The resilience revolution is here

PwC's Middle East Crisis and Resilience Survey 2023

Business leaders face an unprecedented level of disruption and uncertainty in today's rapidly changing environment. From geopolitical instability to climate crises, cyber threats and faltering supply chains – a multitude of external macro forces are converging on the market. Organisations are also facing heightened levels of internal complexity and challenges – all intensifying the frequency and scale of disruption.

This ceaseless cycle of change and disruption is the hallmark of today's global business climate.

Organisations are contending with an uncertain environment – constant movement, continuous disruption – as they attempt to undertake broader business transformations to adapt and address each challenge, emerge stronger from unplanned events, and thrive.

Against this backdrop, resilience has become one of the most vital strategic priorities in the corporate world.

What is Enterprise resilience?

Enterprise resilience requires your business to evolve continuously, protected from shocks, while at the same time being able to adapt, create value and maintain a competitive edge. However, tension can exist between being resilient versus being agile. Balancing these two competing demands can be challenging. The core components of enterprise resilience are:

01 **Strategic resilience:** the ability to evolve and build agility into the organisation

02 **Operational resilience:** the ability to maintain critical operations during disruption

03 **Financial resilience:** the ability to maintain capital and cash flow during disruption

Disruptions are on the rise:

In 2019:

69% of organisations said they **experienced a disruption in the last five years**

Recent trends continue to tick upward

In 2023:

95% of Middle East organisations have **experienced disruption in the past two years (96% globally)**

57% of Middle East organisations have experienced **operational disruption other than the pandemic (59% globally)**

PwC's Middle East Crisis and Resilience Survey 2023 is focused on understanding today's threats and how organisations direct their resources, efforts and investments to become more resilient.

Data from nearly 100 respondents throughout Middle East provides insights into how business leaders are preparing for and responding to this new world. And what has emerged from the voices of global business leaders is that a resilience revolution is here.

Long-relegated to the halls of compliance exercises and checklists, resilience has evolved from a capability designed merely to mitigate potential losses or meet regulatory obligations.

Today, true resilience is a core competitive advantage and a prerequisite for any successful business strategy.

As the revolution moves ahead, intentional resilience by design is critical – and our respondents agree: 91% noted that resilience is one of their most important strategic organisational priorities. Yet many also report that their organisations have not taken the steps needed to implement an integrated enterprise resilience programme or even identified the steps to move forward on that journey.

Business leaders express confidence in their ability to recover from a crisis. But the data is clear: Too many organisations lack the foundational elements of resilience needed to succeed.

What are organisations concerned about in the next two years?

01 Technology Disruption / Failure

02 Climate Change/ Natural Disaster

03 Employee retention and recruitment

04 Competitive Market Place Disruption

05 Cyberattack

It is with these insights in mind, and amid the current state of constant disruption, that we believe all organisations should be asking these key questions to rethink their approach to resilience:

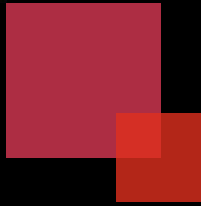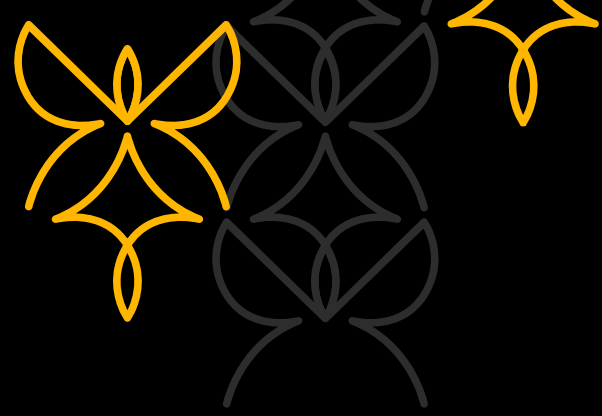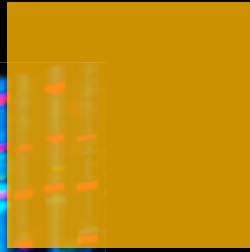Why do we need to build resilience – and for whom?

