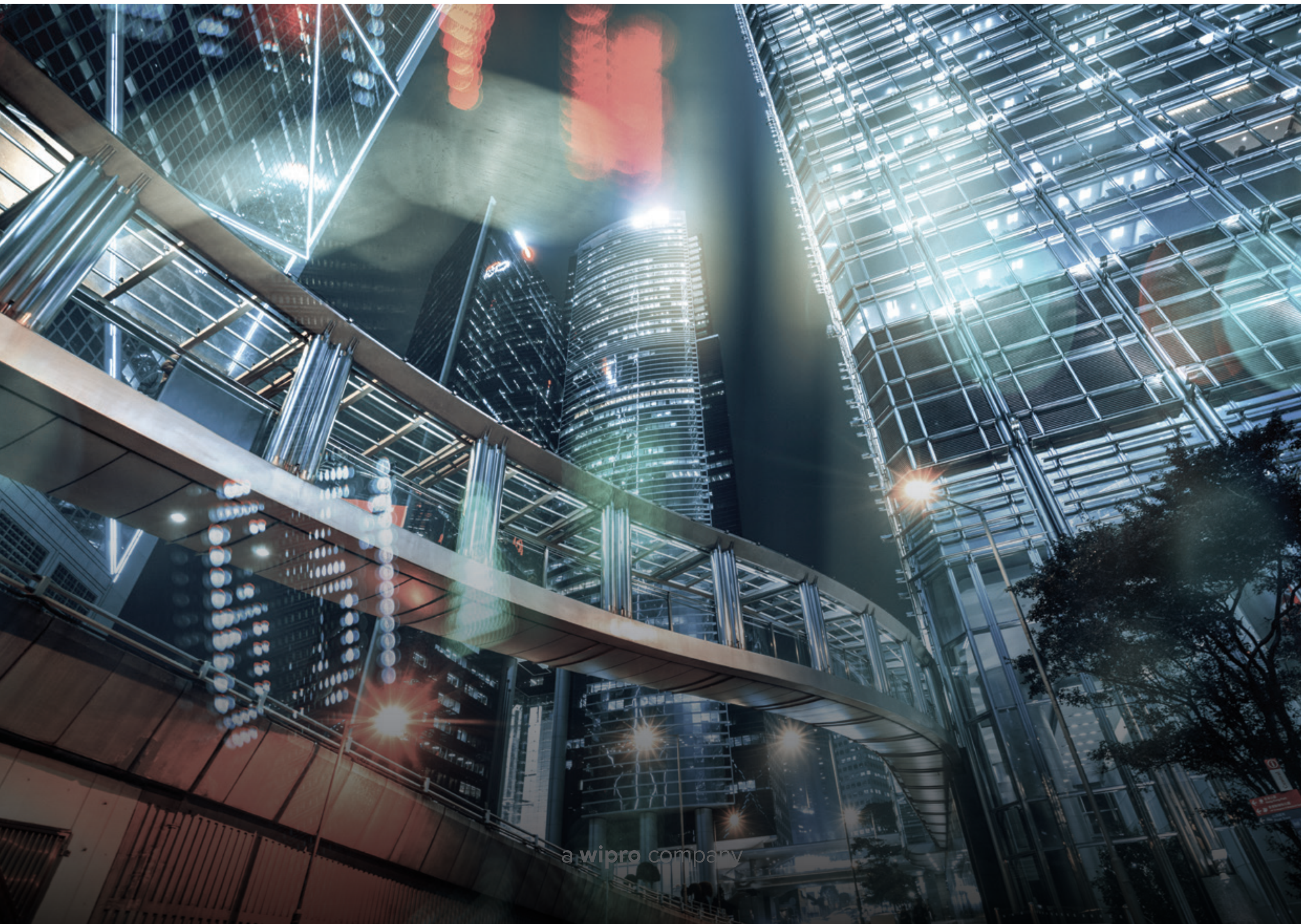
CAPCO

TACKLING HKMA OPERATIONAL RESILIENCE STEP BY STEP



a wipro company

INTRODUCTION

Operational disruptions including pandemics, cyber-attacks, technology failures, and the effects of climate change, can threaten the viability of firms, and cause instability in the broader financial system. To ensure that banks are well prepared to mitigate the potential harm, Hong Kong Monetary Authority (HKMA) launched a consultation[1] in December 2021 to align the previous Supervisory Policy Manual (SPM) with the Basel Committee on Banking Supervision's Principles for Operational Resilience, released in March 2021.[2] The consultations closed in early 2022, and by May 2022 the HKMA had issued the new requirements and a revised timetable for implementation – as we discuss in the next section.

