Operational resilience

Current changes in the supervisory landscape and how banks can benefit

SSM beyond COVID-19 series

September 2020

home.kpmg/be/banking

Contents

Introduction

Since the financial crisis of 2008 the ECB and other supervisors have understandably focused on improving banks' financial resilience. Over time however, banks' growing complexity, interconnections and exposure to external events have made them increasingly vulnerable to operational disruption.

In response, operational resilience has climbed the agendas of supervisors and regulators. For instance, in the EU, individual components of operational resilience are addressed via dedicated guidelines from the EBA and The Basel Committee.

At the same time, COVID-19 is putting banks' operational resilience to the test and stimulating debate over new supervisory or regulatory requirements. The pandemic is putting customer needs and new collaboration models into the spotlight, and may yet bring further changes or disruption.

It follows that banks must thoroughly assess their ability to respond to disruption, close any gaps and strengthen their overall operational resilience. In this publication we define operational resilience and set out how to implement an efficient, effective framework by asking:

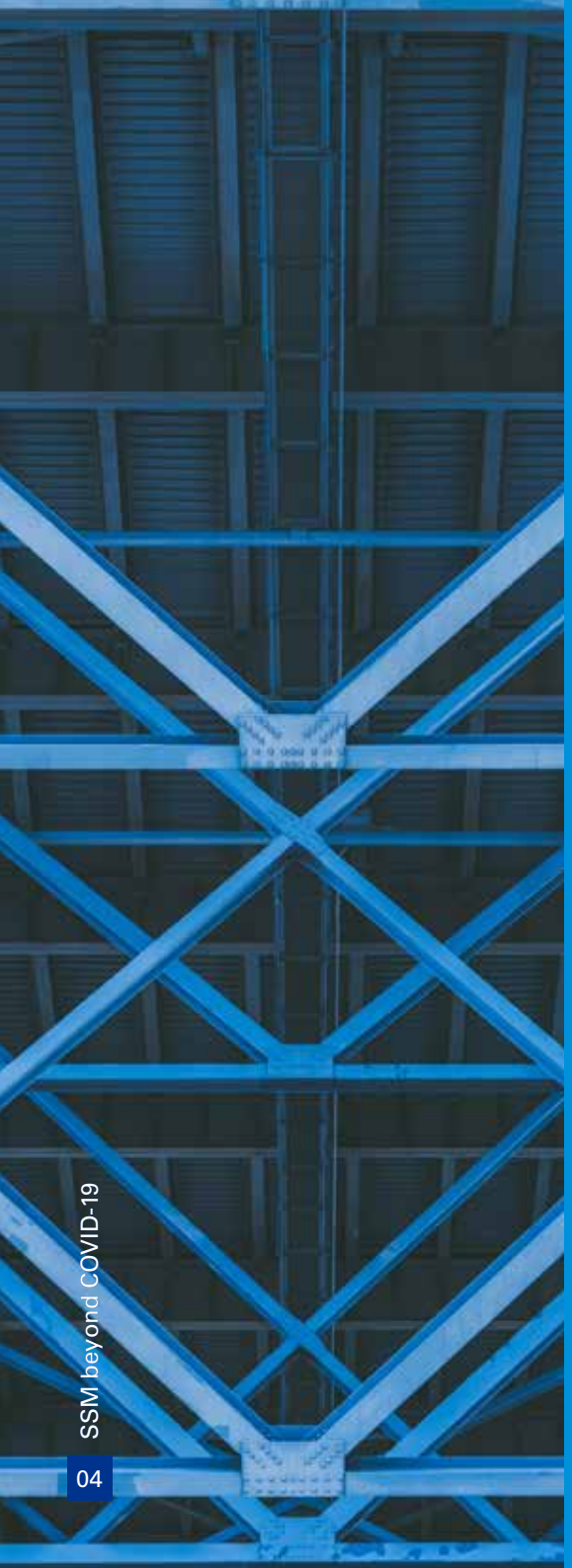
1. What is operational resilience and why is it more important than ever?
2. How has the supervisor viewed the topic to date and what is the outlook?
3. How can operational resilience be achieved?
4. How can banks benefit from strengthening their operational resilience?

