pwc.com

Building Sustainable Resilience

January 2024

Arab Bankers Association
جمعية المصرفيين العرب

Agenda

Introductions

01 Market update: global megatrends

02 Resilience: regulatory insights

03 Cyber resilience

04 Rethink your resilience

05 Q&A

01

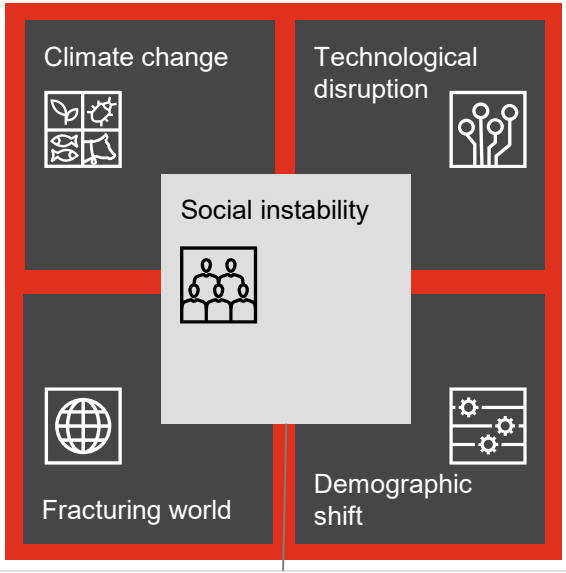
Market update: global megatrends

Megatrends: five global shifts reshaping the world we live in

Almost a decade has passed since the PwC network identified five Megatrends, which we characterised as deep and profound trends, global in scope and long-term in effect, touching everyone on the planet and shaping our world for many years to come. It is now clear that these Megatrends have transformed our world even faster than we predicted. Largely this is due to the interaction between the trends, which has turbocharged both the speed and pervasiveness of change.

While the Megatrends have been unfolding, they have also evolved, and the way they are manifesting today has shifted compared to ten years ago.

- Business failure unless organisations fundamentally reconfigure operations and actively manage ecosystems
- Resource insecurity / scarcity / cost increase
- Supply chain disruption
- Job creation through investments in climate tech



- Competitive differentiation through technology
- Business failure without digital transformation and faster speed of execution
- Concentration of power in the hands of a few; failure of small businesses
- Mismatch between required and available skills
- Increased cyber risk

- Pressure for boycotts and taking a stand on ‘political issues’
- Disruption of global supply chains
- Difficulty of doing business in a world of conflicting rules and regulations
- Pressure for global businesses to be deeply embedded in key countries

- Shift in needs and consumption patterns, slow-down of consumption-based sectors
- Mismatch between available and required skills
- Conflicts related to a multi-generational workforce with differing views on work and the world
- Lack of relevant skills in the workforce

- Need to reconcile divergent requirements of stakeholders
- Pressure to increase transparency while managing reputational risk
- Responsibility to take care of all needs of employees
- Greater need to invest in the creation of trust