What do we care most about protecting in our organisation, and what is our strategy to preserve those critical business services?
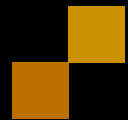
Have we embedded the right mindset and culture to drive the necessary investment in resilience?

Three takeaways

So, if building a resilient organisation by design has become a strategic imperative, what are today's business leaders doing to make it happen? And what are the key components of an effective resilience programme?

The survey data revealed three key takeaways:

1 Integration

An integrated resilience programme is essential – and if you aren't developing a strategy to move in that direction, you are falling behind.
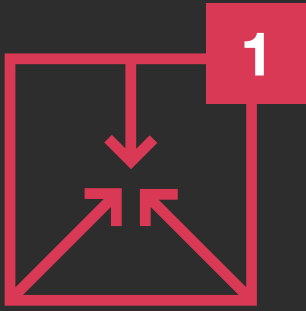
2 Leadership

Thriving in crisis requires a senior leader, executive sponsorship and upskilled teams.

3 Operational Resilience

Leading organisations are adopting an operational resilience (OpRes) approach and leveraging technology to enable a panoramic view of their risk and resilience landscape.

1

An integrated resilience programme is essential

Resilience programmes are too often siloed, with little coordination across functions. It is no longer sufficient for organisations to be in silos as they address today's complex and interconnected risks. Enterprises are actively moving to an integrated approach to resilience, centrally governing and aligning multiple resilience competencies around what matters most to the business, and embedding the programme into operations and the corporate culture (ie crisis management, business continuity, disaster recovery, emergency management, cyber resilience, etc.)

To start, leaders should consider the roles, responsibilities, governance, objectives, strategy and other key elements – and design a programme that extends across the enterprise and into every facet of the business.

Organisations with a resilience strategy driving an integrated programme not only can identify and manage risks better, but can identify opportunities amid disruption. This allows business leaders to take appropriate risks in a way that's aligned with the overall business plan. Prioritising investment based on what is critical to the organisation and stakeholders also enable senior leaders to coordinate their response to disruption and execute a faster and more effective recovery.

The result

Improved risk management, better financial performance, competitive advantage in the marketplace, a protected reputation and stakeholder trust.

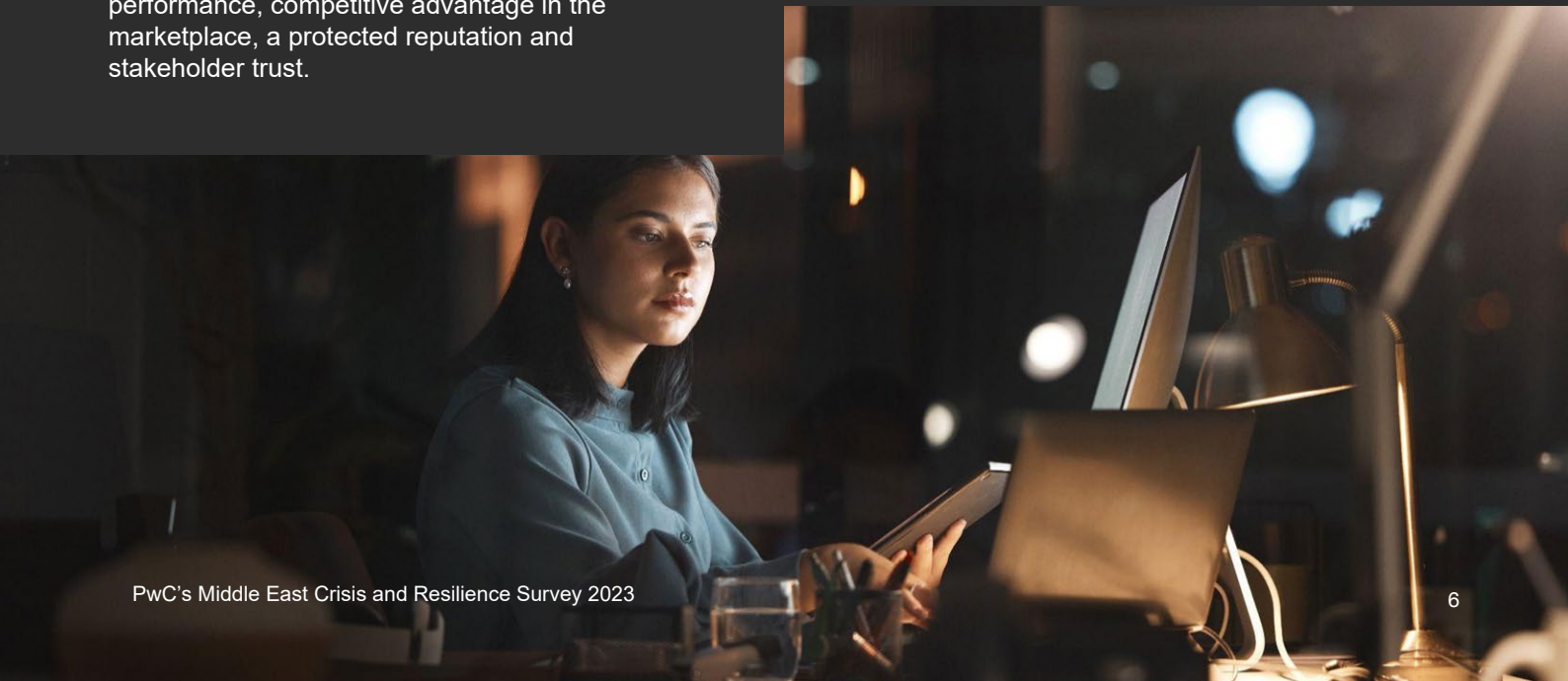**33% of Middle East organisations have fully integrated approach compared to the global average of 21.**

