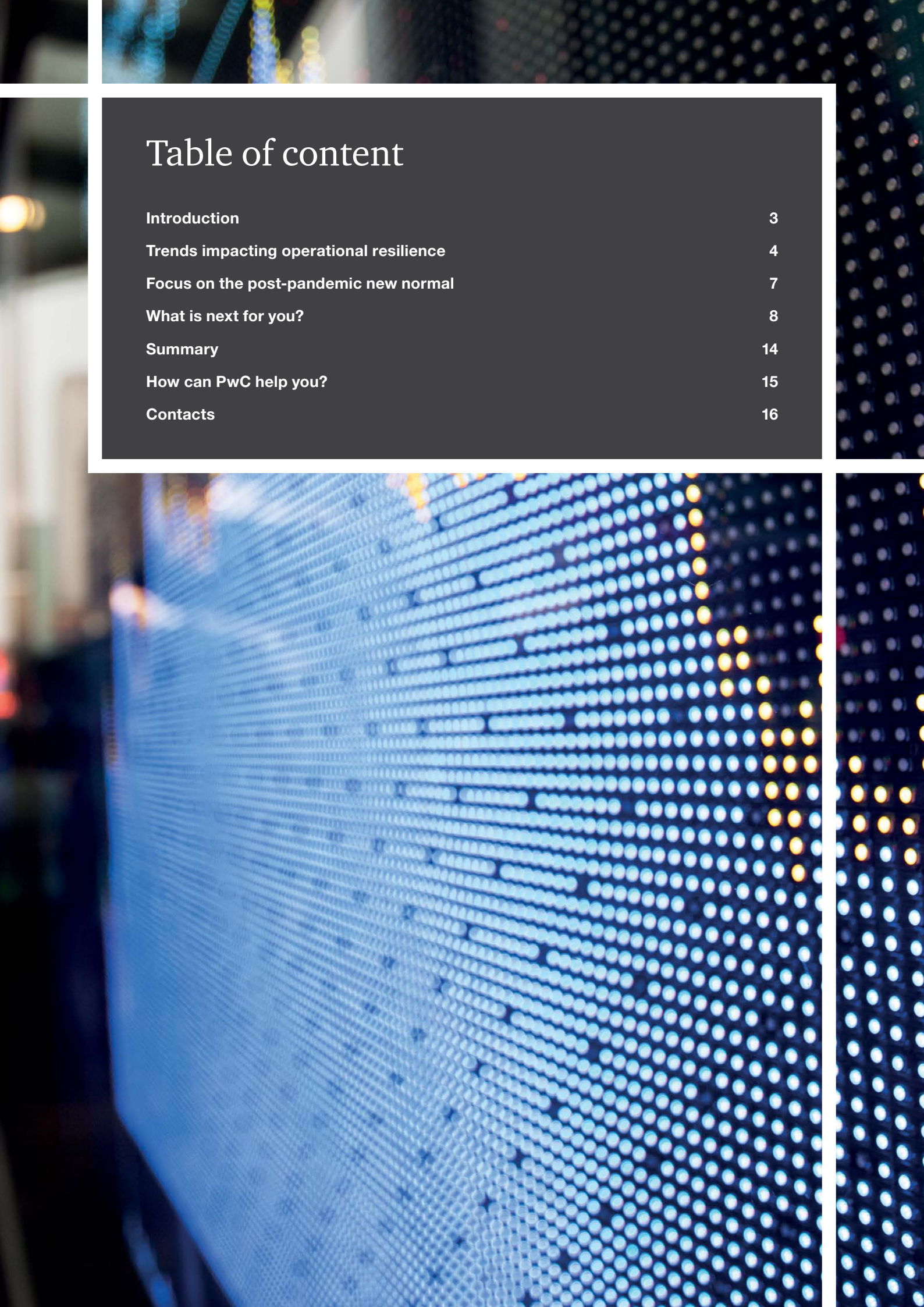
Boosting your operational resilience for the new normal