"The Committee defines operational resilience as 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."

BCBS, Consultative Document "Principles for operational resilience", August 2020

"Supervised entities are expected to review their business continuity plans and consider what actions can be taken to enhance preparedness to minimise the potential adverse effects of the spread of COVID-19. In particular, banks could be challenged in their operational capabilities in affected areas [...]. Challenges could also arise due to constraints of key third party outsourcers and suppliers to maintain critical processes."

ECB Banking Supervision, Letter to all Significant Institutions: Contingency preparedness in the context of COVID-19, March 2020



The need for operational resilience

Vulnerabilities caused by the changing environment

The COVID-19 pandemic may be exceptional, but it shows how unforeseen events can change banks' operating environment and expose their vulnerabilities. The last few years have seen a steady increase in the number and unpredictability of threats to banks' financial and operational stability. If COVID-19 teaches us anything, it is to expect the unexpected.

Events with the potential to heavily disrupt banks' operating models include increasingly sophisticated cyber-attacks throughout the supply chain, Brexit, the launch of Libra or central bank digital currencies, and more frequent and violent natural disasters.

A multitude of potential threats to operational stability

New technologies and related implementation risks, third-party failures, IT outages, cyber-attacks

Banks increasingly rely on technology and that of third parties. Failures can significantly harm their ability to operate.

Climate-change and related natural disasters such as extreme heat, fire, floods

Climate-change can impact banks' operations from both direct physical risks, such as power interruptions due to natural disasters, and indirect effects like changing customer needs or regulatory pressure.

Political instability and related risks such as trade wars, protectionism, terrorism

Brexit, trade wars, and other geopolitical events could all threaten banks' operating models, for example through the loss of operating licences in certain jurisdictions.

Business model evolution due to new products, markets and participants, ultra-low interest rates and other factors

Changing business models means changing services - and their underlying resources. This can lead to skill shortages, for example those needed to meet altered customer expectations.

A new approach to operational resilience is needed

Most banks' operations performed well during the acute phase of the COVID-19 crisis. Even so, the pandemic still held up a mirror to institutions' resilience under pressure. Faced with an increased threat landscape, banks need to accept that it's impractical – and too costly - to prevent all disruption. Instead, their whole organisations should be ready to limit, respond to, recover and learn from a wide variety of events.

This means investing in operational resilience. The following table summarises our view of a sustainable operational resilience framework:

What does operational resilience need to offer?

Operational resilience is the ability to deliver critical operations in the face of disruption. It allows organisations to absorb internal and external shocks, ensuring the continuity of critical operations by protecting key processes and resources such as systems, data, people and property.

To achieve this, an effective framework for operational resilience needs to be:

Enterprise-wide
Moving away from siloed functions to develop an end-to-end view, driven by customer needs and linked to banks' goals

