Deloitte.

# Resilience by design

Financial services operating models and operational resilience

# Contents

# Executive summary

**Financial services operating models** are facing a growing need to be modernized in order to support the ability of organizations to compete in a more digital, decentralized, and data-driven environment. As parts of the world emerge from the COVID-19 pandemic, these operating models must also be able to cope with rapidly changing customer and employee preferences for services delivery and work.

**There is a growing competitive advantage** from having resilient operating models in financial services. As it becomes a measure of organization health that is seen as equal or comparable to financial resilience, organizations with operating models that can withstand severe disruptions will not only be more likely to win the confidence of regulators, but also of their customers, shareholders, and other stakeholders.

**Organizations need to integrate an operational resilience mindset into operating model design** in order to deliver on this ambition. Most operational resilience regulatory frameworks prioritize a set of critical operations, so in the eyes of the regulators not all operations will be equal. Organizations should be able to pinpoint where regulatory pressure is most likely to increase and focus on building resilience by design in those areas.

**Operational resilience** is a top regulatory priority in financial services that has enormous implications for organizations' design of their future operating models. In a growing number of jurisdictions, organizations will have no choice but to move quickly to implement new regulatory frameworks around operational resilience and address vulnerabilities that are identified in how they operate.

**This regulatory push creates both an opportunity and a necessity** for organizations to rethink how they design and implement their target operating models. Boards and senior leadership should be able to articulate clearly how any change program—from digitization, outsourcing, regulatory change, or new business—will strengthen the operational resilience of the organization and its services.

**We put forward three principles** for integrating operating model design with an operational resilience mindset. This activity needs to be led from the top and carried out consistently across the financial services group. The thinking should be guided by impact tolerances, where they apply, and over time organizations should aim to deploy operational resilience tools to evaluate operating model changes dynamically for their impact on resilience as modifications are proposed.

# Growing pressure to modernize operating models

Financial services organizations are facing a pressing need to modernize their operating models to remain competitive and execute their strategy in a post-pandemic environment. They are simultaneously coming under pressure from regulators to enhance their operational resilience.

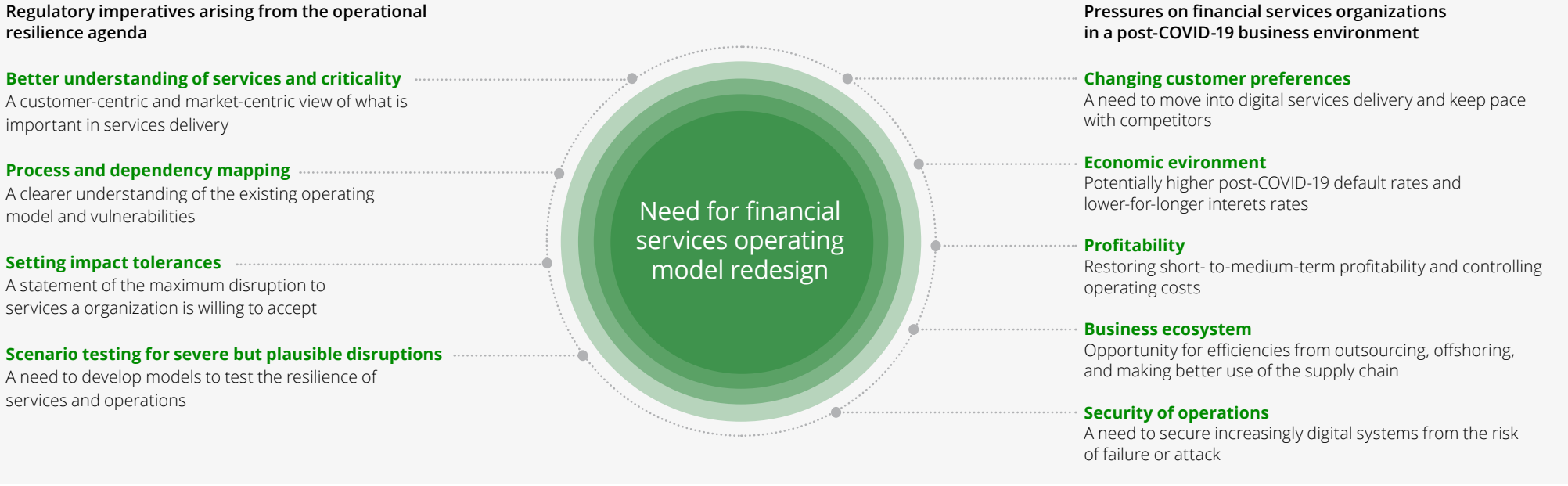
The recent regulatory push into financial services' operational resilience is the closest regulators have come yet to scrutinizing how a organization designs its internal operations. It's also an initiative that has rapidly gained momentum around the world as regulators become more alert to the risk that operational disruptions could pose just as significant a threat to the stability and soundness of the sector as financial ones.

Given all this, **organizations are going to have to learn to live with continual and increasing regulatory scrutiny of the resilience of their operations.** Financial services' operating models will have to adapt to this reality.

Organizations' operating models will also need to respond to new trends in the business environment as countries emerge from the pandemic. They cannot simply go back to the status quo of early 2020.

An updated design will have to reflect changing customer and employee preferences, location strategies, new technologies, and economic imperatives that have emerged in the last year.

**Figure 1: Contributors to the current need for operating model redesign**



**We believe that financial services organizations must consider the business pressures of a post-COVID-19 operating environment and the regulatory push for operational resilience hand in hand.** The most prominent features of each (set out in Figure 1) will all have significant implications for how a organization should design its target operating model.