74% have a dedicated resource

Only **20%** have supply chain resilience competencies

49% have had a programme in place for at least 5 years

2

Thriving in crisis requires an executive leader and upskilled teams

We often refer to resilience as the enterprise's immune system. Building immunity requires layers of resilience – from employees to leadership and the board. A successful resilience strategy and programme needs (1) executive sponsorship from the C-suite, (2) a programme leader with clear responsibility, and (3) a skilled team to do the day-to-day work.

37% of enterprise resilience programmes are **sponsored by the organisation's CEO**

57% of Middle East organisations cite upskilling future leaders as one of their **top three most important elements** of future-proofing resilience

What does the data show?

1 Accountability:

We are seeing real progress on senior leadership taking accountability of resilience. In 2021, 61% of our Global Crisis Survey respondents said their head of crisis or resilience was accountable (at that time, data was related to the pandemic). Today, 93% of organisations in the Middle East with a resilience programme in place have established a C-level sponsor. In fact, 37% of respondents have named their CEO as the executive sponsor for resilience, demonstrating the role's criticality to the success of the organisation. Executive sponsors are accountable for establishing the target maturity for the resilience programme and making sure it is appropriately funded and staffed, ensuring it meets expectations.

2 Responsibility:

On the other hand, we do not see organisations coalesce around a single role that is responsible for managing the implementation of an enterprise resilience programme – a Chief Resilience Officer, for instance, was named by only 11% of our survey respondents. Appointing a Chief Resilience Officer might not be the answer for every industry, but this lack of clear enterprise-wide responsibility undermines focus and direction. Absent a dedicated role with responsibility for the programme, organisations are unlikely to fully integrate resilience into operations and culture.

3 Upskilling:

Resilience expertise constraints present another challenge: 40% of our respondents said building a team with the right skills is a major hurdle in establishing a resilience programme. The field needs a pool of talented resilience professionals with the experience and skills to execute a strategic, integrated programme and respond effectively during a crisis. To build resilience, senior resilience leaders must be clear about how the organisation works, how to deliver on the right priorities, and their role as leaders. So how do we get there if the expertise pool is shallow? Providing suitable investment in training and professional development helps organisations overcome this challenge and develop the team they need.

