Comparing international expectations on operational resilience

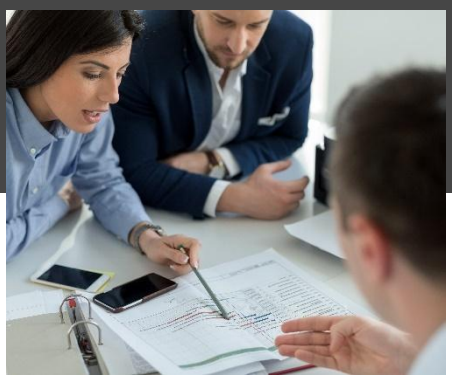
Version: April 2021

pwc

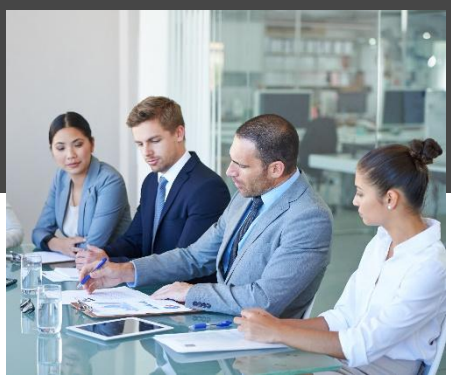
Context

Operational resilience regulation continues to gather pace around the world. The Basel Committee on Banking Supervision (BCBS), the European Commission and the US Federal Banking agencies have all added their perspectives on this subject.

Here we summarise the perspectives from leading bodies on the subject to help firms in building a globally consistent approach. This is particularly important as regulators have made public messages of supervisory coordination such as the December 2020 announcement by the UK's Prudential Regulation Authority, European Central Bank and the US Federal Reserve Board.



We include summaries on papers from UK, European Commission, Basel Committee on Banking Supervision (BCBS) and US. We see these as the foremost papers on the broad topic of operational resilience.



It is worth remembering that there are also many other jurisdictions (e.g. Singapore, Australia and Canada) publishing supervisory or policy papers on specific aspects of operational resilience including technology risk, business continuity management and outsourcing.

Sample of operational resilience policy and standards

UK (link)

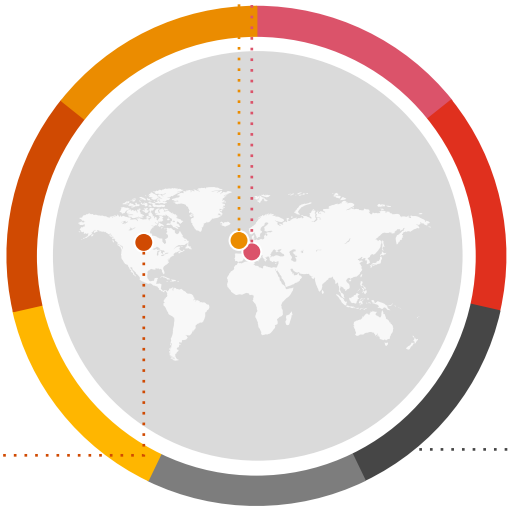
The UK is driving a step change in looking at resilience through the lenses of customers and markets as well as firms. Identifying important business services, mapping their end-to-end delivery, and testing the ability to remain within impact tolerances all help to drive investment to build resilience.

Next steps: Final papers on operational resilience were published in March 2021 with a one year implementation period to operationalise the policy framework and a further transitional period of up to three years for firms to remain within their impact tolerances.

Europe (link)

European Commission published draft legislation on digital operational resilience in 2020. The paper focuses on technology (and, by association, data) and third party risk. It focuses on risk management of assets and suppliers and associated activities, and does not adopt a functional/service view as we see in the other operational resilience papers.

Next steps: A set of proposed amendments to the draft is currently under consideration. Member State discussions are ongoing. Final legislation may drift into 2022.



USA (link)

A 2020 joint agency paper set out sound practices for operational resilience drawn from existing regulations, guidance, and statements.

Next steps: No fixed timetable but a pledge for continued public dialogue to help the agencies refine their approach.

BCBS standard (link)

The Basel Committee on Banking Supervision (BCBS) has published high level principles for operational resilience targeted at banks worldwide. These principles were published alongside an update to the Principles for the Sound Management of Operational Risk.