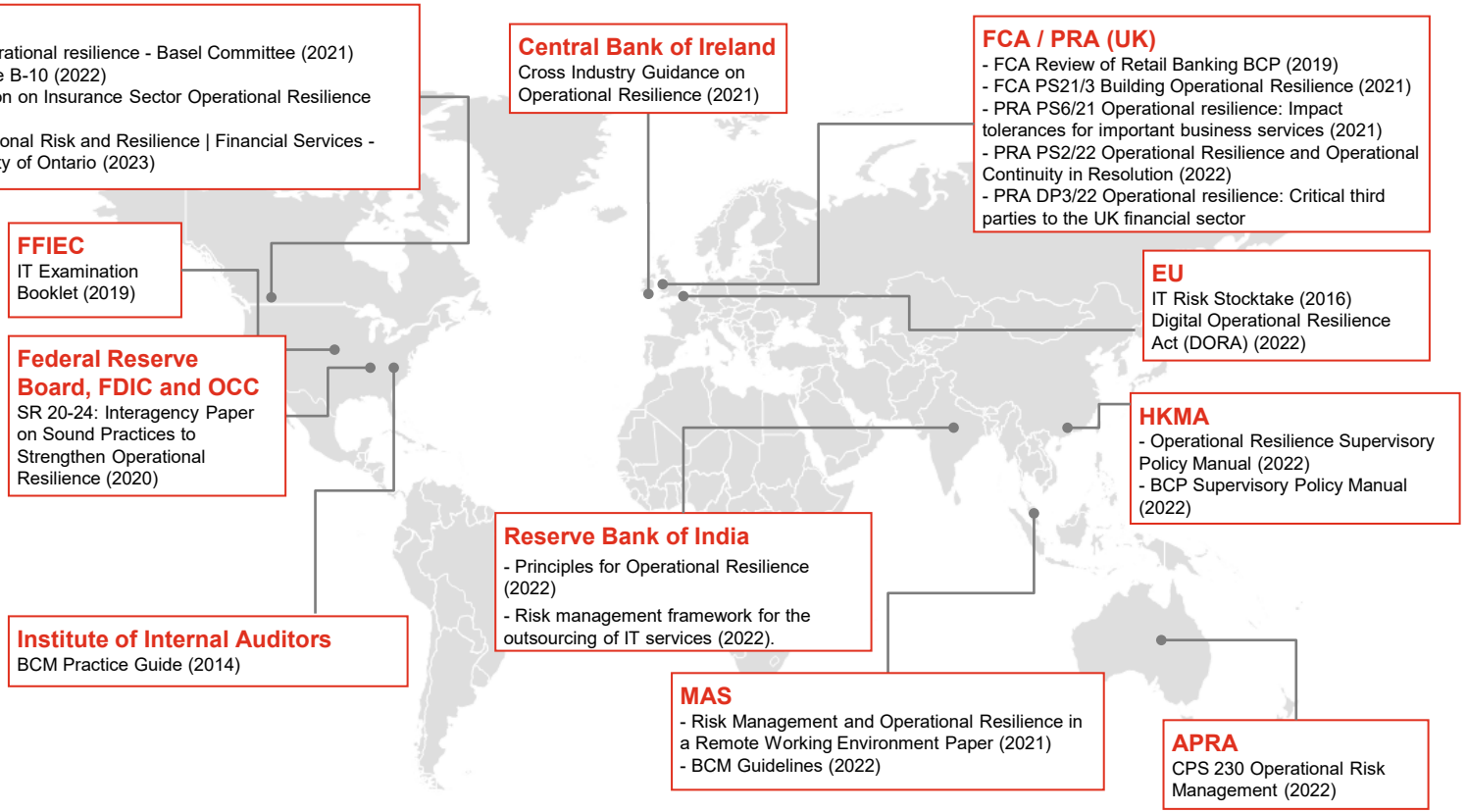
02

Resilience: regulatory insights

Operational resilience global view

Global regulatory expectations and standards

Operational resilience regulation is developing across the international Financial Services sector and as a result, it is important to consider how efforts already undertaken can support new and differing requirements. This means there is a need for firms to approach regulatory compliance with a global outlook.

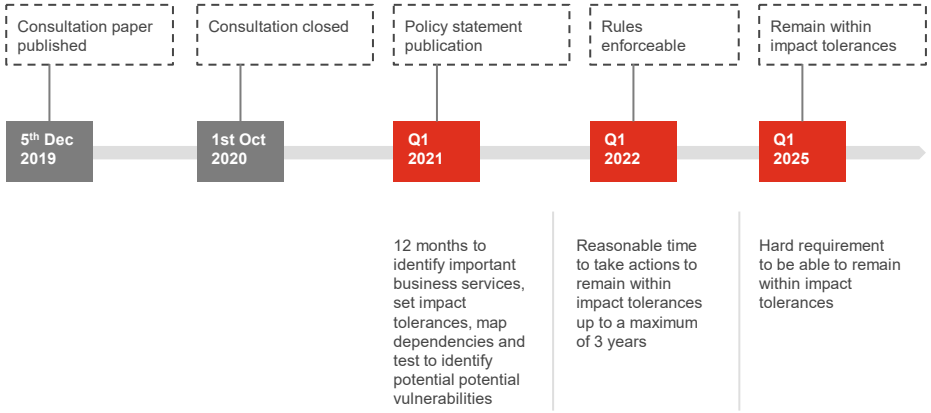


Operational resilience: latest industry insights (UK)

Firms have until March 2025 to continue mapping and testing, and build resilience to ensure their Important Business Services can remain within their impact tolerances in the event of disruption.

