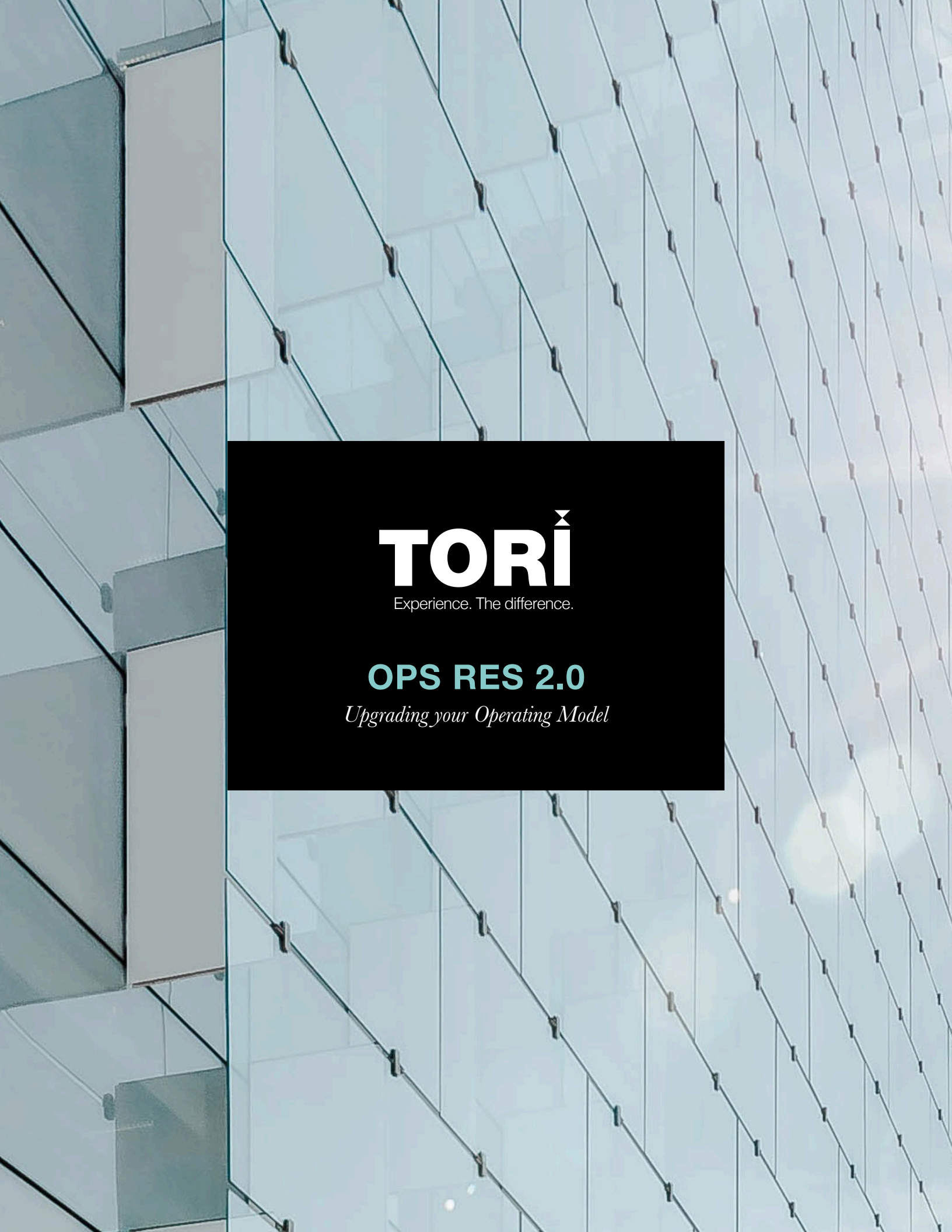


TORÍ

Experience. The difference.

OPS RES 2.0

Upgrading your Operating Model

Since 2019, we have been monitoring closely how financial institutions are adopting Operational Resilience and embracing this challenge.