Next steps: Final principles were published in March 2021.

UK: Impact tolerances for important business services

The UK dialogue on operational resilience started with the discussion paper in July 2018 and has remained consistent since then. The UK is intentionally driving a step change in how firms consider resilience through the lenses of customers and markets as well as firms, which have traditionally been the narrow focus of business continuity. See our summary here.

Scope

'Operational resilience is the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions.'

The scope is limited to:

c. 1,050 banks, building societies, PRA designated investment firms, Solvency II firms, Recognised Investment Exchanges, Enhanced scope SM&CR firms

c. 1,100 entities authorised or registered under the Payments Services Regulations 2017 or the Electronic Money Regulations 2011.

Central Counterparties; Recognised Payment System Operators and Specified Service Providers; Central Securities Depositories

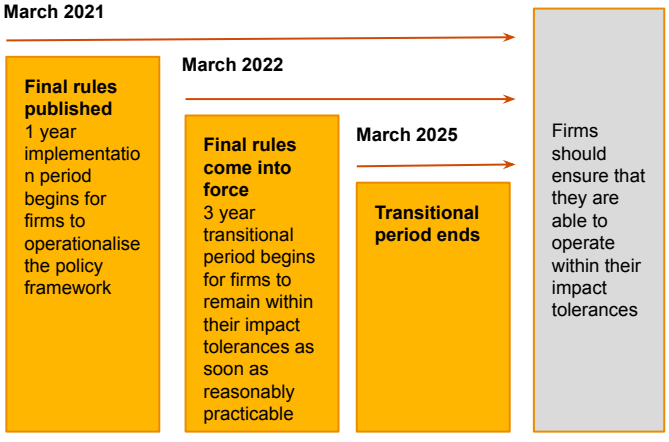
Key themes

An operationally resilient firm is considered one which:

- **Prioritises the things that matter** – Know which of your services for end users are the most important and understand how they are delivered
- **Sets standards of resilience** – Define the maximum tolerable level of disruption to these services (called impact tolerances), expressed by reference to specific outcomes and metrics.
- **Invests to build resilience** – Test your ability to remain within your impact tolerances and identify where vulnerabilities need to be addressed, while being prepared to invest to build resilience.

All of this must be demonstrated within a **self-assessment document**.

Timeline



Points of interest

- Arguably the most important aspect to get right is the determination of important business services (IBS) as this is what drives all other activity set out in the draft policy.
- The aspect we are asked about the most relates to impact tolerances. Firms find it challenging to work out the 'maximum tolerable level of disruption' and then to justify it with sufficient evidence. This is particularly true for firms trying to work out when disruption leads to customer inconvenience, (tolerable) harm or intolerable harm.
- The mapping of IBS end-to-end is widely regarded as the element requiring the most resource given the complexity of linking individual assets (whether technology, data, third parties, people or premises) to each step in the service.
- The most important aspect from the regulators' perspective is the testing phase as this will demonstrate the level of preparedness of each firm to withstand and recover from operational disruptions.
- Perhaps recognising these points the authorities have slightly softened their expectations during the 12 month implementation period such that firms are not required to have performed the full mapping and testing exercises to the full extent of sophistication by 31 March 2022.
- As a complement to the operational resilience consultation the PRA has published a policy statement and supervisory statement regarding firms' outsourcing and third party risk management. This takes into account relevant EBA and EIOPA guidelines on outsourcing and ICT and security risk management. The FCA has not changed its approach to outsourcing at this time.

BCBS: Principles for Operational Resilience

Both the BCBS and UK approaches drive the same set of familiar activities: identify what is important to make resilient; understand how those things are delivered; set standards of resilience; and test against them. However, there are some key differences including the 'currency' of the regime, being important business services for UK and critical operations for BCBS.

Scope

'Operational resilience is the ability of a bank to deliver critical operations through disruption. This ability enables a bank to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from disruptive events in order to minimise their impact on the delivery of critical operations through disruption.'

