Operational resilience

as strategic imperative

The foundation for an unbreakable financial services sector in Saudi Arabia

KPMG. Make the Difference.

January 2026

Foreword

The Saudi Arabian financial services sector stands at a pivotal moment. As the Vision 2030 transformation agenda accelerates and enters its third phase, financial institutions face an unprecedented convergence of opportunities and risks. Digital transformation, cloud adoption, fintech integration, and expanding customer expectations are reshaping how banks operate, and this transformation and broader geopolitics come with new emerging risks and dependencies which will challenge operational resilience.

The Saudi Central Bank (SAMA) has responded to this evolving landscape with reinforced expectations around operational resilience, issuing recommendations that go beyond the traditional BCM framework and adjacent technology and cyber pillars. Similarly, financial regulators across the middle east, such as the central banks of the UAE, Kuwait, Jordan, Qatar, and Bahrain, are each working on new operational resilience regulations – some expected by 2026. These developments in the region underscore a global trend and a fundamental fact: operational resilience is more than ever a strategic imperative for financial institutions to ensure customer centricity and market stability.

Operational resilience is no longer a regulatory checkbox; it is the foundation upon which sustainable banking operations are built in an increasingly volatile world.

Marcus Threadgold

Partner,
Operational Resilience Lead
KPMG Middle East

Table of contents

Building a resilient ecosystem is a strategic imperative

Firms have long been operating in an environment of interconnected and overlapping crises, and in the current era it seems that polycrisis is the new normal. To survive and thrive, the most valuable currency for firms is the trust of their stakeholders – be it regulators, investors, customers, suppliers, or employees.

The question firms need to ask themselves is not "if" but "when" will the next crisis strike? And when it does – will they be prepared to remain worthy of their stakeholders' trust, and recover quicker than their competitors? Firms have a tremendous opportunity to build this trustworthiness by demonstrating their ability to remain operationally resilient and bounce back stronger through any crisis or disruption.

Firms that recognize this opportunity and invest in building a strategic operational resilience capability will gain a significant competitive advantage enabling them to capitalize on opportunities where their competitors may be less prepared. It's a very exciting time to sit at the heart of operational resilience in the financial services sector of the region, and the next few years promise to inculcate a feeling of permanent dynamism. Now is the time to invest in and prepare for the future. Are you in?

The fundamentals of operational resilience and real-life cost examples

The fundamentals of operational resilience

At its core, operational resilience answers a fundamental question: "As an organization, what would happen to our most critical services if everything that could go wrong, did go wrong?"

This requires a shift in perspective from incident response to service resilience and represents a fundamental transformation in how financial institutions must think about risk. Rather than cataloging assets and creating recovery procedures, organizations should understand their critical services end-to-end, map the complex web of dependencies that support those services, and build genuine capabilities to maintain or rapidly restore operations under severe but plausible scenarios.

Figure 1: Operational resilience fundamental activities

It is important then to clarify that business continuity, risk management, and operational resilience are not different disciplines but rather complementary pillars of a robust organizational strategy (table 1). Traditional business continuity management (BCM) emerged in an era when technology was simpler, supply chains were shorter, and the pace of change was slower. BCM focuses on restoring specific systems and processes after disruption, ensuring the firm returns to business as usual. Risk management operates at a broader level, identifying and mitigating threats before they materialize, using tools like risk appetite frameworks and key risk indicators (KRIs) to maintain compliance and protect value. Operational resilience goes further by assuming severe but plausible disruptions will occur and designing systems and capabilities to withstand and adapt to them, prioritizing customer and market stability over internal recovery alone.

