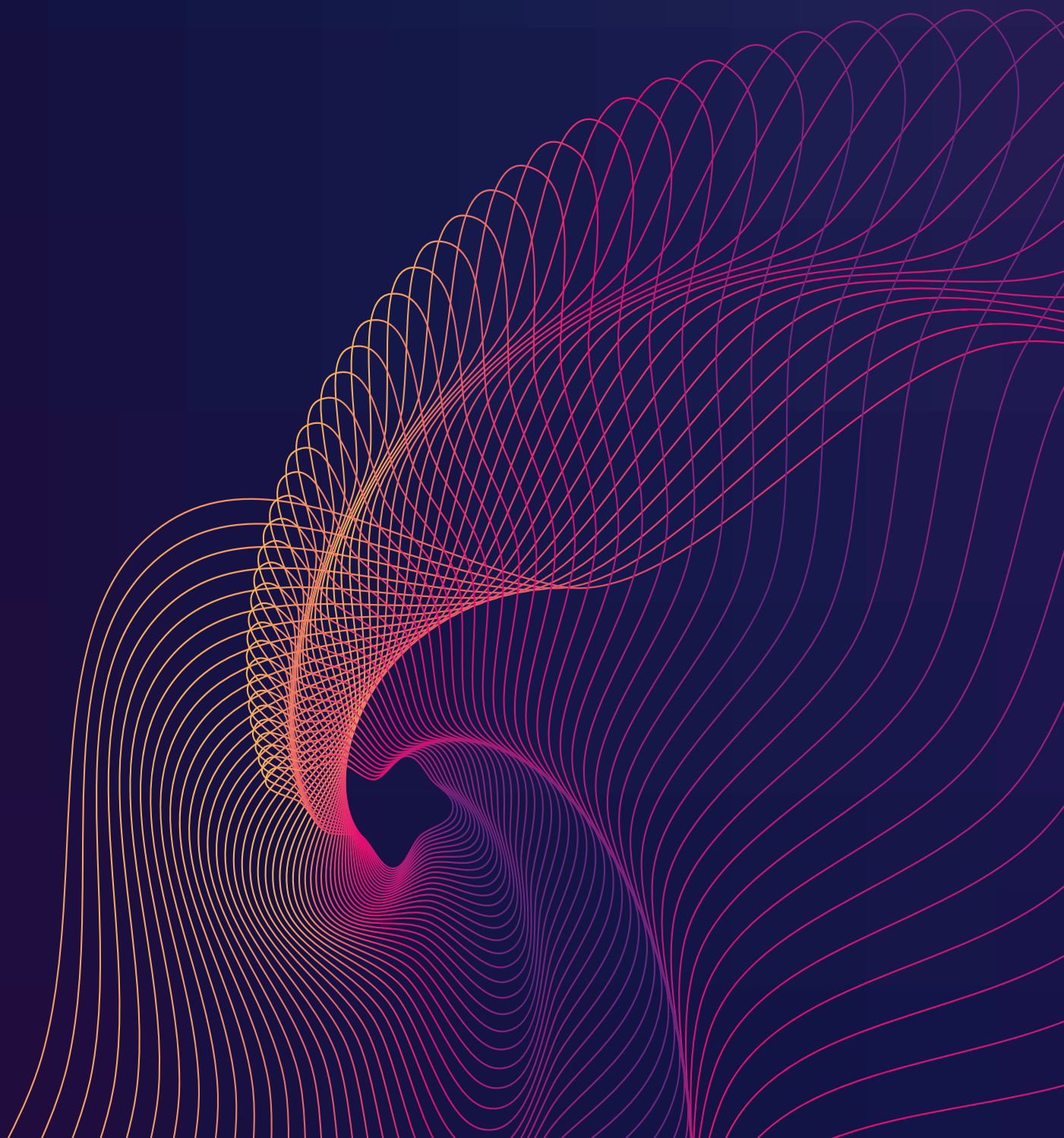
airmic

bci Leading the way to resilience

Putting Organizational Resilience Into Practice



CONTENTS

FOREWORD

Some inconsistent language has been creeping into the world of managing resilience. Without stepping back and examining the effect of this and without the benefit of up-to-date international standards to help guide professional practice, language creep has resulted in a corrosion of agreed good practice across countries, regions, and sectors. This has the effect of undermining the ability to reliably benchmark performance given the weakened platform against which to assess and develop continuous improvement. Yet, standards and models of resilience good practice have never been more important.

The external context today is one of complexity and connectivity, which demands a different focus for leadership and strategy. Models based on prediction and control are being replaced by models based on uncertainty, interdependence, and rapid change. Deep uncertainty and limited available information incubate emerging risks that can be difficult to manage – as emerging risks are typified by a lack of reliable data, can materialise quickly, may constantly change, and can significantly affect an organization and its operations. While all risks in an organization carry some residual uncertainty, with emerging risks, higher levels of residual risk are common. Procedures must be in place for continuous monitoring of these risks to allow organizations to follow change and adapt. The ability of an organization to be flexible and innovate in response to change and to adapt decision-making and operations is an established principle of resilience.

Contemporary developments in technologies and data management, including artificial intelligence (AI), machine learning, and critical thinking, are playing an important role in enhancing our capabilities to identify and forecast, monitor, and mitigate risk. Future developments and use of these technologies are likely to yield solutions that underpin resilience in a complex world. Taken individually, some of the transformational capabilities of technology are not particularly new. Taken collectively, they are shaping strategic and organizational challenges and risks for all organizations.

Insurance is one key component of resilience. Insurers not only play a critical role in scanning for emerging threats, while ensuring that resilience is built into national policies and planning, they also safeguard businesses and invest billions in infrastructure for long-term growth. Airmic and its members are dedicated to championing the strategic value of risk management and insurance in a changing world where resilience is more crucial than ever.

People who possess personal resilience skills will cope most effectively with the demands and challenges they come across in the workplace. Resilient people are more likely to thrive in a context or environment with constantly changing priorities, organizational change, and a different culture and style of working. However, an outdated sensitivity to the changing purpose of an organization – and an inappropriate culture – can lead to a lack of psychological safety for people and an organization out of tune with the needs of personal resilience, leading to disenchantment, lack of innovation, and missed business opportunities. Organizations must remain people and culture-centric. This scenario touches upon several principles of resilience involving relationships, networks, communication, and the need to embrace new technologies.

The reality of today is not the accumulation of the experiences of yesterday. We face a new reality where the world is increasingly blocking the open sharing of resources, including data. The world is chaotic and uncertain. Supply chains are increasingly volatile and fractured. The old world is not well suited to this context and long-established trust has been broken.

Airmic is delighted to be working with the BCI to create a principles-based body of knowledge that can guide organizations and their professionals, collaborating to share emerging good practice that contributes to building resilience for all.

Julia Graham
CEO, Airmic

FOREWORD

The BCI has long taken a leadership role in the resilience space, exemplified by the simple fact that our aim is *Leading the way to resilience* and our vision is to work towards a resilient world.

As long ago as 2016, the BCI published a *Position Statement on Organizational Resilience* (1), which sets out the BCI's long-standing viewpoint that:

- Business continuity is not the same as organizational resilience.
- The effective enhancement of organizational resilience will require a collaborative effort between many management disciplines.
- No single management discipline ... can credibly claim 'ownership' of organizational resilience; and organizational resilience cannot be described as a subset of another management discipline or standard.
- Business continuity principles and practices are an essential contribution for an organization seeking to develop and enhance effective resilience capabilities.

Since 2016, the BCI has continued to develop reports and guidance relating to organizational resilience, with the most recent outputs being *The Resilience Framework* in 2024 (2) – which developed eight Core Principles of Resilience Development and Management – and the *BCI Resilience Vision 2030 Report* in 2025 (3). This report used a survey approach to look ahead to how resilience practices and the wider profession are expected to develop through to 2030.

I am very pleased, therefore, to be working with Airmic to take another step in our journey to provide clear guidance to organizations on resilience. *Putting Organizational Resilience into Practice* provides insights into how real-life organizations are actually managing and governing resilience. It is not a standard or a Good Practice Guidelines document in BCI terms; instead, it offers a unique snapshot of strategic resilience management and, as such, is a strong addition to the resilience profession's body of knowledge.

David Thorp
Executive Director, BCI

INTRODUCTION

Resilience as an organizational capability has developed over the past decade, but it is not yet a fully mature discipline; it is still in the emergent phase.

The reality is that the majority of organizations are creating their own roadmaps for navigating their organizational resilience journey and there is not a consistent approach. This is something that Airmic and the BCI identified and decided to explore together. Both associations have been at the forefront of resilience development for many years and have a commitment to developing knowledge resources to help businesses and organizations to understand how to develop resilience capabilities. It was, therefore, a natural progression for Airmic and the BCI to come together to develop joint guidance in this area, and this document is the first output from this partnership.

Based on seven detailed case studies conducted during 2025, *Putting Organizational Resilience into Practice* has two key aims. The first is to re-examine the Principles of Resilience previously developed by Airmic and determine whether they remain relevant. The second is to consider what these principles look like in today's organizations – highlighting key themes and innovative practices from the case studies, with particular emphasis on the governance of resilience. *Putting Organizational Resilience into Practice* is a practical guidance document for organizations. It is not aligned to any particular standard and recognises that while there is awareness of the existence of organizational resilience standards amongst professionals, the actual adoption and use of those standards appear to be low (4).

Putting Organizational Resilience into Practice is aimed at resilience professionals who are tasked with leading and developing resilience strategies within their organizations, as well as C-level executives and boards who are seeking to understand how to structure the governance of resilience and to increase the maturity of organizational resilience capabilities.

EXECUTIVE SUMMARY

Organizational resilience is at a pivotal moment of development. Over the past decade, the concept has matured and broadened, and is now shifting from being a primarily operational discipline into a strategic capability linked to competitiveness, long-term sustainability, and thriving organizations.

This document explores the current organizational resilience landscape through the prism of resilience factors that have been established by Airmic and, at the same time, considers whether these are still current. These factors are the eight Principles of Resilience and the four Business Enablers.

To achieve the above aims, seven detailed case studies were conducted, providing a unique cross-sector snapshot of how resilience is actually being governed, delivered, and embedded today.

Despite different industries, geographies, regulatory environments, and organizational structures, the case study interviews reveal a striking degree of commonality. The following Executive Summary synthesises these recurring themes into a set of clear insights about *what good resilience looks like*, *where organizations struggle*, and *how leading organizations are evolving resilience practice for the future*.

These insights fall into five overarching groups:

- **Resilience as Strategy and Competitive Advantage**
- **Governance, Leadership, and Decision-Making**
- **Integration, Structures, and Culture**
- **Capabilities, Technology, and Measurement**
- **People-Centric Resilience and the Human Foundations of Adaptation**

Resilience as Strategy and Competitive Advantage

Resilience is shifting decisively from compliance to competitive advantage

In many organizations, resilience is no longer viewed as a regulatory obligation or operational cost. Instead, it is becoming a mechanism to:

- Protect and enhance customer trust,
- Differentiate in competitive markets,
- Improve strategic decision-making,
- Accelerate recovery and adaptation, and
- Enable innovation and long-term opportunity capture.

The most mature organizations clearly treat resilience as a strategic outcome rather than a compliance necessity.

Thriving, not just surviving, is emerging as a defining resilience objective

Resilience is increasingly understood as the capacity not only to withstand disruption but to thrive as an organization. Resilience enables organizations to benefit competitively from crisis situations and also creates a general strategic and operational environment for organizational success. Highly resilient organizations adapt to change and pressures faster than competitors, as well as using disruption as an opportunity to:

- Capture market share,
- Catalyse transformation,
- Strengthen customer loyalty, and
- Integrate new technologies.

Resilience is an enabler of opportunity – not simply a way of controlling and responding to incidents and crises.

Governance, Leadership, and Decision-Making

C-Suite ownership and the rise of the Chief Resilience Officer

A consistent theme across the case study interviews is the need for resilience to sit at, or near, the top of the organization. Some interviewees explicitly called for a Chief Resilience Officer (CRO), even when the role does not currently exist. Where organizations lack C-Suite responsibility for resilience, resilience professionals may experience:

- Fragmented delivery,
- Siloed leadership,
- Limited influence on capital investment, mission, and strategy, and
- Slow progress in moving from compliance to strategic resilience.

Where senior-level ownership is strong, resilience gains visibility, coherence, and empowerment.

Small, empowered crisis management teams outperform larger structures

A notable cross-case study theme is that small crisis management teams make better decisions under pressure. Across sectors, smaller groups of senior leaders with clear delegated authority, fast access to expertise, and streamlined escalation paths consistently outperform larger, consensus-driven structures.

Large crisis teams dilute accountability, slow decisions, and introduce unnecessary hierarchy. Small teams act decisively.

Empowered crisis management teams enable rapid, strategic decisions

The strongest crisis responses emerge where crisis leaders have:

- Explicit delegated decision authority and freedom,
- Clarity on escalation thresholds, and
- Support from specialist operational and tactical advisors.

Boards are asking for forward-looking assurance

When it comes to resilience reporting and measurement, boards increasingly want to move beyond backward-looking compliance reporting. They expect:

- Meaningful resilience KPIs,
- Maturity assessments,
- Horizon scanning which is filtered for strategic relevance, and
- Structured lessons-learned loops.

Boards also value challenge – whether internal or independent – to validate assumptions and review major incidents.

Integration, Structures, and Culture

Silos are one of the largest barriers to resilience maturity

Every case study organization reported challenges with silos. These include:

- Different departments owning different elements of resilience,
- Fragmented budgets,
- Disconnected tools and platforms,
- Duplicated or contradictory processes, and
- Gaps in cross-functional decision-making.

Successful organizations do not necessarily remove silos, but overcome the issues that silos create through:

- Cross-functional forums (not committees – see below),
- Unified senior resilience leadership,
- Common data models,
- Shared risk taxonomies, and
- Integrated crisis exercising and structures.

Forums surface issues better than formal committees

A recurring insight is that committees often suppress discussion, while forums tend to encourage it. Strong forums:

- Are collaborative rather than bureaucratic and top-down,
- Bring the right people together informally,
- Encourage honest challenge,
- Identify weak signals earlier, and
- Avoid the politics and hierarchy of committees.

This difference is particularly important for surfacing risks early.

Collaboration across business units is essential

Cross-disciplinary collaboration is not optional – instead, it is central to resilience. Resilient organizations integrate. This entails:

- Embedding resilience in technology, operations, HR, security, procurement, and communications,
- Using integrated playbooks,
- Co-designing exercises,
- Involving suppliers and partners in organizational resilience,
- Maintaining joint crisis structures, and
- Sharing intelligence and information across ecosystems.

HR is often a weak link in resilience integration

Despite employees being fundamental to resilience, the Human Resources (HR) function is often:

- Peripheral to crisis structures,
- Not involved in resilience forums,
- Disconnected from hybrid working risks,
- Weak on workforce impact modelling, and
- Limited in modelling long-term people risks.

Where HR is fully engaged, people resilience strengthens dramatically.