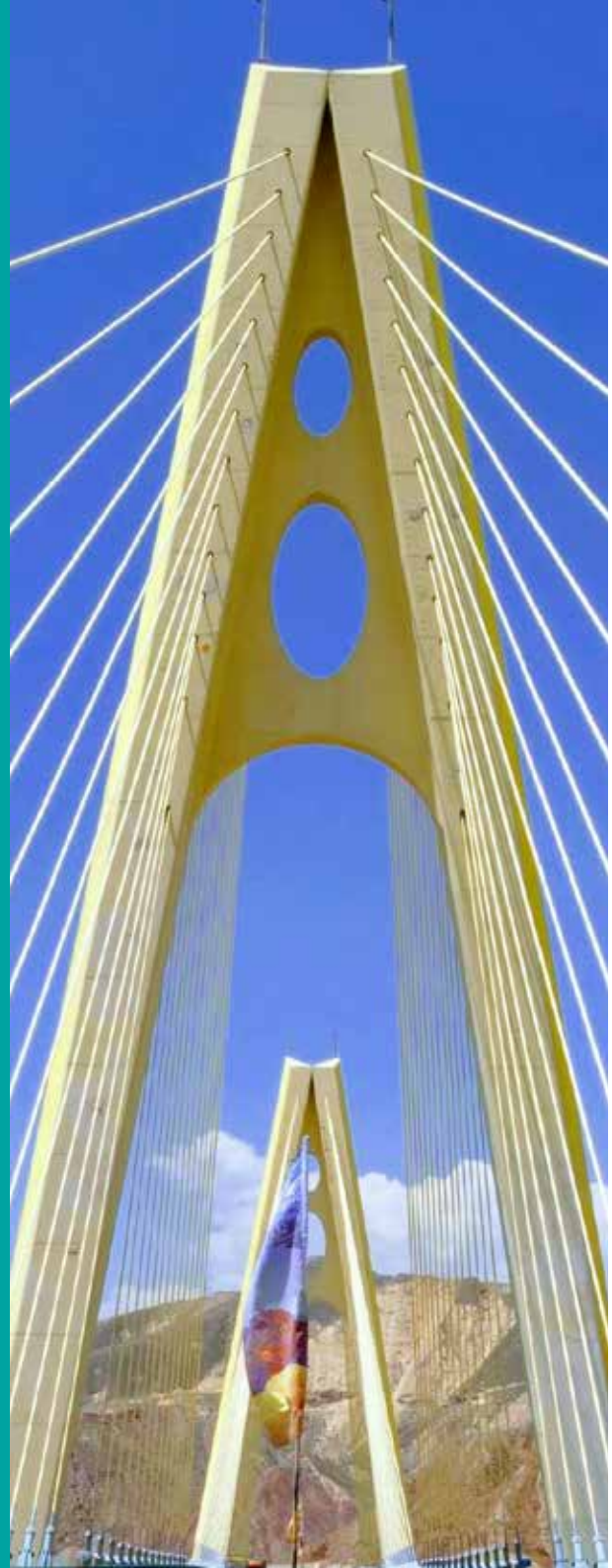
Measurable
Putting operational resilience on the same footing as financial resilience, with specific and quantifiable KPIs, thresholds, stress-tests and reporting

Flexible
Enabling the bank to react appropriately to unknown situations and adapt to changing circumstances, instead of following rigid action plans

Top-down
Integrating operational resilience into overall bank management, starting at the top with adequate attention from senior management

Faced with creating such an operational resilience framework – and integrating it with existing functions – banks can learn from their experience of strengthening financial resilience after the crisis of 2008. As well as enhancing financial risk management through monitoring and stress-testing, this involved a structural program to build recovery and resolution planning into day-to-day management. Institutions can use a similar approach to build the key elements of an effective operational resilience framework:

- Overarching crisis governance including clear roles and responsibilities among senior management, well-defined escalation mechanisms based on measurable indicators, and an effective reporting framework.
- Identifying and prioritising important business functions, their underlying operational resources and key interconnections and interdependencies.
- Promoting enterprise-wide cooperation and strengthening existing interfaces and communication channels, for example through creating playbooks and performing dry runs.
- Creating recovery and communication strategies to deal with severe disruptions, and performing paper-based and live scenario exercises that put each element – and their interplay – to the test.



Supervision and regulation in the light of the changing environment

While EU supervision already covers single aspects of operational stability…

The ECB already expects banks to meet a range of requirements relating to operational continuity. The ECB's assessments have increasingly emphasised the importance of banks' operational stability, and several EU regulations cover individual aspects of resilience such as ICT, security risk management and outsourcing arrangements. Cyber resilience was also named as a topic of focus for the 2020 SREP, following the publication of oversight expectations for FMIs[1] and statements in interviews[2]. In addition, concerns regarding banks' resilience to climate-change risks were expressed[3] in 2019.

Following the outbreak of COVID-19, it has become increasingly clear to the ECB that operational resilience can be threatened by banks' reliance on third parties and suppliers to deliver critical processes[4]. The ECB has also expressed concern about systemic risks during a crisis, given the need for banks to support distressed businesses while maintaining their own operational capacity[5]. As part of its response to COVID-19, the ECB has requested banks to report various metrics relating to their operational capabilities – a further sign of increased supervisory interest in resilience.