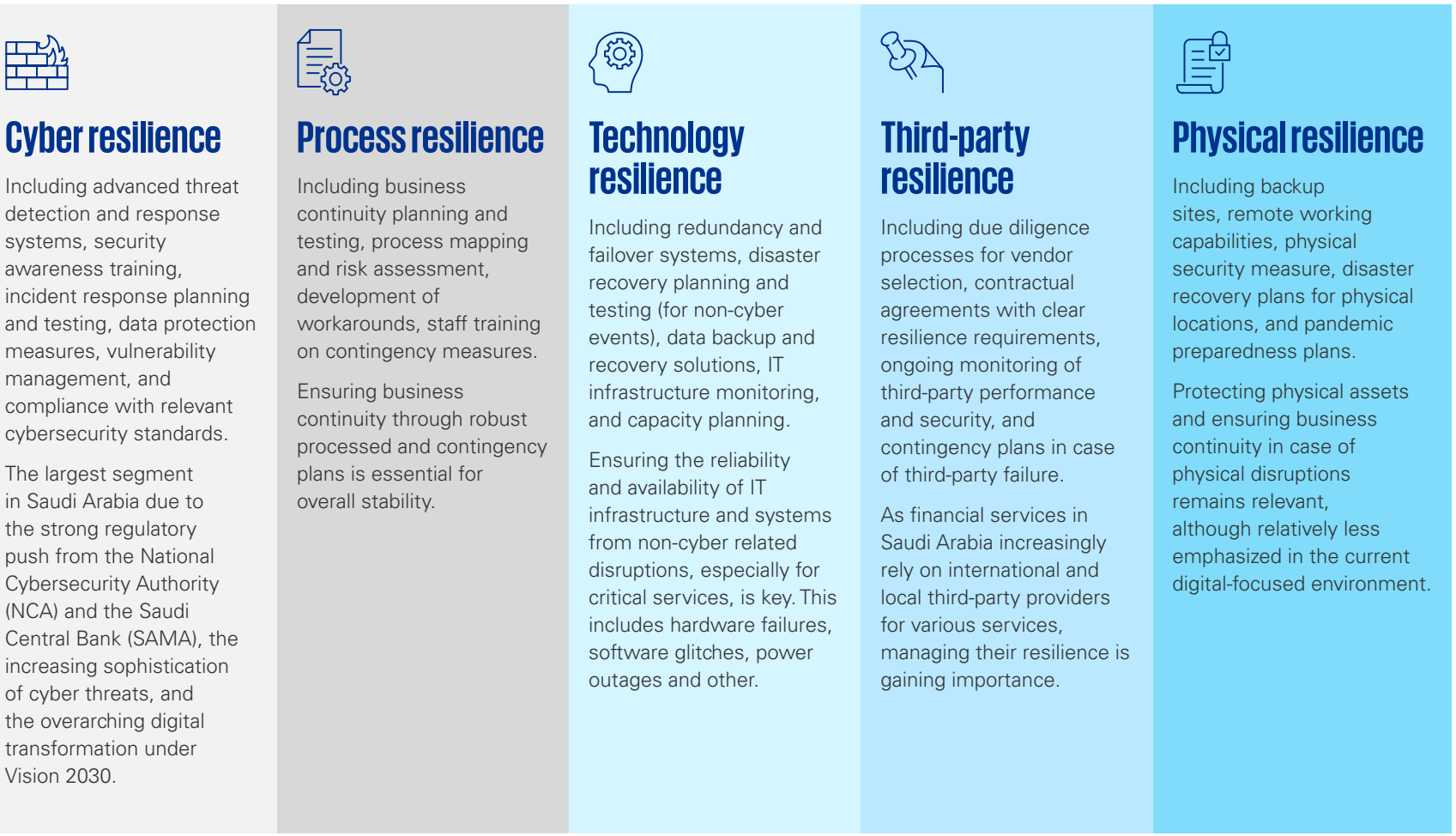
Together, these disciplines create a layered defense: proactive risk identification, structured recovery planning, and resilience engineering that anticipates and absorbs shocks. This integrated approach is essential for meeting regulatory expectations while safeguarding reputation and client trust in the Saudi Arabian financial services market.

Table 1: Business continuity, risk management and operational resilience complementary disciplines

	Business continuity	Risk management	Operational resilience
Objective	Ensure continuity of critical operations during and after disruption, ensuring the firm return to business-as-usual.	Identify, assess, and mitigate risks to achieve strategic objectives and regulatory compliance.	Maintain delivery of important business services within defined impact tolerances under severe but plausible scenarios (survival).
Scope	Individual processes and components supporting critical services.	Enterprise-wide risks (strategic, operational, financial, compliance) across all functions.	End-to-end business services vital to customers and market stability.
Metrics	Recovery time objective (RTO), recovery point objective (RPO), availability targets.	Risk appetite statements, key risk indicators (KRIs), stress testing results.	Impact tolerances (time-based and harm-based thresholds for intolerable disruption).
Solution	Documented business continuity plans (BCPs), disaster recovery plans (DRPs).	Risk mitigation strategies, controls, governance frameworks.	Resilience scenario testing, adaptive operating models, minimum viable service recovery.
Assurance	Regular BCP/DRP testing, ISO 22301 compliance audits.	Risk assessments, internal audits, regulatory reviews (e.g., Basel, SAMA, PRA).	Ongoing resilience scenario testing, board-level oversight, regulatory attestation.