pwc

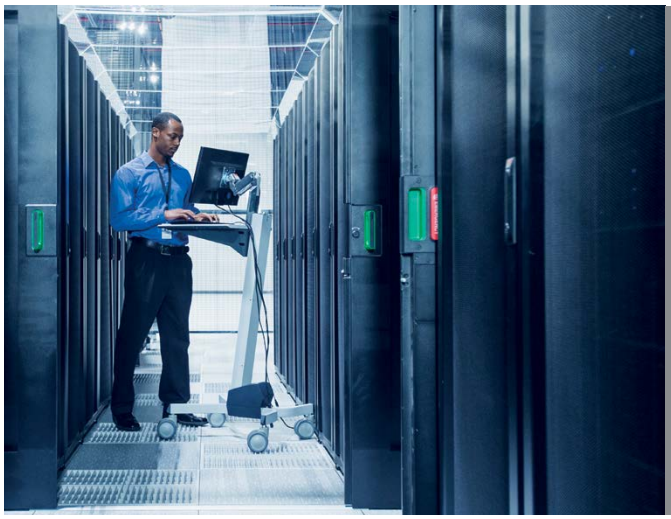
www.pwc.ch

Table of content



Introduction

Operational resilience has increasingly been a focus area for the financial services industry over the past several years. Reasons for this include high-profile cyber security incidents, the global pandemic and even macroeconomic uncertainties as recently seen with the Russian invasion of Ukraine. Financial institutions had to quickly scale up their abilities to react and withstand unexpected internal failures and external disturbances, as well as adapt their risk appetite and service model to the changing landscape, learning from their experience to minimise the downtime of services.



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

Definition according to Basel Committee on Banking Supervision (BCBS)

Operational resilience quick check – How is your company impacted?

1.	Have you or will you introduce digital services due to the pandemic or competition?	☐ Yes	☐ No
2.	Have you experienced challenges when including remote working in your operating model?	☐ Yes	☐ No
3.	Do you give consideration to the geographical risk exposure of your operations? On different levels (e.g. exposure within countries and its regions)?	☐ Yes	☐ No
4.	Have you or will you move some services to the cloud?	☐ Yes	☐ No
5.	Have you assessed your operational resilience maturity?	☐ Yes	☐ No
6.	Do you know how you would be impacted by the latest FINMA (e.g. RS08/21) or EU regulations (e.g. DORA) around operational resilience?	☐ Yes	☐ No
7.	Do you have a designated operational resilience officer?	☐ Yes	☐ No

Trends impacting operational resilience

The global pandemic has rapidly shifted the momentum for operational resilience in financial institutions. Emerging or growing trends are challenging financial institutions to elevate their traditional operational resilience framework to a more strategic and holistic approach:

1. **Client's shift towards digital channels, products and services**
2. **New ways of working and agility**
3. **Multiplication of third parties' involvement**
4. **Increased regulatory focus**

1. Client's shift towards digital channels, products and services

One of the most profound changes due to the pandemic is the accelerated shift in client expectations. Although customers have been drawn towards digital channels and the adoption of new technologies in the last few years, the global pandemic accelerated this trend massively. On the one hand, customers were forced to use only digital channels for their professional and personal needs. On the other hand, new platforms ranging from e-commerce to subscription-based digital services generated a huge influx of new users who became accustomed to the client-centric approach of these businesses.

As a result, financial institutions are pressured to enhance their service offerings with new technologies to enable client-centric capabilities. In terms of operational resilience, many financial institutions face uncharted territory, as legacy systems are still widely used in the financial industry. Client-centric capabilities demand a better understanding of data management and a higher dependency on new technologies including their third-party providers. Nonetheless, delaying the digital transformation is no option, as BigTech and FinTech companies are pushing into the financial sector providing the level of customer-centricity to which customers have become accustomed.

2. New ways of working and agility

Due to the global pandemic, most employees became accustomed to working from home and demand the flexibility to do so in the future. As remote working is increasing, agile ways of working are being adopted in parallel across the financial industry. Cross-functional teams become the norm as business agility is being introduced into the workforce to support the focus on outcomes and products over outputs and projects.

Consequently, a cross-functional team setup and a flexible way of working demand a higher network capacity and increase the dependency upon new productivity tools. In terms of infrastructure, most financial institutions move to the cloud to benefit from the increased flexibility of on-demand cloud network capacity and to decentralise their infrastructure. Decentralised teams and infrastructures also contribute towards exacerbating underlying tensions, especially in environments where agile is limited to specific functions that are not fully aligned with the company structure. Furthermore, the distribution of the workforce and exposure of data centres across geographies expose financial institutions to new risks that need to be considered in terms of resilience.

To be sustainable, these new operating models need a better understanding and monitoring of related cyber-risks as well as political, geographical and societal risks regarding the location of data centres and team members.

3. Multiplication of third parties' involvement

There is a growing trend for financial institutions to increase their service offerings by including services and products from external third-party service providers. Various financial institutions are bundling their services to offer customers an entire ecosystem of financial services including banking, insurance and brokerage services. As a result, financial institutions are increasingly seeking to outsource critical functions to a concentrated set of vendors to gain access to capabilities that are not readily available to the industry and to save costs. Increasing outsourcing makes it harder for institutions to quantify and manage their third-party risks.