The EU's regulatory and supervisory authorities have expressed concerns over the operational stability of financial institutions in the past. Drawing lessons from the COVID-19 pandemic, we expect the emphasis to shift from individual aspects of operational continuity towards an overarching operational resilience framework.

1: "Cyber Resilience Oversight expectations for FMIs" – December 2018
2: "Cyber Resilience – Objectives and tools" - Interview Sabine Lautenschläger, March 2018
3: "Resilience to climate-change risk" - Interview with Frank Elderson, Member of the Supervisory Board of the ECB, Supervision Newsletter, May 2019
4: "Contingency preparedness in the context of COVID-19" - Letter to all SSM institutes, March 2020
5: "Operational capacity to deal with distressed debtors in the context of the coronavirus (COVID-19) pandemic" – Letter to all SSM institutes, July 2020

… here is a worldwide trend towards holistic operational resilience frameworks

Supervisors, regulators and standard-setters around the world are increasingly focused on the importance of overarching operational resilience frameworks. New requirements are being drafted and consulted on. These new approaches are highlighting some areas that banks have previously tended to neglect.

While cyber resilience, IT infrastructure and outsourcing clearly play an important role, authorities have realised that a broader approach to operational resilience - incorporating equally important components such as processes and people - is needed. This makes it critical to have transparency over banks' operating models, including the resources that support important business functions.

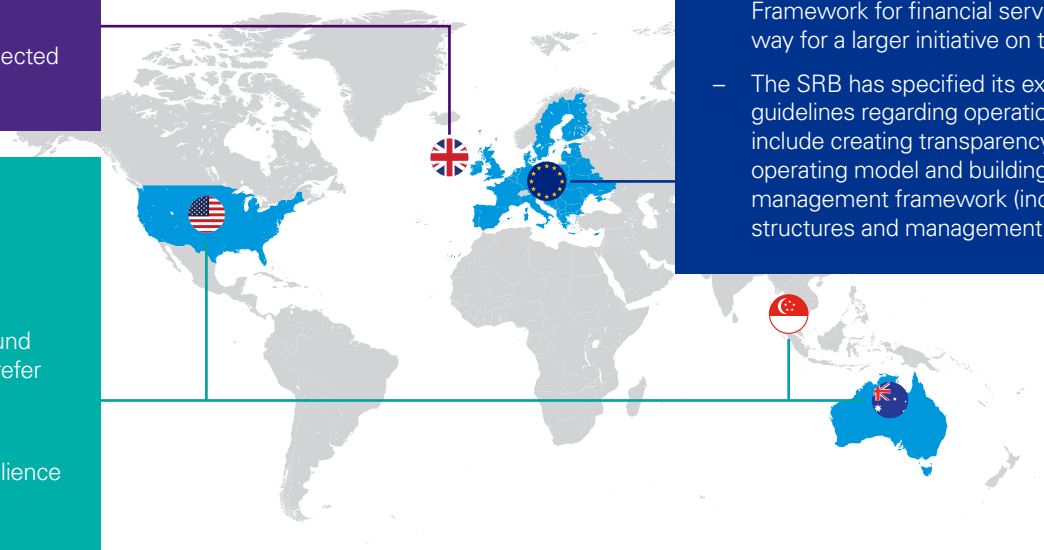
In addition, new regulations highlight the importance of identifying severe but plausible tailored scenarios, and of performing stress-tests to reveal weaknesses in operating models. In the UK in particular, the authorities emphasise the importance of consumer protection during periods of disruption. They also require banks to set impact tolerance and metrics must be defined to monitor and measure the firm's ability to remain within the tolerance.