At the heart of the regulatory agenda is for organizations to have a better understanding of how their operations would be affected by a severe but plausible disruption and to take action to enhance the resilience of their most critical operations in the face of such a threat.

## *The resilience of critical operations should be prioritized*

Not all of a organization's operations will receive the same scrutiny from regulators. The global approach to operational resilience is built on the principle that regulators will focus on those operations that are necessary to deliver business services that are important to external stakeholders such as clients, counterparties, or the financial market as a whole.[i] The emerging global approach, as best represented by the Basel Committee on Banking Supervision's (BCBS) principles issued in March 2021, is equally clear that the resilience of critical operations should be prioritized.[ii]

Even though the resilience of all operations is important, this regulatory prioritization exercise will allow organizations to understand better where putting resilience considerations first in their operating model design will have the maximum benefit and, conversely, where such efforts can be deprioritized.

### Building resilience by design

The operating models of financial services organizations were in a state of almost constant flux in the years leading up to the pandemic due to a plethora of technological and regulatory developments. Since the coronavirus crisis, organizations have had to modify their operations in order to cope with on-and-off restrictions on social and economic life, and they've had to put many change programs on hold. As these restrictions lift, the demand to upgrade and refine operating models will return quickly. But with that will come the risk that these upgrades will not be suited to a world with significantly more regulatory involvement in financial services' operational resilience.

We believe now is the right time for organizations to take a longer view and consider what the operational resilience agenda means for the target operating model in four to five years' time. If these are not considered together, there is a real risk that future regulatory intervention might derail change initiatives in the coming years and that a reactive approach to fixing any operational vulnerabilities regulators identify will add to the costs and complexity that organizations are seeking to avoid.

A better approach is to understand how the regulatory agenda will affect operating model design over the course of its implementation, and to identify ways to build resilience by design into operations as they evolve.[1] Ideally, organizations should use their work on operational resilience as a catalyst for revamping their operating model.

This report sets out our approach to the operating model and the challenges and opportunities that we see operational resilience posing for it. We then propose an approach for how senior leadership can instill an operational resilience mindset into organization-wide operating model design.

Finally, we explain why we believe that resilient operating models will be a key competitive advantage for financial services organizations in a post-COVID-19 environment where efficiency, speed, and the digital delivery of services will be critical for business success.

[1] Resilience by design is when an organization has built diversity, redundancy, and resourcefulness into its operating model in such a way that allows it to respond, adapt, and ultimately thrive in conditions of adversity.

# The financial services operating model

An effective operating model should enable a organization to deliver its strategic objectives and its purpose.

For financial services organizations, there is a growing need for operating models that can enable the delivery of more sustainable, competitive services that can control costs as well as take advantage of technological opportunities such as big data, analytics, decentralization, and digital delivery methods.

We view the operating model as having four discrete components that support the organization's strategy (as visualized in Figure 2):

- **The customer proposition** focuses on understanding the products or services that are delivered to the organization's end users (whether they are customers, clients, counterparties, or other stakeholders) and the channels that are used. The customer proposition is intrinsically linked to the organization's strategy and is supported by the three other components of the operating model.
- **Process and governance** provides clarity on the end-to-end steps required to deliver products and services to end users/consumers. Within this component, the organization evaluates opportunities for simplification, automation, or elimination of non-value-add activities.
- **Digital and data assets** are the systems, tools, and data used by the organization to deliver its services. They facilitate the way the organization operates and performs tasks.
- **Work structure** considers the roles, capabilities, responsibilities, methods of working, location of employees, and outsourcing models that are required to deliver services to the end user/consumer.

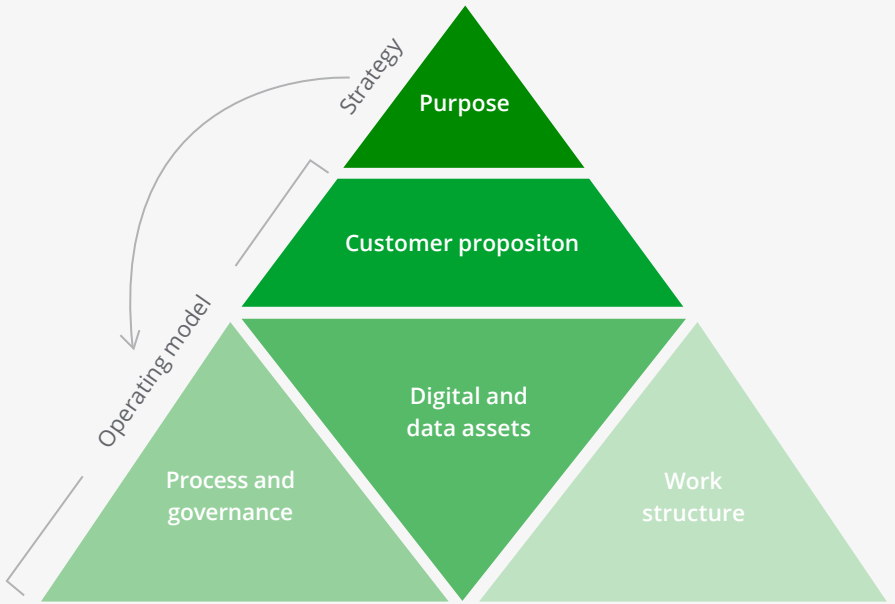
### The intersection with operational resilience

There are clear parallels between operating model design and enhancing the operational resilience of a organization's most critical operations.