As the number of third parties grows, there is also an increase in cyber-attack risks due to the vulnerability of third-party integrations and reliance on information security measures outside the financial institutions. So, careful monitoring and understanding of third-party providers plays a crucial role. Third parties need to be diligently reviewed before onboarding and must be monitored throughout the entire lifecycle of the relationship.

4. Increased regulatory focus

With the growing need for financial institutions to absorb operational risk-related events to remain financially resilient, regulators are increasingly considering operational resilience to be as equally significant as financial resilience.

Subsequently, they are focusing on operational resilience, drawn by the risk to customers, as well as the financial stability risks that operational outages can bring. Regulators are currently revising or introducing new regulations aiming to close the gap in terms of operational resilience. On the one hand, the European Union is introducing new regulations specifically for operational resilience under the new Digital Operational Resilience Act (DORA) planned for implementation in Q1 2023. On the other hand, FINMA is revising its circular RS08/21 on operational risks as well as the Federal Act on Data Protection (FADP) clarifying data processing and increasing the number of cyber reviews.

Being compliant and mitigating the risk of regulatory censure should be the minimum expectation for an operational resilience capability. To go further, having a robust, forward-looking operational resilience capability allows financial institutions to capitalise on a range of business benefits, as for example, evolving their services with confidence, making better board and investment decisions, and building customer trust. Leading financial institutions are proactively updating their operational resilience frameworks to ensure that they are prepared for all upcoming regulations in this area.

Focus on the post-pandemic new normal

1. Borders matter again

With the global pandemic, we saw the resurgence of the importance of local differences in terms of policies and cross-border travel limitations. On top of disruptions caused by the fact that it was impossible to visit affiliates, many companies faced challenges when trying to activate back-up infrastructure or organisation around the globe as initially designed. As an example, many back-up service centres in India failed to operate simultaneously with their main service centres in Switzerland. In hindsight, leveraging the different cantonal rules could have allowed for a more efficient solution in another Swiss canton. As geographical segregation becomes stronger, we see the need to rethink the organisation within individual countries and sometimes within individual regions.

2. Macroeconomic uncertainties are getting closer

On a similar note, macroeconomic uncertainties are also getting increasingly closer to Swiss financial institutions, as exemplified by the large-scale military assault of Russian forces on Ukraine, disrupting the peace in Europe. Millions of Ukrainians are fleeing in search of safety, leaving everything behind. At the same time, the fear of an expansion of the conflict to other countries is increasing, with potential consequences for the whole region. From an operational resilience perspective, Eastern Europe is a leading offshore delivery region for Swiss financial institutions with, for instance, Poland being a strong partner. In the short term, potential service disruptions and interruptions or even office closures can be expected, while in the long term, the risk of outsourcing to this region must be reassessed due to new threats. Additionally, the invasion also bears heavy consequences for Russia in the form of sanctions such as the SWIFT exclusion for certain banks and freezing of assets across the United States, the European Union and even Switzerland. As a result, Swiss financial institutions should consider if they have any ties to Russia or Belarus, as client relationships or payments from and to third-party service providers, for example, are directly impacted by international sanctions.

3. Crisis management's role is evolving

The role of crisis management will not disappear in the post-covid stabilisation phase - there will always be fires to fight as new problems arise. Having a dedicated crisis management team frees up senior leaders to focus on other critical areas of the business. If a crisis management unit was already in place before the pandemic, it is now a good time for an after-action review to adjust as needed. The global pandemic highlighted the fact that a crisis can keep going for an indefinite amount of time, requiring not only coping mechanisms to survive but also to continue operating the business sustainably. These new challenges introduce new crisis scenarios as well as new possible ways to foresee and respond to them. As preparation remains key, it is essential to keep comprehensive crisis management documentation up to date, including reviewed processes and solid crisis scenarios to test response mechanisms.

4. The workforce is developing new needs

With the strong penetration of remote working in the financial services industry, the most important part of an organisation, its people, have also faced tremendous changes in their ways of working. Although the workforce has gained mobility from a geographical perspective and has grown accustomed to this newfound flexibility, it comes with challenges. On the one hand, flexible working impacts the firm's culture, as dynamics are different when employees work on site, remotely or in a hybrid setup. Potential connection and know-how gaps can emerge requiring a broader reconsideration of recognition mechanisms and communication channels from a firm-wide perspective. On the other hand, training plans also need to be adapted to the new normal. Primarily, key topics like cyber awareness are gaining importance, requiring a fast and strong upskilling of the workforce. What is more, new ways to engage with the workforce and help awareness are also needed to establish a fine balance between training efficiency and the respect of remote working constraints.