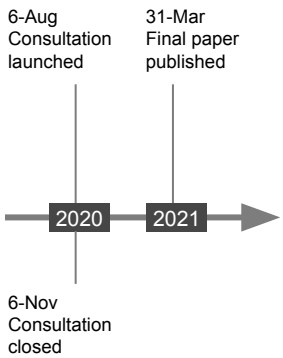
The principles are directly relevant only for banks. However, given it's influential role as a standard-setter they could be applied more broadly as regulators around the world seek to harmonise arrangements. The Bank of England has a prominent role at the BCBS Operational Resilience Working Group so we expected to see the alignment which has materialised.

Key themes

7 principles are outlined in the paper, namely:

- Governance
- Operational risk management
- Business continuity planning and testing
- Mapping of interconnections and interdependencies of critical operations
- Third party dependency management
- Incident management
- Resilient ICT, including cybersecurity

Timeline



Points of interest

- The BCBS paper sets out high-level principles joining the dots on the practices including risk management, business continuity and third party risk management, as well as the recovery and resolution regime. Being rooted in operational risk discipline helps BCBS to convey the importance of balancing activities aimed at preventing incidents with those focused on the response.
- The currency of 'critical operations' seems to leave a material gap in not explicitly considering the customer as advocated by the UK authorities. For instance, the PRA paper CP29/19 states: *'for many firms, [the new approach] will mean a shift away from thinking about the resilience of individual systems and resources and a shift towards considering services that are provided to users.'*
- BCBS has avoided the concept of 'impact tolerances' and is instead relying on firms adapting their existing risk appetite and their 'tolerance for disruption'. The final principles clarify that this should be applied at the critical operations level.
- BCBS suggests that 'internationally active banks' leverage their Recovery and Resolution Plans (RRP) for definitions of critical operations and consider whether their operational resilience efforts are appropriately harmonised with their recovery and resolution plans.
- In parallel BCBS published an updated set of principles for the sound management of operational risk. There are strong links referenced between the discipline of operational risk management and the outcome of operational resilience.

US: Sound Practices to Strengthen Operational Resilience

The US agencies state that this paper does not introduce new rules but clarifies existing ones for the benefit of the largest and most complex banks, and focuses on safety and soundness and market stability (as per the PRA in the UK). Firms, however, see new expectations creeping in. The US continues to drive the agenda through supervision more than policy-making.

Scope

'Operational resilience is the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.'

Principles are aimed at: individual national banks, state member banks, state non-member banks, savings associations, U.S. bank holding companies, and savings and loan holding companies that have average total consolidated assets greater than or equal to (a) $250 billion or (b) $100 billion and have $75 billion or more in average cross-jurisdictional activity, average weighted short-term wholesale funding, average nonbank assets, or average off-balance sheet exposure.

Key themes

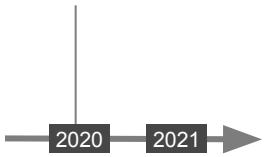
7 principles are outlined in the paper, namely:

- Governance
- Operational risk management
- Business continuity management
- Third party risk management
- scenario analysis
- secure and resilient information system management
- surveillance and reporting
- ...plus an annex on 'Sound practices for cyber risk management'

Note, the paper excludes principles on mapping or incident mgt like BCBS

Timeline

30-Oct
Joint agencies' paper published



No fixed date for future publications but they have signalled that firms can expect to hear more on the subject. They state:

'continued dialogue with the public will allow the agencies to further refine their approach to support the operational resilience of firms'.

Points of interest

- The sound practices are drawn from existing regulations, guidance, and statements as well as common industry standards that address operational risk management, business continuity management, third-party risk management, cybersecurity risk management, and recovery and resolution planning. The sound practices do not amend, expand, or alter the agencies' existing regulations or guidance.
- They focus on critical operations (which could affect the financial stability of the US) and core business lines (which could lead to a material loss of revenue, profit or franchise value) which aligns with US RRP work, and is wider in scope than the UK's 'important business services' (but aligns with UK plans to expand scope of Operational Continuity in Resolution regime).
- Mapping (of operations) is required in the context of running scenario analysis.
- Firms should set a 'tolerance for disruption' (at a firm level) in line with risk appetite.
- Ultimately firms should be able to maintain a globally consistent approach which aligns UK and US views by rolling up IBS and impact tolerances (UK) to critical operations and (firmwide) tolerance for disruption (US view).
- It mandates the existence of an alternative site to execute critical operations and core business lines with its own risk profile, as well as remote working arrangements, and the use of backup roles for personnel to help recover from disruption.
- Expectation that firms have processes to manage disruption to public and critical infrastructure (e.g. energy and telecomms.) to enable it to stay within its tolerance for disruption. In UK, these may be the type of breaches where it may be accepted that firms breach their impact tolerances, at least in the short term.