The customer proposition component of an operating model is focused on identifying the value delivered to external end users/consumers much in the same way that operational resilience pushes organizations to identify how the failure of critical operations could harm external stakeholders.

The three supporting components of the operating model are all key factors in enhancing operational resilience. However, the regulatory objective is ultimately to protect the customer and the market from disruption. As such, the primary focus on the customer proposition challenges organizations to understand how any changes made to the three underlying components could affect their ability to deliver services during a disruption to normal operations.

**Figure 2: How the operating model supports a organization's strategy and purpose**



# Challenges and opportunities

The integration of an operational resilience mindset into operating model design will present organizations with two types of insights as they examine what this means for their specific circumstances:

- **Challenges arising from the regulatory agenda,** where the preferred design of the target operating model for business or economic reasons may be less feasible because of regulatory expectations or concerns. For instance, where a organization is seeking to outsource a business process to a third-party provider (TPP), that process could support the delivery of a service that has been identified as important from an operational resilience point of view. In such a scenario the organization may then need to consider what substitute capabilities can be put in place to maintain the service if the TPP were to be disrupted. This example is explored further in the In Focus section of this report on pages 13 and 14.

- **Opportunities to make use of operational resilience,** where the activity of implementing regulatory requirements for operational resilience or the end-state of more operationally resilient systems unlocks operating model design opportunities not previously available to the organization. One example of this are the benefits that can flow from mapping the underlying processes and dependencies of critical operations. This exercise can be used to give transformation teams a better understanding of a organization's operational vulnerabilities and help them identify risks or potential difficulties they might encounter during a change program.

We provide some further examples in Figure 3.

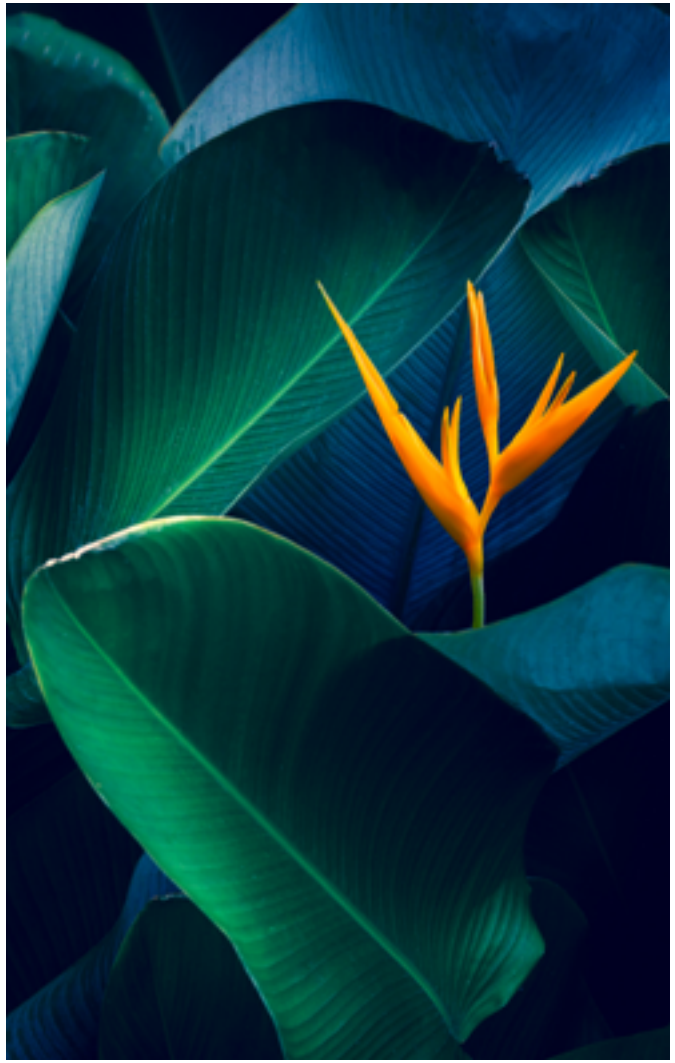
**Organizations should consider carefully how the challenges and opportunities they could face might crystallize across the three supporting components of their operating model—**process and governance, digital and data assets, and work structure—because an understanding of each will enable them to assess better how their operating model can evolve in a regulatory environment where operational resilience comes under much greater scrutiny.

### A challenging world of grey swans

The post-COVID-19 operating environment will bring obstacles for financial services organizations that cut across both operating model design and operational resilience.

The global pandemic showed that non-financial events can have a system-wide impact on the functioning of the financial services sector. Regulators have already said that they are now even more alert to operational threats that might undermine the financial system.

The potential sources of these threats are many. The growing ecosystem of the Internet of Things (IoT) will rapidly increase the cyberattack surface of financial services organizations, their customers, and suppliers, and will make it more conceivable that a future cyberattack on a organization could have systemic effects, with implications for broader financial stability.



More generally, **organizations should take the experience of COVID-19 as a signal that they need to design operating models that are resilient to 'grey swans'—** risks that may seem improbable but that are nevertheless conceivable, have some precedent (including in other sectors), and would cause widespread disruption to normal activities if they occured.[iv]

This means that when regulators ask organizations to test their resilience against a severe but plausible scenario, they want those organizations to take their thinking beyond Business as Usual-type disruptions that occur and are resolved in the sector routinely. Change and transformation teams should adopt the same mindset to think about how organizations' operating models can and should change to be resilient to risks of this severity.