What is next for you?

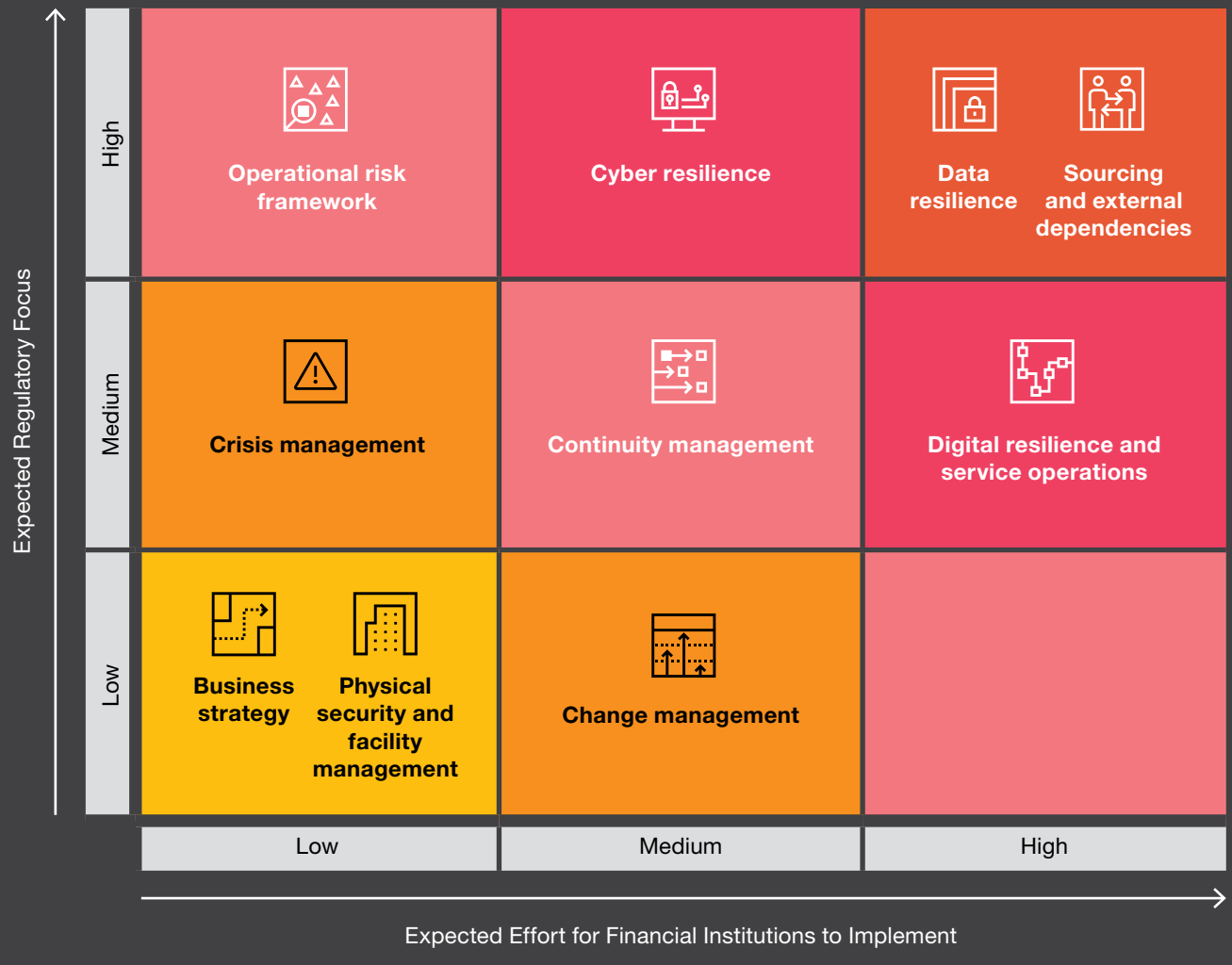
Overall, the global pandemic has triggered and accelerated trends which have an immense impact on the operational resilience of financial institutions. Leading financial institutions have already taken up the challenge to assess and improve their operational resilience capabilities. These institutions have recognised that operational resilience is not only about dealing with the problems of today, but rather a need to embed a culture of resilience across the company. This can be achieved by building bridges across different functions and adopting a cross-functional approach when dealing with operational resiliency.