## Emotional resilience, leadership upskilling and thriving through disruption

A standout stat in our PwC Global Crisis Survey 2021 was health-related: 80% of organisations reported an investment in employee well-being as the single-most important action they'd taken that year. Considering the pandemic, economic turmoil, profound cultural changes and other challenges of the time, mental health was top of mind in the corporate world and in personal lives.

That focus on well-being hasn't waned. In fact, more and more organisations have embedded well-being programmes into their culture over the past few years, recognising the need to support employees and encourage balance and wellness in all parts of their lives.

And resilient leaders grow resilient organisations. That's the message at the heart of the PwC Crisis Leadership Centre, where professional training focuses on attributes like emotional intelligence, adaptability and flexibility – all central to a business leader's ability to thrive, personally and professionally, through disruption.

In this year's survey, 40% of businesses report that they plan to invest in personal and emotional resilience over the next two years. And the larger the company, the more likely they are to make the investment. The number climbs to 40% for organisations with a revenue of $5B to $10B.
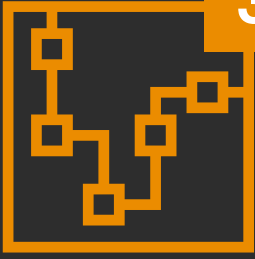
Building operational resilience is the future

3

As more organisations move to integrate their resilience programmes, there is a clear trend toward adopting core principles of an operational resilience (OpRes) approach that allows organisations to manage risks with high reliability and to drive efficiency.

OpRes focuses on establishing and continuously maintaining core elements of non-financial resilience, informed by a strategic view of what is most important to the organisation and its stakeholders. What is most important should determine business service outcomes — not just systems that deliver them, as conventional business continuity approaches generally dictate. So Step 1 is identifying the Critical Business Services for the organisation.

From there, organisations should carefully map them, end-to-end; clearly understand the impact and priority of systems, applications, third parties, people, physical property and data; and establish mature exercise and testing capabilities based on arduous — but plausible — scenarios. Existing risk appetite can help determine the degree of resilience required, but leaders should also consider setting tolerances based on external impacts on customers and the wider system or market in which the organisation operates.