### Opportunities in the post-pandemic working world

Across the three supporting components of the operating model, work structure is perhaps the most likely to see substantial operating model implications arise following COVID-19 given that many organizations look likely to adopt hybrid approaches to the day-to-day location of their teams.

A hybrid working model comes with a number of attractive possibilities. These could include the ability to staff teams more flexibly, based on a global or multi-regional talent pool. Allowing employees to choose the location and schedule of their work also looks set to become a key differentiator for financial services organizations in employee attraction and retention.[v]

To take advantage of this, however, organizations will need to ensure that this way of working does not make their operations more vulnerable. While their pandemic experience has shown that they were mostly resilient to a rapid shift to remote working, the resilience implications of a permanent hybrid model, assuming this becomes the norm, will still need thorough consideration. This could include the potential that organizations will be less successful in instilling the right risk culture among employees that have spent little-to-no time on site, and that certain controls may become gradually more susceptible to workarounds devised by unmonitored remote workers. Exceptions granted to compensate control restrictions due to hybrid working models may need to be revisited to avoid becoming standard business practice.

Organizations operating in the capital markets space should consider the implications of work structure changes for the treatment and control of price-sensitive information, especially where traders might no longer solely work in segregated office space.

Regulators have already made clear that the relatively resilient functioning of organizations in the last year has not satisfied them that the resilience of the sector is already up to the level they are seeking.[vi] Reaching that level will require concerted organization-wide and sector-wide efforts that help the financial services sector find a more resilient, but also more efficient, way of operating.

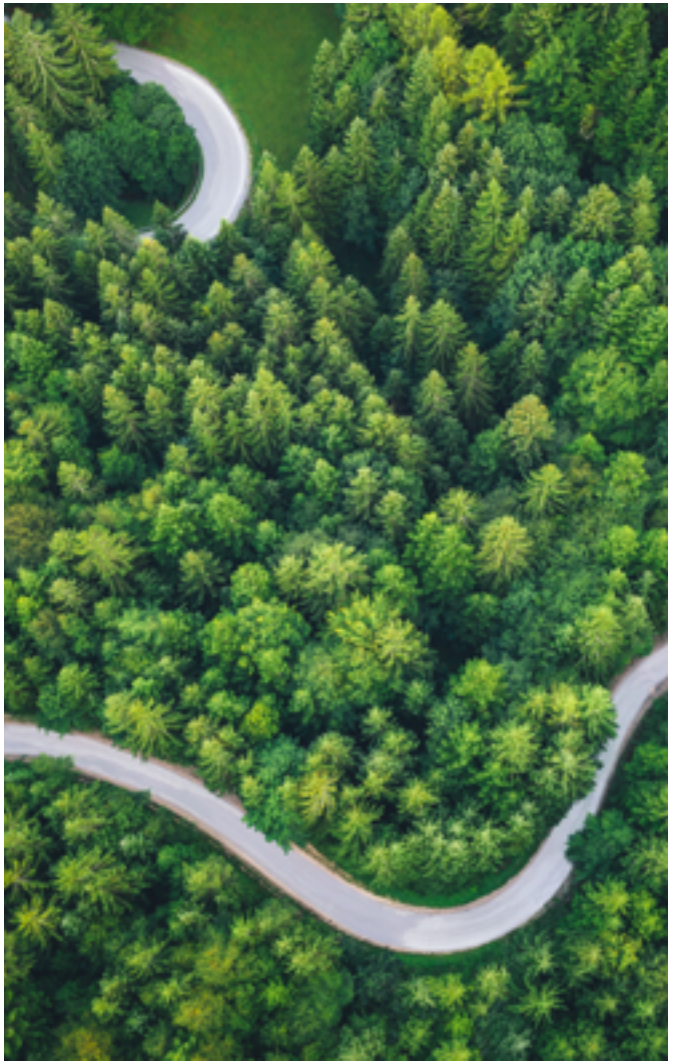


**Figure 3: Operational resilience challenges and opportunities for operating model design and change**

| Challenges | | Opportunities | |
|---|---|---|---|
| **Process and governance** | • Additional security controls and processes will add more complexity to service delivery<br>• Outsourced processes will give a organization less direct control over how it can meet regulatory expectations<br>• Executives responsible for resilience will be accountable for resilience failures in operating model change | **Process and governance** | • Better understanding of business architecture through process mapping<br>• Clearer understanding of needing to be hands-off between processes to deliver a service<br>• To streamline existing processes and responsibilities as well as reduce operating costs |
| **Digital and data assets** | • Potential regulatory resistance to outsourcing if security or concentration risks are identified<br>• Frequent IT operating model change will necessitate more mapping and/or testing for regulatory purposes<br>• Increasing reliance on digital increases the need for potentially costly manual substitute systems | **Digital and data assets** | • Better understanding of digital and data assets will enable change teams to improve IT change management<br>• Deeper understanding of the various technology applications used across the organization and streamline them<br>• To implement more consistent approaches to technology security across legal entities and geographies |
| **Work structure** | • Heightened cyber risks arising from a hybrid work structure<br>• Decentralized or offshore work structure more vulnerable to border restrictions and political intervention<br>• Offshored centres that are less technologically advanced may be less resilient in workforce disruptions | **Work structure** | • Resilient remote work structure can enable a global or multi-regional staffing model<br>• Hybrid working model that enables flexible work location could improve staff attraction and retention<br>• To increase automation as roles and inputs into the operating model are better understood |

# Integrating an operational resilience mindset into operating model design

The objective of enhancing operational resilience must also drive operating model design decisions and investment. **We see this as a strategic priority for financial services organizations that needs to be championed by their boards and senior leadership.**

Executives responsible for the overall operational resilience of the organization should take a top-down approach and set a consistent and resonating tone throughout the group, across geographies and legal entities, on how change and transformation teams should integrate an operational resilience mindset into their decisions.