Most financial institutions have an operational resilience framework in place due to the above-mentioned requirements. Nevertheless, in many cases the institution's operational resilience capabilities are underdeveloped and are not embedded into the culture. So, in many instances, gaps are not recognised until it is too late.

The graphic below highlights which building blocks have been identified as important focus areas for financial institutions to improve their operational resilience capabilities.

On the one hand, the expected regulatory focus was considered in terms of regulatory activities, like new and expected regulations within the European Union and Switzerland.

On the other hand, the expected effort for financial institutions was considered in terms of the resources and skills required to implement measures and strengthen their operational resilience capabilities, based on our experience with multiple Swiss-based financial institutions.



Based on the two parameters ‘expected regulatory focus’ and ‘expected effort for financial institutions to implement’, we have identified the following four building blocks[1] that need attention and should be tackled as a priority by financial institutions:

1. **Data resilience:** protect and leverage your data.
2. **Sourcing and external dependencies:** put third-party risk management at the centre of your ecosystem thinking.
3. **Cyber resilience:** anticipate adverse cyber events and develop detection, response and recovery capabilities to manage a cyber incident.
4. **Digital resilience and service operations:** build a sustainable competitive advantage with resilience embedded at the core of your operating model.

One of the main use cases where these building blocks have been observed in action is in the context of migrating to the cloud. Since operational resilience on the cloud, especially with an external service provider, will add another layer of complexity, financial institutions on the cloud or ones considering moving to the cloud should focus on the following building blocks: data resilience, sourcing and external dependencies, cyber resilience, and digital resilience and service operations.

Assessing the current arrangement of financial institutions and identifying the gaps will allow to deliver in the areas which require the most attention. These areas should be reviewed before starting any transformation work.

[1] Building blocks are defined according to the PwC Operational Resilience framework developed in our paper Operational Resilience – Your Swiss army knife to survive the next crisis. https://www.pwc.ch/en/publications/2019/operational-resilience_final_web-singles.pdf

1. Data resilience: protect and leverage your data

Most industries today are extremely data intensive. Ensuring the quality and availability of data is vital if you want to be resilient. Data resilience is also about knowing what data is critical to provide the key services and products to your client and establishing capabilities to maintain, protect and leverage data.

For years, the aim of financial institutions has been to collect as much data as possible. But due to enhanced regulations as well as maintaining costs, data has increasingly become a liability and a cost driver. Regulatory agencies such as FINMA have indeed started to focus on critical data as the 'crown jewels' of an organisation in recent years. As an example, several large Swiss financial institutions faced FINMA criticisms for failing to have a distinct definition of their critical data and a good understanding of their location. This clearly indicates a trend towards tighter regulatory requirements to improve data resilience, calling for financial institutions to act. It is nowadays crucial to understand what and where your critical data is and to have strong data governance in place that regularly analyses and monitors such critical data assets.

The first step to build data resilience is therefore to identify the required IT applications and data storage location (lakes, warehouses etc.), with a focus on critical data, and to establish relevant control mechanisms to maintain this understanding of data over time. By creating data inventories that feed into adaptive data models and data flows, financial institutions gain a holistic end-to-end view on the use of data across all functions.

By focusing on the journey of the data, institutions will not fall into the trap of only modernising applications without considering the interdependency between the different applications. This allows companies to identify the weakest links and increase data resilience across the whole organisation. In addition, having a clear view of critical data for the organisation allows resilience in terms of data protection, focusing on the quality, availability and confidentiality of data.

To ensure data resilience, a strengthened data governance structure is required that has a clear view on what data is collected for what purpose and in which application or storage unit. A clear definition of roles and responsibilities both from an IT and business perspective, and a definition of standards and processes from a firm-wide perspective are important success factors for integrating data resilience into the day-to-day job.

Lastly, IT applications generate rich data sets, but many financial institutions are challenged in leveraging this data for insights, discovery and capacity planning due to a lack of intelligent capabilities and tools. A clear data strategy and cohesive data governance structure (including a focus on critical data, as the 'crown jewels' of an organisation) would help optimise the cost of data: it would reduce data redundancy, thereby cutting storage and protection costs, but also allowing for increased data utilisation and monetisation. Data can indeed be leveraged to support decision-making and provide better reporting. For instance, by enhancing or enriching your data, advanced analytic tools can generate valuable insights such as customer behaviour patterns which can potentially be used to get accustomed to new client needs. A clear data structure is also the foundation of successful data migration or cloud adoption programs that could represent significant productivity gains for your organisation. As a result, the implementation of regulatory guidelines could be an ideal opportunity to create value far beyond regulatory compliance.