Moreover, operational **resilience is multi-dimensional**, encompassing cyber resilience, technology resilience, third-party resilience, process resilience, and physical resilience. These resilience categories are entirely interconnected and a holistic approach that considers these interdependencies is vital to ensure end-to-end resilience vulnerabilities are identified and timely remediated.

Figure 2: Operational resilience investment categories



Recent high-profile incidents across global financial services demonstrate that operational resilience failures carry severe financial financial, reputational, and regulatory consequences.

The following case studies provide examples of the real-world cost of operational resilience failures and critical lessons for other financial institutions.

Case study 1

Barclays IT outage (January 2025)

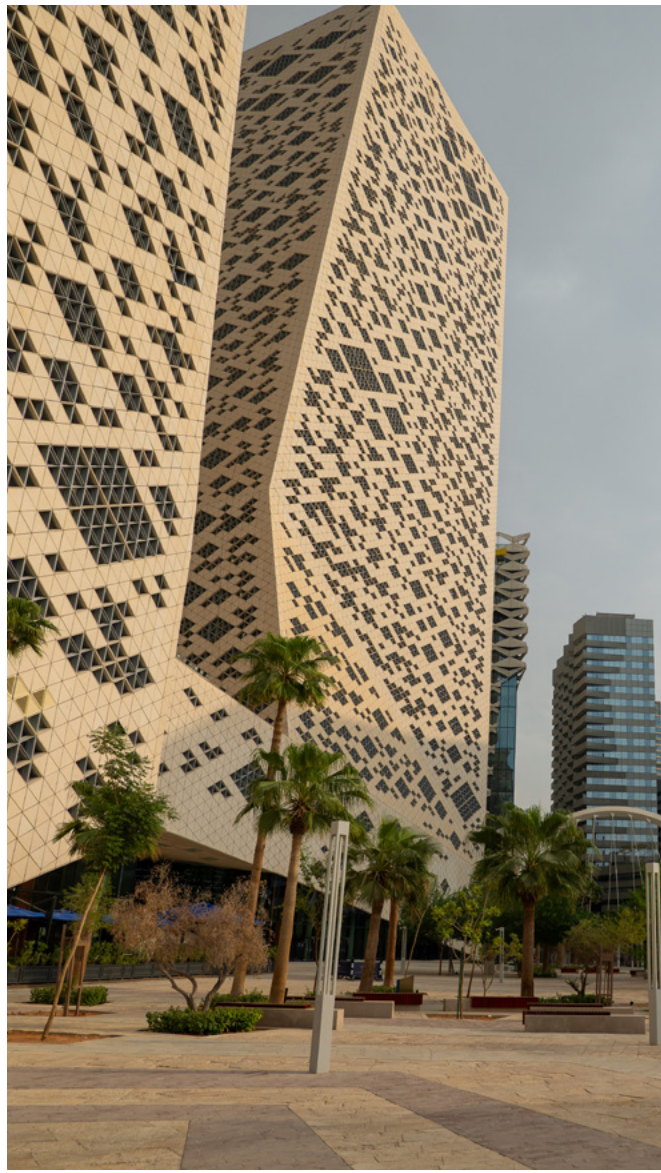
On 31 January 2025, Barclays Bank, a global systemically important bank (G-SIB), experienced a catastrophic IT outage lasting over 24 hours. The timing could not have been worse: it coincided with both payday for millions of UK workers and the HMRC self-assessment tax deadline.

Impact summary

- Online payment attempts failed over a three-day period
- Customers were unable to access accounts, make rent payments, complete house purchases, or pay suppliers
- Compensation costs reached £5-7.5 million for this incident alone (Financial Times)
- Root cause was identified as a software issue within UK mainframe operating system (not a cyber-attack)
- UK Treasury Committee investigation launched; regulatory scrutiny intensified

Key lesson

The Treasury Committee found that UK banks accumulated 803 hours of outages across 158 separate incidents between January 2023 and February 2025. This represents over 33 days of cumulative service disruption, **roughly one month worth of banking system failures over 2 years**, underscoring that operational resilience failures are not isolated events but systemic challenges requiring sustained investment.