Psychological safety underpins true resilience

When psychological safety is encouraged and seen as an essential aspect of organizational culture, resilience is substantially strengthened. Psychological safety enables:

- Timely and open reporting of near-misses,
- Early escalation of concerns,
- Honest contributions during crises and exercises,
- Constructive challenge,
- Avoidance of groupthink, and
- Transparent post-incident and post-exercise learning.

Where employees fear blame or repercussion, issues remain hidden until they escalate.

Capabilities, Technology, and Measurement

Resilience-by-design is widely recognised – but often not implemented

Many organizations identify resilience-by-design as essential, yet admit that:

- Cost pressures during build phases sometimes result in resilience features not being implemented,
- Resilience is introduced too late in design cycles,
- Short-term deliverables override long-term robustness, and
- Major opportunities are missed during digital transformation or facility construction.

This is one of the most distinct gaps across the case studies: organizations know what resilience-by-design looks like but cannot reliably deliver it.

AI, automation, and digital twins are transforming resilience practice

A strong cross-case trend is the growing awareness of the advantages that the following can bring to resilience:

- AI-driven supplier assessments,
- Automated document review,
- Predictive maintenance modelling,
- Data-driven horizon scanning,
- Risk summarisation tools, and
- Digital twins.

These technologies are active capabilities that are currently reshaping how resilience is monitored, tested, and governed.

A shift is taking place from process-based business continuity techniques to customer and service-focused resilience

Particularly in financial services, but increasingly in other sectors, organizations are shifting focus away from traditional business continuity approaches, which focus on business processes and the impacts upon these, towards operational resilience techniques, which put the customer and critical services first. This customer-centric approach is becoming the dominant resilience model.

Supplier and ecosystem resilience is now critical

Today's organizations have ever-increasing dependence on:

- Cloud providers,
- Technology vendors,
- Logistics partners,
- Managed service suppliers, and
- Data and platform providers.

Due to this, supplier resilience is now treated as:

- Equal in importance to internal resilience,
- A strategic risk, and
- A potential point of systemic failure.

Leading organizations recognise concentration risks, maintain appropriate playbooks, conduct joint exercises with suppliers, enforce stronger contracts, and have enhanced supplier assurance.

The growth of external, systemic risk

The case studies highlight that systemic, externally driven risks are now evolving faster than internal resilience controls and governance models. Increasing concentration in critical technology providers, highly interconnected global supply chains, and shared digital infrastructure mean that organizations are increasingly exposed to vulnerabilities outside their direct control. This is shifting resilience from mainly an internal management challenge to a broader systemic and ecosystem-level issue.

Resilience measurement is underdeveloped

While boards increasingly demand meaningful metrics, many organizations struggle with this area. Some still rely on business continuity KPIs such as:

- Plan status,
- Compliance indicators,
- Exercise attendance, and
- Audit results.

However, stronger resilience measurement models have broader aspects, including:

- Time-to-mitigation KPIs,
- Percentage of risks actively under mitigation,
- Impact tolerance breaches, and
- Recovery performance trends.

Horizon scanning is helpful but often limited

Organizations report that horizon scanning:

- Needs contextual interpretation,
- Results in risks being too broad or generic,
- Requires integration with internal risk processes, and

- Only delivers value when connected to decision-making.

Horizon scanning alone is not resilience, but it is a vital aspect enabling long-term strategic decisions to be made and catalysing adaptation.

People-Centric Resilience and Culture

Resilience must be people-centric to be effective

The importance of people runs through every case study interview. Resilient individuals and resilient teams are crucial assets – not just during crises but in ensuring that the organization grows and thrives.

Resilient organizations emphasise:

- Leadership development,
- Empowerment,
- Training at all levels,
- High levels of engagement during exercises,
- Open communication,
- Psychological safety (see above),
- Good wellbeing practices,
- Clear roles and responsibilities, and
- Access to 24/7 support teams.

People are at the heart of resilience.

Culture determines whether resilience is lived or theoretical

Cultures that support resilience:

- Encourage issue raising,
- Value transparency,
- Reward learning,
- Support innovation,
- Mobilise quickly in crises,
- Embrace no-blame principles, and
- Integrate resilience into everyday decision-making.

Cultures that undermine resilience:

- Penalise mistakes,
- Operate in opaque silos,
- Hide issues,
- Suppress challenge, and
- Prize short-term production or delivery over long-term capability.

Culture is the single most reliable indicator of organizational resilience.

Conclusion

The case studies in this document reinforce a clear message: resilience is no longer a peripheral discipline – *it is a strategic capability rooted in leadership, culture, integration, and people.*

Resilient organizations are distinguished by:

- The maturity of their decision structures,
- The empowerment of their teams,
- Their willingness to learn, adapt, and experiment,
- The clarity of their resilience accountabilities and governance,
- Their ability to integrate diverse protective disciplines,
- Their strategic use of technology and data, and
- The degree to which resilience is embedded into strategy, culture, and customer value.

At its core, resilience is about *creating organizations that can adapt, evolve, and thrive in a world of uncertainty.*

The insights in this Executive Summary – built upon in the rest of the document – provide both a reflection of current practice and a roadmap for leaders seeking to advance resilience within their organizations.

The Evolving Role of Boards

Board leadership emerges from the case studies as an important determinant of organizational resilience. Boards set tone, appetite, and resource priorities. They are responsible for ensuring that resilience is not treated as a technical or compliance matter, but as an integrated strategic capability underpinning trust, performance, and long-term value.

Board engagement must extend to active governance, with clear accountability for resilience strategy, metrics, and improvement. The report advocates for formal board-level roles or committees dedicated to resilience, supported by regular reporting and scenario testing.

The following 'Board Briefing on Resilience Governance' provides a tool that organizations can use to develop and improve board engagement with resilience and to ensure that active governance of resilience is in place.

Board Briefing on Resilience Governance

Boards have a clear role in organizational resilience – *to provide governance, oversight, and professional curiosity, ensuring that resilience is embedded in culture, strategy, and operations.*

The board's role in resilience

Set the tone from the top: establish resilience as a strategic priority, not just a compliance function. Signal that resilience is about a people-focused culture, long-term sustainability, competitiveness, and trust.

Mandate clear governance: ensure that resilience has a defined place in governance structures, with board-level oversight, reporting lines, and accountability (e.g. Risk Committee, Audit Committee, or dedicated Resilience Committee).

Appoint leadership: consider the case for a Chief Resilience Officer or equivalent C-Suite ownership, ensuring that resilience has visibility and authority across silos.

Define appetite: agree and communicate the organization's tolerance for disruption and its appetite for resilience investment, in parallel with risk appetite.

Oversee integration: test whether resilience is embedded across strategy, operations, culture, and business structures – not confined to business continuity or IT disaster recovery.

Ensure alignment: with regulatory and industry requirements, while avoiding a tick-box compliance mindset.

Demand evidence: require metrics and reporting that go beyond compliance (e.g. maturity assessments, horizon scanning outputs, stakeholder feedback, lessons learned from incidents).

Champion continuous improvement: insist that after-action reviews, near-miss analyses, and lessons learned are reported to the board, acted upon, and tracked to closure at board level.

Balance protection and opportunity: recognise resilience as both defensive and reactive (protecting against shocks) and proactive (enabling adaption, agility, innovation, seizing opportunities, and competitive advantage).

Support investment: ensure that appropriate resources are allocated to people, culture, systems, and processes to sustain resilience over the long term.

Engage stakeholders: understand how resilience is communicated to investors, regulators, customers, employees, and communities – and hold executive management to account for building trust.

Probing questions for boards to ask

Leadership and governance

- Do we have a clear board mandate for resilience and who owns it at executive level?
- Should we appoint a Chief Resilience Officer with direct reporting to the board?
- How often do resilience updates appear on our agenda – is it only during crises?
- What is our process for challenging assumptions at board level?

Business structure

- Are crisis roles and responsibilities unambiguous and tested?
- Do our governance structures bring together all protective disciplines (risk management, cyber resilience, business continuity, physical security, supplier resilience, etc.)?
- Are resilience budgets fragmented or are they consolidated under clear ownership?

Strategy, tactics, and operations

- How is resilience integrated into our corporate strategy and long-term plans?
- Do we use resilience as a lens for identifying opportunities, not just threats?
- What are our impact tolerances for critical services and how are breaches reported to the board?
- How do we test and validate the resilience of our technology, digital, and supply-chain dependencies?
- How is resilience factored into long-term transformation, sustainability, and ESG strategies?

People and culture

- How are staff trained and empowered to respond to incidents?
- Do we foster a no-blame culture of psychological safety where near-misses are reported and lessons learned?
- How do we measure employee resilience awareness across the organization?

Risk radar

- What mechanisms do we have for horizon scanning and identifying risk signals?

Lessons learned

- How are lessons from incidents and exercises captured and embedded into strategy and operations?

Stakeholder trust

- How are resilience expectations communicated to regulators, investors, and customers?
- Are we engaging suppliers, partners, and clients in joint resilience planning?
- How do we monitor and retain stakeholder trust during times of change or crisis?

Practical Board Checklist

Have these things been achieved?

- Resilience appears regularly on the board agenda.
- Clear ownership and leadership.
- Crisis management roles are defined and rehearsed.
- Metrics and dashboards provide meaningful insight, not just compliance data.
- Budgets and resources match resilience ambitions.
- Lessons learned are acted upon and tracked at board level.
- Stakeholder trust is actively measured and managed.
- Resilience is embedded in long-term strategic planning.

THE PRINCIPLES OF RESILIENCE

As highlighted in the Introduction, one of the key aims of this document is to re-examine the Principles of Resilience that were previously developed by Airmic and determine whether they remain relevant, exploring this through a series of case studies.

The Principles of Resilience were developed in two stages by Airmic, starting in *Roads to Resilience* in 2014 (8) and further developed in *Roads to Revolution* in 2018 (9).

In *Roads to Resilience*, five Principles of Resilience were developed and described. These were subsequently reviewed in *Roads to Revolution* and expanded to eight principles and incorporated into a wider *Resilience and Transformation* model.

The eight Principles of Resilience function within four Business Enablers within organizations.

The Principles of Resilience are:

Exceptional Risk Radar

Risk Radar involves having the organizational capability to detect, interpret, and act on emerging risks and opportunities at a timely stage. This includes developing early warning systems for existing risks that may affect the organization, as well as building the capability to identify and anticipate future risks.

The requirement for *Exceptional* Risk Radar relates to the opportunity side of resilience. Understanding risks better than peers places the organization in a stronger competitive position. Resilience is not only about survival or just continuity; it is about being positioned to develop, grow, and thrive. In this sense, resilience becomes a source of competitive advantage. The ability to identify risks ahead of others – and to prepare for their potential realisation – can allow an organization to capture market share when those risks materialise and less resilient competitors struggle or fail.

Exceptional Risk Radar requires both a clear understanding of the current and emerging risk landscape and the development of a horizon scanning capability to anticipate longer-term risks, including chronic risks. Chronic risks are those that build slowly over time, rather than arriving as sudden shocks. They are persistent, long-term, and structural in nature, and they often erode resilience gradually.

Capabilities must therefore include a strong focus on emerging risks and opportunities, looking beyond the immediate situation. A thorough understanding of emerging risks involves assessing their shaping factors, probable trajectory, and potential impacts and consequences to determine where and how they might affect the organization.

Core components of Exceptional Risk Radar include:

Broad involvement

- Promote cooperation across the extended ecosystem, not just internally.
- Draw on diverse perspectives to identify risks earlier.

Constant vigilance

- Stay alert to weak signals that may indicate change.
- Use horizon scanning and scenario analysis to detect potential threats and opportunities.

Avoid complacency

- Learn from the mistakes and failures of other organizations.
- Regularly challenge assumptions and established practices.

Challenging questions

- Create forums where assumptions, plans, and strategies can be tested openly.
- Encourage a culture that welcomes difficult questions and constructive dissent.

Emerging risks

- Conduct structured horizon scanning to identify new trends and risks.
- Integrate early warnings into strategy, planning, and decision-making.

Flexible and Diversified Resources and Assets

Resilient organizations maintain resources and assets that are flexible and diversified. Where resources are insufficient, they must be strengthened to fully capitalise on technological advancements and other opportunities. The aim is to ensure that resources are adaptable, robust, and aligned with organizational purpose and risk appetite.

Having Flexible and Diversified Resources and Assets is related to:

- **Diversity of resources** – not relying on a single source of supply, type of asset, or way of operating.
- **Flexibility** – resources are adaptable so they can be repurposed during disruptions.
- **Technology use** – leveraging new technologies to improve adaptability and keep resource strategies current.
- **Workarounds** – enabling continuity when primary assets are unavailable.

Resilient organizations deliberately reduce dependency on single critical resources such as customers, suppliers, markets, brands, products, investors, knowledge, or business partners. They establish a clear operational risk appetite, then use scenario analyses and stress testing to identify vulnerabilities in strategy, tactics, and operations.

Core components of Flexible and Diversified Resources and Assets include:

- **Risk appetite** – defines operating boundaries, aligns with board-level risk attitude, and prompts consideration of dependencies.
- **Limiting dependencies** – avoids single points of failure.
- **Building flexibility** – ensures multiple ways to respond, such as alternative production sites or asset configurations.
- **Scenario planning** – examines resource implications, challenges assumptions, and prepares for uncertain futures.
- **Strengthening resources** – analyses and addresses weaknesses in the resource base to build resilience and better respond to opportunities.

Strong Relationships and Networks

Resilient organizations value and cultivate Strong Relationships and Networks, these will be both within the organization and externally, including with suppliers, contractors, business partners, and customers. Relationships need to be founded on trust, collaboration, and willingness to share information to ensure that issues are detected early and responses are rapid and effective. Transparently communicating about risks and incidents is required as part of this. Networks may need to be extended in unconventional ways, such as engaging in joint ventures with competitors, forming unconventional alliances, acquiring companies with totally new capabilities, and building networks across ecosystems to access new opportunities, technologies, and resilience strengths.

Core components of Strong Relationships and Networks include:

- **Shared purpose and values** – builds trust across organizational boundaries.
- **No-blame culture** – encourages openness, accountability, and learning rather than punishment when things go wrong. It also encourages people not to withhold information about organizational issues, risks, and mistakes.
- **Open communication** – real-time information sharing is vital to keep organizations aware of emerging risks. Flatter organizational structures, cross-functional collaboration, and self-organizing teams help in this area and avoid 'glass ceilings' or closed silos that block risk and resilience information flow.
- **Customer focus** – customer experience is central to resilience: this is the experience created by all of a customer's interactions and touchpoints with the organization.
- **Extend networks** – evaluate the scope for extending existing partnerships and networks.

Decisive and Rapid Response

Resilient organizations have the capability to carry out a rapid response to issues, incidents, and crises. This means ensuring that an organization can make well-informed decisions quickly and can act on them decisively, and successfully. This helps prevent escalation into crises, but when these do occur, the Decisive and Rapid Response capabilities ensure that impacts are minimised.