Feedback continues to be received by the regulator both in terms of industry themes / observations, as well as firm specific feedback. Emphasis is being placed on increasing the sophistication of operational resilience practices in terms of mapping, approach to impact tolerance assessments and scenario testing.

Firms are now seeking to understand where they are on their operational resilience journey in relation to the March 2025 deadline and to gauge if their identified vulnerabilities are likely to be resolved within this period.

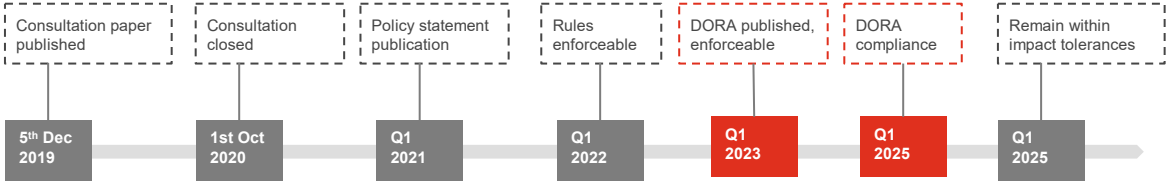


Key messages from the UK Regulators

- **Foundations are still to be achieved:** The view from policy makers is that issues still exist with the granularity, clarity and robustness around service definition, impact tolerance setting and scenario testing. These must be resolved quickly to deliver by 2025.
- **More challenging scenarios:** Firms need to focus on increasing sophistication in severe but plausible scenarios as well as testing multiple events in succession and across multiple Important Business Services.
- **Lack of articulation of workings:** Firms need to clearly document their approach and justifications to selecting Important Business Services and setting impact tolerances.
- **Impact tolerance bias:** Some firms have exclusively focused on time-based impact tolerances, without considering non-time based metrics.
- **Primary focus on consumer harm:** Firms have primarily focused on consumer harm with less consideration of firm safety and soundness and market impact.
- **Self assessments:** Regulatory supervisors are unlikely to believe a self assessment which asserts that the firm is fully and sufficiently operationally resilient.
- **Delivering value beyond compliance:** The initial focus of some firms has been on achieving compliance with the regulations rather than on being truly resilient. Firms should be focusing on an outcomes focused approach and embedding resilience into the firms DNA.
- **Industry collaboration is key:** Industry collaboration is crucial for enduring best practices. This effort fosters knowledge exchange, expertise sharing, and a collective commitment to continuous improvement, ensuring sustained evolution in industry standards.

Spotlight on DORA (EU): considerations and timelines

Regulation Timelines: UK Operational Resilience / DORA



Acceleration areas: there are some key areas of interaction between DORA and the UK Operational Resilience Regulations, and firms will be able to leverage some of the work done to date in the pursuit of DORA compliance, namely in the following areas:

- Mapping of technology and ICT third parties
- Impact tolerances
- Testing, especially in line with maturing scenario testing approaches
- Identification and remediation of vulnerabilities

Chapter	DORA Pillars	Requirements	Overlap to Op Res
I	ICT Risk Management	• Set-up and maintain resilient ICT systems • Identify, classify and document critical functions and assets • Continuously monitor all sources of ICT risk	Moderate
II	ICT Incident Reporting	• Develop a process to log/classify all ICT incidents • Submit reports on ICT-related incidents to regulator • Harmonise the reporting of ICT-related incidents	Minor / No
III	Digital Operational Resilience Testing	• Annually perform basic ICT testing of ICT tools and systems • Identify, mitigate and promptly eliminate any weaknesses etc • Periodically perform threat-led penetration testing	Moderate
IV	ICT Third Party Risk Management	• Monitor risks emanating from ICT third-party providers • Report register of outsourced activities, including intra-group services • Critical ICT third-party service providers will be subject to a Union Oversight Framework	Moderate
V	Information Sharing Arrangements	• Arrangements for exchanging of threat intelligence • Collaboration among trusted communities of financial entities • Mechanisms to review and act on shared intelligence	Minor / No