In addition to the shift toward OpRes, organisations are looking to technology as a driving enabler. Almost 60% of business leaders understand the need to underpin resilience strategies with technology that allows them to mine actionable intelligence from data across a business. The goal is to provide an integrated, insight-driven single pane of glass and to enable greater agility in times of crisis. Business leaders are also looking to use technology to create a living resilience programme they can continually test and evolve.
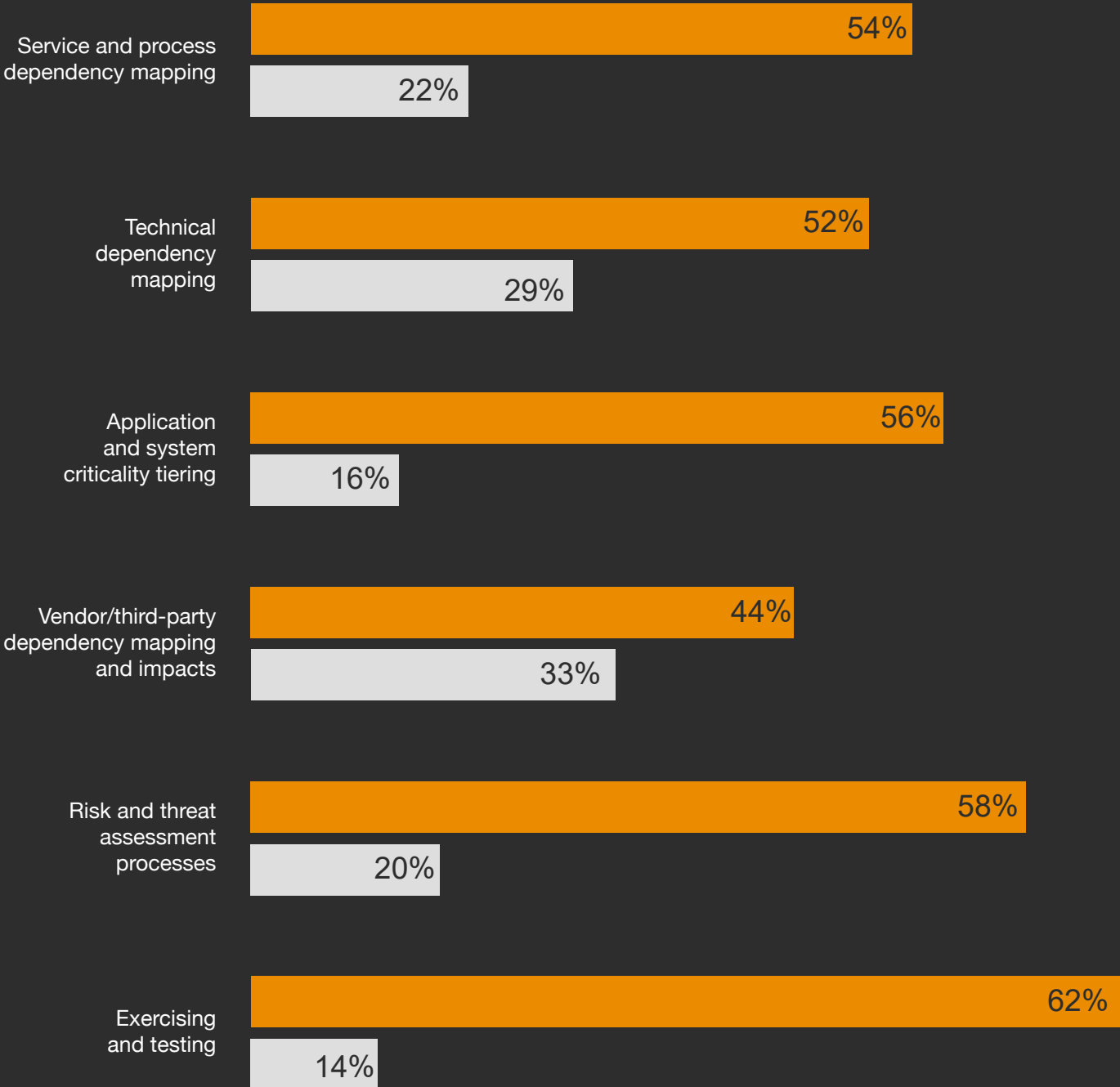
78% of organisations said their most serious crisis **had a medium-to-high impact on operations** – disrupting critical business processes and services

Our data shows that those who have moved to an integrated resilience programme are significantly further ahead in many of the core elements of OpRes.

Percent of respondents with "defined" or "optimised" program elements:

|	
Service and process dependency mapping	54%
	22%
Technical dependency mapping	52%
	29%
Application and system criticality tiering	56%
	16%
Vendor/third-party dependency mapping and impacts	44%
	33%
Risk and threat assessment processes	58%
	20%
Exercising and testing	62%
	14%

Optimised and defined   Initial, Informal and ad hoc
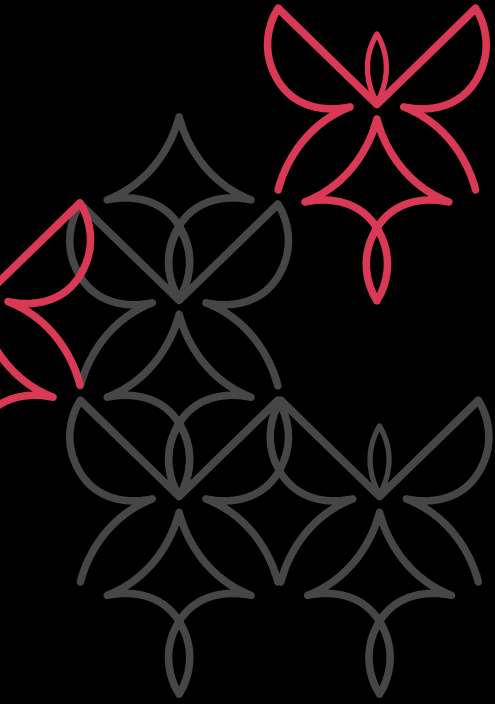
The big picture