Although in its new operational resilience requirements HKMA addresses the banking industry specifically, all financial institutions should consider the far-reaching impact of significant disruptions to their own operations, and the benefits they can derive by embedding operational resilience into their business-as-usual activities. Resilient firms can recover more quickly and effectively from a significant disruption to best serve clients and markets. However, achieving true operational resilience requires a shift in mindset away from resilience as a 'check-the-box' compliance exercise towards resilience as a key organizational capability that must be continuously improved.

To align with the Basel Committee, the HKMA has proposed a new SPM module on operational resilience (OR-2) as well as some amendments to previous SPM modules on operational risk[3] (OR-1) and business continuity planning[4] (TM-G-2). HKMA will assess the effectiveness of bank operational resilience frameworks through a combination of risk-focused on-site examinations, off-site reviews, and prudential meetings.

This paper looks at the timeline for taking action to meet the new requirements and discusses the series of steps that financial institutions need to take to achieve and sustain operational resilience. We offer insights drawn from our experiences in this area, intended to catalyse industry thinking on how to build the resilience needed to operate in these challenging and disruptive times.

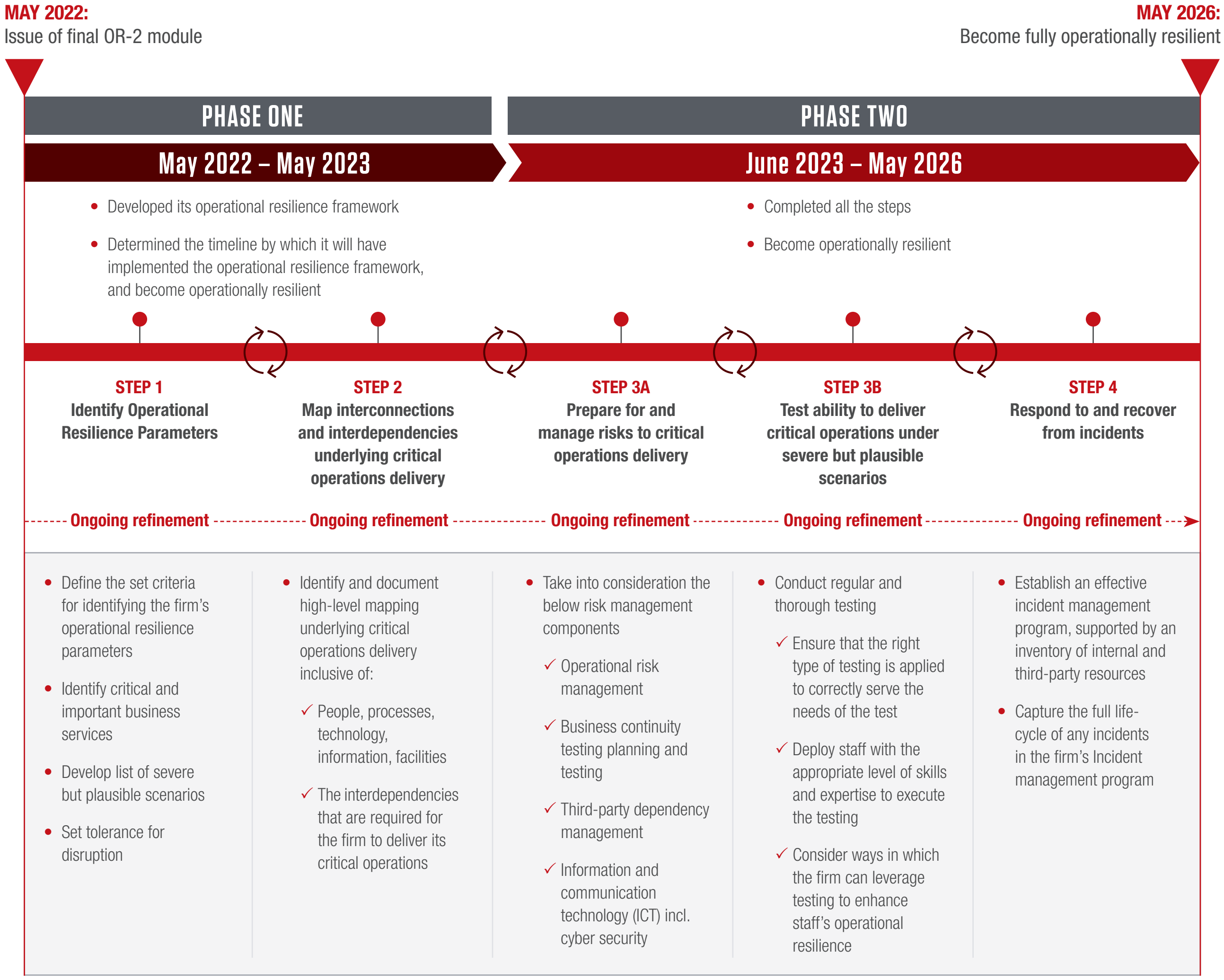
TIMELINE

The consultation on the new requirements closed on February 4, 2022. Under the HKMA's confirmed timeline, by 31st May 2023, authorized institutions are expected to have i) developed an operational resilience framework; and ii) determined the timeline by which they will have implemented the framework and become operationally resilient.