United Kingdom (UK)

- Joint campaign of BoE, PRA and FCA to strengthen operational resilience started in July 2018
- Implementation of the rules by banks expected in mid-2021

International

- The BCBS published the consultative document "Principles for operational resilience" in August 2020 together with the "revisions to the principles for the sound management of operational risk", which refer to one another
- Other countries such as Singapore and Australia have already put operational resilience in the spotlight and issued first rules or guidance



European Union (EU)

- The European Commission recently concluded its consultation on "Digital Operational Resilience Framework for financial services", potentially paving a way for a larger initiative on the topic
- The SRB has specified its expectations, and its guidelines regarding operational continuity in resolution include creating transparency regarding the overall operating model and building a comprehensive crisis management framework (including governance structures and management information systems)

Achieving operational resilience

Five action items to build operational resilience

Banks seeking to achieve operational resilience need to develop enterprise-wide frameworks that allow them to respond flexibly to unexpected disruption. We propose five action items that will allow banks to meet this goal, while also fulfilling future supervisory expectations.

1

Set the stage

- Create an operational resilience strategy
- Assign roles and responsibilities from the top down
- Break up siloed functions

2

Take stock

- Identify critical operations
- Map resources and identify interdependencies
- Identify vulnerabilities

3

Know your limits

- Define indicators
- Define thresholds aligned with risk appetite
- Consolidate and harmonise reporting

4

Prepare for reaction

- Develop inventory of contingency measures and related preparatory steps
- Adapt business continuity plans and incident management
- Execute business continuity plans and stress-testing

5

Roll out

- Implement the operational resilience framework
- Promote an operational resilience culture
- Learn and improve continuously

1 Set the stage

Create an operational resilience strategy

Senior managers must define the strategic goals for setting up and running the operational resilience framework. This should include the business objectives to be protected and the risk appetite. The strategy should also set the primary goals for the operational resilience programme, including which operations should be prioritised during crisis management, and taking relevant stakeholders into account. The strategy should be integrated into the broader planning process and aligned with the business strategy and operational risk management.

Assign roles and responsibilities from the top down

For an operational resilience framework to be effective, banks need to define clear enterprise-wide roles and responsibilities. Active board involvement is key to integrating operational resilience into the bank's business and risk strategies, and to setting the tone at the top. One board member should take direct responsibility for ensuring the bank's operational resilience efforts are suitably resourced. We also recommend appointing a Head of Operational Resilience at senior management level, responsible for implementing the operational resilience strategy.

Break up siloed functions

Operational resilience can only be achieved through the joint efforts of many functions such as Business Continuity Planning (BCP), Internal Control Systems, Cyber and Information Security and Recovery & Resolution Planning. Open communication, effective information sharing and the clear division of tasks are key to developing resilience against a wide variety of threats. Creating an enterprise-wide understanding of operational resilience is essential. This includes the definition of an operational resilience target model, the elimination of redundancies, and clear lines of communication.

2 Take stock

Identify critical operations

A bank is operationally resilient when it can reliably provide its critical operations in the face of disruption. So it is paramount to identify critical operations based on clear criteria, such as the impact of disruption on the bank's viability, financial stability or customers. As part of this process, banks should consider and align the critical functions and core business lines set by RRP[1], BCP's "critical business functions", outsourcing's "critical/important functions" and other common definitions. Once the criteria are defined and approved, a complete inventory of the critical operations in their entirety must be made.

Map resources and identify interdependencies

To ensure transparency, all internal and external resources required to maintain critical operations should be identified, mapped, and documented in the inventory of critical operations. Resources can include people, technologies, systems, processes, information, data, facilities and external services. Most critical operations will share some common resources with other functions or operations. This web of internal and external connections and interdependencies must be clearly documented in the inventory.

Identify vulnerabilities

A clear view of critical operations, their resources and their interdependencies creates transparency. It also allows for a complete identification of operating models' vulnerabilities, and of the potential triggers for disruption. The inventory of critical operations should highlight these vulnerabilities and risk drivers, allowing targeted improvements to be planned.

1: Recovery and Resolution Planning

3 Know your limits

Define indicators

For each critical operation, indicators should be defined that provide an effective early warning signal along the entire value chain. Existing indicators should be reviewed and assessed for usability in regular monitoring and reporting. The indicators should cover the critical operations themselves, their key resources, and any interdependencies. They should address the identified vulnerabilities and be documented in the critical operations inventory.