The confidence gap: Understanding the risk – and opportunity – of disruption
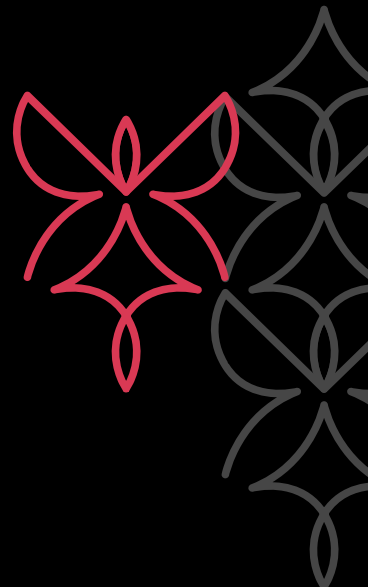
While our survey results confirm that business leaders recognise resilience as a strategic imperative, the data also reveals a "confidence gap" for certain organisations: Only one fifth of the Middle East companies have confidence in their ability to successfully navigate operational disruption or failure.

While many organisations feel bolstered – either because they haven't experienced many crises or because they survived those they confronted – our data shows they are leaving themselves exposed to a number of threats:

1 **Inadequate risk management:**

- Less likely to have a clear understanding of risks and vulnerabilities, and may not have a plan in place to mitigate them
- Increased risk of unexpected disruption and the costs associated with responding
- No link between Enterprise Risk Management and resilience strategy

2 **Lack of cultural resilience:**

- Less likely to have a strong culture of resilience, including a leadership team that sets the tone for the rest of the organisation
- Increased risk of workforce that's not flexible or adaptable

3 **Inadequate technology and resources:**

- Less likely to have the right tools in place, including the latest data and analytics, to support resilience
- Less likely to have an established network of experts to provide guidance and support when needed

4 **Increased costs and decreased competitiveness:**

- More likely to scramble to respond to disruption, rather than proactively prepare
- Likely to result in decreased competitiveness and loss of market share

Percent of respondents identified the below within their top 5 challenges.

32%	Managing critical business services and processes through continuity measures
31%	Incident and crisis management escalation and mobilization of senior team
30%	Prioritising actions
26%	Making timely and deliberate decisions
26%	Getting appropriate information quickly and effectively

Key guidelines in the Middle East

Examples of key guidelines in the Middle East on Business Continuity and Crisis Management

Kingdom of Saudi Arabia

- The Digital Government Authority (DGA) has launched Business Continuity Management Standards to enhance the flexibility of government and private agencies to respond toward any potential outages and to raise the resilience capabilities of the technical infrastructure in the Kingdom.

- The Saudi Central Bank has established a Business Continuity Management (BCM) framework for member organizations to enhance the organizational resilience capability

- Ministry of Communications and Information Technology (MCIT) issued business continuity and crisis management guidelines for the ICT industry.

- Communications & Information Technology Commission (CITC) published the Guidelines on Disaster Recovery Planning for the ICT Industry to enhance the disaster recovery capabilities of the all Facilities Based Providers (FBPs).

- Currently, one of the key national regulators of Saudi Arabia is developing a Risk management and crisis management standard which would be published soon

United Arab Emirates

The National Emergency Crisis and Disaster Management Authority (NCEMA) has updated the second version of the Business Continuity Management Specifications which provides guidance to the organizations to implement and maintain an effective management system.

Sultanate of Oman

IT Service Continuity Framework (ITSCF) was published by the Ministry of Transport, Communication and Information Technology (MTCIT) for the benefit of Oman Public Sector entities.

Kingdom of Bahrain

The Central Bank of Bahrain has published the BCM requirements to be fulfilled by the licensees in the country

Qatar

- Qatar Central Bank has published the Business Continuity Management Guidelines for enhancing the continuity of the Banks.