After 31st May 2023, banks are expected to become operationally resilient as soon as possible. By 31st May 2026, authorized institutions are expected to be operationally resilient.

Firms should not delay in identifying their key operational resilience parameters and starting a process mapping program, with the aim of meeting the indicative timeline and steps proposed in the consultation paper. The timeline below includes our own estimates of the approximate time each key step might take.

TIMELINE: COUNTDOWN TO OPERATIONAL RESILIENCE



MAY 2022:
Issue of final OR-2 module

MAY 2026:
Become fully operationally resilient

PHASE ONE

May 2022 – May 2023

- Developed its operational resilience framework
- Determined the timeline by which it will have implemented the operational resilience framework, and become operationally resilient

PHASE TWO

June 2023 – May 2026

- Completed all the steps
- Become operationally resilient

STEP 1
Identify Operational Resilience Parameters

- Define the set criteria for identifying the firm's operational resilience parameters
- Identify critical and important business services
- Develop list of severe but plausible scenarios
- Set tolerance for disruption

STEP 2
Map interconnections and interdependencies underlying critical operations delivery

- Identify and document high-level mapping underlying critical operations delivery inclusive of:
  - ✓ People, processes, technology, information, facilities
  - ✓ The interdependencies that are required for the firm to deliver its critical operations

STEP 3A
Prepare for and manage risks to critical operations delivery

- Take into consideration the below risk management components
  - ✓ Operational risk management
  - ✓ Business continuity testing planning and testing
  - ✓ Third-party dependency management
  - ✓ Information and communication technology (ICT) incl. cyber security

STEP 3B
Test ability to deliver critical operations under severe but plausible scenarios

- Conduct regular and thorough testing
  - ✓ Ensure that the right type of testing is applied to correctly serve the needs of the test
  - ✓ Deploy staff with the appropriate level of skills and expertise to execute the testing
  - ✓ Consider ways in which the firm can leverage testing to enhance staff's operational resilience

STEP 4
Respond to and recover from incidents

- Establish an effective incident management program, supported by an inventory of internal and third-party resources
- Capture the full life-cycle of any incidents in the firm's Incident management program

Source: HKMA[5] and Capco estimates

KEY NEXT STEPS FOR HONG KONG BANKS AND FINANCIAL INSTITUTIONS

Traditional planning and long-established risk management tools and processes are essential – but typically insufficient to meet fast-evolving or emerging challenges. They must be complemented by more agile arrangements that help financial institutions to adapt and learn. Below we outline the steps financial institutions need to consider to achieve and sustain this kind of adaptive operational resilience, and offer insights drawn from our experiences.

While HKMA has assigned Operational Risk Management (ORM) and Business Continuity Planning (BCP) to Step 3a (i.e., Preparing for and managing risks to critical operations delivery) in its proposed framework, it is imperative to also consider ORM and BCP elements right from the start, while planning for the operational resilience program, to ensure that the selected framework covers all essential components without duplicating efforts and resources.

Step 1: Determining operational resilience parameters

Due Date: To identify critical operational resilience parameters by 31st May 2023; to meet all HKMA requirements by 31st May 2026

HKMA recommends that firms test their ability to remain within their impact tolerances for each of their critical business services in the event of a severe but plausible disruption of their operations. This enables firms to be assured of the resilience of their critical business services and identify where they might need to act to increase their operational resilience.

The key challenge here is that determining operational resilience parameters – identifying critical operations, setting impact tolerances and identifying severe but plausible scenarios – must be customized to each institution. That means, as our summary table below sets out, that the organization needs to communicate with stakeholders, make the appropriate selections based on its unique offerings and quickly formulate a robust plan that enables reprioritization during macroeconomic shifts or other major operational-risk related events.