We expect this to save costs by avoiding a proliferation of bespoke methods to satisfy individual owners.

We have made the case in our report Resilience without borders: How financial services organizations should approach the worldwide development of operational resilience regulation for why taking a group-wide approach to operational resilience makes sense for cross-border organizations.

The success of the approach will be in how it prioritizes this integration for the operations that are most likely to be subject to regulatory scrutiny. As noted in Figure 4, this scrutiny is likely to be most acute where impact tolerances set a high bar for expected resilience. Early signals from existing regulatory initiatives show us that these will likely include areas where a organization plays a role in the functioning of a broader system, such as in payments.

This approach needs to focus on helping the organization remain within its impact tolerance thresholds and to use the tools the organization develops as part of its operational resilience work (particularly testing methods) to improve how it makes operating model design choices.

**To do this, boards and senior leadership can use the three principles set out in Figure 4.**

**Figure 4: Three principles for integrating an operational resilience mindset into operating model design**

### 1. Taking a consistent group-wide approach to integration

Senior leadership needs to instill a common approach to operational resilience and operating model design throughout the group by creating a common set of objectives, a clear accountability structure for designing operating models that deliver critical operations, and a unified set of outcomes that operating model design choices should support. Done well, implementing this principle amounts to a group-wide cultural shift in thinking about operational resilience as a primary business objective.

### 2. Prioritizing action using impact tolerances

Operational resilience considerations should take precedence in operating model design when particular operations support critical operations. In such cases, teams need to understand how the applicable impact tolerance will affect the expected resilience of the service over time and be able to articulate how operating model changes made in that timeframe will support reaching the target impact tolerance.

### 3. Using testing to refine operating model design choices

As more sophisticated, model-based, operational resilience scenario-testing methods are developed, organizations should have the ambition not only to test service resilience periodically, but also to deploy this testing to evaluate how proposed changes to the operating model could affect the organization's ability to remain within its impact tolerance. This could pinpoint where additional investment, such as building substitutability, back-ups, and redundancies, will be needed in order to proceed with operating model change.

# Stages of integration in the coming years

Implementing a group-wide approach to integrating operating model design with operational resilience considerations will be a multi-stage project for most organizations.

Depending on the jurisdiction(s) the organization operates in, it is likely that efforts in the coming year will need to focus first on implementing new operational resilience frameworks.

While teams responsible for operating model design have an important role to play at every stage of the process, we see a particular opportunity for them in what we have called the integrative phase (see Figure 5).

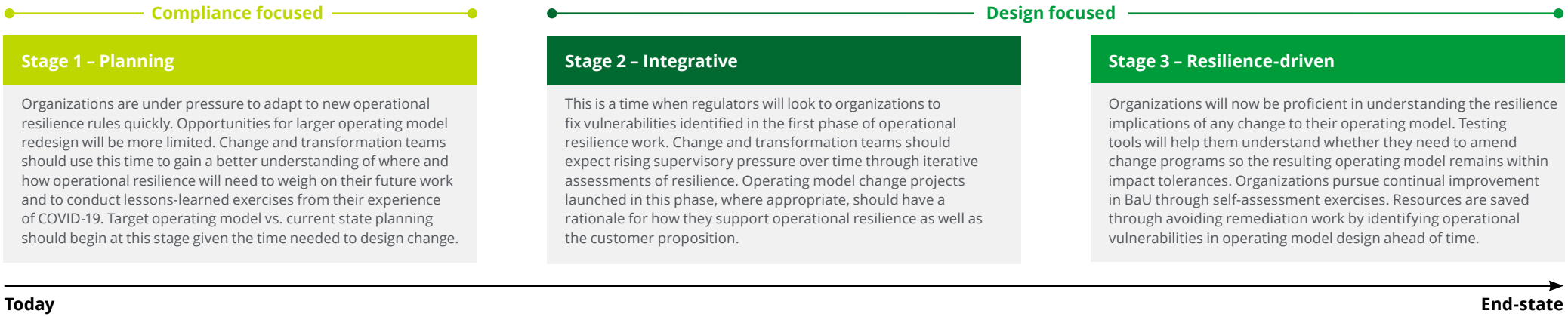
This is where the initial implementation work will have been done and regulators will expect organizations to remediate vulnerabilities and bring critical operations up to their set level of impact tolerance.

In any jurisdiction, it will be the time when organizations are expected to revamp their operations in order to strengthen their resilience in the way identified or requested by regulators.

This will be a critical time when smart operating model design decisions can serve both this purpose and the organization's broader business strategy. It is equally when **operating model change decisions that are not driven by an operational resilience mindset are likely to run into regulatory objections** and could be vulnerable to stagnant planning, cancellation, or remediation demands after the decisions have been implemented.

Boards and senior leadership also need to **consider what the operational resilience agenda means for mergers and acquisitions activity during and after the implementation of the regulatory framework.** Change and transformation teams will need to lay out clearly how, post-merger, they will integrate and streamline the different operating models while remaining within impact tolerances. This will satisfy an important regulatory concern and could make the transaction less failure-prone from an IT and operations perspective. Conducting model-based testing on operational failure scenarios arising from the combination would strengthen its case further.