Define thresholds aligned with risk appetite

To enable a timely response before the disruption of a critical operation exceeds the tolerated level, indicator thresholds should be set up and calibrated. Setting disruption tolerances and response thresholds is a responsibility for the board. At a minimum, banks will want to maintain their viability. However, future requirements for financial stability and consumer protection should also be anticipated. Thresholds need to be aligned with risk appetites.

Consolidate and harmonise reporting

An appropriate reporting framework is essential if boards are to maintain oversight of operational resilience. Existing reporting of relevant functions should be harnessed where possible, augmented to provide an accurate picture of the status of critical operations. Reports must be addressed to senior management up to the board of directors, aligned with existing risk reporting and taking defined roles and responsibilities into account. It is reasonable to assume that additional regulatory reporting will be required in the near future (cf. the ECB's COVID-19 reporting requirements).

4 Prepare for reaction

Develop inventory of contingency measures and related preparatory steps

Based on the vulnerabilities identified, a flexible scenario-independent toolkit of responses should be set up. Existing contingency measures should be reviewed and amended, with a focus on completeness, universality and flexibility. Banks should also assess how easy contingency measures will be to implement, and what preparatory steps may be required.

Adapt business continuity plans and incident management

To improve the likelihood of remaining within the thresholds and withstanding disruption, banks will need a comprehensive framework for incident management and business continuity planning. This should build on existing processes; define severe but plausible scenarios tailored to the institution; and develop business continuity, response and recovery plans using the response toolkit. Scenarios must not be too narrow and should cover a wide range of potential types of disruption. All plans should be highly flexible, so they can be adapted to the specific features of any actual crisis.

Execute business continuity plans and stress-testing

The inventory of measures and business continuity plans need to be thoroughly and regularly tested against the identified scenarios. This should include live tests as well as computer simulations. End-to-end tests involving all relevant functions and third parties will have the biggest learning effects. They should be used to refine measures and plans, and to define further preparatory steps. Reverse stress-testing can complement the exercise and may lead to a recalibration of the thresholds.

5 Roll out

Implement the operational resilience framework

Investment in people, organisations and technology will be needed to bring the operational resilience framework into force. Any vulnerabilities need to be addressed by replacing outdated or weak infrastructure, increasing system capacity and addressing key person dependencies. Employees need to be trained in their new roles, and policies, processes and management information systems must be set up. To help anchor the new roles in the mindset of employees, we recommend creating a guideline for operational resilience that explains the main objectives.

Promote an operational resilience culture

Embedding the framework in a bank's corporate and risk culture is essential to successfully achieving and maintaining operational resilience. Risk-conscious behaviour should be fostered by sensitising and training employees, and through published crisis management guidelines. Keeping employees updated about actual disruption and its effects will help staff to identify threats early, understand how to respond and who to report to. Creating a shared culture of openness and transparency in which people are encouraged to admit mistakes is key to the timely detection and management of potential disruption.

Learn and improve continuously

Banks must be able to constantly adapt to the ever-changing risk landscape. The suitability, effectiveness and efficiency of measures should be systematically and regularly reviewed. Banks must act where necessary to improve their prevention, response and recovery capabilities. In particular, the five action items outlined here should be repeated at least annually to keep the operational resilience framework aligned with banks' current business and risk profiles.

Benefits of operational resilience

As well as making banks more flexible and effective in their response to disruption, improved operational resilience can deliver other significant commercial benefits:

Make crisis responses faster and more effective

- Current siloed approaches create redundancies and can distort priorities in overall bank management. An overarching operational resilience framework enables better coordination, reducing the time and costs of responses.
- Preparing for a wide range of potential threats and identifying the interdependencies of critical operations makes it easier for banks to adapt and respond to unexpected events.

Enhance experiences, trust and loyalty for customers and investors

- Greater operational resilience naturally reduces the frequency of reputationally damaging disruption, in turn leading to increased customer satisfaction.
- Being viewed as operationally resilient by customers and investors alike offers a key competitive edge.