KEY CONSIDERATIONS FOR STEP 1

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Identify critical operations	**No 'one-size-fits-all' model** • HKMA expects that there should be a clear logic applied in selecting critical operations and in derivation of impact tolerances • While on the surface, the offerings of many firms appear similar, there are **differences in detail**, e.g. customers, geographies, meaning every firm will need to approach the **selection from a fresh start**	• Making the appropriate differentiation between critical and non-critical activities **based on the organization's unique offerings** is crucial so that a firm can focus on the essential elements of its operations in the face of extreme disruption	**Vulnerability identification** • Review the people, processes and technology that deliver critical operations, including third-party service providers
Set tolerance for disruption	**Stakeholders may have different levels of tolerances for the same impact** • Stakeholders could have varying impact tolerances depending on their interests and responsibilities	• **On-going and close coordination with senior management and stakeholders** is necessary to define impact tolerances for operational threats and vulnerabilities	**Critical operations & impact tolerance assessment** • Set impact tolerance for each critical operation at the point where disruption becomes intolerable and then robustly validate the tolerance level with stakeholders
	Lack of risk tolerance benchmark • By framing recovery in terms of the bank's own risk tolerance, it sets a lower standard that is internally focused without giving any guidance on what good looks like • In this complex and interconnected environment, **setting tolerance** that aligns with **multiple regulatory obligations** can be difficult for a global organization	• **Basis of determining impact tolerances** should be assessed from the **top-down**, based on the impact on clients, impact on market stability/integrity and impact on the soundness of the firm • **Establish a minimum base standard across global programs** and design organization-wide training on operational resilience concepts so that understandings and expectations can be aligned across regional operations	**Critical operations & impact tolerance assessment** • Review the services offered by a firm and **rate them** by the impact on **customers**, the **market** and the soundness of the firm if disrupted
Identifying severe but plausible scenarios	• **Prioritizations of events** may be challenging due to unexpected macro-economic shifts	• **Identify scenarios** against macro-economic shifts from impacted industries, clients and counterparties to understand the ways critical functions may shift and **reprioritize through different periods**	**Scenario analysis** • **Create a library** of severe but plausible events and independently select which to apply • **Identify transmission pathways** into the delivery processes, and evaluate the impact on the steady-state and **response protocols** to assess whether impact tolerance for each service is breached

Step 2: Mapping interconnections and interdependencies underlying critical operations delivery

Due Date: To complete mapping within by 31st May 2023; to meet all HKMA requirements by 31st May 2026

An operationally resilient firm is expected to have a comprehensive understanding and mapping of the systems and processes that support its critical business services, including those systems and processes over which the firm may not have direct control, such as outsourcing and third-party service providers. By identifying and mapping operational dependencies and key interactions that provide the critical business service, firms can pinpoint where disruptions could have the greatest impact, determine how best to support their resilience, and develop more effective contingency or business continuity plans.

The primary challenge associated with system and process mapping is understanding and identifying interdependencies regarding supply chains, which are mostly multi-layered. This challenge is best solved by creating and analyzing an organization's 'digital twin', that is, a digital representation of the company's real systems. Firms can navigate the digital model layer by layer to visualize and identify interconnections without disrupting their day-to-day activities.

KEY CONSIDERATIONS FOR STEP 2

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Map internal and external dependencies	**Understand interdependencies with third parties thoroughly** • Not only do organizations need to understand their internal workings thoroughly to **identify critical activities** effectively, but they also need to **understand** how each of these activities is underpinned by third-party suppliers • Considering the size and scale of financial institutions, this is no simple task – and yet **more complexity** is added by the multi-layered nature of supply chains	• Methodologies such as creating **'digital twins'** can turn this step into a better representation of the reality on the ground and **deliver greater utility** in managing incidents and process design	**Digital twin** • Use a cutting-edge approach to create a **'digital twin'** that dynamically **identifies interconnections** and can be used for vulnerability assessments, scenario testing and incident management

Step 3a: Preparing for and managing risks to critical operations delivery

Due Date: To meet all requirements by 31st May 2026

This is a key step that ensures banks have a robust operational risk management (ORM) framework in place, have a robust approach to business continuity and testing, manage their third-party dependencies, and address all their ICT vulnerabilities, including cyber security.

3a.1 Operational risk management

HKMA is keen that banks explore connections between their ORM frameworks and their approach to operational resilience. This is because operational risk management contributes to operational resilience. Furthermore, operational risk management frameworks can be retrospective in nature, driven by control failings and losses only after they have happened. A process that does not appear to have much operational risk based on empirical evidence (e.g., very few actual losses) may be inherently unsound with a very low tolerance for any disruption – and hence, not operationally resilient. Therefore, specific leading indicators might need to be incorporated into the existing ORM framework, and all risk-related functions should be adequately trained and informed to ensure alignment with the operational resilience program.