To achieve this principle, any communication barriers within the organization should be addressed. There is a need for cooperation between, or elimination of, silos within the organization, but in a way that does not create confusion of roles and responsibilities.

The core components of Decisive and Rapid Response are:

Decisive and appropriate actions

- Quick action helps prevent escalation.
- Ignoring issues is not acceptable – even small, repeated issues may indicate trends.
- Early recognition of opportunities is also a resilience benefit.

Identified teams and processes

- Processes provide a platform for response but must be adapted to specific circumstances.
- Skilled, trained, and frequently exercised cross-functional crisis teams take control of the crisis or emergency.

Empowered responses

- Flexible organizational capacity ensures space to respond effectively.
- Employees who are empowered to directly resolve issues (especially customer-facing employees) can prevent escalation.

Rehearsed reaction plans

- While exact scenarios can't be predicted, organizations can rehearse likely responses to plausible situations.
- Scenario exercises, crisis simulations, and awareness training build readiness.

Remove barriers

- Improve both internal and external communications by removing barriers, but without blurring responsibilities.

Review and Adapt

This principle requires organizations to review and analyse events, incidents, and crises, and adapt their strategies based on the information gathered, as well as using lessons learned from what went well and what did not do so. This is a continuous cycle of learning from things that have happened, as well as from changing circumstances, to improve resilience and performance over time.

Resilient organizations adapt not only processes and risk appetite but also strategy, tactics, and structures. They embed feedback loops into resilience, ensuring not just recovery but improvement too.

The core components of the Review and Adapt principle are:

Structured learning

- Risk management and resilience are always open to improvement and actively seek opportunities to adapt.
- Employees are trained in risk, and processes are regularly enhanced beyond the basics needed for compliance.
- Knowledge is captured and shared so that resilience isn't reliant on a few key people.

Near-miss reporting

- Every near-miss is reported and reviewed, with required actions recorded, identified, and taken.
- Detects small warning signs that behaviours or processes may need adaptation.

Independent reviewing

- Review of risk and resilience structures, processes, and performance by independent expert panels, non-executive directors, and auditors to help identify issues that may have been missed by internal teams.

Desire to improve

- Continuous improvement is embedded as a value.
- Lessons learned lead to real changes in strategy, tactics, operations, and structures.
- The board reviews lessons from incidents and near-misses as standing agenda items.

Enhance reputation

- Recognise the importance of resilience to organizational and brand reputation.
- Understand that resilience practices can directly affect how stakeholders perceive the organization. Adaptation is linked directly with trust and reputation management.

Redesign Processes

This principle is about using the capability to adapt to strategically rethink and restructure organizational processes in response to resilience requirements, as well as to fully exploit new technologies and opportunities. Success in this area is fundamentally based on a forward-looking culture that encourages innovation while retaining mechanisms to rapidly challenge and validate decisions.

Organizations must go beyond incremental improvements to be able to fundamentally Redesign Processes. This requires a culture of agility, experimentation, and forward planning that is aligned with strategy and operations. Mechanisms for validation are crucial to ensure that innovation and adoption of new technologies are robust and not simply fads or based on industry hype.

Core components of Redesign Processes include:

Embrace technology

- Identify opportunities to integrate new tools and capabilities.
- Use technologies such as AI, automation, and data analytics to improve efficiency and outcomes.

Process improvement

- Map the full customer journey and value chain to identify weaknesses.
- Continuously refine processes to improve speed, safety, cost, and environmental impact.

Encourage innovation

- Create space for experimentation, and reward innovative thinking.
- Build agility into the culture so that ideas can be tested and scaled quickly.

Validate decisions

- Use transparent, evidence-based methods to confirm that changes are robust.
- Avoid 'black-box' decision-making and challenge hype or untested assumptions.

Forward-looking

- Ensure that redesign efforts are aligned with long-term strategy and operational plans.
- Embed foresight into planning so that processes remain relevant as technologies evolve.

Retain Stakeholders

The ability to Redesign Processes will not maximise the benefits of doing so unless the organization also retains stakeholders through the process – and that is predicated to a large extent, in today's digital age, on the analysis of big data and on the leverage of technology including AI.

However, retaining stakeholders is also a wider resilience principle. In terms of revenue, the most important set of stakeholders are customers; and resilience management has customers at the heart of it. There is also a wide range of other stakeholders that need consideration, including suppliers, contractors, financiers, regulators, and communities.

Being able to easily communicate with stakeholders is an important aspect of the Retain Stakeholders principle – this not only helps ensure that stakeholder relationships remain positive and strong, but it also feeds into the organizational risk radar. Customers and suppliers, in particular, are often the first to notice emerging risks linked to organizational processes.

Redesigning processes should always include a consultation phase with stakeholders where opinions of the planned changes are obtained. Negative viewpoints may either result in a review and change in direction for the process redesign or, if no changes are made, they can provide the basis for a marketing and communications campaign to address the viewpoints.

Analysis of customer and stakeholder preferences using big data will provide a proactive mechanism for identifying stakeholder expectations.

Core components of Retain Stakeholders include:

Engage stakeholders

- Involve stakeholders in redesign and transformation planning, making use of digital channels, where appropriate, to ensure accessibility and transparency.

Share opinions

- Create channels for stakeholders to easily express views, concerns, and expectations.

Explain benefits

- Communicate clearly how the change, redesign, or transformation delivers tangible value.

Analyse big data

- Use customer, stakeholder, and other organizational data to understand behaviours and preferences, anticipate needs, and identify risks to customer and stakeholder trust.

Reinvent Purpose

The last of the eight Principles of Resilience – and perhaps the most radical – is Reinvent Purpose. Organizational purpose is an entity's fundamental reason for existing. It expresses what the organization is and does, and what value it creates for stakeholders. Reinventing purpose is based on a changing organizational environment and ecosystem, and requires opportunity awareness, the active commitment of stakeholders, and the availability of the necessary capabilities.

This principle emphasises the need for organizations to constantly consider whether their purpose should evolve or adapt. It requires attentiveness to emerging risks that may reshape the organizational environment and ecosystem, alertness to new opportunities, decisive commitment to new directions when required, and the development or acquisition of the capabilities needed to deliver change. The principle of Reinvent Purpose fosters a culture of constant evolution and adaptation within the organization, as well as the willingness and ability to make rapid changes where necessary.

Core components of Reinvent Purpose include:

Opportunity awareness

- Use risk radar to identify opportunities from digital technologies, market shifts, and societal changes.
- Build a culture that actively seeks new possibilities and challenges existing assumptions.

Active commitment

- Secure genuine buy-in from leadership, employees, and stakeholders.
- Ensure that reinventing purpose is not a top-down initiative but embraced across the organization.

Acquire capabilities

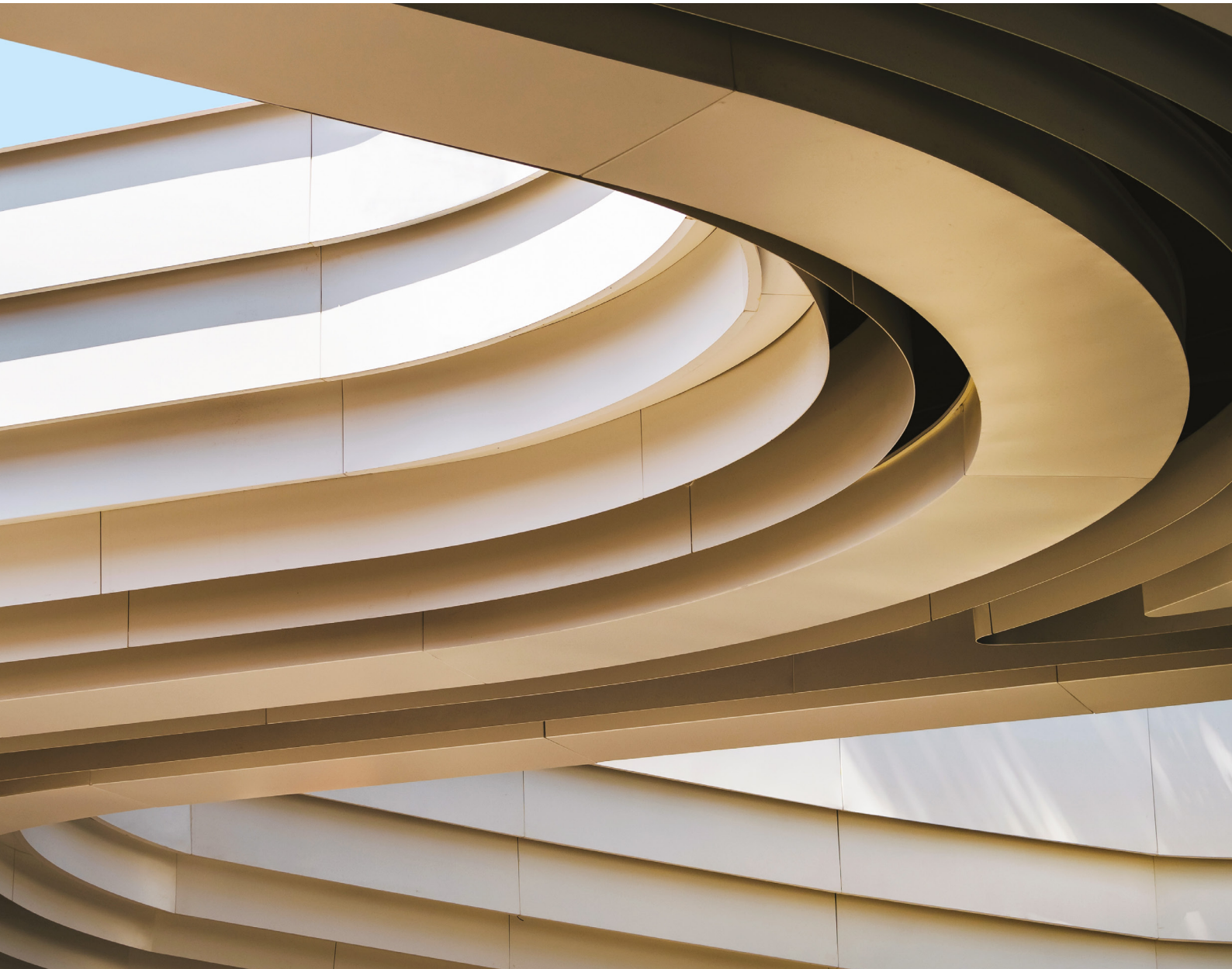
- Bring in the new skills, technologies, and expertise required.
- Invest in training and development to keep pace with changing needs.

Reward confidence

- Encourage and support forward-looking behaviour, experimentation, and innovation.
- Recognise and reward leaders and teams who successfully pursue new opportunities.

Constant evolution

- Treat reinvention as an ongoing adaptive process, not a one-off project.
- Continuously adapt purpose, strategy, and culture to stay relevant and resilient.



THE FOUR BUSINESS ENABLERS

For organizational resilience to be successfully introduced, developed, and sustained, board and C-level commitment, leadership, and oversight are essential. Without these, the Principles of Resilience will either be held back, reduced in effectiveness, or impossible to implement. In *Roads to Revolution* (9), Airmic introduced four Business Enablers that organizations need to have in place to provide the top-level structures, governance, and support that organizations need to be able to implement the Resilience Principles and to manage resilience effectively.

As with every aspect of resilience strategy, the board must take responsibility and provide leadership by setting the tone from the top, such that each Business Enabler supports the resilience agenda.

The Resilience Principles do not just happen; they reflect the fact that companies have nurtured a resilient environment through the Business Enablers.

The Business Enablers are:

- Leadership and Governance,
- Business Structure,
- Strategy, Tactics, and Operations, and
- People and Culture.

Whilst all organizations have these enablers, in some organizations, they are better developed than in others.

Leadership and Governance

This enabler focuses on establishing a proactive, relevant, and dynamic resilience agenda, supported by a clear board mandate. It involves robust leadership and governance arrangements, appropriate risk governance with proactive arrangements for receiving and examining risk information, and sufficient resources to explore and develop opportunities, including transformative options.

Business Structure

This enabler emphasises creating an inclusive and open organizational structure with an established resilience architecture, including representation from the extended ecosystem. It requires planned and rehearsed crisis management plans with nominated crisis management teams (CMT) and the absence of communication barriers, while avoiding confusion of roles and responsibilities. The aim is to ensure robust resilience governance protocols, procedures, and reports, and to evaluate and enhance resources, assets, relationships, and networks.

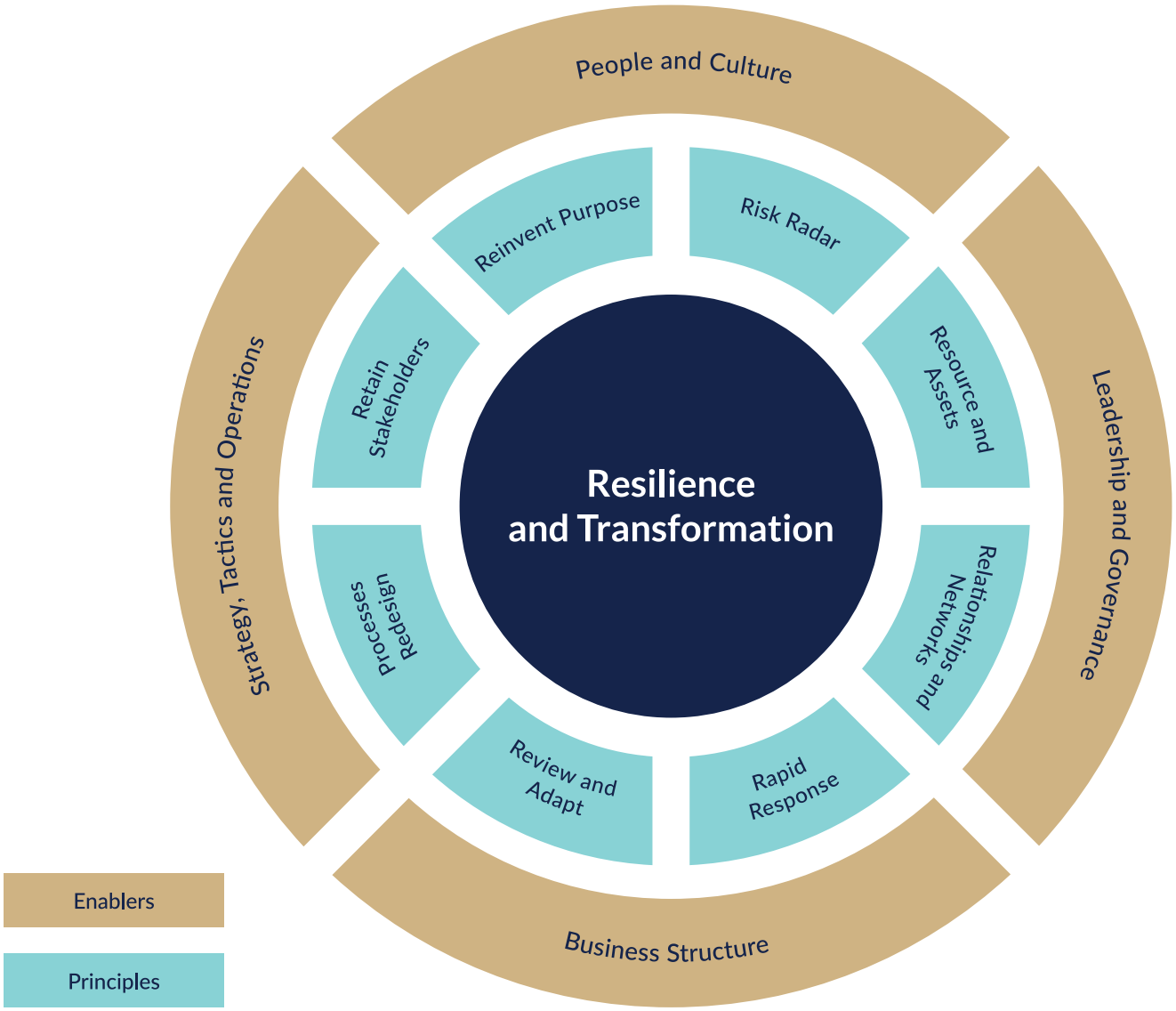
Strategy, Tactics, and Operations

This enabler aims to establish a resilience-based, well-informed, and integrated approach to organizational strategy, tactics, and operations. This includes a dynamic approach to resilience with a resilience development and action plan. Organizations must ensure that strategy, tactics, and operations progress smoothly and at the same pace, avoiding lags that can emerge from external developments moving faster than internal organizational processes. It involves establishing the organizational attitude to resilience, which includes considering opportunities as well as threats and undertaking suitable resilience assessment exercises.