To better leverage your data, the following questions need to be answered:

1. Does your data governance provide a clear definition of your critical data? Is guidance provided on where this data must be stored (e.g. location)?
2. Do you have a well-established data governance structure aligned with the data strategy to monitor and regularly enhance your data?
3. How do you establish clear data lineage and key data governance principles? Do you understand where data is coming from, where it has been, how it is used and who is using it?
4. What are the pilot use cases where data-driven decision-making including advanced technologies can be experienced?

2. Sourcing and external dependencies: put third-party risk management at the centre of your ecosystem thinking

Sourcing and external dependencies (including TPRM – third-party risk management) serve to make sure that key services for clients are maintained. This is fundamental for understanding the dependencies of such services on third parties, and for managing the respective risks adequately.

Third-party failures can cause significant disruption and jeopardise the security of outsourcing financial institutions, as controls are circumvented through the targeting of vendors. Localised outages can quickly become contagious due to the interconnectedness of the financial services industry, especially where multiple financial institutions depend on the same service provider (e.g. cloud service provider). For all these reasons, third-party risk management has been a highly regulated topic which remains top of mind today given its importance in the latest draft of the European Digital Operational Resilience Act (DORA).

Careful management of third parties is becoming increasingly important from an operational perspective, and best-in-class service providers often come with strong bargaining power. As a result, it can sometimes be difficult to reconcile business needs, procurement constraints and regulatory requirements under one single roof as many global players struggle to tailor their solutions to the Swiss market's specificities and regulatory requirements. This is especially true with cloud service providers (CSP). Dependency upon a cloud service provider must be carefully considered and diligently assessed before entering such an agreement, to make sure that the cloud strategy and third-party risk management are closely aligned.

The current approach to third-party risk management is often siloed with individual teams focusing on different areas. To gain visibility across the vendor landscape, financial institutions should consider procuring a centralised third-party management tool and integrate it across all relevant capabilities, in order to reduce manual work and ensure proper oversight throughout the entire relationship lifecycle (i.e. due diligence, contract conclusion, performance tracking, contract termination and post-contractual stage). Financial institutions need to make sure they retain appropriate oversight of third-party providers and take responsibility for the service they provide. Doing so will reduce the risk of outages and accidental information disclosure.

To increase transparency of third-party providers to strengthen operational resilience, the following questions should help to identify the gaps:

1. How do you assemble and keep the inventory of outsourced functions up to date? In the European ICT (Information and Communication Technology) context, this would include all your contractual relationships (and not only the most critical ones).
2. How do you monitor the robustness and the quality of your third parties: what control points are needed and how do you evaluate associated risks (i.e. non-compliance of service provider)?
3. How do you monitor outsourcing contracts and adherence to contractual clauses? Do you have an exit strategy defined according to the level of risk and the type of third party involved?

3. Cyber resilience: anticipate adverse cyber events and develop detection, response and recovery capabilities to manage a cyber incident

Cyber resilience covers mechanisms required to anticipate adverse cyber events and develop detection, response and recovery capabilities to manage a cyber incident while continuing to operate business effectively.

According to PwC's 25th Annual Global CEO Survey: 'CEOs rank cyber risks as the top threat to growth'.[2] One reason for this is the rise of cyber-attacks on the financial services industry, including nation state-sponsored incidents. Ramifications of cyber events can be systemic when they impact a financial institution's strategic assets which are critical to the wellbeing of the overall market. As a result, regulators have ramped up regulatory efforts to mitigate important cyber risks (e.g. European Cybersecurity Resilience Act – proposal to be published in Q3 2022).

Financial institutions are rethinking their approach to cyber resilience and preparing their response to large-scale cyber-attacks. The board and executive management must face the new reality that cyber-attacks are no longer a question of 'if' but 'when'. This is why PwC's approach to resilience focuses on four key areas that are essential in developing and maintaining a resilient organisation. This methodology accepts that disruptions are inevitable and, in response, makes sure established and mature processes exist across your environment in the following domains:

- **Anticipate and prepare**
  Preventing incidents is preferred to responding to incidents. Leading financial institutions should therefore continuously assess their own resilience capabilities to better anticipate and prepare for new cyber threats. This includes leading practices such as incident readiness (IR plans, playbooks etc.), threat modelling, asset identification and dependency mapping. Additionally, 'resilient by design' needs to be considered when developing new solutions or selecting new components. An example of resilient design is the 'zero trust' approach in information security, where network systems and services are designed to 'never trust, always verify'[3] (e.g. devices are never trusted based on their physical or network location).