KEY CONSIDERATIONS FOR STEP 3A

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Ongoing identification, documentation and management of operational threats with the potential to disrupt critical operations	• ORM processes **need to evolve as risks shift**. Therefore, assessments based on past performances could be irrelevant or misleading • Ongoing update of material risk inventory that includes potential disruptive events would be essential	• ORM should focus not only on past performance but also **forward-looking risk indicators** to provide insights on how the process should/ could evolve	• **Design and implement risk transformation programs** to comply with regulatory change initiatives, and meet emerging challenges, including risk frameworks and risk assessments
	• Existing ORM processes need to be reassessed to **ensure tighter alignment with risk tolerance, BCP, and third-party/ICT management processes**	• All risk-related functions, including internal audit, should be **adequately trained** and informed to ensure the consistency of operational resilience standards in operation risks evaluations • An **effective communication channel** will enable **transparency** and alignment among teams with different focus areas (e.g. ORM, BCP/ third-party due diligence/ scenario testing)	• Evaluate current state and **perform target state analysis** to tighten alignments with other focus areas in operational resilience program and enable more **effective communications** across departments

3a.2 Business continuity planning and testing

Most companies spend much of their time operating the business and only occasionally train to deal with a crisis. Armed forces around the world do the opposite. They spend the bulk of their time preparing to deal with the occasional crisis. Armed forces assume that they will operate in environments that they describe as VUCA – volatile, uncertain, complex, and ambiguous. They employ tactics built around the need to anticipate, detect, deter, withstand, respond, and recover from threats.

For instance, the 'OODA loop' is a highly effective framework used by militaries to respond better and faster in unstable environments. Each of the four phases (observe, orient, decide and act) is taken in isolation, improved in terms of both accuracy and time, and then recombined and repeatedly run as a cycle at pace to gain and retain the initiative. This concept can be put to work in conjunction with traditional response and recovery planning, to continually refine the operational resilience framework.

Set out below are some of the key lessons that can be drawn from a battle-tested approach to resilience and business continuity planning and testing.

KEY CONSIDERATIONS FOR STEP 3A

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Business continuity planning (BCP)	**Lack of coherence in crisis management** • Most organizations aim to have an enterprise-wide resilience program, but acknowledge that, in reality, this is not easily achieved • Particularly for banks, implementing any **centralized initiative** is challenging, considering their complex organizational structures • Therefore, BCP often focuses on specific business areas without considering the broader impact and **internal dependencies** across the organization	• The role of intelligence in the military is to build a **coherent understanding** of the opposition. While managing an event, the rate of information received is likely to be closer to the military tempo than normal/BAU business activity for a typical financial services firm. • Therefore, firms should look to **nominate and train a group of executives who can maintain a holistic picture** of what is going on externally and internally to feed information coherently into the operations room and executive committee during a major crisis.	**Business impact analysis** • Run scenarios through a **business impact assessment** to gauge disruptions and internal dependencies • Conduct **readiness assessments** to understand any gaps in the current process **Workforce model/dashboard** • Leverage data and machine learning to monitor employee capacity and internal dependencies to inform executives **Organizational strategy & design** • Determine size, shape, layers, the span of control, and geographical distribution for the new organizational design

KEY CONSIDERATIONS FOR STEP 3A CONTINUED

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Business continuity planning (BCP)	**Ineffective decision-making in volatile environments** • The key challenge that firms have when managing a disruptive event is in pivoting their decision making and execution approach from a BAU flat consultative one to a more top-down version while at the same time maintaining control and, to the extent necessary, consensus	• A key element of the military approach is that **command is achieved by relinquishing a part of control to others** • The commander is supported by an operations room that provides continuity to the response by acting as a **central point of contact** and executing decisions once they have been taken • With this separation, the commander has carved out **crucial time** to focus on making the right decisions • Firms should look to set up an **operations room** like the military example and ensure the individual filling the **leadership role** has sufficient seniority like a commander in an army to ensure their directions are taken seriously	• Craft **playbooks** for rapid workforce reorganization (personnel ramp up/down) and transition to steady-state • Define **interim workforce configurations** and accompanying operating models to support critical functions across geographies
Business continuity testing	**Training not being part of testing** • **Use of simulation testing** may lack the element of **human involvement**, which is essential in responding to **actual threats or crises**, rendering the testing procedures **inaccurate or ineffective** to respond to real-life threats	• Armed forces put significant effort and resources into undertaking training exercises to simulate the environment that units need to operate in • The training cycle usually **starts by focusing on the smallest element** before building up with each successive exercise. • After every exercise, there should be **a 'wash-up' session that runs through the events**, highlighting what went well and what could be improved. This is a key element in teasing out all the lessons and materially adds to the training benefits of the exercise. • **All the 'players' in the exercise should take part** to benefit from the experience fully	• **Establish and design testing exercises** that maximize employee involvement and help employees remain familiar with what to do
	• **Responses and recovery procedures** should be highly **adaptable** to a wide range of **volatile scenarios**	• Adopt the **'OODA Loop' approach** to respond to disruptive events and adapt responses to changing circumstances that may not be covered in the existing recovery procedures	**OODA loop** • Help implement OODA loop to improve decision making in changing circumstances

3a.3 Third-party dependency management

There is always a close relationship between banks and third-party providers. Third-party failures often result in operational disruption to banks themselves. However, firms often overlook dependencies on their suppliers and give little thought to contingency plans that address third-party failures. We recommend firms assess third parties' operational resilience levels more frequently and maintain an inventory of alternative suppliers to minimize the impact to business operations during severe disruptions.