People and Culture

This enabler is about fostering a culture that encourages a high level of resilience awareness across the organization to identify opportunities and threats, moving away from siloed thinking and inappropriate risk aversion. It involves enhancing people's resources, skills, and capabilities to achieve contextual resilience.

Resilience principles and enablers of the Airmic Resilience and Transformation Model.



THE CASE STUDIES

Research methodology

To explore how the Principles of Resilience and Business Enablers are reflected in practice, seven in-depth case study interviews were conducted with senior resilience leaders between July and September 2025. The interviewees were selected to provide a cross-sector snapshot of how organizational resilience is governed and delivered in practice, rather than to represent any statistically representative sample.

Participating organizations were chosen to reflect diversity across:

- Sector (including manufacturing, professional services, technology, financial services, and critical infrastructure),
- Geographic footprint (regional, multinational, and global),
- Organizational scale and maturity, and
- Regulatory exposure.

Each interview was semi-structured and followed a consistent framework aligned to the four Business Enablers. Additional questions explored current resilience maturity, future ambition, challenges, and innovation.

Interviews were conducted under conditions of anonymity to enable openness and frank discussion of challenges, shortcomings, and internal dynamics. As a result, all organizational references have been anonymised to avoid disclosure of sensitive or commercially identifying information.

Following the interviews, transcripts and notes were analysed thematically to identify recurring patterns, points of convergence, and areas of divergence across the case studies. These themes informed both the Executive Summary and the structuring of insights throughout the document.

This approach does not provide statistically proven information; instead, it offers structured, practice-based insights into how organizational resilience is currently being interpreted, governed, and embedded across real-world organizational contexts, with the intention of providing practical learning and strategic reflection for boards, executives, and resilience professionals.

The case studies follow a consistent structure:

Background information

- Organizational context
- Vision and approach to resilience

The four Business Enablers in reality

- Leadership and Governance
- Business Structure – resilience structure and integration
- Strategy, Tactics, and Operations
- People and Culture

Maturity

- Current resilience maturity and future vision
- Challenges that need addressing

Innovation

- Notable innovations and areas of focus.

Case Study One: Global Energy Manufacturer

Interviewee: Senior Business Continuity Manager

Organizational context

This organization is a fast-growing energy manufacturer that has scaled up quickly. Its first major factory in the western United States was established a decade ago, with output soaring year on year, in what is one of the world's largest facilities of its kind. A new, even larger facility was launched in 2025 to support additional production. Further expansions are planned over the next decade.

The pace of development has been rapid, yet this growth has also created new vulnerabilities. While the first factory supplies a single customer and sits physically adjacent to that client's operations, the newer site must serve multiple global customers and deliver across complex logistics networks, as well as cementing its role and reputation within its local community. The organization's challenge is to balance relentless production targets with a need for resilience at a scale that matches its ambitions.

Vision and approach to resilience

Resilience is currently defined around three separate functions: risk management, business continuity, and emergency management. The organization uses a Risk Council model to assure a joint approach to risk assessment and management, and to enhance cross-function resilience communications.

While the current resilience structure provides a functional baseline, the interviewee had a much wider vision for organizational resilience at the company. This is for resilience direction to move to the C-level, led by a Chief Resilience Officer, who can provide unified strategic leadership for all the organization's protective functions – the existing business continuity, risk management, and emergency management functions – and bring information security, physical security, and health and safety under their remit. This role would also provide a direct channel to and from the C-Suite, as well as direct reporting to the Board, ensuring that all the company's top leadership has visibility of, influence over, and responsibility for organizational resilience.

The interviewee had a very clear philosophy: resilience is not simply about recovery, it can be a strong competitive advantage in its own right. By embedding resilience into design, operations, and strategy, the organization can recover faster and adapt better than its competitors, when impacted by the same issue (a pandemic, for example). This approach enables highly resilient organizations to seek opportunities and exploit them, when competitors struggle to respond as quickly, or at all.

The four Business Enablers in reality

Leadership and Governance

At present, governance is anchored in ISO compliance and audit cycles. This ensures that the organization meets external requirements, but while many in the wider resilience profession see ISO certification as an end goal, this organization sees it as a minimum threshold to build upon.

Formal governance policies exist for risk, business continuity, and emergency management, which set out organizational expectations.

Resilience is reviewed quarterly at executive level, but it is not included in the organization's 10-Year Strategic Plan. This was seen by the interviewee as a missed opportunity to embed resilience into the organizational DNA, particularly since the Strategic Plan is used as the agenda for leadership summits. In attempts to compensate, where possible, the interviewee reframed company language around resilience – for example, redefining the word 'sustainability' in mission statements as not only environmentalism but organizational survivability. This creative repositioning has helped keep the concept of resilience alive in board-level discussions, but genuine top-down ownership was still missing. As highlighted above, the interviewee saw the creation of a Chief Resilience Officer role as essential to elevate resilience beyond compliance, align resources, and prevent strategic blind spots.

Business Structure – resilience structure and integration

The lack of a Chief Resilience Officer means that resilience responsibilities remain fragmented across departments, said the interviewee. This led to the interviewee estimating the maturity of integration between various aspects of resilience management as being four out of ten.

To counter this, factory-level Risk Councils have been established. These multidisciplinary forums meet monthly and draw together representatives from business continuity, emergency management, employee health and safety, information security management, quality, finance, production, physical security, and legal (as a non-voting advisor).

The Risk Councils follow a structured process:

- **Risk submission** – any employee or Risk Council participant can submit and escalate risks.
- **Classification** – risks are assessed as major or minor. Minors return to the individual business units that own that risk; majors go onto the risk registry.
- **Scoring** – each Risk Council member rates risks against weighting factors, including impact, likelihood, velocity, vulnerability, preparedness, and demonstrated recovery capability.
- **Prioritisation** – scores are averaged and ranked, with the top risks escalated.
- **Executive reporting** – Quarterly Risk Review Boards receive information about the top three unmitigated risks with recommended actions, in addition to updates on previously presented risks and mitigation strategies that are ongoing.

Various metrics have also been identified, which are under development. These include:

- The percent of the top 15 risks that are under mitigation (target >75%).
- The average days from identification to mitigation (target <90 days).
- The proportion of risks that have been 'hibernated' (partially mitigated, insured, and now actively monitored).

This approach has cut through 'risk fatigue', giving confidence that issues are consolidated and objectively prioritised. It has also created a scalable model that could, in time, feed into enterprise-wide resilience oversight.

Resilience budgets are fragmented across risk, business continuity, emergency, and physical security management. As a result, the interviewee often had to be creative about enhancing the budget, for example, by persuading organizational peers to co-fund initiatives.

Strategy, Tactics, and Operations

The Risk Council provides the baseline starting point for all resilience outputs, as well as being the 'glue' that helps inter-departmental communication, acting as an integrated starting point for resilience requirements, and giving insight into the different protective silos.

Tactically, structured risk scoring and targeted exercises anchor resilience in operational reality. Executives are engaged through memorable tabletop simulations that mirror the risks being escalated to them. These exercises make resilience tangible and keep it in leaders' minds when investment decisions are made.

Operationally, production pressures remain a challenge. In the new plant, for example, resilience recommendations made during construction were overridden in favour of short-term cost savings, the implementation of a distributed antenna system was stopped, resulting in communications dead zones, and the opportunity to include predictive maintenance systems was not taken, missing a strong resilience-by-design opportunity.

These issues exemplify the cost of resilience not being embedded in C-Suite decision-making, said the interviewee. Without authority, resilience leaders cannot advocate against or prevent short-term cost-saving measures that reduce resilience. Critical decisions are being made without the voice of a single resilience advocate in the room.

People and Culture

Resilience awareness across the workforce is limited and typically only occurs during the new employee onboarding process. Efforts to address this include short annual supervisor training sessions and a light-hearted communications campaign based on the TV series *Breaking Bad*, which is branded 'Better Call Business Continuity'. This is aimed at building recognition across breakrooms and factory displays. The success of resilience education and awareness is not measured – and this is a challenge that needs to be addressed, said the interviewee.

At the leadership level, engagement is stronger. Tabletop exercises are remembered long after they are run, helping resilience messages cut through. However, a production-first culture dominates. With executives focused on 'ever-increasing numbers', resilience is often sidelined and initiatives to embed resilience into processes or strategy can be crowded out by short-term production goals. The production-centric teams' focus on resilience is at the most granular level, missing the larger picture and often inadvertently building a lack of resilience into the larger system.

When operating at the forefront of production output, it becomes extremely difficult to squeeze even a tenth of a percentage-point of additional output, despite tremendous attention, resources, and effort. The focus on production is so myopic that the organization fails to see giant boulders of opportunity, while grasping at a grain of sand. The interviewee had been attempting, without much success, to convince leadership that much more efficiency and output could be achieved by focusing on resilience efforts. By preventing the shutdown of lines or phases due to completely foreseen risks, tens of millions of units in production a year could be preserved.

Maturity

Current resilience maturity and future vision

Resilience maturity was estimated by the interviewee at six out of ten. There is real progress – in terms of the Risk Councils, formalised plans, policies, and ISO compliance – but also significant gaps. The function remains under-resourced, often only one person deep at each site, and lacks an executive voice. The interviewee, a 20+ year MBCP, presenter, and thought leader in this field, had been spending 90% of their efforts and energy in completing specialist level tasks due to the lack of personnel.

The interviewee's future vision was clear: establishment of a centralised resilience function led by a senior executive, supported by dedicated teams of professionals at each major facility. Budgets would be consolidated under this structure, allowing more consistent investment and oversight. Resilience would also be integrated into corporate strategy, facility design, and long-term planning. Emerging technologies, in particular AI and digital twins, are expected to play a transformative role in achieving this vision.

The interviewee saw digital twins as the best way to imbed predictive operations, creating a highly detailed digital map of each factory and mapping every component to generate value stream mapping. The advantages of this include:

- **Predictive maintenance** – identifying when machines/components are likely to fail before breakdowns occur.
- **Hazard simulation** – for example, a water leak on the second floor could be mapped against nearby hazmat storage or comms closets below, allowing pre-emptive action.
- **Incident response** – enabling responders to see the impact of an issue across layers (e.g. water flow, hazardous materials, camera systems, and critical equipment).
- **System-wide awareness** – moving from siloed data to integrated insight by feeding all departmental data into a single model, driven by Essential Elements of Information (EEIs).

Challenges that need addressing

Several obstacles need to be overcome for resilience to advance:

- **Lack of senior representation** – without C-Suite ownership, resilience representatives find it difficult to influence strategy.
- **Fragmented ownership** – protective functions are siloed, although the Risk Council provides some cross-silo communication and focus. As a minimum, business continuity, emergency management, and risk management must be consolidated under a single leader, said the interviewee.
- **Resource scarcity** – resilience is currently one-person deep in some areas. To mature, the interviewee believes that the organization needs a team of at least two resilience professionals (specialist and manager) per site, but optimally should consist of an emergency management professional, a business continuity professional, and a risk management professional.
- **Budgets** – fragmented budgets make it difficult to make the required resilience investments. Mitigation strategies must be 'pitched' to whichever business unit the risk aligns closest with, in the hope that they can 'sell' them on committing their resources. The organization should instead have a large resilience reserve fund.
- **Production obsession** – a cultural focus on output almost always sidelines resilience according to the interviewee. Resilience only gets some traction in the immediate aftermath of a disruption event.
- **Missed opportunities** – cost-saving during facility construction has undermined resilience-by-design opportunities. When every leader is fixated on today's production, the organization becomes blind to the strategic projects that would transform tomorrow. A true-to-scale ArcGIS digital twin would elevate every function, but production urgency buries anything that isn't immediate.

Innovation

Notable innovations and areas of focus

Despite constraints, the organization has developed several innovative practices:

- **The Risk Council model** – a structured, highly metric-driven system that consolidates risks, reduces executive overload, and prioritises action.
- **AI and data use** – the interviewee was very pro-AI and saw it as an emerging force multiplier in three areas:

  Supplier resilience scoring – using AI to evaluate hundreds of vendors rapidly, reviewing documents, comparing against standards, and generating prioritised risk lists.

  Maintenance optimisation – analysing thousands of records to identify patterns, predict failures, and improve production efficiency.

  Digital twin augmentation – linking data layers to create predictive, real-time situational awareness and to create value stream mapping.
- **Reframing language** – using the language of sustainability and competitiveness to embed resilience concepts into executive priorities.

Conclusion

This case study highlights strong achievements as well as the challenges of building resilience within a fast-growing manufacturing company. The Risk Council model demonstrates how structured processes and clear metrics can cut through risk fatigue and deliver practical improvements, while reframing resilience in the language of competitiveness shows how resilience can be positioned as a business advantage rather than simply a cost. Yet, the organization's resilience remains constrained by silos, limited resources, and a cost-saving production-first culture. The interviewee's vision for a Chief Resilience Officer and an integrated, strategically-led resilience function offered a clear pathway forward – one in which resilience is not just compliance or recovery, but a true competitive advantage embedded at the heart of corporate decision-making.

Case Study Two: Global Professional Services Firm

Interviewee: Risk and Resilience Director

Organizational context

This global professional services firm operates across multiple jurisdictions, with thousands of employees and a highly complex structure. The organization is client-facing and heavily dependent on technology, data, and supplier networks. Its business model is both people-centric and software-driven, requiring a large number of applications to deliver client value.