Europe: Digital Operational Resilience Act (DORA)

A focus on managing ICT risks, sharing threat intelligence, reporting ICT-related incidents and the management and oversight of ICT third parties. There is a lot of detail to be worked through in discussions between the European Commission and Member States. The timeline for implementation will be long when considering details to be set out in Technical Standards.

Scope

'Digital operational resilience means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality.'

The regulation will apply to an estimated 22,000 firms and forms part of a wider European Digital Finance package as well as linking with European measures on cybersecurity and the European strategy for data. Given the strong connection to existing guidelines from the EBA[1] on outsourcing and ICT and security risk management, we see DORA as a more significant change for firms within ESMA or EIOPA supervision as their own programmes of work have been slower to progress.

Key requirements

The Act proposes to improve the robustness of the following areas:

- Governance (of ICT risks)
- ICT risk management
- ICT-related incident reporting
- Digital operational resilience testing
- Information sharing
- ICT third-party risk management

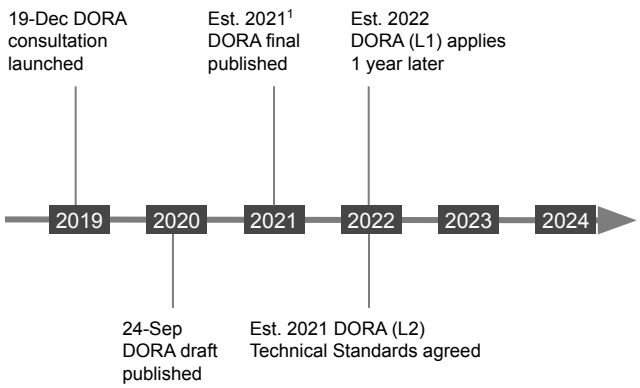
New rules cover all financial entities ('firms') but they will be tailored, to some extent, to be proportionate to the specific size and risk profile of the firm.

Points of interest

We understand the main areas of discussion between Member States include:

1. The principle of proportionality – the proposed tiering between 'microenterprises' and all others does not seem to offer a proportionate solution for many firms.
2. The designation of, and oversight framework for, critical third party providers (TPP)
3. Areas of interaction with other rules and guidelines (e.g. NIS Directive, PSD2)
4. Simplification of reporting requirements given overlap with existing regimes
5. The level of prescribed detail in telling firms *how* to meet the requirements
6. The focus on entity-level requirements rather than group-level
7. Roles and responsibilities of ESAs and National Competent Authorities

Timeline



Beyond the (Level 1) regulation, more detail will come via (Level 2) Technical Standards.

Draft Technical Standards due **1 yr later**:

- ICT risk management tools, methods, processes and policies
- Classification of incidents
- Reporting content and templates
- ICT Third Party Register of Information
- Assessment of sub-contracting
- For critical ICT TPP, designation of the members of joint examination teams from relevant competent authorities
- Conditions enabling oversight of critical ICT Third Parties

Draft Technical Standards due **3 yrs later**:

- Centralisation of reporting through single EU Hub
- Advanced testing

[1] European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA). Together they are referred to as the European Supervisory Authorities (ESAs).

[2] Estimate based on an acceleration of the standard 18 months finalisation period, given public messaging on the importance of this Act

EU DORA: Brief summary for financial services firms

EBA firms will see a lot of similarity with existing guidelines on outsourcing and ICT and security risk management. Below we set out a brief summary of what is captured in the key articles.

ICT governance and organisation (Article. 4)

Sets out the role of the management body including their final responsibility for managing ICT risks, setting clear roles and responsibilities for ICT–related functions, and determining the appropriate risk tolerance level of ICT risk.

1

ICT risk management (Art. 5 – 14)

Sets out the requirement for an ICT risk management framework, including a digital resilience strategy. The framework should include: risk tolerance levels for ICT risk and the impact tolerance of ICT disruptions; holistic ICT multi-vendor strategy at entity level (where this exists) showing key dependencies; and implementation of operational resilience testing).