KEY CONSIDERATIONS FOR STEP 3A

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Risk assessment and due diligence	• **Evaluation of third-party risk exposure** and operational resilience maturity may not be frequent enough since they are often assumed to be a **minor dependency** that would not affect core business functions	• **Assess** third-party operational resilience through **due diligence** on an ongoing basis • Include expectations for maintaining operational resilience in all formal agreements	• **Review** current SLAs, contacts, key factors in delivering services, information flows, the third parties BCP and recovery plans, cyber security and change protocols
Exit strategies	• Companies may be **over-relying on a few third parties** to provide and support core business services and operations	• Identify contingency service providers in the event a contractor is unable to support operations as a result of an incident or disruption • **Maintain an inventory** of potential third parties to which operations can be **transferred or outsourced** if a risk event impacts those already under contract	• **Review and develop** change control processes, early warning, backup, and recovery protocols • **Design and implement** an instant incidence response framework and playbook to **minimize reaction** time in the case of an incident that involves third parties

3a.4 Information and Communication Technology (ICT), including cyber security

CYBER-SECURITY

Amid escalating geopolitical tensions and increasing rates of cyber crime, there is a heightened risk that cyber-attacks could affect banks directly or have important knock-on effects by affecting third parties. According to S&P Global Ratings[6], the economic impact from such an attack could exceed the $10 billion estimated from the 2017 'NotPetya' attack, given increased interconnectedness and digitalization. Focusing attention on the early prevention and mitigation of cyber risks has become critical.

For most organizations, however, embedding resilience into their current cybersecurity model is difficult. Planning needs to take account of unforeseen short-term hazards resulting from misconfigurations, limited staff awareness, and security breaches from third parties. One way to address this is to implement additional protective measures that cover remote access capacity and enhance the financial institution's short-term cyber-security posture, while also adapting to longer-term operational changes.

KEY CONSIDERATIONS FOR STEP 3A

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Identify and address new cyber risks that emerge from changes in the operating model	**Technology Risks** • **Increased attack surface** due to change in operating model • **Reduced security posture** from misconfigurations /short-cuts used to set up new work environments rapidly **Systemic Risks** • **Heightened third-party risks** due to challenges in accessing third-party applications/infrastructure **People Risks** • **Limited staff awareness** of threats in the new operational environment	• **Review existing infrastructure** to enable remote work (e.g. VPN connections, security tokens, laptops), access capacity, bandwidth, and authentication mechanisms • **Add additional protective measures** to mitigate cybersecurity and data protection weaknesses	• **Review current operational setup** to identify, prioritize, and address critical security risks • **Develop a plan to enhance short-term cybersecurity posture** while adapting to operational change • **Design target-state cyber resilience framework** to ensure continuity in future severe adverse scenarios

IT FUNCTIONS

IT functions must respond quickly to changing technology needs and develop strategic plans to ensure resilience. However, human disruption, gaps in current infrastructure, and uncertainty around short-term organizational goals can challenge organizations looking to improve system availability and stability. Organizations should look for ways to reduce human dependencies and accelerate threat detection and recovery.

KEY CONSIDERATIONS FOR STEP 3A

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Improve system availability	• **Increased outages** or delayed system availability due to human disruption and gaps in current infrastructure	• **Revise remote working procedures** to allow for resources flexibility and continuity • Double down on **DDoS threat detection and mitigation** • Enable on-demand computing power, storage expansion, and outsourcing maintenance needs	• **Conduct a digital readiness assessment** to understand any gaps in the current infrastructure.
Enhance network stability	• **Delayed upgrades and maintenance** and uncertainty around short-term organizational goals	• Revise and upgrade schedule to **prioritize critical updates** • **Implement AI chatbots** as the first interaction agent to **reduce burden on workforce** and customer waiting times	• **AI & chatbot development** to upgrade customer support through **increased demand**
Ameliorate platform capacity	• Infrastructure disruptions from **overloaded platforms/servers** and resources scalability	• Reassess Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to allow for **resources rationalization** • **Plan to reallocate/augment server** by leveraging additional resources such as network bandwidth and digital channels, as well as offloading from low priority capabilities	• **Expedite cloud adoption roadmap** to facilitate the transition away from physical dependencies

Step 3b: Testing ability to deliver critical operations under severe but plausible scenarios

Due Date: To meet all HKMA requirements by 31st May 2026

Successful crisis management is underpinned by a well-developed scenario testing plan. However, estimating the severity or probability of events and establishing effective testing standards can be a challenge, as it requires an adequate understanding of interdependencies between critical functions. Companies often lack experience in reacting to severe events, many of which evolve through periods – and they need to adapt and reassess the relevance of their current models frequently.