- The Supreme Committee for Delivery & Legacy (SCDL) had developed the Qatar 2022 Cybersecurity Framework which includes the Recovery and Continuity capability related requirements

Note: The above-mentioned list of guidelines/ frameworks is not an exhaustive list and is limited to select ones only

Case study
Organisational maturity

An integrated resilience programme makes all the difference when disruption strikes. Here's what can happen:

Company A	Company B

Evaluation Criteria

Company A

A ransomware attack disabled a global manufacturer's critical business services. Lacking key strategic components needed for resilience in the face of disruption, the organisation lost several weeks of business – and close to one billion dollars.

Company B

But on the other hand, when a massive disruption dismantled a global manufacturer's shipping operations, the organisation's integrated plan kicked in and the business was able to swiftly shift its shipping routes and supply chain without interrupting service to customers. The organisation tapped into its resilience to weather the disruption – and emerged stronger.

Sponsorship & Integration

Company A

The organisation went into the crisis with resilience in silos. There was no clear sponsorship nor dedicated central resources with authority over the resilience programme. The organisation lost valuable time, money and energy attempting to come to consensus on critical processes and tactics.

Company B

With an executive-level "owner" to oversee the entire resilience programme, the organisation had invested in integrating its resilience programme prior to the crisis. The integrated approach laid the foundation for holistic insight into the impact of the issue as it arose as well as clarity on who was accountable and had the authority to make decisions.

	Company A	Company B
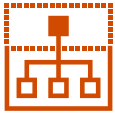
Prioritisation

Without an established agreement regarding the most important elements of the business, the crisis forced executives to waste valuable time trying to reach consensus on what to address first.

The executives had agreed on the critical business services, hammered out in resilience planning over the course of designing their overall programme. They were able to quickly execute their continuity strategies in a prioritised fashion.

Mapped end-to-end processes

Each team knew their individual process/part, but there was not a clear understanding of end-to-end business processes and associated dependencies. Individual teams trying to reduce the effects of the crisis on their process exacerbated certain processes downstream.

By mapping their entire operational capabilities, leveraging a holistic resilience software tool, executives also knew at the start of the crisis how each process would affect functions down the line and had the ability to quickly assess the broader impact of the event.

Regular testing

Executives didn't regularly test their crisis response plan, and there was a lack of awareness of broader recovery plans and strategies, so gaps that could have previously been identified and closed resulted in additional pain points. Moreover, the organisation lacked response muscle memory and essentially developed response plans and playbooks on the fly, costing valuable time.

The organisation updated its programme periodically in response to external pressures and internal changes – enhanced technology, for instance, alerted the testing team to needed adaptations in several key processes. Gaps that could have haunted them with this crisis had been previously addressed as a result.
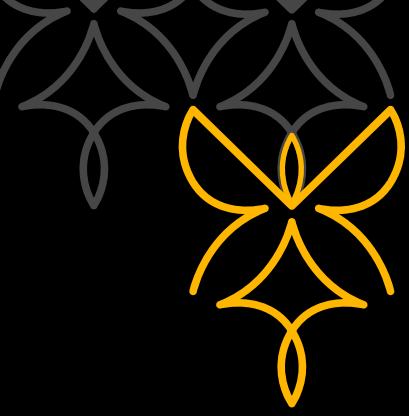
Where are businesses investing?

Despite market conditions, organisations aren't reducing their investment in resilience – further testament to business leaders' recognition that it is critically important.

Almost 86% of our respondents plan to invest in cyber resilience, reflecting concern over the rise in ransomware and other cyber attacks. Crisis management and emergency management follow closely to round out the top three areas of investment, with 88% and 92% of respondents, respectively, planning to invest during the next two years.

Given the volatility of the past few years, we're surprised to see that some respondents are not planning any investment whatsoever in a number of areas foundational to resilience: 8% are not investing in threat monitoring; 8% in supply chain resilience; and 7% in disaster recovery.

The lack of investment isn't just a potential threat in the event of disruption. These organisations are putting themselves at a disadvantage in day-to-day operations.

Businesses making the greatest overall investment in resilience are characterised by a few key traits that deliver results over the long term. For starters, they consider investment a strategic move, rather than a tactic motivated by compliance needs or fear.