- **Withstand**
  In case of a disruption or critical outage, financial institutions should continue essential mission-critical functions by limiting significant impact and downtime. The organisation's preparation is key to withstanding disruptions. A well-trained incident response team with an updated incident response playbook can make the difference between failure and success.

- **Recover**
  After a major disruption, financial institutions should execute response procedures and restore mission-critical functions to the maximum extent possible. Prepared organisations can follow their cyber and disaster recovery plans. Recovering also means identifying the disturbance root cause and drawing from lessons learned to better prepare for future incidents.

- **Sustain**
  Leading firms leverage knowledge from previous disruptions to enhance resilience processes and limit adverse impacts in the future. This includes leading practices such as resilience training, tabletop exercises and crisis simulations, simulated recovery testing, and further development of resilience testing and plan development.

To better prepare for cyber disruption, you should evaluate:

1. How do you include cyber resilience by design in your critical activities as well as your contractual relationships (e.g. service providers)?
2. How do you test the robustness of the cyber resilience process and its capacity to meet different regulatory requirements?
3. Are resources with the right level of expertise allocated to responding and recovering from breaches? Do you have access to partners that you could activate in case of cyber-attacks (incident response retainers as negotiators)?
4. Would you be able to quickly restore your mission-critical functions in the case of a cyber-attack disrupting the availability of your key systems?
5. Have you assessed the need to insure your institutions against cyber-risks? If you have already taken out cyber insurance, do you understand the key provisions and clauses of the coverage?
6. Is a cyber resilience continuous improvement process in place in your company?

[2] PwC's 25th Annual Global CEO Survey: Cyber risks ranked as top threat (p. 5). https://www.pwc.com/gx/en/ceo-survey/2022/main/content/downloads/25th_CEO_Survey_PDF_report.pdf

[3] Find more information on the 'zero trust' approach in our paper: Zero Trust architecture: a paradigm shift in cybersecurity and privacy. https://www.pwc.ch/en/publications/2020/Zero Trust_White Paper_Final.pdf

4. Digital resilience and service operations: build a sustainable competitive advantage with resilience embedded at the core of your operating model

Digital resilience ensures that your digital processes and systems in the value chain of your core products and services are always operational, and that vital technologies are not disrupted by newly introduced systems. In the era of digital transformation, digital resilience can also act as a driver of investment and risk decisions.

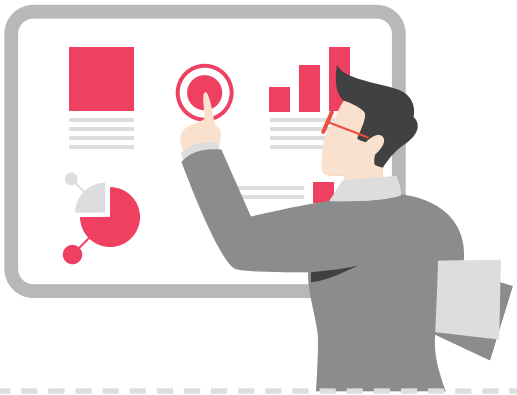
Financial institutions often address resiliency from a purely technological point of view and fail to sufficiently involve business leaders. Subsequently, management is inadequately prepared for business consequences caused by system disruptions. Many financial institutions rely, for example, on manual reporting processes that are slow and complicated to manage. Especially in times of crisis, these manual reporting processes are often not able to provide the necessary reports for the board and executive management which require accurate data for critical decisions.

Leading financial institutions follow a top-down governance approach to establish digital resilience that emphasises the importance of board and executive involvement. Their board frequently assesses the institution's risk appetite for withstanding digital disruptions and works with executive management to assign digital resilience responsibilities to leaders with sufficient expertise and resources across the entire organisation. To that end, a resilience officer at board level is a great asset to make sure that risk appetite and indicators are aligned with the company's strategy and are communicated accordingly at all levels.

At all levels of your organisation, the workforce should also prepare for the unexpected while staying true to the firm's values. Deliberate digital upskilling and soft skills training developing customer focus and growth mindset will be key as people continue to work more flexibly and digitally.

Digital resilience should be embedded in the design of both processes and IT solutions to enable scalability and adjustability within a fast-paced technological environment and to better cope with crises. This allows new components to be removed, replaced or added to the ecosystem with minimal disruption costs, to closely align with current and anticipated business needs. As such, digital resilience should be considered as a criterion in decision-making, from launching a product on the market to contracting a new business partner.