KEY CONSIDERATIONS FOR STEP 3B

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Establish testing standards	• Companies may **not take severe but plausible scenarios into account** when they establish testing standards as they **underestimate** the severity or probability of these events	• Ensure the firm has **identified its critical business operations**, set one or more **impact tolerances** for each of the critical functions, and has a **complete understanding of interdependencies** between components of critical processes[7]	**Conduct simulation-based tests to validate testing standards** • Identify lessons learned from both simulated and real-world cases and the responses from other organizations to refine testing standards
Evaluate testing methods and outcomes	• Companies' current testing methods may have ignored **the interconnections** between those events and their critical operations	• **Backtesting** against previous instances of operational risk events and disruptions • Consider the **interconnections and interdependencies** among the firm's business units, third-party service providers, and information systems	**Process mapping** • Test resilience of critical processes for a series of severe but plausible events based on data in process mapping • Use data from process mapping to evaluate testing methods and outcomes
A formal testing report to record any gaps or weaknesses identified	• Preparation of a **detailed formal report** is required after each scenario testing to detail the response and recovery actions that banks will take to continue the delivery of a critical business service during/after a disruption[8]	• **Review and detect** activities that pose risks to critical operations and business services • The Board **and senior management** should ensure **the report** includes sufficient data and information for suitable and timely decision-making before sign-off	• Help **identify resilience gaps in the report** and assess the actions firms may need to take to increase their operational resilience

Step 4: Responding to and recovering from incidents

Due Date: To meet all HKMA requirements by 31st May 2026

Most banks test their response and recovery capabilities on an annual basis. However, regulators recommend firms evaluate the evolving nature of operational risks so that they can continuously monitor, test, and adapt their recovery plans and capabilities. The ability to quickly learn from the results of testing against hypothetical incidents is crucial for all financial institutions, since it helps them to understand how best to weather the storm.

Accommodating stakeholder expectations and transforming legacy warning systems is often the primary challenge for firms looking to develop response/recovery procedures. Adding to the pain, firms may need to refresh their communication plans to ensure the timely passage of information. To mitigate these challenges, as the table below summarizes, firms need to ensure active stakeholder involvement, maintain an inventory of alternative suppliers and establish a dedicated communication function (or control room).

KEY CONSIDERATIONS FOR STEP 4

What Needs To Be Done?	Key Challenges	Capco Insights	What Capco Can Do
Establish effective incident detection and reporting program	**Inadequacy of the current warning system** • Organizations need to ensure that the existing warning system can promptly detect threats and that the warning system can act as an effective guide for management decisions	• **Existing reporting dashboards should be enhanced** to incorporate real-time monitoring of operational risk exposures and emerging resiliency risks • **Board and senior management participation** is required to enhance incident response	**Incident response review & enhancement** • **Review** the firm's current **incident response** apparatus and improve by applying elements of the military approach to **crisis management** • Elements such as organization, roles and responsibilities, information flows, executive training and rehearsals are covered
Develop a corresponding set of response and recovery procedures	• **Coordination among multiple stakeholders** is required to ensure expectations and realities are aligned	• **Define action plans and owners of the actions** in response to each identified scenario to mitigate disruptions and get **stakeholder buy-in for employee participation and training**	**Re-evaluate/redesign incident response framework** • Design and implement an **instant incidence** response framework and playbook to **minimize reaction time** in the case of an incident • The response apparatus governance includes **regular rehearsal** and thorough post-incident reviews
Update communication plans	• **Potential disruptions are fast-evolving** and can be unexpected, and thus, communication plans need to adapt to stakeholder needs	• Firms can use both **mitigation and proactive outreach** to ensure frequent and transparent communications • Firms can **define alternatives** to enable swift adaptation to minimize disruptions	• **Strategize customer support** and update online capabilities to boost relationships • Evaluate and implement **new communication channels** to enhance remote capabilities

