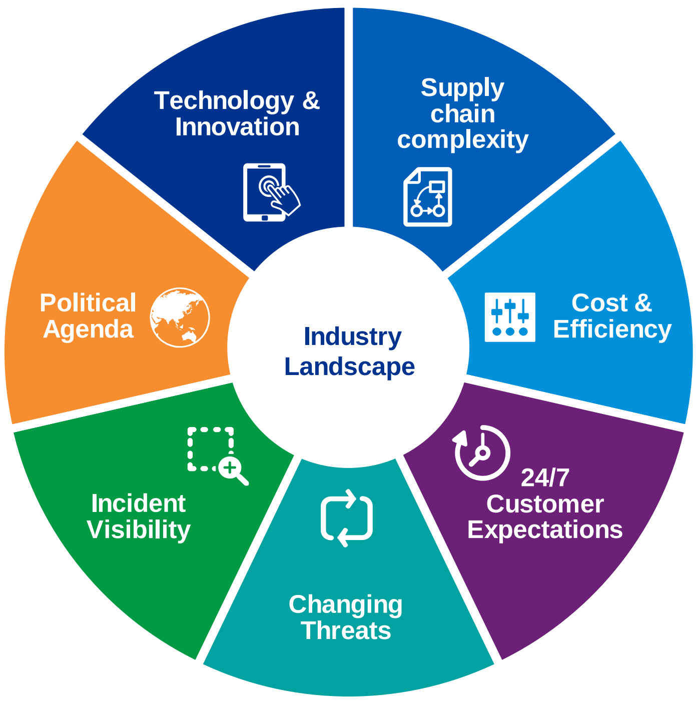
The art of adapting to a changing environment

Operational resilience in Financial Services

Operational resilience is usually defined as an organisation's ability to adapt to rapidly changing environments. This includes the resilience of systems, processes and people and more generally the organisation's ability to continue to operate during disruptive events.

Crisis management becomes BAU

The world, and Hong Kong in particular, has seen its fair share of disruptive events in recent times. Over the past twelve months, we have seen the global spread of the novel coronavirus (COVID-19), social unrest in Hong Kong and uncontrollable wildfires in Australia, among many other significant global and regional events that have severely impacted the day-to-day lives of many people, and the "business-as-usual" operations of many organisations across sectors, including financial services. These disruptions have not been one-off short-term disruptions, but instead, significant enough to force organisations to permanently adapt their ways of working to ensure that they are able to operate under the "new normal".



A broader view of resilience is emerging

Operational resilience has always been an important area of focus for financial institutions, their regulators and supervisors. However, the discipline of resilience was in general more targeted towards specific areas of risk such as cybersecurity or outsourcing. Today, organisations and regulators are starting to take a broader view of resilience covering all risks to the provision of business services.

The magnitude of disruption the industry has experienced means that the financial services sector needs to look at operational resiliency as more than just another compliance exercise – it needs to be part of each organisation's overall strategic plan. Companies need to move away from being reactive to begin proactively planning for not "if" but "when" circumstances change, and strongly consider that these changes may likely be permanent.

Leading banks have adopted the following guiding principles:

- A top-down led approach to operational resilience driven by senior management and the board of directors.
- Embed an operational resilience mindset within the bank's culture.
- Identify and map out the people, data, systems, processes and third parties that support key business services to ensure the end-customer always receives a complete service experience.
- Define threshold tolerances (based on key measurements used in the services) and use extreme scenarios to conduct end-to-end testing.
- Develop approaches beyond traditional BCP planning to focus through a business lens on managing disruption.
- Define appropriate escalation paths and decision-making procedures combined with effective and timely communication plans.
- Assume that disruption <u>will</u> occur.

An enterprise-wide discipline that goes beyond compliance

With this in mind, operational resilience becomes a new end-to-end discipline that requires all parts of the organisation to work together. From what we have seen, organisations are and have been getting better at responding quickly to day-to-day resilience challenges. The focus has been largely on crisis management and 'keeping things going' as much as possible. Our view is that organisations need to start shifting to a more medium and long-term view to really embed resiliency across the board. We have outlined below some of the critical elements that need to be in place, and what this means for the short and medium term.

Critical elements	Capabilities that need to be in place	Longer-term considerations
Operational Resilience Strategy and Operating Model	• Clear Strategy, Operating Model • Enterprise-wide Governance and defined roles and responsibilities	• Do we have a clear view of which services are key to our clients and have we mapped those to our people, technology, facilities and data? • How well has our Operational Resilience Framework operated during recent disruption? • What adjustments need to be made to enhance the framework and clarify roles and responsibilities? • How do we measure the resiliency of our key operational processes?
Customer Experience and Service Management	• Customer expectation and behaviour monitoring • Service catalogue • Service criticality • Service level agreements	• How have consumer behaviours changed, and where are we likely to see permanent adjustment e.g. e-payment adoption, branch usage, digital banking? • Did we have the right criticality of service assessment, and to what extent are adjustments needed?
Third Party/ Supplier Management	• Third party risk management • Contract lifecycle management • Contingency and exit planning	• How has the ongoing disruption impacted on our third and fourth party risk? Do we need to adjust our supplier due diligence assessments and put in place mitigants? • Have we considered end-to-end supply chain risks and sustainability?
Resilience Assessments	• Assessment Framework • Remediation • Risk Radar Scanning	• Have we been monitoring the right risks and do we need to make changes to our risk assessments? • Has our risk appetite changed?
People and Culture	• Resilience Culture and Change Management • Agile ways of working	• How have we managed the people aspects during disruption and do we need to make adjustments to oversight and monitoring, talent management, ways of working, succession planning? • Have we considered the impact of disruption on our location footprint and how we are regionally interconnected?
Scenario Analysis	• Impact assessment • Thresholds • Testing	• Do we need to make adjustments to our stress tests and scenarios? • Are thresholds still relevant for our way of working e.g. trading from home or BCP site? • Have we considered new and emerging threats e.g. fraud risks?
Tooling, Data and Reporting	• Data Analytics • Enterprise tools • Reporting	• Have we got the right data analytics capability and tools to monitor and predict the impact of resilience events?
Recovery Planning	• BCM • Disaster Recovery • Incident response • Communications	• Have there been gaps in our crisis and incident response and lessons learnt that we need to factor into BAU recovery planning?

