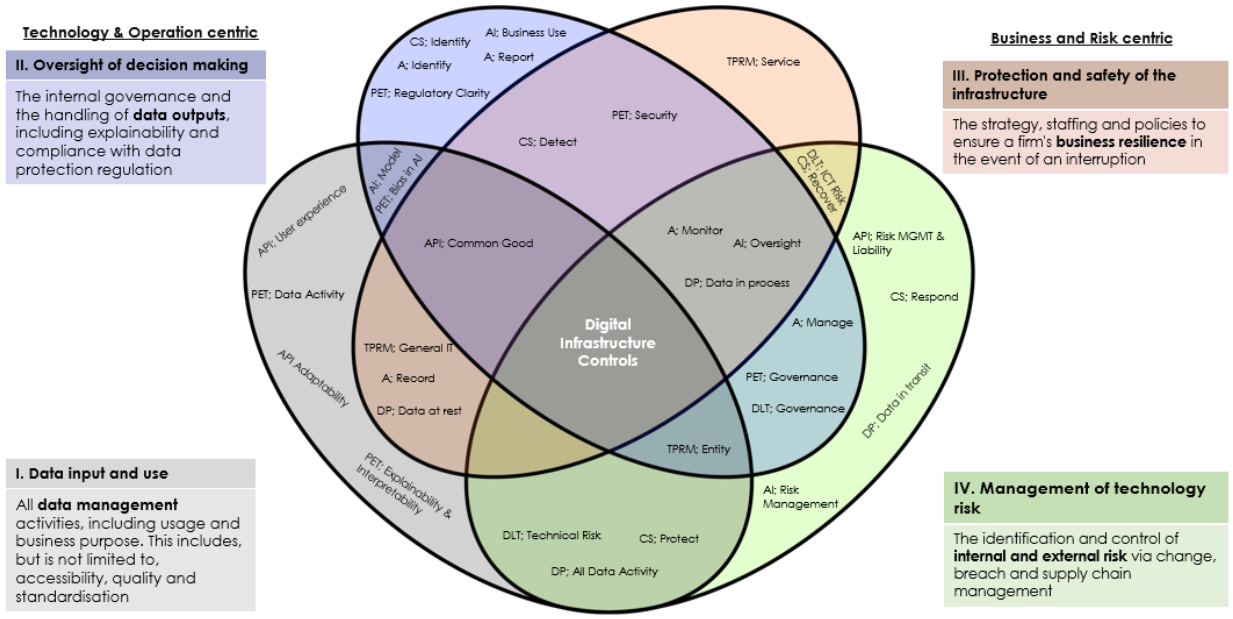
A new infrastructure risk dashboard

To make sense of this complex landscape, we established a global policy baseline and then examined the interdependencies and overlaps to construct a comprehensive view of what it takes to have compliant infrastructure.

We looked at 9,136 Documents across the EU, UK, US and Internationally with 287,897 pages from 1st Jan 2021 – 1st March 2022. By examining these policies, it became clear that while certain duties were specific to their respective technology, there were many that shared commonalities and some notable gaps.

Our thematic dashboard simplifies the technology controls into four actionable imperatives, as shown in Exhibit 3 and described in our broader paper, Managing Digital Infrastructure Risk.

Exhibit 3: Regulatory Infrastructure dashboard analysis



Source: JWG analysis of global regulatory obligations as of March 2022

The dashboard shows that compliance, data and risk functions need to work together to establish end to end controls. For example, API requirements span all lenses of the dashboard. From a data input perspective, the user experience and scalability will be key. From an oversight perspective, the inclusiveness and bias of API performance needs to be monitored. Protection and safety of APIs require oversight of third parties. Finally, technology risk requires testing of information security controls.

Some of the regulation behind these controls is more mature than others, and we discuss this in more detail in the source paper. Regardless of the approach to these obligations, we believe these themes will stand the test of time and help senior manages visualise their control needs via a comprehensive dashboard.

Data input and use. The data obligation requirements can be found most prominently but not exclusively in the controls for AI, data privacy and PET in reports such as the AI Financial Services report by the Alan Turing Institute and regulation, such as the Artificial Intelligence act from the European Commission[vii] which opts for a risk-based approach to control the use of high-risk AI systems.

Oversight of decision making. The governance obligation is concerned with the impact of using data, the outputs of said data and how that is communicated and reported to the public and competent authorities. Oversight is key focus for regulators globally and these requirements can be found most prominently but not exclusively in the controls for AI, TPRM, data privacy and cyber security and in initiatives and regulations such as the UK ICO's guidance on anonymisation, pseudonymisation and privacy enhancing technologies.[viii]

Protection and safety of the infrastructure. The protection and safety of infrastructure emphasises the resiliency and business continuity of the infrastructure as well as accountability for its management. The authorities' overarching driver is to ensure that business can operate under difficult circumstances or recover quickly. While it includes obligations on the institution itself, a company's resilience is not only determined by the strength of its internal structures. It covers a wide spectrum of technical third-party risks, including cybersecurity threats that can occur anywhere along a supply chain, as well as natural disasters like disease and weather.