In our research published in October 2020, we found that 80% of responders said their board approved a strategy, but only 1 out 4 considers there is a high level of awareness about Operational Resilience across the entire organisation.

For several years, businesses and regulators have been focused on developing frameworks to deal with operational disruptions and failures, but these were primarily linked to specific aspects such as business continuity and disaster recovery plans; the goal was to restore operations quickly without considering the ripple effect across the organisation and the market.

However, due to the interconnection between financial institutions and suppliers, this approach needs to adopt a more dynamic strategy to consider the critical part of this story: clients and the services impacted.

Building a dynamic Operational Resilience framework, is not a box ticking activity from the middle office or IT departments. According to our research, only 58% have a clear visibility of their critical systems and processes. This is a clear call-to-action to the Senior Management (SM) to change the traditional approach and embrace more collaboration to better understand the interconnectivity and risks between operations, services and clients.

Here, we identify three critical aspects that should be kept in mind as you move toward adopting a dynamic approach.

A. Adopting a client-centric mindset: Building a framework

B. Data Intelligence: Unlocking the value

C. Operational Resilience 2.0: Upgrade your model

A. Adopting a client-centric mindset: Building a framework

When a disruption occurs, institutions primary focus is to detect the root cause of the trouble and according to the criticality, activate the business or recovery plans. In doing so, institutions minimise the ripple effect on the rest of the organisation and financial ecosystem related to the failure.

For this reason, organisations should start thinking about their Operational Resilience framework, not just as a form to restore operations, but a way to generate and preserve value, minimising reputational and other risk exposure.

Start building a customer-centric view: Finding your value proposition.

1. Start with the services: Identify the products and services that your organisation provides to the clients and classify them according to the level of importance.

2. Map all channels and processes involved: Apply a reverse engineering analysis, starting from how the client receives the service and interacts with your organisation; move across the organisation, identifying processes, people, and systems. Be aware of some fundamental parts of those processes are executed by an external provider.

3. Use data: To support your business strategy, it is essential to track interactions between your customers and the organisation. This information will support your decision-making process when establishing a dynamic risk management framework.

4. Monitor Market dynamics: Customers are constantly demanding new experiences and services. Be sure your risk and business functions are actively involved to perform the analysis, always considering the client as the starting point.

These four pillars will help you to understand your business and value proposition from a customer perspective, while mapping processes, systems and teams involved.

Leveraging actions from data, will support Senior Management to improve the decision-making process, considering critical risk exposure based on materiality to clients and to the ecosystem.

B. Data Intelligence: Unlocking the value.

Data should be considered the main asset that any financial organisation should have. Having a robust data governance framework is critical for financial institutions to understand its risk exposure when delivering services to clients.

For this reason, organisations should have a clear vision about its own data, in order to build a robust and adaptable framework capable of leveraging the customer-centric model.

1. **Data Ownership:** Well defined ownership and accountability for the data governance.
2. **Data Access:** Setting the right access according to the level of confidentiality, functions and responsibilities within the organisation.
3. **Data Security:** Developing and testing systems to prevent cyber-attacks and undesirable risk to third parties. Also, institutions should have a clear view on its IT Architecture and application ecosystem.
4. **Data Quality:** Understanding if the systems provide data with the required quality to perform business functions. Measure the outcomes and tune the tools if necessary.
5. **Data Calibration:** Learn from the past and modify the framework on a periodic basis considering operational and business changes.

Building and maintaining a data framework, will support organisations to understand the connectivity between services, processes, teams, and systems across business functions and operations.