Case study 2

CrowdStrike global IT outage (July 2024)

A flawed software update from cybersecurity firm CrowdStrike caused what has been called 'the largest IT outage in history,' affecting 8.5 million Windows workstations globally, including financial institutions.

Impact summary

- Estimated US$5.4 billion in damage to Fortune 500 companies alone (CNN).
- European banks experienced temporary IT outages affecting retail banking services.
- UK CHAPS (high-value payment system) experienced four-hour outage on same day due to Swift dependency.
- Banks in South Africa reported customers unable to make card payments.
- Highlighted concentration risk: single cybersecurity vendor could create systemic disruption.

Key lesson

Third-party risk extends beyond traditional vendors to include cybersecurity tools themselves. Banks cannot outsource accountability, even when disruption originates from a third party, the bank remains responsible for service continuity under regulatory frameworks like SAMA's operational resilience and TPRM requirements.

Case study 3

ICBC ransomware attack (November 2023)

The world's largest bank by assets, Industrial and Commercial Bank of China (ICBC), suffered a ransomware attack on its US financial services division, demonstrating that even the largest institutions are vulnerable and that cyber incidents can have systemic implications.

Impact summary

- US Treasury market disruption: US$60-plus billion in Treasury repo fails, the highest since March 2020 (resecurity).
- Manual processing required. Staff reportedly used USB drives carried by messengers to settle trades.
- Contributed to weak 30-year Treasury bond auction; primary dealers forced to an unusually high share of the issue, and with broader selling pressure in Treasuries and U.S. equities (reuters).
- Sharp selloff in Treasuries; S&P 500, Dow, and Nasdaq all closed lower.
- Root cause: Unpatched Citrix vulnerability (CVE-2023-4966) exploited by LockBit ransomware group.

Key lesson

This was the first ransomware attack to directly disrupt the US Treasury market, one that underpins global finance. The incident demonstrated that without the broader operational resilience measures in place, considering the important business services lens, a cyber-attack on a single institution can have cascading systemic effects on global financial stability.

Case study 4

TSB Bank IT migration disaster (2018)

TSB's attempted migration to a new core banking platform resulted in one of the worst IT failures in UK banking history and remains the benchmark for operational resilience failures.

Impact summary

- **1.9 million customers** (out of 5.2 million) locked out of their accounts (ekco)
- **225,492 customer complaints** received within the first year (Futurum)
- **£32.7 million** paid in customer compensation (Futurum)
- **£48.65 million regulatory fine** (would have been £69.5 million without settlement discount) (Bank of England)
- **Total cost: over £378 million** including operational costs, remediation, and lost business (bbc)
- **80,000 customers** lost due to the incident (bbc)
- CEO Paul Pester resigned; CIO Carlos Abarca personally fined £81,620 (Bank of England)
- **Recovery time: 8 months** until return to normal operations (December 2018) (Bank of England)
- **Root causes identified by regulators**
  - Overly ambitious migration timeline based on very little information
  - Insufficient testing with critical testing principles deviated from to meet deadlines
  - Inadequate third-party risk management and no formal due diligence on key supplier
  - Poor business continuity planning: expected 2,000 complaints but received 37,000 in first week (protechgroup)
  - Only one of two data centers tested before go-live

Key lesson

It is vital to rigorously test core system migrations, enforce strong third-party risk management, and maintain robust contingency plans, prioritizing resilience over speed to prevent catastrophic outages, regulatory penalties, and reputational damage.

Global perspectives on operational resilience in financial services

Regulators such as the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) in the UK, the EU's Digital Operational Resilience Act (DORA), and the Basel Committee's Principles for Operational Resilience all converge on a common theme: firms must anticipate, withstand, and recover from severe but plausible disruptions. They must shift focus from looking only inwards at firms' health KPIs to looking outwards at protecting customers from harm and the wider market from instability.