Expectations of 1LoD

- Definition of business services (critical functions), process mapping and CMDB.
- Perform threat analysis and scenario management.
- Set security strategy, processes and technologies, including protection of customer data confidentiality, integrity and availability.
- Ensure technical and organisational measures for ICT / cyber protection and prevention.
- Design and implement resilient infrastructures and architectures.
- Predictive monitoring / early detection of anomalies.
- Ensure continuous improvement, root cause and incident post-mortem analysis.
- Set business continuity, backup and disaster recovery strategies based on plausible scenarios and with business service based view.

Expectations of 2LoD

- ICT / cyber risk assessment and management of policies, frameworks and processes integrated in the overall Risk Management Framework.
- Oversight of ICT, third party and cyber risks.
- Oversight of digital operational resilience strategy.
- Assessing firm progress to DORA compliance.
- Definition of impact tolerances, scenario analysis and RAF integration (management body approval).

Spotlight on DORA: Common challenges firms are facing

1. Taxonomy	Interpreting and applying the DORA taxonomy to existing frameworks.
2. Critical and important functions	Defining, identifying and mapping critical and important functions - and understanding the ICT services, information assets and ICT third parties supporting them.
3. ICT risk management framework	Addressing all of the requirements around the ICT risk management framework and operationalising them.
4. Intragroup governance	Maturing intragroup governance arrangements to support effective ICT risk management and oversight.
5. Framework review	Determining how to perform the annual review of the ICT risk management framework - and the level of controls assurance involved in that activity.
6. DOR testing	Developing a Digital Operational Resilience testing strategy. Collating the different, siloed testing activities and aligning them against common scenarios.
7. Testing follow-up	Deriving insight from Digital Operational Resilience testing, automating testing and addressing any gaps identified when developing the testing strategy.
8. Identifying ICT third parties	Identifying ICT third parties and determining whether their contracts address the DORA requirements.
9. Emerging requirements	Incorporating emerging requirements (e.g. DORA Regulation Technical Standards) into existing programmes.

03

Cyber resilience

What do we mean by ‘Cyber Security’ and ‘Cyber Resilience’?

Cyber

Relating to or characteristic of the culture of computers, information technology, and virtual reality.

- Oxford Dictionary

Cyber Security

The **protection** of devices, services and networks — and the **information** on them — from theft or damage.

- National Cyber Security Centre

Cyber Resilience

The **ability to** anticipate, withstand, **recover** from and adapt to adverse conditions, stresses, attacks or compromises on cyber resources.

- MITRE

48%

of CEOs say they are increasing cyber investments to mitigate against exposure to adjusting supply chains and changing geopolitical conflict in the next 12 months - PwC Annual Global CEO Survey 2023.

So what does this mean for your organisation?

1. **Cyber Security** is the resources we put into preventing successful cyber attacks.
2. **Cyber Resilience** is the preparations we make for handling a successful attack and its consequences.

Risks

Disruption to business operations	**Disruption to online services**	**Theft of customer information**
Loss of digital trust	**Accidental leakage of customer information**	**Theft of confidential business information**
Theft of funds		

FS cyber industry and investment trends

Continued Focus:

- Enhanced detection capability
- Cyber hygiene - ‘Hard Basics’
- Vulnerability management
- Supply chain security

Increasing Focus:

- Secure cloud
- Cyber recovery and resilience
- Enhanced ransomware defences
- Security tooling consolidation

Future Focus:

- Zero trust
- Secure AI
- Automation
- Becoming a securable enterprise

Trends shaping the future of cyber and resilience

Geopolitical

Increased regulatory complexity is blocking a globally consistent approach to security - SEC/ECB/DORA.