A defining moment in the firm's history was a major cyber incident nearly a decade ago, which rendered operations unavailable for weeks. This disruption left a deep imprint across the organization, shaping its culture and securing long-term leadership buy-in for resilience. The experience created urgency, ensured sustained investment, and remains a powerful motivator for continuous improvement.

The above meant that at the time the interviewee joined, the firm already had an unusually mature risk and resilience culture compared to peer companies, with particularly strong capabilities in information security, business continuity, IT disaster recovery, and procurement. However, these departmental structures largely operated in silos, with duplication and little integration. The interviewee sought to bring these strands together under a unified framework for organizational resilience, while ensuring alignment with strategy and sustainability objectives. The approach was based on the principle that the best frameworks overlay existing structures rather than demanding wholesale redesign.

Vision and approach to resilience

The interviewee's vision was to embed organizational resilience as a core enabler of sustainable business, rather than adopting a narrower regulation-driven model of operational resilience based on that found in financial services. The approach was holistic and incorporated risk management, business continuity, cyber, supplier management, sustainability, and crisis response.

The guiding principle was to: "Do fewer things, but do them better." Instead of cataloguing hundreds of processes across jurisdictions, the firm mapped its client value chain – from winning work to delivery and billing – and identified 15 to 20 truly critical processes. Similarly, the application landscape was rationalised: of around 700+ systems, approximately 60 were classified as critical after interdependency mapping. Supplier resilience was focused on 'Crown Jewel' partners – i.e. the most important ones.

Resilience is now tied directly to business strategy, ensuring that it supports delivery of the firm's objectives. It is also explicitly linked to the mandate of the current CEO, which is to hand over a more resilient business than was in place when they joined the firm.

The four Business Enablers in reality

Leadership and Governance

Governance is structured around board-level oversight, including non-executive directors with risk and resilience expertise, supported by dedicated Risk and Audit Committees. Quarterly reporting covers post-incident reviews, exercise reports, and details of lessons learned. The board challenges and probes, and non-executives provide external perspective, while also commending good practice. Led by the CEO, who has a personal interest in this area, the board asks for clear resilience metrics to support reporting and to make progress clear.

Strategic resilience leadership is rooted in the Risk and Resilience Senior Leadership Team (SLT), which meets weekly to discuss resilience priorities, set current direction, and review post-incident reports, supplier risks and issues, and improvement actions. These are escalated from the SLT to the board's Risk Committee, creating a feedback loop where improvements are tracked and embedded.

The SLT is a multidisciplinary senior group coordinated by the Risk and Resilience Director. It consists of leaders from:

- Risk and Resilience
- Cyber/Information Security

- IT/Technology
- Business Continuity and Disaster Recovery (BCDR)
- Procurement
- Legal/General Counsel's office (especially providing input on supplier and contract resilience)
- Communications and travel risk (regularly integrated into SLT discussions).

A Gold–Silver–Bronze structure governs incident response. A 'Core Gold' group of four senior leaders has delegated authority to make rapid strategic decisions, supported by the communications and risk functions. Core Gold can make decisions without full C-Suite involvement, preventing 'paralysis by debate' and ensuring decisive action. Silver teams provide tactical coordination, led by resilience professionals and supported by scribes, while Bronze teams consist of local managers and technical specialists.

In addition, a Business Emergency Response Team (BERT) provides 24/7 cross-functional incident response across cyber, IT, BCDR, travel, security, communications, and geopolitical risk. Specialist Business Response Teams (BRTs) exist for high-risk domains such as cyber and critical suppliers.

Policies exist across all relevant areas: business continuity, disaster recovery, cyber security, supplier resilience, procurement, crisis management, and sustainability/ESG. These are complemented by assurance mechanisms. Internal audit, newly created under the interviewee's leadership, benchmarks resilience arrangements and feeds findings to the Audit Committee. External audits, including ISO certification processes, provide further scrutiny.

The firm is aligned to ISO 22316 (5) and is pursuing ISO 22301 (10) certification to meet client expectations. The interviewee, however, cautioned against over-prescriptive audits turning into 'paper exercises', emphasising the importance of lived practice over documentation. In terms of ISO 22301, the interviewee recognised the standard as a good template and useful for external assurance, but believed that it often forces the creation of more documentation than is genuinely useful – mainly due to auditors who insist on prescriptive language and evidence.

Business Structure – resilience structure and integration

Resilience and risk functions are deliberately combined under a single director, elevating resilience from a supporting role to a strategic capability. This contrasts with the previous structure, where risk sat with compliance and resilience was fragmented. Integration has reduced duplication, increased profile, and clarified accountability.

Cross-functional forums bring together IT, cyber, procurement, legal, and resilience teams to align on priorities such as supplier due diligence, technology tiering, and incident response. These are framed deliberately as forums rather than formal committees, to emphasise collaboration over bureaucracy.

Supplier and value chain resilience is a particular focus. The legal team embeds resilience requirements into contracts and procurement undertakes detailed due diligence, which requires evidence from suppliers. Crown Jewel suppliers are managed through playbooks and exercises, while less critical suppliers are monitored through lighter-touch arrangements.

The integration agenda remains an ongoing journey. Constant organizational change, including new offices, products, acquisitions, and employee flux, means that silos can re-emerge, requiring continuous effort in this area.

Strategy, Tactics, and Operations

Strategically, resilience is aligned to the firm's business plan. A new corporate strategy was reviewed through a resilience lens, with critical processes mapped against its delivery. This now ensures that resilience actively enables growth. This has been further enhanced by a strong focus on customers. Mapping the client value chain and identifying processes that are truly critical to enable client services and making these the focus of resilience activities has been a vital step, ensuring that resilience is directly tied to client value delivery.

Supplier resilience has also been framed in client terms: the firm has identified and focused on the suppliers that are the most critical to client delivery outcomes, developing playbooks and exercises around those. Supplier SLAs (service level agreements) are now aligned with client SLAs, identifying gaps and exploring insurance solutions to protect against situations

where supplier failures could prevent the firm meeting client commitments.

Operationally, incident response structures provide round-the-clock coverage. BERT operates continuously, monitoring global risks and escalating to Gold teams when required. Employees in every office have an emergency hotline printed on ID cards, enabling rapid contact with resilience teams. Playbooks for Crown Jewel suppliers are tested through both tabletop and hands-on exercises, while broader functions such as finance are also brought into resilience testing.

This integrated approach was proven during the CrowdStrike incident, where the firm identified and acted ahead of peers, preventing wider disruption.

People and Culture

Resilience culture is built through widespread engagement and training. Employees receive resilience information during induction training, supplemented by roadshows and targeted awareness sessions. Local resilience champions – often property or workplace managers at each office location – act as the 'eyes and ears' of the programme. In addition, the BERT number, printed on all staff ID cards, gives employees direct, rapid, and universal access to resilience teams.

Success is measured not only by training completion rates but by performance in post-incident reviews. Initially, success meant more staff reporting incidents via hotlines. Over time, the measure has evolved: now, the aim is for resilience teams to detect and act before staff notice issues. Third-party testing and exercising is an instrumental component for measuring, embedding, and improving performance.

Leadership engagement is a critical cultural driver. The CEO personally reviews emergency messaging test results and reinforces the importance of resilience in communications. The CEO's explicit mandate (to leave a more resilient firm than they inherited) provides a powerful signal across the organization.

The interviewee emphasised the importance of persuasion skills in resilience leadership. Much of the role involves 'selling the vision', securing buy-in across departments and maintaining momentum in the face of organizational complexity.

Maturity

Current resilience maturity and future vision

The interviewee estimated the firm's resilience maturity to be eight out of ten. This reflects the depth of integration, board engagement, and cultural embedding achieved. Resilience is viewed as a core enabler, not just a compliance obligation, and is well resourced.

The future vision is to continue to develop a self-sustaining, proactive capability. This will include greater use of data analytics for horizon scanning and stress testing, deeper integration with strategy, and further rationalisation of resilience processes to avoid bureaucracy.

Challenges that need addressing

Despite maturity, challenges remain:

- **Scale and complexity** – as a global, matrixed organization, uniform processes are hard to implement consistently.
- **Constant change** – new products, acquisitions, and staff changes demand a constant focus on integrating resilience.
- **Analytics gap** – while geopolitical horizon scanning is in place, advanced analytics for resilience insights and scenario modelling remain underdeveloped or underutilised.

Innovation

The case study highlights several innovations:

- **Client value chain focus** – mapping resilience to 15 to 20 critical processes tied directly to client delivery, rather than attempting to document hundreds of peripheral processes.
- **Application rationalisation** – reducing the critical application set to just 10% and tiering the rest, ensuring that resources are focused.

- **24/7 Business Emergency Response Team (BERT)** – a cross-functional team covering cyber, IT, resilience, security, communications, travel, and geopolitics, on rotation, and actively monitoring risks.
- **Core Gold Team** – a small group with delegated authority for rapid decision-making, ensuring speed and clarity in crisis response.
- **Risk and Resilience Senior Leadership Team** – a holistic team consisting of leaders from across the operational areas, which meets weekly to prioritise and review.
- **Supplier playbooks** – bespoke resilience arrangements for Crown Jewel suppliers, exercised jointly to ensure preparedness.
- **Integrated forums** – bringing together procurement, legal, IT, and resilience functions to coordinate supplier resilience and technology priorities.
- **Emergency hotline** – universal access for staff to resilience teams, supported by ID card numbers and local champions.

Conclusion

This case study demonstrates how a global professional services firm has transformed resilience from a siloed set of functions into an integrated, strategic capability. The journey has been shaped by lived experience, in particular by a major cyber incident that created lasting cultural awareness and board-level commitment. Under the interviewee's leadership, resilience has been reframed as a value enabler, tied directly to client delivery, corporate strategy, and the CEO's individual mandate.

Key enablers of success include a clear governance structure with active non-executive involvement, the creation of a multidisciplinary Risk and Resilience Senior Leadership Team, and an emphasis on prioritisation – focusing on a small number of critical processes, applications, and suppliers. Innovative practices such as the 24/7 Business Emergency Response Team, bespoke supplier playbooks, and a Core Gold rapid decision-making team provide operational strength, while extensive staff engagement and cultural embedding ensure that resilience is something that all employees are aware of and encouraged to support.

Although the firm has reached a high level of maturity, ongoing challenges stem from its global scale, rapid pace of change, and the need to strengthen data analytics for horizon scanning and proactive insights. Addressing these will be central to realising the vision of a self-sustaining, forward-looking resilience capability.

Overall, the case study illustrates how resilience, when embedded strategically and culturally, not only safeguards continuity but also enhances client value and organizational sustainability.

Case Study Three: Multinational Corporate

Interviewee: Global Business Continuity Manager

Organizational context

This large organization has operations spanning Europe, Africa, and parts of Asia. It delivers a variety of consumer services and enterprise solutions for multinational businesses, and an expanding suite of digital services that includes Internet of Things (IoT), payments, and cloud.

Its global structure combines a group-level governance framework with local market autonomy. National entities retain operational independence but must align to overarching policies and standards. This creates a balance between flexibility to serve local customers and consistency across the enterprise.

The interviewee works within the Corporate Security function, holding global responsibility for business continuity and crisis management. The remit covers policy development, strategic coordination, and support for local markets. Enterprise clients – in particular governments, banks, and manufacturers – set especially high expectations for resilience, requiring robust business continuity capabilities as a precondition for partnership.

The organization's critical operations focus on network availability, data services, and customer-facing platforms. As these constitute critical national infrastructure in some cases, resilience priorities are shaped not only by business needs but also by national regulations and directives.

Vision and approach to resilience

The interviewee described organizational resilience as a holistic capability extending far beyond traditional business continuity planning. The approach spans:

- **Business continuity and crisis management** – the interviewee's direct area of oversight.
- **Cyber resilience** – embedded within the technology and IT function.
- **Physical, travel, and event security** – incorporated into the wider Corporate Security domain.
- **Fraud and regulatory security** – complementary areas linked to resilience.
- **Operational resilience** – an emerging focus, particularly driven by financial-sector and EU regulation.

Resilience is thus multidimensional, cutting across technical, physical, operational, and cultural domains. The interviewee emphasised that while compliance with international standards is important, true resilience comes from embedding capabilities as strategic advantages. Resilience is understood not simply as recovery, but as a capacity to adapt, evolve, and thrive in a challenging environment.

The four Business Enablers in reality

Leadership and Governance

Governance within the organization is multilayered, reflecting the size and complexity of its operations.

- **Executive Committee** members champion resilience within their own domains – technology, HR, external affairs, and others. They review risks, audit findings, and resilience issues as part of regular oversight.
- **The Audit and Risk Committee** provides independent scrutiny of principal risks, including resilience.
- **Second line assurance** is delivered by central assurance and testing teams, measuring compliance against policy.
- **Third line assurance** comes from internal and external audits, including certification against standards such as ISO 22301 (10) and 27001 (11) in selected markets.
- **First line assurance** is carried out by operational teams who implement and deliver resilience activities day to day.

Policies are developed by a dedicated security policy unit, with each policy owned by a senior Executive Committee member. For example, the Technology Resilience policy is owned by the Chief Technology Officer.

Resilience is regularly on the agenda of the Executive Committee and Audit and Risk Committee, supported by dashboards that track key metrics such as risk assessment results, completion of business impact analyses, business continuity plan reviews, crisis exercises, and policy compliance. Dashboards are available at both local and group levels, ensuring transparency across the organization.

Budget responsibilities remain fragmented across domains. The interviewee manages business continuity and crisis management budgets, while cyber and physical security maintain their own. This fragmentation makes collaboration essential, though it sometimes dilutes holistic oversight.

The interviewee articulated a vision of bringing resilience functions under a single vertical to overcome siloed approaches. They stressed that external pressures – in particular, regulation and geopolitical risk – are accelerating movement towards more integrated governance.

Business Structure – resilience structure and integration

Resilience functions are currently distributed:

- **Corporate Security** encompasses business continuity management, crisis management, travel, physical, and event security.
- **Technology/IT** is responsible for cyber resilience.
- **Risk Management** oversees enterprise risk.

This distribution inevitably results in silos, yet integration mechanisms exist, including simulations and crisis exercises that bring domains and multiple functions together.

In addition, the Audit and Risk Committee provides a forum for cross-domain governance, while external sector forums allow collaboration with industry peers, despite commercial competition.

The interviewee acknowledged the transitional nature of the current model. Progress has been made towards greater integration, but true holistic oversight remains a work in progress.

Strategy, Tactics, and Operations

The organization maintains a comprehensive set of global capabilities covering business continuity, crisis management, cyber, and physical resilience. While these are assessed regularly to reflect changing international standards and regulatory obligations, the interviewee stressed the importance of moving beyond compliance being the driver for resilience. ISO certification, while valuable, is treated as a minimum baseline. The aim is to position resilience as a source of strategic advantage – demonstrating reliability to clients and regulators, while enabling agility in rapidly changing environments.