The UK framework in particular required full compliance by 31 March 2025 and defined the following fundamental operational resilience activities:

- Identifying important business services and setting impact tolerances for maximum tolerable disruption, considering customer harm, market stability and firm safety
- Mapping resources and dependencies supporting each important business service across five key pillars:
  - Processes: the set of repeatable steps to deliver a service to the end customer
  - People: the workforce that executes processes, makes decisions, and responds to disruptions
  - Technology: the applications, infrastructure, data centers, and networks that enable service delivery
  - Data: the information assets that flow through systems and enable decision-making
  - Third Parties: the vendors, partners, and infrastructure providers upon whom services depend
- Designing and running scenario testing within impact tolerances, bringing together the different functions and resource dimensions to enable a holistic identification of vulnerabilities

DORA became fully applicable on January 17, 2025, establishing a comprehensive prescriptive digital operational resilience framework with focus on:

- ICT risk management framework: comprehensive policies covering identification, protection, detection, response, and recovery
- Incident reporting: mandatory notification of major ICT-related incidents to competent authorities
- Digital operational resilience Testing: regular testing including threat-led penetration testing (TLPT)
- Third-party risk management: stringent requirements for ICT third-party service providers
- Oversight framework: Direct EU-level supervision of critical ICT third-party providers

While the case studies above illustrate the cost of failure, several global banks have emerged as leaders in operational resilience, investing proactively and building capabilities that Saudi institutions can learn from. JPMorgan Chase for instance, the largest US bank by assets, has made cybersecurity and operational resilience a cornerstone of its strategy following a major data breach in 2014 that affected 83 million customers. US$1.5 trillion Security and Resiliency Initiative was announced in 2025 for their strategic investments.

Similarly, DBS Bank Singapore has been recognized by Harvard Business Review as one of the top ten strategic transformations of the decade. Their initiatives include built-in resilience into platforms and data centers as core principle, and 'Not if, but when' philosophy regarding attacks. Another example is Standard Chartered's approach to operational resilience spanning their operations across Asia, Africa, and the Middle East, providing insights relevant to Saudi institutions operating in diverse regulatory environments. Most notably, they implemented the multi-dimensional resilience approach across cybersecurity, data quality, IT resilience, product resilience, and geopolitical resilience.

Key challenges facing banks in Saudi Arabia

Although SAMA has not yet published a specific operational resilience framework or detailed guidance for financial services firms to follow, the regulator's approach to supervision has evolved significantly. Extended on-sites examinations, technical validation of actual capabilities, and forensic analysis of operational evidence have replaced documentation-focused assessments. The banks are facing increased pressure to address core operational resilience processes and capabilities.

01 Organizational challenges

Saudi financial institutions face significant challenges in building operational resilience capabilities, starting with organizational challenges that make building operational resilience a complex task. Key functions such as business continuity, disaster recovery, cybersecurity, and third-party risk often operate in silos, creating fragmented capabilities. Adding to the challenge is the absence of a unified resilience strategy and framework, unclear accountability for end-to-end service resilience, and resource constraints driven by competing priorities. Cultural perceptions also play a role, with resilience frequently seen as a compliance checkbox rather than a strategic imperative.

02 Foundational gaps

Foundational gaps further complicate the resilience journey. Many institutions lack complete and accurate asset inventories, relying on scattered spreadsheets and disconnected tools instead of a single source of truth. Architectural documentation is often incomplete or outdated, leaving critical blind spots. Hidden single points of failure and reliance on aging legacy systems introduce vulnerabilities that threaten service continuity and stability.

03 Technical complexity and third-party dependencies

These add another layer of risk. Banks face intricate webs of applications, databases, and networks that require comprehensive mapping to ensure resilience. Moving toward active-active architectures demands significant structural changes, while growing reliance on cloud providers must align with regulatory expectations from SAMA. The expanding fintech ecosystem introduces additional dependencies, making resilience management a moving target in an increasingly interconnected financial landscape.

Critical considerations for an operational resilience journey

Successfully building operational resilience requires a structured, integrated, and phased approach addressing foundational gaps while building toward mature, sustainable capabilities.