Geopolitical tensions increase the risk of state-sponsored attacks.

Technology

Adoption of digital ID schemes poses a challenge in identifying fraud.

Multi-cloud adoption increases the risk of misconfigurations.

Quantum computing could make modern cryptographic controls obsolete.

Artificial Intelligence & Machine Learning can help break, or make security.

Business

Operational and cost optimisation through automation and standardisation.

Complex and legacy environments decrease resilience and recovery capabilities during an incident.

Threats

Ransomware: the most significant and rapidly evolving threat faced by all organisations.

Cloud services breach: Cloud misconfigurations can make cloud environments easy targets for hackers.

Supply chain: continues to be a prominent vector. As an extension to this, software supply chain attacks are on the rise.

Insider threat: potential for significant harm due to the insider's intimate knowledge of the business.

04

Rethink your resilience

Evolving Resilience capabilities beyond compliance

Crises are increasingly frequent and systemic in nature and we live in a world where disruption is commonplace. Organisations that enhance and invest in their resilience are better prepared to thrive in this era of disruption. Achieving resilience can be a challenge. Distributed data, systems, processes and operational silos mean organisations struggle to obtain a holistic view of their resilience, only identifying gaps when disruption hits.

Leadership and Culture

- Establish **visible leadership support** for Resilience and strong "**tone at the top**". Resilience should be viewed as a source of competitive advantage, not just a "cost".
- Recognise **culture as a critical enabler** for Resilience outcomes.
- **Detoxify failure** and create a safe environment for risk identification, timely escalation of issues, collaborative problem solving and continuous improvement.

Resilience-by-design

- **Build** processes, systems, products and services from the ground up **to withstand failure**.
- Clearly define Resilience requirements within **architectural standards** and key decision criteria for Change approval.
- **Align Operational Resilience and Operational Efficiency** initiatives, ensuring that they have complementary (not opposing) outcomes.

Embedding

- Make **BAU transition** a fundamental part of the Resilience programme, considered at all stages and delivered incrementally.
- Define a **Resilience taxonomy** and consistently apply that across the organisation. There should be universal agreement about the priorities and standards for resilience.
- Implement effective and properly resourced operating model, with clear accountabilities, roles and responsibilities across the 3LoDs.

MI, Insights & Reporting

- Establish robust MI for Resilience that enables consistent measurement and messaging regarding Resilience status at all levels of the organisation, up to the Board.
- Develop reporting that addresses three fundamental perspectives - **Compliance** (progress towards completion of regulatory policy requirements); **Performance** (maintaining services within impact tolerance); and **Capability** (operating functional disciplines and resources to meet minimum resilience control standards).

Using technology to accelerate outcomes

Our most recent Global Crisis & Resilience Survey in 2023 found that 58% of organisations report that technology enablement of their resilience programme is one of the most important future focus areas. We are seeing that firms that have a tool for resilience are better able to accelerate their resilience capabilities, break down organisational silos, improve their approach to testing and deliver deeper resilience insights.

Benefits of resilience tooling

Identify & prioritise critical business services by mapping and prioritising services according to impact tolerances. Build a consistent set of resilience capabilities and controls across disciplines.

Create a single source of the truth, streamline activities, identify and map dependencies across the key resilience pillars with seamless integration with your existing technology and data sources and providing a connected view.

Stress testing organisational resilience by utilising data and insights in a much more connected way to understand the likely impact to the business across a library of loss scenarios; enabling better preparedness and planning.

Quickly visualise key dependencies and relationships allowing you to understand the impacts of disruption, the actions required to respond, recover, driving effective management and coordination of response.

Holistic insight into operations and associated vulnerabilities to allow informed decisions and prioritisation of investment, as well as proactively manage and mitigate your risks.

Availability of interactive real-time dashboards and reporting, intelligently aggregating your data to provide the insights you need do drive change in the areas needing it most.

Thank you

pwc.com