**Figure 5: Three stages for integrating operation model design with an operational resilience mindset**



## **In focus:** Putting the principles of integration into practice

The role that operational resilience considerations should play in operating model design will vary based on the timing and circumstances of the change. **This example considers how a organization can factor in operational resilience when outsourcing to a TPP** during the integrative phase from Figure 5 (where operational resilience rules are in place and regulatory expectations of organizations' resilience are gradually increasing).

During this time, new change programs initiated by organizations will come under significant scrutiny. Supervisors will want to ensure that such programs do not detract from the organization's ongoing efforts to build its resilience, and—where possible—enhance them. Growing regulatory interest in the potential systemic risks of concentration among TPPs in their provision of services to financial services organizations will only heighten this scrutiny.

Figure 6 shows a number of questions that change and transformation teams can ask to determine the relevance of operational resilience to their target operating model design.

One of the first is to determine whether the operating model supports a critical operation that has been identified for regulatory purposes. If so, this means that they can expect a higher level of regulatory interest in their operational resilience and a greater onus placed on executives responsible for its oversight in addition to their compliance with the applicable guidelines on outsourcing and third-party risk management such as those from the UK Prudential Regulation Authority and the European Supervisory Authorities (e.g., Basel Committee).

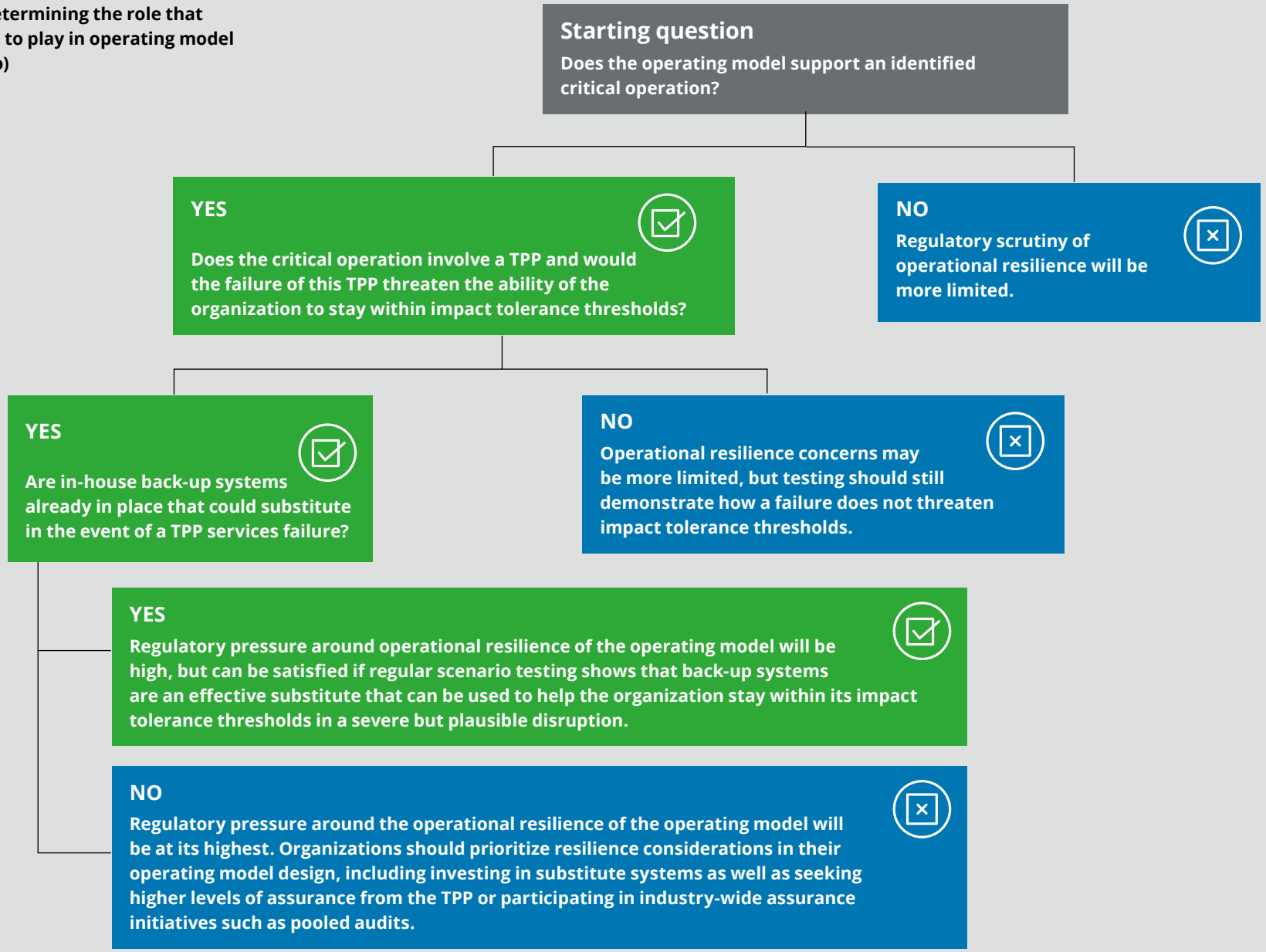
Beyond this point, teams also need to consider whether the failure of the TPP or the outsourced function would jeopardize the organization's ability to deliver the critical operation within the impact tolerances that have been set for it. If it would, then it is likely that this third-party relationship will be considered a point of vulnerability. In such cases, the operational resilience of the operating model changes being considered must be made a priority.