Operationally, crisis escalation procedures are clearly defined. Severe incidents are escalated to a triage team, which includes a director, the interviewee, and the relevant function lead. This team determines whether to invoke a full crisis response, which may then be escalated to the Executive Committee. The structure ensures that rapid, informed decisions can be made at the right level.

Technology and data play an increasing role. Dashboards consolidate key information, while artificial intelligence is being piloted to summarise data, generate personas for training, and enhance situational awareness. These tools are helping the organization to manage the sheer scale of global risk data and other relevant information.

Exercises and simulations are an essential tactic, ensuring that disparate functions can come together under pressure. Reviews and lessons-learned exercises are mandatory, with findings reported to group level and occasionally validated by external consultants. The enterprise also takes part in larger-scale simulations organized by external third parties. These often include competitors.

People and Culture

The interviewee placed strong emphasis on resilience as a cultural attribute. Formal processes and policies are necessary but are insufficient without a workforce that internalises resilience as part of its mindset.

Awareness is reinforced through multiple mechanisms:

- Induction programmes for new employees include resilience from the outset.

- Mandatory training is recorded in HR profiles for staff with specific business continuity or crisis response responsibilities.
- A digital learning platform provides on-demand modules, videos, and campaigns.
- A dedicated security awareness team runs communications and simulations to embed resilience knowledge.

Top leadership advocacy is seen as vital. Senior leaders are expected to model resilient behaviours, allocate resources, and talk about resilience in employee forums. Transparency is also important – sharing lessons learned openly after incidents builds collective understanding.

The organization participates in peer-learning forums, adopting best practices from other companies and industries where appropriate.

The interviewee noted an opportunity to deepen integration with HR, particularly around hybrid working. Resilience considerations are not always systematically embedded in HR-driven initiatives, but could be in the future.

Maturity

Current resilience maturity and future vision

The organization's resilience journey spans many years. Early on, functions operated largely in silos, with local markets maintaining autonomy and showing varying maturity levels. Over time, group-wide standards have been introduced, supported by audits, crisis exercises, and harmonised policy frameworks.

Today, most local markets exhibit advanced levels of maturity, although some entities are still developing. At group level, maturity is recognised as a moving target – resilience must be continuously updated rather than treated as a fixed end state.

The interviewee's future vision rests on several pillars:

- **Holistic integration** of resilience functions into a single vertical.
- **Culture-driven resilience** where leaders advocate and employees take responsibility.
- **Resilience-by-design**, embedding redundancy, flexibility, and adaptability into operations and systems from the outset.
- **Continuous learning,** with no sense of completion but constant improvement.

Leveraging technology, including AI, digital twins, and data lakes, to transform how resilience is analysed, tested, and embedded.

Innovation

Notable innovations and areas of focus

Innovation is an area of increasing emphasis. The interviewee highlighted several current initiatives:

- **Use of AI and automation:** AI tools are employed to process large datasets, generate scenarios, and support training. This allows for faster analysis and richer insight into emerging risks.
- **Dashboards and visualisation:** Power business interruption dashboards provide transparent, multi-level reporting to both local and group leaders.
- **Geopolitical risk intelligence** – a dedicated team produces forward-looking risk reports, helping the organization anticipate global disruptions such as tariffs, wars, or regional instability.
- **Industry collaboration** – by participating in various sector forums, the organization shares intelligence and best practices even with competitors, recognising that resilience challenges often transcend competition.
- **Post-incident reviews** – the organization enforces structured after-action reviews, sometimes using external consultants, to drive genuine learning rather than tick-box compliance.

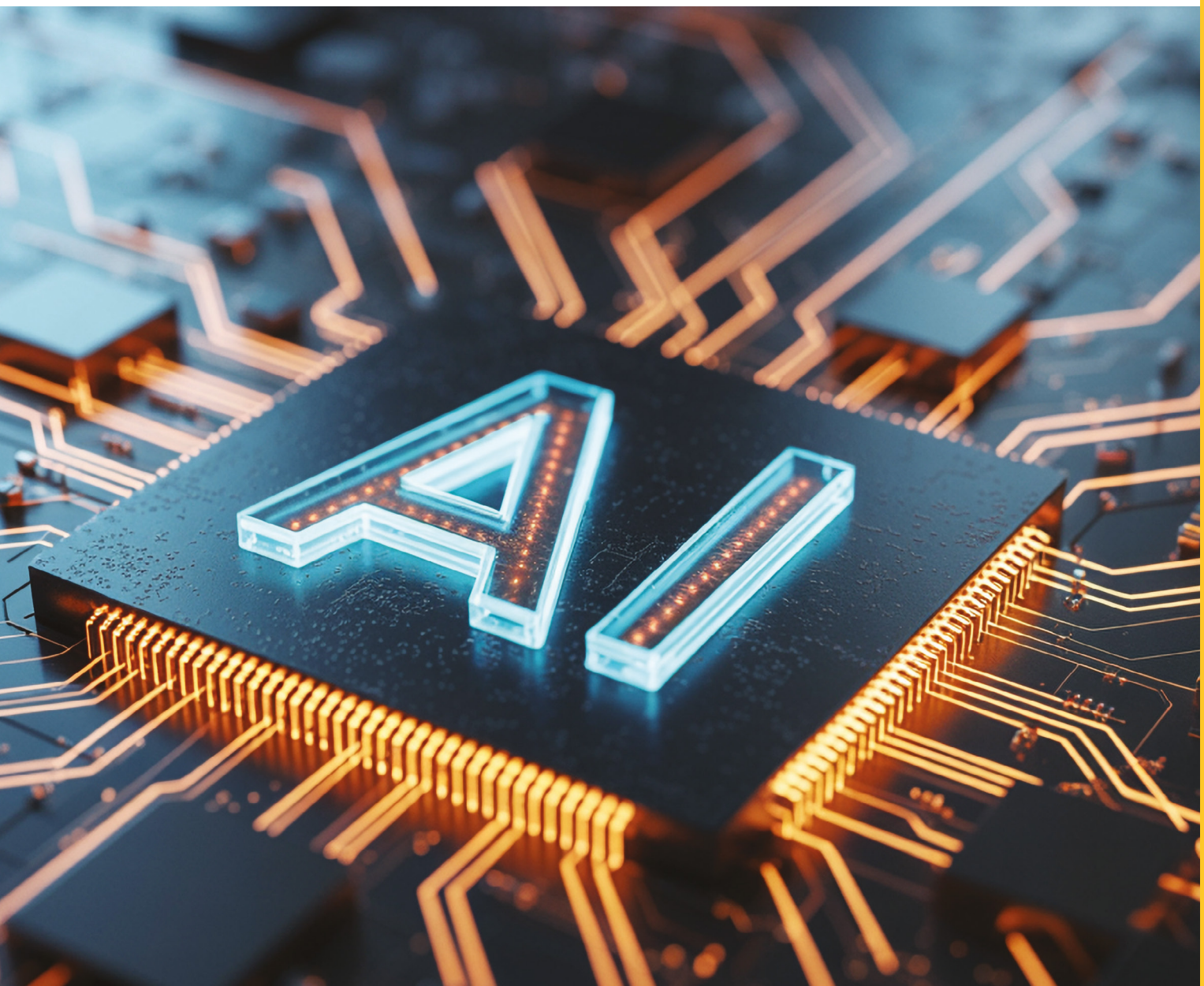
The interviewee also noted the importance of adaptability in practice. The rapid shift to hybrid working during the pandemic showcased the organization's ability to Redesign Processes under pressure. Looking forward, digital twins and other advanced technologies are seen as potentially transformative, enabling simulations and resilience testing at unprecedented scale.

Conclusion

This case study highlights the journey of a global organization striving to embed resilience as both a compliance necessity and a strategic advantage. Its scale and complexity require a balance between central oversight and local autonomy, with resilience functions distributed across domains yet increasingly converging through governance structures, exercises, and shared standards.

The interviewee described a vision that moves beyond siloed compliance, emphasising holistic integration, culture-driven resilience, and resilience-by-design. While current maturity varies across markets, the organization demonstrates an advanced and evolving approach, underpinned by strong governance, continuous learning, and transparent reporting. The commitment to leveraging technology – through AI, dashboards, and digital twins – shows how resilience is being transformed into a forward-looking, data-driven capability.

Crucially, resilience in this organization is understood not as a fixed end state but as a living, adaptive attribute that combines people, processes, and systems. By embedding resilience into culture, strategy, and innovation, the organization aims to thrive amid uncertainty, maintaining trust with stakeholders, while preparing for the next generation of global risks.



Case Study Four: North American Insurance Company

Interviewees:

- **Senior Director, Enterprise Resilience**
- **Director, Enterprise Resilience**

Organizational context

The organization is a mid-sized financial services provider, working with a large network of agents. Its operations are primarily concentrated in North America, with a limited presence overseas. The business is strongly regulated at state level, with some states imposing more rigorous oversight than others. In this environment, resilience is largely driven by the need to comply with regulatory requirements, although the resilience leaders have their own wider vision.

The enterprise has undergone significant changes in recent years, including a rebranding exercise. It has also invested in leadership development, new headquarters, and technology upgrades, signalling ongoing organizational growth.

Vision and approach to resilience

The interviewees described two contrasting visions for resilience.

The pragmatic approach that is in place views resilience as something to be done because regulators require it. Under this view, the organization must maintain business continuity, disaster recovery, and incident response plans, ensuring that they are reviewed and demonstrating their existence to regulators. Meeting regulatory standards is the reason for the existence of Enterprise Resilience, and the organization's top leadership has no current appetite to reach beyond this goal.

The aspirational vision held by the interviewees, by contrast, is one in which resilience is embedded into strategy as a unifying, wide-ranging, C-level driven initiative. In this model, resilience would be championed at the highest levels and underpinned by a formal organizational resilience policy. The interviewees expressed a strong desire to move towards this strategic and holistic approach, but due to the current organizational constraints, progress has been limited.

One of the interviewees had a particularly strong vision concerning the requirement for a Chief Resilience Officer, describing the absence of this role as a major gap in the current governance structure. In this view, the Chief Resilience Officer would be tasked with the long-term resilience of the company, looking beyond short-term compliance. The remit envisioned includes:

- Product resilience (ensuring that offerings remain relevant in the long term).
- Technology resilience (adapting to and investing in change).
- People resilience (attracting, retaining, and developing skills).
- Operational resilience (integrating across all resilience disciplines).

The Chief Resilience Officer would potentially lead an Organizational Resilience Committee and would be a conduit between this committee, executive leadership, and the board. The role would ensure upstream and downstream communication, aligning the board's concerns with operational realities, and vice versa.

In essence, the Chief Resilience Officer is seen as the missing piece to elevate resilience from a tactical, compliance-driven activity into a strategic, integrated, and future-oriented function.

The four Business Enablers in reality

Leadership and Governance

Given its compliance role, Enterprise Resilience currently reports through the legal function, which places it low in the overall governance hierarchy. This structure gives resilience a tactical importance but limits its strategic influence. The reporting line flows through a Senior Vice President to an Executive Vice President before reaching the C-Suite and board.

Two formal governance groups exist:

- **Executive Steering Committee** – oversees risk and resilience. Enterprise Resilience presents policies, exercises, and budget needs, here.

- **Middle to Upper Management Working Group** – meets quarterly. Reviews business continuity plans, crisis management updates, incident response, safety, and emergency preparedness. This is often more "informational than transformational", according to the interviewees.

The board receives informational resilience updates twice yearly, usually in brief, but the crisis management team has greater engagement during actual crises.

Audit and review functions are in place, but are not joined up. Internal audit assesses business continuity on a three-year cycle and IT disaster recovery is reviewed separately. Other resilience pillars such as vendor resilience, crisis management, and employee safety receive less systematic audit attention. External consultants are sometimes used for targeted assessments of technical areas such as enterprise risk management and information security.

Limited metrics are in place for measuring performance and success in resilience areas. These are tactical in nature, such as business continuity plan status (approved versus out of date, for example). Incident response has a more mature system of key performance indicators (KPIs), which provides a RAG (Red, Amber, Green) rating for ten key functional areas. These are assessed on an annual basis.

The interviewees identified several governance gaps: the absence of a Chief Resilience Officer, limited board engagement, fragmented tools and data, and the lack of clear risk appetite guidance – which can result in blocked decisions. An increasing use of external counsel to provide legal advice on key decisions has also led to slow decision-making and a lack of agility.

Business Structure – resilience structure and integration

The remit of Enterprise Resilience covers emergency preparedness, incident management, crisis management, business continuity, vendor resilience, and employee safety. However, several important areas remain outside its orbit, including enterprise risk management, IT disaster recovery, information security, corporate communications (internal, external, and crisis communications), and physical security.

Despite these exclusions, the interviewees stressed that strong collaboration exists, with informal conversations bridging gaps across functions. Cross-functional groups, such as quarterly risk meetings, bring together staff from different disciplines and departments to share information and align objectives.

Integration challenges persist. Business continuity planning remains department-based rather than value stream-based, limiting visibility into important business services.

Tools are fragmented, with heavy reliance on spreadsheets and word-processed documents. A newly appointed Governance, Risk Management, and Compliance GRC Director has been tasked with addressing this by exploring integrated software solutions.

Strategy, Tactics, and Operations

Operationally, resilience activities are well structured. The organization has a three-tier escalation process: department-level incident management, an incident management team, and a crisis management team, with clear roles and responsibilities up to and including C-level involvement. These escalation mechanisms have been tested and performed well during past disruptions.

However, an integrated strategy is lacking. Resilience is not embedded into corporate vision or annual planning. Horizon scanning is shorter term and is managed primarily through the enterprise risk function.

Budgeting for resilience is piecemeal, with no dedicated line item. Funding for exercises, training, and contracts is generally approved when requested, but there is no structured resilience budget or forward investment plan.

People and Culture

The interviewees emphasised that people resilience is one of the organization's strongest areas. The Human Resources (HR) function has invested heavily in leadership development, with structured programmes delivered in partnership with universities. These initiatives aim to attract, retain, and develop talent at different stages of management responsibility.

Employee wellbeing is also a priority, with initiatives focused on mental health and personal wellbeing. These investments reflect a people-focused culture, even though they are not formally labelled as resilience.

Resilience awareness campaigns have evolved over time. Initially focused on educating staff about business continuity and incident escalation, they have since expanded into broader wellbeing themes. Site-specific awareness sessions introduce staff to resilience pillars and escalation processes.

Although not labelled as organizational resilience, there is evidence of a gradually maturing culture of people resilience.

Maturity

Current resilience maturity and future vision

The interviewees estimated current organizational resilience maturity as seven out of ten – very competent at meeting regulatory requirements but lacking strategic integration. In practice, this means strong crisis management mechanisms and compartments of excellence in people development, but weaker alignment across domains (integration was given a maturity estimate of five out of ten) and limited C-level and board engagement.

The desired future vision expressed by the interviewees is significantly more ambitious. It includes appointing a Chief Resilience Officer, creating an organizational resilience policy, and establishing a long-term resilience roadmap.