Establish strong governance foundations

Take a service-centric view

Build foundational capabilities first

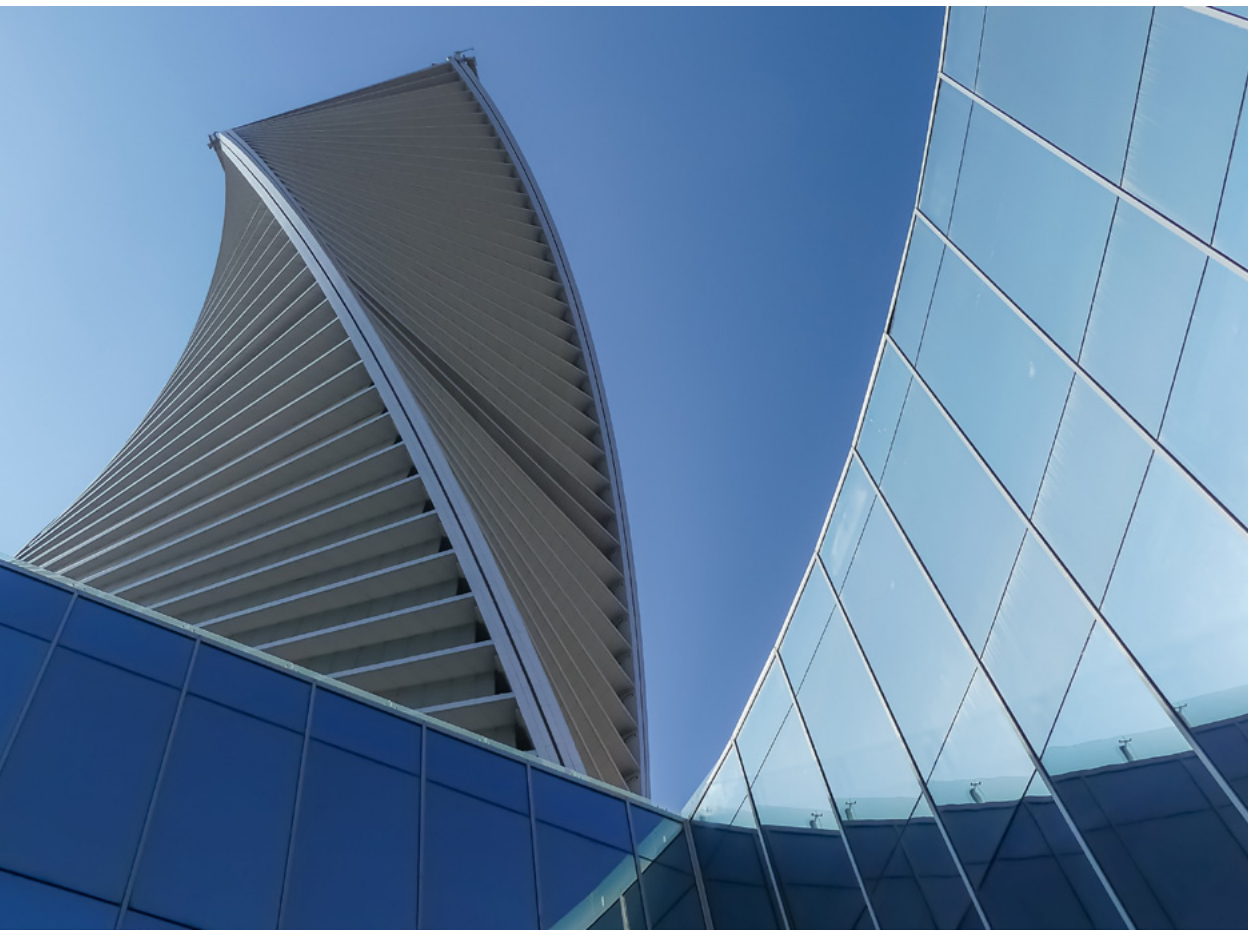
Implement comprehensive testing

Address third-party risk systematically

Hover your cursor on each step to find out more.

By taking these steps, the bank increases its resilience and therefore its reliability in the market, which becomes a key differentiator as digital banking becomes ubiquitous. Moreover, mature resilience capabilities create constructive regulatory relationships and build regulatory confidence in the bank.

How KPMG can help



KPMG has developed a multi-solution capability to enable an integrated delivery model bringing the most added value to our clients in shaping and implementing their operational resilience transformation: risk advisory supported by BCM, technology and cybersecurity, with access to KPMG's global network of resilience specialists and Saudi-based team who has a hands-on experience executing operational resilience activities for UK, EU and tier-1 global banks.

KPMG's operational resilience market-leading framework was developed in close consultation with regulators. This reduces risk and accelerates delivery. The framework and associated toolkit have supported more than 300 financial services firms globally over the last seven years to design and embed operational resilience into business-as-usual and foster resilience by design mindset.