Foster innovation and a sustainable business model

- Innovation essential to remaining competitive and seizing potential business opportunities. However, innovation can increase operational complexity and the risk of disruption. Operational resilience helps firms to innovate safely and adapt to changes in the business environment.
- Strong innovative capabilities increase banks' resilience to changing market environments.

Leverage synergies and improve decision making

- Harmonising and aligning relevant functions and moving away from a siloed approach eliminates redundancies and reduces costs.
- Creating a common language and streamlining reporting improves transparency and enhances decision-making when selecting responses.

Increase adaptability to changing regulation

- Regulatory scrutiny has increased year-on-year, and the direction of travel through the COVID-19 crisis will remain on an upward trend.
- An operationally resilient organisation has the flexibility to react easily and adapt to changing regulatory requirements.

Allocate resources more effectively and efficiently

- Developing a detailed understanding of critical services and the resources they require can help to improve day-to-day delivery, and to enhance any restructuring activities.
- Prioritising investment decisions around the continuity of key business services can help to reduce costs.

How KPMG can help

The KPMG network brings together subject matter experts that cover all aspects of operational resilience. We can leverage synergies to meet your exact business needs and help save costs. With our international best practices and our experience with supervisors and regulators we provide future-proof solutions.

What is needed?

Understand your organisation

The organisation's operations, their vulnerabilities and the existing functions ensuring the operational continuity of the bank have to be well understood to specify the need for action. Therefore, a maturity assessment needs to performed, identifying existing weak points and gaps compared to the new regulations on operational resilience.

Define your bank's specific target operating model

Based on the results of the maturity assessment, a target model has to be derived that fits the needs and nature of the firm. While stronger operational resilience provides many benefits, operational resilience is resource intensive and requires cultural and organisational change. Therefore, it is important for banks to find their optimal level of operational resilience balancing costs and benefits.

Set-up a strategic work programme

For the implementation of the target model, banks should build future-proof solutions leveraging existing synergies to avoid unnecessary costs. Therefore, banks should set-up a forward-looking multi-year project plan aligned with existing transformation efforts and taking into account strategic business directions.

Throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International

KPMG's added value

With a global team of industry experts, KPMG can help analyse your organisation's operations and control functions to gain insights into what has already been achieved and to identify your need for action.

With subject matter experts covering all aspects of operational resilience, such as business continuity management, cyber, IT and operational risk as well as recovery and resolution planning, KPMG can help to support developing a target model tailored to your organisation's business needs across all lines of defence.

KPMG can evaluate your readiness by performing a maturity assessment. This is based on KPMG's continuous tracking of regulatory developments, a profound knowledge of the interpretation of regulatory requirements and their interplay in the overall context.

KPMG's long-standing project management experience improves project efficiency. In the process of preparing a roadmap to an enterprise-wide, flexible, measurable and top-down target operational resilience framework, KPMG can identify potential quick wins.

Our KPMG professionals support the implementation of operational resilience along the five action items. KPMG has vast experience in building the organisational conditions, ncluding the establishment of clear responsibilities on all levels, breaking down silos in the control framework, and strengthening leadership to further develop skills and culture.

KPMG has gained hands-on experience and can look back at a large number of credentials. KPMG's ECB Office and European network enable a holistic European view and can provide insights on how other institutions deal with the challenge of operational resilience by means of best practice.

Contacts

To discuss the issues raised in this report, please contact:

Koen De Loose
Head of Banking & Capital Markets
KPMG in Belgium
T: +32 2 708 43 17
E: kdeloose@kpmg.com

Dr. Henning Dankenbring
Partner, Co-Head KPMG ECB Office
EMA Region
T: +49 69 9587 3535
E: hdankenbring@kpmg.com

Francisco Uria Fernandez
EMA Head of Financial Services and Banking & Capital Markets
KPMG in Spain
T: +34 9145 13067
E: furia@kpmg.es

Olivier Macq
Head of Financial Services
KPMG in Belgium
T: +32 2 708 36 86
E: omacq@kpmg.com

Michael Meyer
Partner
KPMG in Germany
T: +49 89 9282 1494
E: mmeyer5@kpmg.com

kpmg.com/ecb

Designed by CREATE | CRT127868