Challenges that need addressing

Several key challenges were identified:

- **Strategic positioning** – resilience remains positioned within the legal function, limiting influence.
- **Leadership gap** – there is an absence of direct C-level and board-level representation for organizational resilience.
- **Budgeting** – there is no dedicated resilience budget, making investment fragmented and difficult to plan.
- **Risk appetite** – there is a lack of clear guidance, leading to blocked initiatives.
- **Data and tools** – fragmented systems and reliance on spreadsheets inhibit insight. Plans are in place to address this.
- **Decision-making** – outsourcing of some decisions to external counsel reduces agility.
- **Quantification** – a weak ability to measure the financial and operational impacts of disruptions makes it difficult to quantify the return on investment in resilience.

Innovation

Notable innovations and areas of focus

Despite its challenges, the organization has shown innovation in several areas.

- **Crisis escalation structure** – a clear three-tier process with defined roles has been embedded and proven effective.
- **People resilience** – structured leadership development programmes and wellbeing initiatives represent a significant investment in the resilience of human capital.
- **Awareness campaigns** – the evolution from compliance-focused training to broader wellbeing resilience initiatives illustrates creative approaches to staff engagement.
- **External partnerships** – successful external collaboration and partnerships are in place, such as with local emergency services. These highlight strong networking potential.

Conclusion

This organization illustrates a common picture: a resilience function that is operationally competent yet strategically constrained and compliance focused. Compliance with regulatory requirements ensures that business continuity and crisis management structures are in place and effective, but organizational resilience is not positioned as a strategic enabler of long-term growth and competitiveness.

The interviewees' aspirations were clear – to move from fragmented 'pockets of resilience' to a coherent organizational strategy championed by executive leadership. Doing so will require structural change, investment in integrated tools, and a cultural shift towards embedding resilience as a core value. Until then, resilience remains adequate for regulatory compliance, but is not yet the strategic differentiator that it has the potential to become.

Case Study Five: Global Bank

Interviewee: Global Head of Resilience and Continuity

Organizational context

The interviewee works within a large EU-based bank that operates around the world, providing retail and wholesale services.

The bank is highly globalised, with a model of balancing onshore and offshore teams to build capacity and centres of expertise. This structure means that the organization is hyperconnected: disruptions in one location can quickly cascade across other global regions.

The bank competes in an environment where technology has reshaped the sector. It is essentially a technology company behind the scenes with a banking, customer-facing front-end.

The regulatory environment is complex. The bank is subject to European frameworks such as the Digital Operational Resilience Act (DORA), oversight from the European Central Bank (ECB), and local requirements in each market where it operates. Non-EU regimes, such as those in Australia and Asia, also shape its approach, necessitating a global framework with minimal local deviations.

Vision and approach to resilience

The bank has a forward-looking approach to resilience, which is viewed very much as a strategic ambition, not just a compliance exercise. Resilience is seen as enterprise-wide and end-to-end, requiring coordination between technology, operations, and front-line business.

Operational resilience is central to the strategic and operational approach; it is one of the strategic pillars that have been designated by the CEO.

When changing the mindset, in the interviewee's words, from the old-school business continuity orthodoxy, the key strategic starting point is Critical Business Services (CBS). The bank prioritises functions that are essential for customers, markets, and reputation. This perspective shifts resilience from an internal viewpoint to an external one.

Continuous improvement and evolution are built into the bank's approach. This is partly in response to internal learning cycles but also in recognition that threats such as ransomware, cyber attacks, and geopolitical shocks are escalating. The bank aims to use resilience as a source of competitive advantage, customer trust, retention, and growth, as well as helping maintain overall market and system stability.

The four Business Enablers in reality

Leadership and Governance

Business Structure – resilience structure and integration

The resilience function is jointly owned by the Chief Operations Officer (COO) and the Chief Technology Officer (CTO). This ensures that both business and technology perspectives are represented at a strategic level and, as a result, resilience is embedded into operations as well as infrastructure. Within this structure, the interviewee serves as Global Head of Resilience and Continuity, with a counterpart in technology focused on reliability engineering.

Governance is robust. Quarterly reporting goes to the bank's managing board, and quarterly reviews are held at both board and executive level.

Board members take a detailed interest, often requesting extensive data on testing, availability, and resilience performance. Risk appetite and resilience expectations are also explicitly reviewed.

The crisis management structure places the COO or CTO in the chair depending on the type of incident. Impact tolerance breaches and major events are reported to board level, with resilience included in board KPIs. Internal audit and external regulators conduct frequent reviews, and audit findings are tracked with follow-up actions.

Budgeting follows a hybrid model. Large-scale investments, such as immutable storage for ransomware resilience, are approved at board level, while smaller initiatives are funded within business-as-usual operational budgets by service

owners. This ensures that both strategic and operational needs are covered.

Business continuity standards, such as ISO 22301, are not used as a starting point – the bank has moved on from them, seeing them as bureaucratic and no longer fitting into the current organizational context.

Strategy, Tactics, and Operations

The resilience organization combines central and local teams. At the centre, the global Resilience and Continuity team defines frameworks, strategy, and regulatory engagement. Local teams in each region/country handle day-to-day resilience activities, such as business continuity planning, exercising, testing, and crisis response.

Operational resilience, business continuity, cyber resilience, crisis management, and risk management are linked. ESG is less formally integrated at present but is seen as an area relevant to resilience.

As a result, the interviewee estimated current integration of resilience-related disciplines at six out of ten.

Actions to reduce silos and increase integration include establishing common forums, embedding shared goals, and creating dedicated roles that translate resilience requirements between business and technology.

Supplier resilience is managed through business continuity documentation, audits, and a global supplier risk framework. However, the interviewee highlighted challenges in influencing large third-party providers outside the EU, noting that some vendors remain resistant to regulatory expectations.

Strategically, resilience is aligned to transformation programmes, especially the ones focusing on digitalisation.

Horizon scanning is conducted through the regular risk processes. The output usually highlights emerging risks such as cyber threats, geopolitical instability, and climate-related shocks, and these insights are fed into risk and resilience planning.

Tactically, impact tolerances are the primary tool for resilience management. These tolerances are set for Critical Business Services and cascaded into IT assets, with breaches reported at board level. The bank has set an ambition to reduce breaches year-on-year, with remuneration linked to performance against impact tolerances.

Testing is conducted at both global and local levels, with an increasing emphasis on live and simulated exercises rather than desktop tests.

People and Culture

Resilience education and awareness are central. All staff undertake mandatory resilience training through e-learning and regular awareness sessions. Survey results show that resilience awareness and training are well received across the organization.

Resilience is becoming part of everyday decision-making, with leaders considering resilience impacts when developing products or entering markets.

Maturity

Current resilience maturity and future vision

The interviewee estimated overall resilience maturity at seven out of ten.

Strengths include board-level engagement, customer-focused resilience, integration into the risk taxonomy, and cultural progress. The programme is well embedded across the organization, with resilience increasingly part of daily conversations at all levels.

The vision for the future includes extending resilience beyond CBSs, deepening integration across all functions, and building stronger third-party resilience. Greater use of data analytics is also seen as a priority, with the potential to improve monitoring, prediction, and response.

Challenges that need addressing

- **Prioritisation** – balancing resilience investments across competing regulatory and strategic demands.
- **Global versus local alignment** – ensuring consistent implementation across diverse markets while meeting local requirements.
- **Third-party resilience** – building understanding and transparency with major external providers when it comes to resilience.
- **Integration** – overcoming silos between functions and embedding resilience more deeply across risk, IT, procurement, and ESG.
- **Regulatory overload** – navigating a growing number of global, regional, and national requirements.
- **Benchmarking** – the bank would like to be able to benchmark its operational resilience practices with other banks, but there are limited opportunities to formally achieve this.

Innovation

Notable innovations and areas of focus

The organization is pursuing several innovative practices:

- **Client-focused resilience** – framing CBSs around client impact, embedding this perspective across risk frameworks, IT strategies, and business continuity planning.
- **Joint governance model** – establishing parallel resilience functions within COO and CTO organizations, with dedicated roles to translate between business and technology.
- **Addressing silos** – breaking down silos internally is seen as a key resilience enabler.
- **Cross-bank collaboration** – engaging with peer institutions through alliances, joint exercises, and shared learning to accelerate sector-wide resilience.
- **Scenario testing evolution** – prioritising live and simulation exercises to better reflect severe but plausible scenarios.
- **Change and transformation integration** – ensuring that resilience is part of strategic transformation and digital innovation programmes.

These innovations illustrate an organization that is not only responding to regulatory requirements but going beyond, using resilience as a lever for cultural change, client trust, and long-term competitiveness.

Conclusion

This bank has deliberately positioned resilience as a strategic advantage rather than a compliance burden. By embedding resilience as a primary risk, co-owning it across business operations and technology, and linking outcomes to client impacts, the bank has created a model that is both structured and dynamic.

The interviewee's estimated maturity level reflected strong board engagement, cultural progress, and an integrated risk framework. At the same time, the challenges of global versus local alignment, third-party dependencies, regulatory overload, and cross-functional integration remain significant.

What sets this bank apart is its willingness to innovate: reframing resilience around Critical Business Services, linking tolerances to board KPIs, prioritising live testing, and integrating resilience into transformation programmes. Such initiatives, combined with active collaboration with peer institutions, show how the bank is shaping resilience not only for its own operations but also as part of wider systemic stability.

Overall, the bank provides a benchmark for how large global financial institutions can shift resilience from a bureaucratic function to a source of trust, agility, and long-term competitiveness. Its progress illustrates that, while compliance may be the starting point, strategic advantage lies in embedding resilience into the culture, decision-making, and purpose of the organization.

Case Study Six: Global Logistics Company

Interviewee: Senior Director, Global Resilience

Organizational context

The interviewee leads global resilience within a large multinational enterprise operating across multiple continents and markets. The organization's operations span both physical services and technology systems, with critical dependencies on IT platforms, logistics, and front-line services. Because of its scale and diverse geographical footprint, resilience resources differ widely: larger markets may have dedicated staff for business continuity and recovery, while smaller markets rely on local managers who carry resilience as one of several responsibilities.

The resilience function sits within the remit of the Chief Information Security Officer (CISO), alongside information security and data privacy. This structural positioning reflects the organization's recognition that resilience is a strategic concern but is also deeply interconnected with security and technology. The global Resilience and Continuity team itself is small – just five individuals including the interviewee – but resilience responsibilities are distributed across regional and national levels, with an estimated 12 to 15 personnel contributing part-time to resilience alongside other duties. The team is responsible for business / operational resilience, technology resilience, and crisis management.

The enterprise operates in a highly regulated environment. Resilience reporting is now a recurring feature of board and C-Suite governance cycles, presented alongside metrics such as cost efficiency, market expansion, and strategic investment. Regulatory requirements are met, but the interviewee's philosophy placed emphasis on demonstrating outcomes rather than adhering strictly to prescriptive deliverables, such as business impact analyses or risk registers.

Vision and approach to resilience

The interviewee's personal and programme vision was straightforward: continuous improvement of organizational resilience capabilities. This vision is operationalised through two complementary lenses:

- **Stability and reliability** – preventing failures by strengthening systems and processes.
- **Recoverability** – ensuring effective restoration of services when disruptions inevitably occur.

A distinctive feature of the programme is the *confidence scoring model*, a framework combining qualitative and quantitative data that generates resilience 'confidence percentages' for IT systems, applications, branches, and services. Each score combines *reliability* metrics (e.g. patching status, end-of-life components, incident history) with *recoverability* metrics (e.g. documented recovery strategies, testing, ownership). On the operations side, qualitative surveys of front-line managers assess resources, competence, and authority.

The results are aggregated into dashboards available at multiple levels – application owners, business managers, and executives – providing visibility from business unit level to the boardroom. Crucially, confidence scores are not presented as compliance audits but as engagement tools, encouraging teams to identify improvement opportunities and seek support.

Strategically, resilience confidence now acts as a decision factor. Executives weigh resilience alongside cost, risk, and benefit: when two investments are otherwise equal, the option that contributes to stronger resilience scores often prevails. This integration has elevated resilience from a compliance checkbox to a consideration in corporate strategy.

The four Business Enablers in reality

Leadership and Governance

Resilience governance has evolved from informal practices to a more structured approach. Initially, resilience data was available but not consistently shared upwards. Today, confidence scores and resilience reporting are embedded into strategic packs reviewed by the CISO, CIO, CFO, CEO, executive leadership, and ultimately the board.

Board and executive engagement vary: some directors ask probing questions informed by prior expertise, while others are

less familiar. Nevertheless, resilience data is now consistently visible, and executives expect it during strategy discussions.

The interviewee emphasised that resilience and risk management remain distinct. Risk management identifies and seeks to mitigate threats; resilience assumes that disruption will occur and focuses on recovery capabilities, although stability and reliability are components of reporting. This separation avoids diluting accountability, while ensuring coordination with cyber and risk teams when needed.

Governance is also 'bottom-up'. Rather than starting with board priorities, the programme begins with ground-level surveys of operational managers. Findings are then shared with their managers and regional leaders, and are only later elevated to executives. This staged reporting ensures buy-in at every level, reduces surprises, and builds trust in the data.

Resilience governance is supported by the usual formal corporate structure for audit and review via an internal audit department. Large and regulated customers also conduct their own audit and assessment of the organization, and will provide feedback as appropriate.

Business Structure – resilience structure and integration

The global Resilience and Continuity team provides central leadership, supported by regional coordinators and national staff who combine resilience with other roles. Large in-country operations such as those in the US, Brazil, and France have dedicated resilience personnel; smaller markets rely on local managers. This distributed model ensures effective reach despite being constrained by resource limitations.

Integration across functions is a deliberate focus. Resilience reports into the CISO, who also oversees security and privacy, but operational resilience responsibilities extend into logistics, customer services, compliance, and physical security. Silos exist, but efforts are underway to reduce them by using common frameworks such as the confidence model, and by embedding resilience considerations into broader transformation initiatives.

Externally, resilience expectations extend to suppliers. Third-party criticality is assessed, often aligning with certifications such as ISO 27001 or SOC2 (12), supplemented by targeted questions where gaps exist. This ensures that supplier resilience evaluations are consistent with internal processes.

Strategy, Tactics, and Operations

Strategically, resilience is positioned as a differentiator in market expansion and service delivery.

Confidence scores inform investment choices and resource allocation. Tactically, assessments of IT and operations drive targeted improvements. For example, remediation of end-of-life components, or migration to high-availability platforms, directly increase resilience confidence. On the operations side, redundant connectivity, backup power, and alternative logistics capacity are assessed for stability, while competence and authority are evaluated for recoverability.

Exercises are conducted for both IT recovery and business resilience. Regulatory, legal, or contractual requirements often dictate frequency, but the organization also adopts a deliberately low threshold for activating response frameworks. This creates more practice opportunities, reinforcing competence and collaboration – even if full recovery is not executed.

For IT resilience, periodic recovery tests are performed. The type of testing determines the level of certainty and confidence in recoverability. Types of tests range from testing in isolation during a pre-determined outage / unavailability period, through to running full production from the recovery environment.