Moving to the cloud can, for example, be the right moment to re-think your legacy infrastructure and organise your data, processes and governance to support your company in the long term. Depending on the business' readiness, such changes can also be an opportunity to experiment with advanced technology like Machine Learning (ML) in specific pilot cases to reduce risk and mitigate potential incidents.



An understanding of the following would bring you closer to operational resilience:

1. How are your services evolving with digitalisation and what core services are you digitalising?
2. How do you ensure that your resilience appetite is understood at all levels and lines of defence within your organisation and that it is reflected in the risk and control framework?
3. Are your frameworks adapted to new technologies, from data quality and compliance to controls?
4. Are your teams trained to quickly adapt to new processes and new technologies?

Summary

In a world where unpredictability is increasing, the principle ‘resilient by design’ is critical.

Competent management of your operational resilience will help you to better anticipate risks and disruptions, prepare the response to them and continue delivering your products and services to your clients under any circumstances, resulting in a resilient operating model.

In our approach, operational resilience materialises when you make effective use of the capabilities you already have and begin to take a holistic approach to the value chain relating to products and services that are important for your clients.

You should be able to do so for existing processes and systems and aim to incorporate this thinking into your strategy and change management framework – to create a ‘resilient-by-default’ culture in your organisation.

How can PwC help you?

We are a global team of professionals with deep expertise in all the building blocks of operational resilience. We have supported our clients on their journey to resilience, and we can help you achieve the resilience maturity level that you are aiming for.

Thanks to our methodology, you can set up your operational resilience function while leveraging your existing frameworks.

1

Assess your current operational resilience status

1.1 ssess your operational resilience maturity: assessment of current operational resilience maturity by reviewing your operational resilience capabilities against our key building blocks that define a successful operational resilience programme.

1.2 Define your operational resilience goal: Develop a goal for your operational resilience capabilities, by taking into consideration the assessment outcome and your organisation's overall strategy.

2

Design the operating model

2.1 Establish a mandate for resilience: Board level mandate, with unity of purpose through a common definition and strategy for resilience. Set up an operational resilience function, with ad-interim nominations.

2.2 Identify what matters most: Customer first, alignment with firm's strategy, commercial objectives and social licence to operate. Regulatory landscape, market integrity and stability, customer detriment, key business services.

2.3 Understand the risks and set the risk appetite: Top down from the board. Integrated with enterprise risk manage-ment – applied at the firm and critical service level.

3

Deliver the operating model

3.1 Build and sustain an integrated operating model: Design and implement an operational resilience model. Coherence through alignment of operating and business engagement model across resilience disciplines.

3.2 Governance and control environment: Active board oversight of resilience activity. Measure, report, challenge – Key Performance and Risk Indicators, adequate and effective governance.

4

Deliver business as usual

4.1 Assess resilience of critical services end-to-end: Service ownership for resilience, map and assess business process against critical dependencies end to end, including the associated people, technology, premises and third parties.

4.2 Remediate resilience gaps: Execute a BAU programme to remediate resilience gaps – maximise ROI by targeting what matters most. At speed and in an order that reflects the organisation's capacity and risk appetite.

4.3 A sustainable, operational resilience function: Set up operational resilience function transitions to BAU, with final appointments and clear governance oversight. Operates within the first line with second line oversight.

Contacts

For additional information, please contact our experts:

Patrick Akiki
Partner,
Management Consulting Leader
PwC Switzerland

+41 79 708 11 07
akiki.patrick@pwc.ch

Alexandra Burns
Partner,
Risk Consulting
PwC Switzerland

+41 58 792 46 28
alexandra.burns@pwc.ch

Morris Naqib
Director,
Resilience, TOM and Transformation
PwC Switzerland

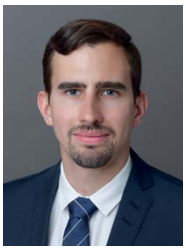
+41 79 902 31 45
morris.naqib@pwc.ch

Vincent Colonna
Director,
Cybersecurity & Privacy
PwC Switzerland

+41 79 257 88 40
vincent.colonna@pwc.ch

Megi Dhima
Senior Associate,
FS Operations and Digitization
PwC Switzerland

+41 75 434 52 77
megi.dhima@pwc.ch



Carlo Emanuel Schmid
Senior Associate,
FS Digital and Cloud Transformation
PwC Switzerland

+41 79 336 32 48
carlo.e.schmid@pwc.ch

We would like to thank Tim Niedermann for his valuable contribution to this publication.

PwC, Birchstrasse 160, 8050 Zurich, +41 58 792 44 00