KEY CONSIDERATIONS FOR STEP 4 CONTINUED

Update communication plans	**Difficulty in maintaining communications discipline** - In organizations not used to crisis management, **managers tend to spend time trying to fix a new problem themselves before they tell others about it**. - As a result, there is a clear risk that other parts of the organization are unable to respond effectively because they have a limited understanding that the situation has changed	- In a military operation, there are individuals dedicated to ensuring the passage of information in each key component of the organization - A control station is responsible for maintaining communications discipline within each network, ensuring that critical information is passed on and that the communication 'nets' operate effectively - This is a function that should be covered by the operations room in a financial services firm	- **Refresh communication plans** to enable the establishment of a control station and strategic alignment on crisis management
Conduct root cause analysis of incidents	- **Information overload** and **interdependencies** with third parties or intragroup can make root cause analysis difficult and time-consuming	- **Root cause elimination and lessons learned** should include documenting **root causes from other entities**, third parties, and intra-group entities - **Adoption of robotic process automation** (RPA) can enable faster detection of actual causes of disruptions in processes with complex interconnections	- **Perform process mining to** expedite root cause detection processes - **Create an operational resilience self-assessment document** available for inspection by regulators upon request

CONCLUSION

Sound operational resilience planning is more vital than ever in order to minimize disruptions to markets and economies around the globe, maintain the confidence of customers, and defend the strategic viability of firms. Traditional business continuity planning and operational risk management have revolved around localized technology, operational failure events, and national disasters. They often did not focus on the most severe scenarios with significant global impact.

The global pandemic gave rise to many events that rocked institutions across a range of operational dimensions, including workforces requiring time off for sickness, vaccinations, quarantines, working remotely over the long term, and including in some locations the complete shutdown of offices due to social unrest. Yet during the crisis there were examples of firms that not only survived, but thrived. This was not merely a case of luck. Many of these organizations had spent years preparing their infrastructures to be resilient through disruption.

The pandemic is only one of many possible disruptive events. Incorporating the effect of severe disruptions into scenario analysis is uniquely complex given the number of unknown variables such as scale, duration, and public response. Firms must tackle their operational resilience preparations for future events with a real sense of urgency, while they still have the time to prepare thoroughly.

How Capco can support robust operational resilience management across organizations:

- Capco has Operational Resilience expertise and SMEs with experience in all phases of an improvement program. We will apply best practices to ensure that firms have a sustainable approach and the governance to improve operational resilience.

- Capco has significant experience working with major financial services firms on operating models and process design. We will draw upon our proven methodologies to map your critical operations. We can apply the latest technology, e.g., in the creation of 'digital twins', to give a richer, more usable understanding of how services are delivered.

- Capco partners with various tier 1 banks to deliver data innovation (e.g. graph and semantic data technology, modern technical stack design). We will use our suite of data solutions and SME knowledge to help you 'complete the jigsaw.'

- Capco has deep capabilities in technology and digital architecture design, robotics, machine learning and other large-scale IT transformational deliveries. We can position you with fit-for-purpose architecture to maintain operational resilience during planned and unplanned events, while preparing the way for much richer management information to allow you to better monitor your services and status.

FURTHER READING

1. Excelling In Crisis – Lessons For Financial Services From The UK Military Approach
   Will Packard, Managing Principal, Capco
   Lucinda Szebrat, Executive Director, Capco
   James Arnett, Partner, Capco
   Owen Jelf, Partner, Capco

2. Managing The Inevitable – A Primer On Operational Resilience
   Will Packard, Managing Principal, Capco
   James Arnett, Partner, Capco
   Owen Jelf, Partner, Capco

3. Getting The Mix Right – A Look At The Issues Around Outsourcing And Operational Resilience
   Will Packard, Managing Principal, Capco

4. Operational Resilience: Industry Benchmarking
   Matt Paisley, Principal Consultant, Capco
   Will Packard, Managing Principal, Capco
   Samer Baghdadi, Principal Consultant, Capco
   Chris Rhodes, Consultant, Capco

5. Operational Resilience Approach
   Michelle Leon, Managing Principal, Capco
   Carl Repoli, Managing Principal, Capco

REFERENCES

1. https://www.hkma.gov.hk/media/SPM_module_OR-2_Consultation_(20211222).pdf
2. https://www.bis.org/bcbs/publ/d516.pdf
3. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-1.pdf
4. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-2.pdf
5. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220531e1.pdf
6. https://www.spglobal.com/ratings/en/research/articles/200204-coronavirus-impact-key-takeaways-from-our-articles-11337257
7. https://www.theia.org/sites/default/files/2021-12/IA%20Scenario%20Testing%20Severe%20but%20Plausible%20Dec21.pdf
8. https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/IN.pdf

AUTHORS

Angelina Ng, Partner, angelina.ng@capco.com
Lisa Huang, Senior Consultant, lisa.huang@capco.com
Shannon Wong, Consultant, shannon.wong@capco.com
Doris Chow, Associate, doris.chow@capco.com
Rex Lo, Associate, rex.lo@capco.com

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC

Bangalore
Bangkok
Dubai
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE

Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA

Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Washington, DC

SOUTH AMERICA

São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company