Moreover, our experience working directly with SAMA provides us with an understanding of local regulatory requirements, while bringing international best practices to Saudi banks.

KPMG's experience working with Saudi banks and other organizations align with requirements for operational resilience improvements, including enhancing IT governance and asset management, implementing improved enterprise configuration management database (CMBD), designing active-active architecture for core banking and payment systems, enhancing incident management and business continuity, as well as rolling out scenario testing and vulnerability remediations.

The way forward

It is clear that financial institutions in Saudi Arabia face a defining moment. SAMA's evolving supervision has made clear that superficial compliance is no longer tenable. Organizations that build robust operational resilience capabilities will not only satisfy regulatory requirements, they will build competitive advantage.

- SAMA's intensified supervision is exposing fundamental gaps in how banks define their important business services, manage technology assets, and set up their recovery capabilities
- The cost of reactive remediation and regulatory fines observed globally after adverse findings far exceeds proactive investment in building sustainable operational resilience capabilities
- Banks that embed resilience into their culture and prioritize resilience over speed will be better positioned to support Vision 2030 objectives and serve the evolving needs of Saudi customers
- Successful resilience requires an integrated approach spanning strategy, governance, tech, cyber, and third-party risk, under C-suite accountability, often anchored with the COO, not fragmented compliance silos.
- Rigorous operational resilience scenario testing and intelligent timely remediations are the key differentiators of a proactively resilient organization ready to weather any storm.

Lessons learned from the global market as well as the efficiency brought by the introduction of AI tools in recent times, bring a great advantage for banks to act fast and accelerate their operational resilience.

The investment required is significant. The cost of inaction is far greater. Banks pursuing compliance theaters will face ongoing regulatory pressure, expensive emergency remediation, and competitive disadvantages.

Operational resilience is the foundation upon which Saudi Arabia's financial services sector will build its digital future. The time for action is now.

About KPMG Middle East

KPMG Middle East LLP is a part of the KPMG global organization of independent member firms that operate in 143 countries and territories and are affiliated with KPMG International Limited. We provide audit, tax and advisory services to public and private sector clients across Saudi Arabia, United Arab Emirates, Jordan, Lebanon, Oman, and Iraq, contracting through separate legal entities. We have a strong legacy in the region, where we have been established for over 50 years. KPMG Middle East LLP is well-connected with its global member network and combines its local knowledge with international expertise.

KPMG serves the diverse needs of businesses, governments, public-sector agencies, not-for-profit organizations, and the capital markets.

Our commitment to quality and service excellence underpins everything we do. We strive to deliver to the highest standards for our stakeholders, building trust through our actions and behavior, both professionally and personally.

Our values guide our day-to-day behavior, informing how we act, the decisions we make, and how we work with each other, our clients, and all our stakeholders.

Integrity:
We do what is right

Excellence:
We never stop learning and improving

Courage:
We think and act boldly

Together:
We respect each other and draw strength from our differences

For Better:
We do what matters.

Our purpose is to inspire confidence and empower change. By inspiring confidence in our people, clients and society, we help empower the change needed to solve the toughest challenges and lead the way forward.

KPMG's Our Impact Plan guides our commitments to serving our clients, people and communities across four categories: Planet, People, Prosperity, and Governance. These four priority areas assist us in defining and managing our environmental, social, economic and governance impacts to create a more sustainable future. We aim to deliver growth with purpose. We unite the best of KPMG to help our clients fulfil their purpose and deliver against the United Nations Sustainable Development Goals, so all our communities can thrive and prosper.

We are dedicated to delivering growth with purpose, helping our clients achieve their goals, and advancing sustainable progress to ensure that all our communities thrive. Empowered by our values, and committed to our purpose, our people are our greatest strength. Together, we are building a values-led organization of the future. For better.

Contact us

Yousaf Mir

Partner
Financial Services Lead – Advisory
KPMG Middle East
ymir@kpmg.com

Marcus Threadgold

Partner
Operational Resilience Lead
KPMG Middle East
mthreadgold1@kpmg.com

Ton Diemont

Partner
Cybersecurity Lead
KPMG Middle East
antondiemont@kpmg.com

Petra Daher

Associate Director
Operational Resilience
KPMG Middle East
pdaher@kpmg.com

Follow us on:

Designed by KPMG ME Design Studio

Publication name: Operational resilience as strategic imperative
Publication number: 5780
Publication date: January 2026