A focus on operational resilience pays off

We can see that a broader approach to operational resilience is paying off. A more coordinated approach coupled with business or service simplification can result in efficiency and cost savings. A strategic and analytics-driven process can allow for better customer and supplier experience and more dynamic risk management. In addition, a strong and coordinated framework helps with regulatory compliance. With an increased regulatory focus on resilience as well as likely ongoing disruption, it makes sense to tackle this topic today.

By adopting these guiding principles, banks will be able to experience five key areas of benefit:

Business benefits of operational resilience

- **Allow better work in a dynamic ecosystem e.g. use of Fintech and start-ups**
- **Generate synergies across strategic, financial and operational resilience**
- **Reduce operational risks and the costs of disruption**

  Enhance Governance and inter-regional/ global collaboration
- **Allocate resources more effectively and efficiently**

  Improve supplier and third party relationships
- **Enhance customer (buy-side and sell-side) trust and loyalty**

Regulators are beginning to issue standards covering operational resilience

Regulators in the UK recently issued a number of consultation papers on this topic and we expect other regulators to follow. The UK Prudential Regulation Authority (PRA) has proposed a framework designed to strengthen the ability of banks and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions. The objective of these proposed requirements is to ensure that when a disruption occurs, banks will have robust and reliable arrangements in place to deal with it. These arrangements will have previously been tested. Banks will also be able to show that they are operationally resilient, both to themselves and to the supervisory authorities. The first step is for banks to identify their important business services by considering how disruption to the business services they provide can have impacts beyond their own commercial interests including, where relevant, harm to consumers and to market integrity, and threats to policyholder protection, safety and soundness, and financial stability. Other elements of the proposed approach are set out below:

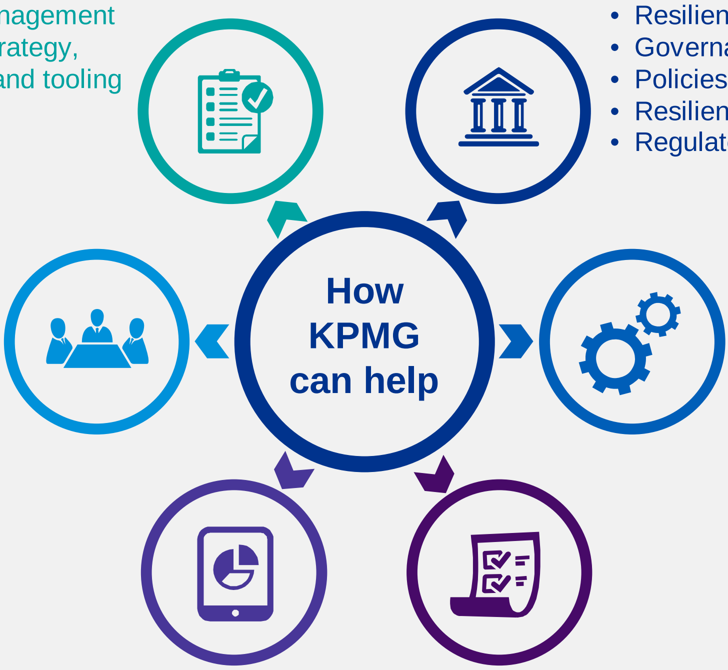
1. **Identification of important business services**
2. **Identification of metrics to cover the maximum tolerable level of disruption**
3. **Mapping of people, processes, technology, facilities and information**
4. **Scenario testing for appropriate range of adverse circumstances**
5. **Identification and remediation of vulnerabilities**

How KPMG can help

KPMG has been helping its clients set up their Operational Resilience Framework and Target Operating Models:

Third party risk management
- Supply Chain Management
- Third party risk strategy, operating model and tooling

Effective Governance
- Resilience strategy
- Governance
- Policies and procedures
- Resilience culture and awareness
- Regulatory requirements



Recovery and response
- Crisis management
- Incident response
- BCP and Disaster Recovery
- Communication management
- Talent management

Target Operating Model
- Governance
- Organisational accountability, roles and responsibilities
- Legal entity and booking strategy
- Location strategy
- Customer Experience
- Critical service definition
- Process and systems alignment
- Business case definition

Analytics
- Data requirements assessment
- Data Management
- Management reporting and KPIs

End-to-end testing
- Tolerance setting
- Scenario analysis
- Risk based test plan
- Testing execution

Contact us

Isabel Zisselsberger
Partner, Hong Kong,
KPMG China
+852 2826 8033
isabel.zisselsberger@kpmg.com

Tom Jenkins
Partner, Hong Kong,
KPMG China
+852 2143 8570
tom.jenkins@kpmg.com

Sean Ren
Associate Director, Hong Kong, KPMG China
+852 3927 5818
sean.ren@kpmg.com

kpmg.com/cn