For new initiatives that involve outsourcing to TPPs, such as migrating legacy on-premises infrastructure to the cloud, organizations must take the opportunity to build resilience by design into their operating models. Regulators looking at operational resilience in jurisdictions such as the United Kingdom have indicated that, in a severe but plausible scenario for a critical relationship where a organization can no longer rely on its TPP, an exit strategy based on substitutability will be paramount. Where a organization has alternative systems or processes that can be used quickly to deliver the same service, investing in those systems and showing their functionality in resilience scenario testing will go a long way to meeting regulatory expectations.

Organizations should also seek a higher level of assurance from the TPP on its own operational resilience in areas such as data security, cybersecurity, and the management of material sub-contracting. For their most critical relationships, organizations should develop real-time risk intelligence tools that can continuously monitor the TPP and allow for proactive risk management. They can also involve the TPP in business continuity and disaster recovery testing to gain an even deeper understanding of potential resilience challenges.

While negotiating contractual terms that allow for such a higher level of assurance may be difficult for individual organizations with a large cloud service provider, we see an opportunity for sector-wide collaboration between organizations in addressing this challenge over the next two to three years. Pooled audits, in which a group of financial services organizations collaborate to assess the resilience and security of a shared TPP, are already a measure that some regulators have signalled will be a recognized part of meeting operational resilience expectations.

**Figure 6: Decision tree for determining the role that operational resilience needs to play in operating model design (outsourcing scenario)**



# Operationally resilient operating models as a competitive advantage

Given the pace at which the complexity and potential impact of operational disruptions in financial services are growing, it is clear why regulators around the world have embarked on such ambitious agendas to strengthen the sector's resilience.

Operational resilience is therefore a regulatory imperative. But **instead of regarding it solely as a compliance exercise, we believe organizations can use it to develop more resilient operating models** to help them become fitter to face future threats.

Figure 7 sets out five ways that we see operationally resilient operating models offering a source of competitive advantage. These advantages are built around how a organization can use its resilience to win confidence—of customers, of regulators and of wider stakeholders (be they shareholders, rating agencies, or others).

Customer confidence will be particularly important as new entrants to the financial services market create a more competitive environment that traditional organizations will need to face.

This confidence can be won directly by developing a reputation for resilient operations—a differentiator that may become more top-of-mind for customers as cyber threats in the financial services sector become more sophisticated, and broader IT failures become more frequent and public.

The confidence of customers can equally be an indirect benefit of more resilient operating models, especially where they allow a organization to act more flexibly and to offer new services and delivery methods more quickly when societal preferences change.

### The risk of doing too little

In the current environment of strict cost control, it is understandable that many organizations will question why they might do more than the regulatory minimum. That approach, however, would risk taking a organization down a path where it becomes an operational resilience laggard while its competitors forge ahead. This is not a position that a organization wants to be in.

Recent events in the financial sector have demonstrated a clear connection between a organization's technological resilience and its ability to transform itself into a leaner, more cost-efficient and competitive organization. In our paper *On the frontier: Operational resilience and the evolution of the European banking sector,* we noted that complex, cross-border organizations in particular have often found poor operational resilience to be a key barrier to digitization efforts (either through change programs or the integration of digital-native businesses into their own).

At least one rating agency has also pointed out a potential link between a financial services organization's individual cyber resilience and its credit rating due to the potential for reputational damage. Reflecting on this, it has called for digitization to go hand in hand with greater efforts to plan for disruption and incident recovery.[vii]

**Figure 7: How operational resilience enables a competitive advantage**

Regulators are also unlikely to respond well to a organization that only seeks to deliver the minimum viable product in its efforts. Operational resilience is not a detailed list of regulatory requirements that need to be complied with to the letter, but rather a set of expectations that demands innovative thinking and independent action on the part of organizations, as well as collaborative action in the financial services industry.

**Regulatory expectations for operational resilience will also evolve over time** given the growing complexity of the technological and operating environment of organizations and the corresponding growth in threats they may face. Indeed, when discussing the evolving nature of cyber threats in the sector, one senior regulator recently acknowledged that there is no end point in the operational resilience journey for financial services organizations.[viii] If there was an end point, then the value of the resilience initially achieved would diminish over time.

Specifically in Canada, the Office of the Superintendent of Financial Institutions (OSFI) recently published the result summary of its consultation on operational resilience in a digital world. This summary contains OSFI's plans to release draft guidance on a range of areas through to 2023.[x] In such an evolving regulatory environment, it makes sense for organizations to think about what operational resilience will mean for their own evolution. This will necessarily reveal some trade-offs between their desired operating model (based on a purely commercial rationale) and one that will stand up to regulatory scrutiny. Identifying these tensions early will contribute to a more stable and sustainable operating model over time. Organizations that can demonstrate to regulators that they have incorporated resilience by design into any changes to the operations that support their critical operations will reduce the likelihood of regulatory intervention (such as formal reviews leading to ex post remediation) and the reputational damage that could come with it.

Achieving and maintaining the confidence of regulators, shareholders, customers, and other stakeholders through proven resilience in the face of financial stress is already a well-recognized competitive advantage for organizations since the Great Recession of 2008-09. It is entirely reasonable to expect that, with the growth of new operational threats to the stability and functioning of the financial sector, similar advantages will increasingly arise for organizations that can demonstrate effective operational resilience.