C. Operational Resilience 2.0: Upgrading your model

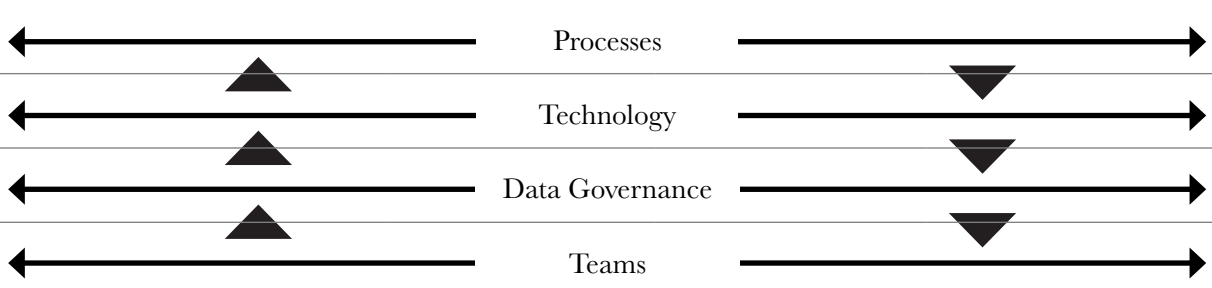
Regulators around the globe are re-evaluating the approach for the traditional Operational Resilience framework, moving from a business-siloed perspective to a more macroprudential-systemic view.

As seen in the following diagram, the traditional Operational Resilience model is primarily focused on Operations and rarely shows interactivity between different layers of the organisation. Conversely, a dynamic Ops Res model embraces the interconnectivity between processes, teams and systems involved on delivering critical services to the clients.

Traditional Operational Resilience Model: Business Continuity and Recovery Plan (Focus on Operations)

GOVERNANCE FRAMEWORK					
Customer Experience using products and services	**Physical and Digital Channels**	**Operations**	**Control Functions**	**Reporting**	
Processes	Processes	Processes	Processes	Internal Stakeholders	External Stakeholders
Technology	Technology	Technology	Technology		
Data Governance	Data Governance	Data Governance	Data Governance		
Teams	Teams	Teams	Teams		

Dynamic Operational Resilience Model: an E2E holistic approach

GOVERNANCE FRAMEWORK					
Customer Experience using products and services	**Physical and Digital Channels**	**Operations**	**Control Functions**	**Reporting**	
				Internal Stakeholders	External Stakeholders

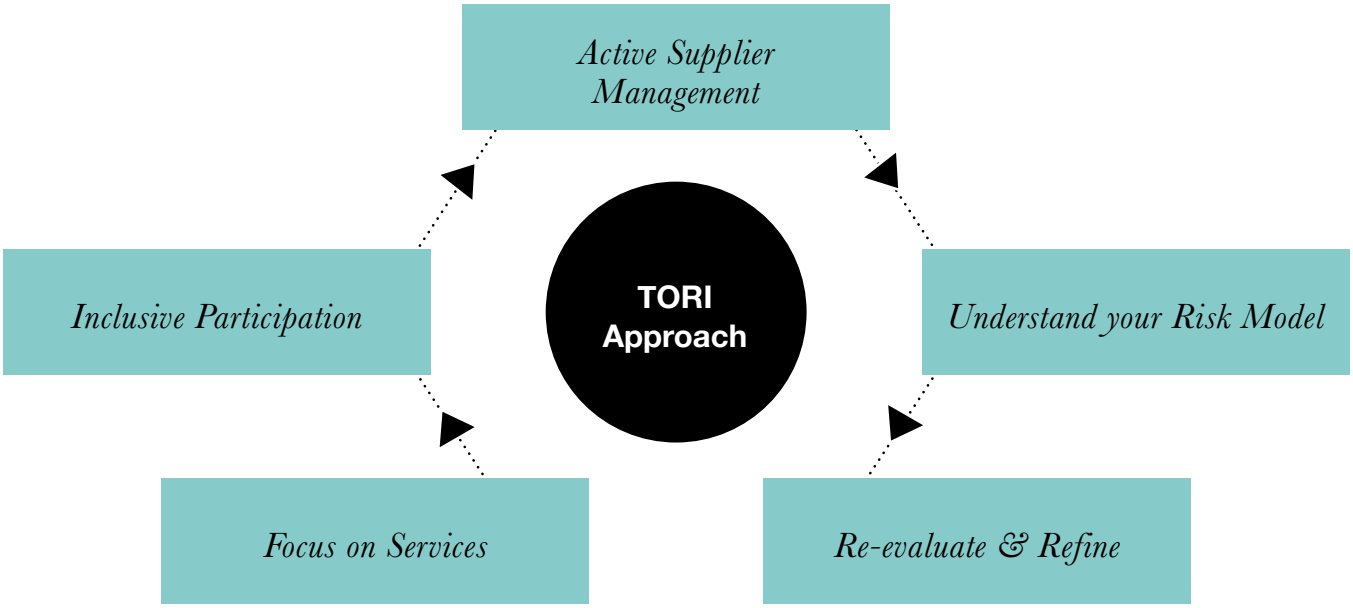
C. Operational Resilience 2.0: Upgrading your model