Management of technology risk. Management of technology risk focuses on identifying and controlling internal and external risks through change, breach, and supply chain management. This topic emphasises the importance of prescriptive controls over services that go beyond day-to-day operations. It also aids as support to the protection and safety of the infrastructure, as preserving the infrastructure's stability necessitates vigilance in the face of potential threats like Cyber.

Board oversight of infrastructure risk

Simply put, technology risk management should move from the back-office to the board room, because while technology has always played an important role, Cloud-based connectivity means, it is quickly becoming core to the business itself.

It is no longer possible to isolate technology risk and leave it to the techies; instead, a comprehensive approach to technology, be it owned by the firm or outsourced, is required.

Boards which can no longer mitigate the effect of losing a significant part of their infrastructure will need to focus on what 'good looks like' and hold their suppliers to it.

Firm: supplier: regulator engagement

Boards are now challenged to put new management information in place which enables excellent communication between the business and the back office. Technology, Data, Risk, and Compliance functions are required to form a common view of the regulatory control needs across the whole organisation and demonstrate compliance with the new rules.

Critically, the supply chain will be looking to owners of the regulatory risk (i.e., the firms) for leadership. No matter how large, a single supplier will not be able to mitigate all regulatory risk for a firm. Rather, firms will need to club together to define holistic standards which the entire supply chain can adopt.

It could prove challenging for firms who may not have deep enough visibility of their supply chain or have the procedures in place to monitor fragmented suppliers.

Supply chain risk not only encompasses technology, such as cloud, but is also a concern in areas such as Environmental, Social, and corporate Governance (ESG) where concern is growing for the carbon emissions in the whole of a firm's value chain.

It will grow increasingly more complicated especially in cases whereby an organisation might be both a supplier and a receiver of financial products, as there will be multiple emissions that need to be considered across many supply chains. A holistic approach to supply chain risk management that includes, ESG, technology, cyber and operational risk and data is required.

V. Recommendations and Conclusion

Quick take:

- The sector has a **short window now** to create a **harmonised set of controls**
- A massive administrative burden could increase **technology cost** and **stifle innovation**
- As a first step, we recommend regulator; regulated and the supply chain convene a cross-trade body platform to align **priorities, frameworks and plans**

Recommendations

The industry, in conjunction with trade bodies, should create a holistic risk management framework for the provision of IT infrastructure to financial services. There is no need to start from scratch, rather industry should utilise existing frameworks and assessment capabilities.

The framework should be developed collaboratively, initially though a task force with its ultimate ownership to be determined.

Exhibit 4: Summary recommendations

Cross-sector risk Framework	Scale assessment capabilities	Compliance knowledge base
► Convene a cross sector working group ► Define and agree to a comprehensive infrastructure risk management framework ► Collaborate with standards bodies to map obligations to existing control frameworks ► Establish priorities and create a series of integrated checklists to account for the holistic set of controls	► Establish a community of practice across audit, law firms and specialist ► Bring professional services firms together to identify the top risks and issues ► Create use cases to establish the characteristics of 'what good looks like' across jurisdictions	► Create a 'single version of the regulatory truth' for human and machine consumption ► Build a technical portal that enables knowledge workers to understand best practices ► Create an oversight committee to review and prioritise global regulatory updates

Conclusion

If IT infrastructure supply chain and data risk controls are not standardised, firms, and their suppliers risk market failures, stifling innovation, massive administrative burden, and large fines.

Regulator: regulated: supplier cooperation will need to grow quickly to meet new regulatory demands in a sustainable and efficient manner. The interconnectedness, and depth demands a multidisciplinary approach which is appropriately resourced and governed.

The effort is not to be taken lightly for a supply chain of this size. Contact pj@jwg-it.eu if you would like to help make it happen.

End notes

[i] Prudential Regulation Authority (PRA) - PS6/21 Operational Resilience: Impact tolerances for important business services

[ii] European Commission – Proposal for a regulation on digital operational resilience for the financial sector - Digital Operational Resilience Act (DORA)

[iii] Prudential Regulation Authority (PRA) - SS2/21 Outsourcing and third-party risk management

[iv] European Central Bank – Centralised Submission Platform (CASPER)

[v] The Association of Banks in Singapore - ABS Guidelines for Outsourced Service Providers

[vi] Federal Reserve, Federal Deposit Insurance Corporation, Department of the Treasury and the Office of the Comptroller of the Currency – Proposed Interagency Guidance on Third-Party Relationships: Risk Management

[vii] Proposal For a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts - Artificial Intelligence Act

[viii] Information Commissioner's Office (ICO) - Introduction to anonymisation, pseudonymisation and privacy enhancing technologies guidance