"If the last decade of bank supervision was about designing rules that lead to more resilient bank balance sheets … the goal in the decade ahead must be for banks to improve their risk culture and operational resilience by at least the same margin as they have improved their financial resilience in the decade past."

**Carolyn Rodgers, secretary general of the Basel Committee on Banking Supervision**[ix]

# A narrow window of opportunity

Never before have regulators so directly looked at, and set expectations for, the internal operations of financial services organizations.

While many regulatory requirements are relevant to changes in a organization's operating model, the operational resilience initiative will merit special consideration for those parts of the operating model that support critical operations.

Financial services organizations now have an important opportunity to use the regulatory drive for operational resilience as a catalyst to build more resilient operating models. Both are much-needed projects in the sector, but are ones that may often come into tension with each other if operating model design choices do not maintain or enhance operational resilience.

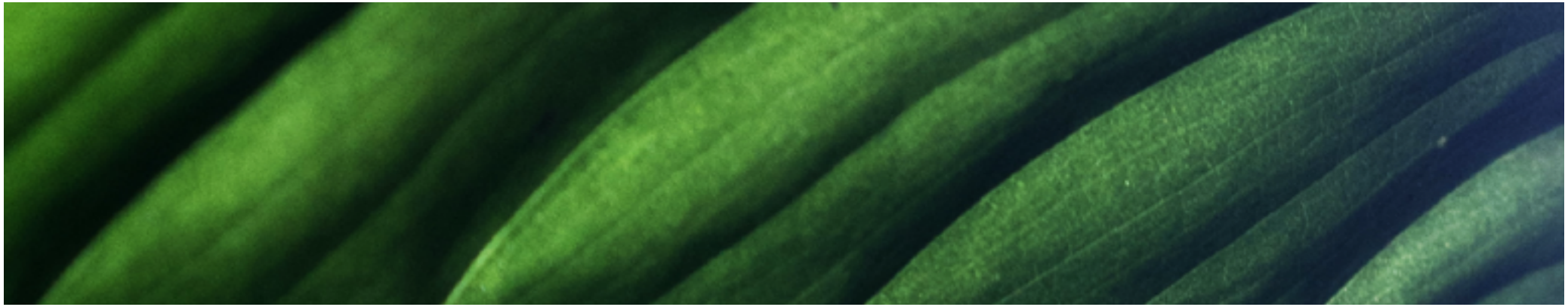
To address these potential tensions, early action will be key, as the best-prepared organizations will use the near-term regulatory imperative to improve their understanding of the implications that operational resilience is likely to have for their operating model over the next four to five years.

The window for organizations to seize this opportunity, however, is a narrow one. Given the likely timelines for the implementation of the regulatory approach to operational resilience in various jurisdictions, many organizations will need to do the bulk of their work on remediating vulnerabilities in the next few years. Spending these years only focusing on the minimum that is required to meet regulatory expectations may allow competitors to pull ahead.

Linking up the operational resilience agenda with a proactive and resilience-driven approach to operating model design is something that change and transformation leaders should begin planning for this year.

*Linking the operational resilience agenda with a proactive, resilience-driven approach to operating model design is something that change and transformation leaders should begin planning for this year.*

Organizations will have a great deal of licence to determine just how wide-ranging an approach they pursue. Our view is that taking early, well thought-out and comprehensive action on integrating an operational resilience mindset into a bold agenda of operating model redesign will serve organizations well from both a regulatory and commercial perspective.



# Contact

If you have any questions about the content covered in this report, please contact a Deloitte specialist in operating model design, operational resilience, cyber risk or third party risk management.

## Contact


**Rob Galaski**
Vice Chair, Managing Partner
Financial Services
rgalaski@deloitte.ca

**Jean-Francois Allard**
Partner
jeallard@deloitte.ca

**Stefanie Ruys**
Director
struys@deloitte.ca


## Canadian contributors


**Nathan Spitse**
Partner

**Roxana Greszta**
Partner

**Nino Montemorano**
Partner

**Zoheir Boualga**
Senior Manager

**Emmanuel Aruwa**
Manager

**Jawad Hameed**
Manager


## United Kingdom contributors


**David Strachan**
Partner

**Scott Martin**
Senior Manager

**Amar Duggal**
Senior Manager

**Ana Garcia**
Senior Consultant

**Orlagh Tuite**
Partner

**Rick Cudworth**
Partner

**Danny Griffiths**
Partner

**Sarah Black**
Partner

**Nick Seaver**
Partner

**Simon Brennan**
Director

# Endnotes


i. Bank of England, Operational Resilience: Impact tolerances for important business services, 29 March 2021.

ii. Basel Committee on Banking Supervision, Principles for operational resilience, 31 March 2021.

iii. Deloitte, Resilience Reimagined: The resilient business, blog, 10 September 2021.

iv. Aon, Respecting the Grey Swan: 40 years of Reputation Crises, 2021.

v. Deloitte, The future of banking: The employee experience imperative, 2021.

vi. Bank of England, Resilience in a time of uncertainty, speech given by Nick Strange, 6 October 2020.

vii. S&P Global Ratings, Cyber risk in a new era: The effect on bank ratings, 24 May 2021.

viii. Bank of England, Cyber Risk: 2015-2027 and the Penrose steps, speech given by Lyndon Nelson, 25 May 2021.

ix. Basel Committee on Banking Supervision, The changing role of a bank supervisor, speech given by Carolyn Rogers, 25 May 2021.

x. Office of the Superintendent of Financial Institutions (OSFI) recently published the Technology risk consultation result summary, 10 May, 2021.