In addition, there is another emerging systemic risk related to the concentration on third party providers for critical services (normally outside of the regulated scope), an aspect that regulators are monitoring closely due to the level of interconnectivity and dependency across the financial ecosystem.

As a result, firms need to shift their mindset from business recovery to a client-centric view, to understand the ripple effect across the organisation and the ecosystem when a failure happens.

Considering this scenario, there are critical factors to take into consideration to upgrade your model:

1. Develop your framework starting from the services rather from the operational aspects: Considering processes, people, and IT infrastructure.
2. Promote inclusive participation: Get all relevant stakeholders involved in the process.
3. Initiate active supplier management: Monitor your suppliers and establish control to mitigate undesirable risk exposures.
4. Understand your risk model: Aligning your key risk indicators according to the risk appetite defined by Senior Management. Risk tolerance can also suffer modifications when re-assessing the model.
5. Re-evaluate and tune: Proactively assess your model to determine if there is any room for enhancements. Circumstances could change, impacting not only your business but also other businesses within the ecosystem.



How TORI can help

Operational Resilience is more than just recovering your operations after an incident, it's about building a holistic view of how Financial Institutions deliver their services to its clients and the potential consequences to the ecosystem.

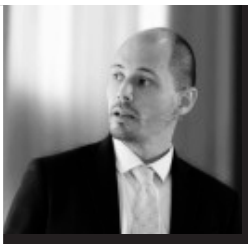
At TORI, we have set a clear methodology to support organisations on this journey, providing a clear strategy and vision for the challenges ahead.

STAGE 1: INITIAL ASSESSMENTS	STAGE 2: CLOSING YOUR GAPS	STAGE 3: MONITOR PROGRESS
Identifying the current point on this journey is essential to determine how robust is your Operational Resilience today. Also, the C-suite needs to define a desirable future state, considering resources business plans and market dynamics. Once is know, the difference between current vs. future state, will determine the areas where the organisation needs to focus to improve its Ops Res. model.	The Senior Management following their mandate, needs to lead and coordinate actions to close any substantial GAP identified on the Stage 1.	Building a robust Ops Res. dynamic framework, requires organisation to track their progress and notify to Senior Management about any deviation from the initial plan.
TORI will perform a: • Operational Resilience Maturity Assessment • Workshops with C-suit to explore the future state	**TORI can help you with:** • Identify IBS and Risk tolerance • Improve your Third Party Risk Management Framework • Building a robust Data Management Framework • Support Senior Management to pursue the right governance	**TORI can help you with:** • Run on a periodic basis the assessment to track progress • Provide independent review related to the progress • Share with C-suite, feedback and recommendations

Next Steps

To discuss the Maturity Assessment and explore how this can benefit your Operational Resilience programme, email Daniel Garcia, TORI's Operational Resilience practice leader.

Read our Operational Resilience Smart Paper
Read our Bank of England Case Study



Daniel Garcia
TORI's Operational Resilience practice leader

Daniel is a Senior Risk professional with over 13 + years of experience, in-depth knowledge of Financial and Non-Financial Risk Management, regulatory change and the digital innovation across business and control functions. He has held various senior risk roles in Top Tier Financial services organisations as well as Big four consulting firms and service providers. Daniel has global expertise in regions such as the EU, Latam, China and the UK.

In addition to his role as SME - GRC, Daniel has been a Lecturer for several years on subjects related to Finance, Investments, Risk Management and Corporate Governance for different Universities and clients.