Organisations that invest in resilience are more likely to:

View resilience as "very important" compared to other priorities

Incorporate resilience competencies, as part of their integrated resilience programme

Have a dedicated resource(s) managing day-to-day operations

Have faced financial crises in the past

Have spent $50 million or more on their most serious disruption

What motivates organisations to invest in resilience?

No. 1 answer ↗

44% Strategy

36% Fear

21% Regulation

After a catastrophic event, most organisations will move quickly to invest in building resilience. That's no surprise; even moderate disruption can be a prime motivator for change, so taking steps to avoid repeating the past is understandable.

But leaders who view investing in resilience as a strategic imperative – and approach that strategy with greater urgency than fear or regulatory requirements – invariably emerge from crisis with better results.

Bottom line: Rethink your investment reasoning. Fortify your resilience programme – not just in the wake of disruption, but before it happens.
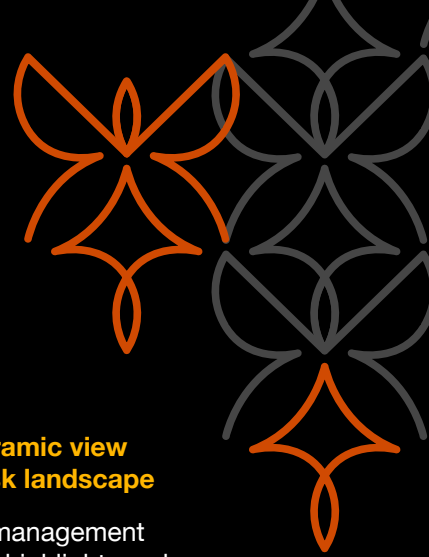
Join the resilience revolution

How to thrive in crisis

Establish executive sponsorship for your resilience programme

Identify a visible senior leader responsible and accountable for the programme

Identify and map your critical business services

Identify your critical business services, map their dependencies, and integrate your resilience capabilities around those services

Build an integrated enterprise resilience programme of cross-functional teams

Align your programme with your strategy, values and investment priorities across the organisation

Establish a panoramic view of your unique risk landscape

Go beyond traditional risk management and leverage technology to highlight weak signals and other key indicators for resilience; organisations most able to mitigate, withstand and recover stronger from a crisis all have a panoramic view of their risk landscape, allowing them to better anticipate risk and act with confidence

Fortify your resilience strategy with technology and regular testing

Underpin strategies with technology and mine actionable intelligence from data to help you anticipate, prevent, prepare for, simulate and learn from risks and disruption; assess your capabilities regularly for relevance, alignment and preparation

Being resilient by design is critical for survival and strategic advantage in an era of disruption as the norm. It's imperative for leading organisations. The ability to adapt and respond to disruption is vital to maintaining the trust built with stakeholders and protecting shareholder value and reputation – all at a time when the expectations for the resilience of businesses and government have never been higher.

Resilient organisations build and maintain trust relationships across their stakeholders: Customers know they can count on consistency and results. This, in turn, preserves and enhances the reputation of the enterprise.

To build a trusted and agile organisation, it is vital to invest in resilience across functions and people, and to focus on an integrated approach.

This includes aligning resilience goals with business and strategy, embedding resilience into key critical services, and fostering a culture of resilience.

Communicate the value of resilience throughout your organisation; embrace resilience as a strategic imperative and an opportunity to strengthen your organisation as you prepare for disruption, manage crises, recover, and thrive.

Be resilient by design.

![pwc logo]

Contacts

Matthew White

Partner, Cybersecurity and Digital Trust Leader, PwC Middle East
Tel: +971 56 113 4205
matthew.white@pwc.com

Nayaz Mohammed

Partner, PwC Middle East
Tel: +968 9942 9679
nayaz.mohammed@pwc.com

Oliver Sykes

Partner, PwC Middle East
Tel: +971 56 480 2447
oliver.sykes@pwc.com

Khaled Kabbara

Partner, PwC Middle East
Tel: +966 54 872 7472
khaled.kabbara@pwc.com

Vishak Jayakumar

Partner, PwC Middle East
Tel: +966 54 747 2884
Tel: +968 9438 0570
vishak.jayakumar@pwc.com

PwC's global network of crisis and resilience professionals