2

ICT-related incident management and reporting (Art. 15 – 20)

On top of the basic need for a process there is a requirement around classification of ICT-related incidents (based on published criteria) with major ICT-related incidents requiring an initial notification (same day), intermediate report (within a week), and a final report. The European Supervisory Authorities (ESAs) will publish standard forms, templates and procedures to harmonise reporting. The ESAs will also explore the use of a single EU Hub for major ICT-related incident reports.

3

Digital operational resilience testing (Art. 21 – 24)

Requires a risk-based approach to testing, undertaken by independent parties. All critical ICT systems and applications must be tested at least yearly. ESAs will identify 'significant financial entities' which will be expected to do advanced testing using Threat Led Penetration Testing at least every 3 years.

4

ICT third-party risk management (Art. 25 – 27)

Proportionate management of ICT third-party risk based on scale, complexity and important of ICT-related dependencies and risks arising from contractual arrangements. Register of Information must be kept in relation to all contractual arrangements provided by ICT third-party providers. Firms must report at least yearly to regulators with information relating to new arrangements of ICT services.

There are circumstances given for when firms are expected to terminate contractual arrangements. Exit strategies/plans should be in place. There are minimum contractual provisions set out for all ICT services. Analysis of potential concentration risk including through sub-outsourcing, notably when using providers in a third country. Voluntary use of standard contractual clauses developed by the Commission for cloud computing.

5

Information sharing (Art. 40)

Expects that firms notify competent authorities where they participant in arrangements to exchange cyber threat information and intelligence within trusted communities and in a way that protects the sensitive information.

6

EU DORA: Implications for ICT third-party providers

The European paper is unique in introducing specific requirements for non-financial services firms, namely for ICT third-party providers. Here we summarise the expectations as currently drafted.

All ICT Third party providers – Key contractual provisions

- The full contract, including the services level agreements, to be documented in one written document (this may well need to be amended for practical reasons).
- Expected minimum contractual provisions largely align with EBA guidelines for critical outsourcing arrangements but include new elements such as the obligation of the ICT third-party service provider to provide assistance in case of an ICT incident at no additional cost or at a cost that is determined ex-ante.
- Firms and ICT Third parties are expected to consider using (voluntary) standard contractual clauses developed for specific services.

Critical ICT Third party providers only – Supervisory oversight framework

Designation (Article 28)

ICT third-party service providers (TPP) will be deemed critical based on the following criteria:

- Systemic impact in event of large scale operational failure by TPP
- No. of Global/Other Systemically Important Institutions relying on the TPP and their interdependence
- Concentration risk on the same TPP
- Degree of substitutability
- No. of Member States where TPP provides services
- No. of Member States where firms using TPP are operating

TPP should be able to voluntarily opt-in to the Oversight Framework.

Critical TPP will be charged a fee to cover Oversight costs, proportionate to their turnover.

Oversight assessment (Art. 30)

Assessment of whether critical TPP has in place comprehensive, sound and effective rules, procedures, mechanisms and arrangements to manage the ICT risks which it may pose to firms. Assessment to include:

- Ability to ensure security, availability, continuity, scalability and quality of services as well as ability to maintain standards of security, confidentiality and integrity of data
- Risk management processes
- Governance arrangements
- Mechanisms to ensure effective exercise of termination rights (e.g. portability of data/ applications)
- Testing of ICT systems, infrastructure and controls

Powers of the Lead Overseer (Art. 31 – 35)

- Request all relevant information and documentation
- Conduct general investigations and inspections
- Request reports after completion of Oversight activities specifying actions which have been taken
- Address recommendations on, for example, the use of conditions and terms to minimise possible systemic impact
- Impost a periodic penalty payment[1] to compel the critical TPP to cooperate as above.
- Termination of contractual arrangements with relevant firms if critical TPP opposes an inspection

This fits within a Union Oversight Framework with one ESA being designated as Lead Overseer and a new Oversight Forum

[1] Penalty payment to be imposed on a daily basis until compliance is achieved and for no more than six months following notification to the critical ICT TPP. Amount shall be 1% of the average daily worldwide turnover of the critical ICT TP in preceding business year.

Adam Stage
Regulatory Lead, Operational Resilience,

T: +44 (0) 7483 422845
E: adam.stage@pwc.com