In terms of crisis management, the resilience team's responsibilities do not extend to emergency management, but cover executive or strategic level response to catastrophic events.

People and Culture

The interviewee repeatedly stressed that resilience is people-centric. Three engagement pillars underpin the programme:

- **Resources** – do teams have what they need?
- **Competence** – do people know what to do?
- **Authority** – are people empowered to act?

These principles shape confidence scores, training, and interventions. Framing surveys as engagement opportunities rather than audits fosters psychological safety, encouraging honest feedback and open discussion of weaknesses.

The interviewee saw psychological safety and diversity of thought as crucial cultural enablers. Diverse teams produce stronger decisions, but only if members feel safe to speak up. Critical thinking is also highlighted as an essential, though often missing, resilience principle: teams must be able to challenge assumptions.

Education is continuous. Twice-annual surveys prompt reflection on recovery competence, while local resilience managers deliver training and awareness to front-line staff. When improvement opportunities are identified, targeted training links are sent to specific teams, mid-level managers may coordinate market-wide initiatives, or issues may be escalated to leadership if systemic.

Maturity

Current resilience maturity and future vision

The interviewee rejected traditional maturity models. They declined to estimate a maturity rating for this case study, arguing that such measures are subjective, outdated almost immediately, and risk being used against the organization by regulators or customers. Instead, they preferred continuous improvement measured through the confidence scoring situation described above, which informs the whole resilience management and development process in this organization.

Looking forward, the vision is for continuation and maturing existing resilience processes rather than radical transformation. Plans include:

- Expanded use of AI to automate surveys, translations, and data analysis.
- Broader metrics encompassing collaboration, diversity of thought, trust, and psychological safety.
- Less reliance on rigid plans and more emphasis on empowered, adaptable teams.
- Careful balancing of global company standards with local nuance.

Challenges that need addressing

Several challenges remain.

- **Executive alignment** – C-Suite leaders engage in crises but have differing priorities, and converting tabletop outputs into programme changes can be inconsistent.
- **Time and pace of change** – engagement-heavy approaches demand significant time with teams, but organizational change and transformation move quickly, risking misalignment.
- **Siloed responsibilities** – while integration has improved, functional silos between IT, operations, and security still exist. Breaking them down requires constant, ongoing effort.
- **Regulatory expectations** – regulators often demand items that the interviewee deems unnecessary, such as BIAs (business impact analyses). The interviewee champions outcomes over process, sometimes requiring negotiation to satisfy oversight without losing programme agility.

Innovation

Notable innovations and areas of focus

The most distinctive innovation is the confidence scoring system. It transforms resilience from an abstract concept into a quantifiable percentage, comprehensible at every level of the organization. It provides a structured quality management system for resilience and supports:

- **Application owners** – who see how remediation or testing improves their scores.
- **Managers** – who allocate budgets based on comparative resilience.
- **Executives** – who incorporate resilience into strategic decision-making.

Other innovative aspects include:

- **Bottom-up governance** – data is generated at front-line level and gradually elevated, ensuring ownership and reducing resistance.

- **Low-threshold exercising** – frequent activation of response frameworks normalises resilience behaviours and provides regular learning opportunities.
- **Integration of qualitative cultural factors** – future metrics aim to include psychological safety, diversity, and trust, recognising that culture drives recoverability as much as systems do.
- **Critical thinking principle** – the interviewee proposed this as an addition to the Airmic Resilience Principles, emphasising the need to continually challenge assumptions to enable improvement, growth, and adaptation.

Conclusion

This case study illustrates how the interviewee has pioneered a resilience approach that is simultaneously measurement and data-driven as well as people-centric. By developing the confidence scoring system, resilience has been reframed as a measurable capability and an important factor in strategic decision-making. Governance now ensures that resilience data is considered alongside financial and market information, while bottom-up reporting builds trust and engagement across all levels.

The programme's cultural underpinnings – psychological safety, empowerment, and critical thinking – distinguish it from compliance-driven and traditional models.

Challenges remain, particularly around executive alignment, silos, and regulatory expectations, but the trajectory is clear: resilience is no longer marginal but central to the organization's strategic direction.

Case Study Seven: Global Aerospace Company

Interviewees:

- **Head of Enterprise Risk Management**
- **BCM Project Leader**
- **Resilience Manager**

Organizational context

This case study looks at a large, complex organization operating across global markets and highly regulated sectors. The company designs and delivers complex, safety-critical products with long development cycles. This environment requires strict compliance with regulatory standards while also requiring adaptability in a fast-changing geopolitical and technological landscape.

Vision and approach to resilience

The resilience programme has grown out of lessons from major disruptions, including the COVID-19 pandemic. A corporate audit in 2021 identified that, while numerous resilience-related activities were underway (business continuity, risk management, crisis response, and threat scanning, for example), they were fragmented. The audit recommended a more integrated, end-to-end model. This prompted the creation of a dedicated Resilience Manager role within the Enterprise Risk Management (ERM) function.

Since the audit in 2021, resilience has developed strongly and the company's resilience framework is now structured around a model consisting of four interconnected 'bricks'. These are:

- Anticipate and Detect
- Prevent and Protect
- React and Recover
- Transform and Thrive

This simple yet robust model, explained in more detail later in this case study, provides clarity, aligns different resilience functions, and has become a cornerstone of resilience strategy and operations.

The four Business Enablers in reality

Leadership and Governance

Governance of resilience sits firmly with the ERM function, which reports quarterly to the Board through the Head of Enterprise Risk Management. These reports cover not only top risks and opportunities but also emerging topics and, where relevant, lessons learned. Although resilience is not always labelled explicitly, it is embedded in this risk-based reporting and, occasionally, forms the subject of board 'deep dives'.

The ERM team is structured as a network, with officers, coordinators, and risk owners spread throughout the business, while a Core Competence Centre sets standards and measures maturity. This ensures consistency while allowing adaptation across divisions.

A notable strategic leadership feature is the conscious decision to connect silos rather than break them down. Leaders see silos as necessary for security and confidentiality, and as positive in that they hold deep competence and accountability – for example, in cyber resilience, supply chain, or engineering. Instead of seeking to dismantle silos, the organization builds 'connectors' – such as jointly defined recovery time objectives (RTOs), multidisciplinary crisis teams, and integrated exercises – that ensure collaboration without undermining expertise.

Business Structure – resilience structure and integration

As highlighted above, a structured resilience framework is anchored in four bricks. Each brick has defined practices and accountabilities:

Anticipate and Detect

The organization treats threat and issue anticipation as the cornerstone of resilience, recognising that uncertainty cannot be eliminated but can be identified early enough to prepare. Horizon scanning, intelligence gathering, and systematic threat identification take place in a highly structured way, with integration of inputs from research, technology, security, and risk functions. These insights are integrated in biannual 'threat radar' meetings at senior level, encouraging a culture where

weak signals are surfaced before they become risks. The goal is to avoid surprises by pre-empting disruptions, reducing both frequency and severity. This anticipatory capacity is not just procedural but cultural, requiring employees at all levels to be attentive and proactive. By embedding detection into everyday operations and aligning foresight with governance processes, the company ensures that it is positioned not simply to react, but to adapt with agility in advance of disruptive events. Anticipation thus underpins all subsequent resilience measures.

Prevent and Protect

This brick focuses on building resilience into operations before crises occur. It combines engineering, supply chain, cyber, and cultural safeguards. Technical resilience-by-design measures include designing redundancy into critical systems, ensuring robustness against failure, and prioritising protection of the 15% to 20% of IT applications that are deemed critical for survival.

Supply chain resilience is reinforced through cascading contractual obligations and supplier audits, ensuring that partners share responsibility for business continuity.

Preventive practices also include single points of failure analysis within each business unit, helping leaders understand vulnerabilities and adapt accordingly.

Beyond technical controls, there is an emphasis on cultural prevention: encouraging recognition of the often invisible value of safeguards. Philosophically, leaders acknowledge that organizational 'firefighters' are celebrated, but those who prevent fires deserve equal recognition.

Prevention and protection reduce recovery costs, safeguard operations, and create confidence that resilience is actively designed into products, processes, and relationships across the value chain.

React and Recover

The third brick recognises that disruption is inevitable, so robust mechanisms are needed to respond decisively and recover quickly. Crisis management teams exist at both site and corporate levels, activated rapidly through notification technology. In parallel, monthly crisis *anticipation groups* meet with the ERM team to envision scenarios and define escalation triggers.

A central practice is the co-definition of RTOs, aligning IT disaster recovery with business continuity priorities. Joint exercises simulate both technical restoration and operational workarounds, ensuring that interdependence is tested in realistic conditions.

The aim of organizational resilience is seen as ensuring that the company can: "Be alive tomorrow, so it can thrive for years." This proactive preparation embeds cross-silo collaboration, minimises downtime, and builds trust in the organization's ability to survive, stabilise, recover, and adapt – even during major crises.

Transform and Thrive

The final brick differentiates survival from long-term competitiveness and growth. It focuses on capturing lessons learned, aligning defences, and embedding structural change. After every crisis, formal reviews assess methodology, performance, and opportunities for improvement. These insights feed into wider ERM processes, ensuring continuous improvement. Circular information flows connect audit, risk, internal control, and performance management, creating consistency across the three lines of defence.

Transform and Thrive also extends to embedding resilience into awareness programmes and policies, while ensuring that resilience is not an abstract concept but a real cultural mindset. Importantly, the organization reframes risk as a driver of innovation and opportunity. The organization also treats disruptions as catalysts for change, revealing inefficiencies and issues that can become lessons for improvement and transformation.

Strategy, Tactics, and Operations

Tactically, the four bricks translate resilience into actionable programmes: foresight meetings, supplier audits, resilience drills, and improvement cycles. Operationally, the company invests in both preventive measures (engineering redundancy, cyber safeguards) and reactive capabilities (tested CMTs and business continuity plans).

A recurring theme is pragmatism: resilience is not about adding new layers of process but about using continuous improvement techniques to help make existing activities more connected, visible, and effective.

People and Culture

Culture is central to the resilience model. Leaders describe resilience as a corporate mindset, not just a technical discipline – and this key messaging flows throughout this area, reinforcing that resilience is both operational and strategic.

Employees are encouraged to play their part, including taking accountability for resilience in their own areas – reporting threats and risks that they are aware of, as well as highlighting opportunities for enhancing resilience.

The organization is experimenting with innovative awareness tools. One initiative is a game-based training approach modelled on a successful climate-change awareness tool. This interactive format encourages discussion, discovery, and collective learning rather than one-way training. The ambition is to 'infuse' resilience across teams and make it something that every individual is aware of, appreciating their own role and importance in helping ensure resilience.

At the same time, leaders are careful to avoid making resilience feel 'artificial'. They recognise that over-formalisation would clash with the company's already complex processes. Instead, they aim to keep the framework simple, tangible, and embedded in everyday work processes and activities.

Maturity

Current resilience maturity and future vision

The interviewees estimated its resilience maturity at six out of ten. This reflects significant progress since COVID-19 but acknowledges there is further room to grow. For example, while resilience is embedded in risk reporting and governance, formal resilience-specific KPIs are not yet defined. Leaders expressed caution about adding more metrics to an already heavy measurement environment, but recognise that this is a potential area for development.

The vision is to raise maturity by further integrating resilience into everyday decision-making, expanding awareness across all levels of the company, and developing clearer ways to measure and communicate resilience. There is also an ambition to embed resilience more explicitly into employee onboarding and other human resource processes.

Challenges that need addressing

Several challenges were highlighted:

- **Measurement** – lack of formal resilience KPIs makes it more difficult to demonstrate progress and reward preventive behaviours.
- **Data integration** – legacy IT systems and organizational complexity hinder effective use of big data and lessons learned.
- **Cultural recognition** – firefighting is culturally rewarded more than prevention. Shifting this balance requires deliberate effort.
- **Silo connectivity** – while progress has been made, maintaining effective connectors across complex siloed structures is a continual challenge.
- **Sustainability of lessons learned** – employee turnover risks losing insights gathered from incidents and other areas. Systems for capturing and embedding lessons learned need to be improved.

Innovation

Notable innovations and areas of focus

The resilience programme has introduced several innovative practices that stand out:

- **The four-brick model** – this simple but comprehensive structure helps the organization focus on holistic organizational resilience and makes it practical and actionable.
- **Connectors, not demolition** – rather than seeking to break down silos, the organization builds connectors – joint targets, integrated exercises, and cross-functional

teams – that bind specialist areas together when it comes to resilience.

- **Game-based awareness training** – an interactive learning tool, inspired by climate-change education, is being developed to build resilience awareness across teams.
- **Positive framing of risk** – risk is treated as input for strategic decisions and innovation, not just as a constraint.
- **Circularity of information** – aligning audit, risk, internal control, and performance management to share lessons learned and sustain improvements.
- **Exploration of AI for lessons learned** – pilots are underway to use AI to extract relevant insights from vast databases of incidents and experiences.
- **Embedding resilience in sustainability goals** – the organization connects long-term resilience to its climate strategy, aiming for Net Zero 2050 and recognising climate change as a resilience challenge, not just an environmental one.

Conclusion

This case study illustrates how a global aerospace company has deliberately built a resilience programme that is both structured and pragmatic, rooted in lessons learned from past disruptions and developed into a coherent model that connects strategy, operations, culture, and governance. The four-brick framework has provided a clear foundation for aligning diverse resilience activities across silos and across the whole organization.

The organization's maturity journey reflects both significant progress and some persistent challenges. While resilience has become more visible in governance, culture, and day-to-day practice, gaps remain in measurement, data integration, cultural incentives, and sustaining lessons learned. The company is self-aware about these gaps and views them as opportunities for development.

Innovations such as connectors between silos, game-based awareness training, and positive framing of risk demonstrate a forward-looking approach. The integration of resilience into sustainability ambitions and the exploration of AI for lessons learned further shows how resilience is being embedded into long-term strategic priorities.

Ultimately, the company frames resilience not just as a survival strategy but as a pathway to adaptation, competitiveness, and longevity. By treating disruptions as catalysts for transformation, resilience becomes a mindset that supports both immediate recovery and long-term thriving in a complex, highly regulated, and fast-changing global environment.

THE RESILIENCE PRINCIPLES IN PRACTICE

This section of *Putting Organizational Resilience into Practice* explores each of the Resilience Principles through the lens of the case study organizations. Interviewees were asked to reflect on each Principle, commenting on how it has been applied in practice and whether they regard it as a relevant and fundamental aspect of resilience.

Exceptional Risk Radar

Risk Radar involves having the organizational capability to detect, interpret, and act on emerging risks and opportunities at an early stage.

1. Case Study One: Global Energy Manufacturer – the organization's Risk Council provides strong detection of operational risks, but horizon scanning is weaker, constrained by production pressures and lack of strategic capacity. The interviewee advocated AI and external intelligence gathering to help the organization better identify systemic and emerging risks.
2. Case Study Two: Global Professional Services Firm – the organization combines formal geopolitical and macroeconomic risk analysis with active peer engagement. External experts provide reports on long-term and country-level risks, while internal teams conduct ongoing risk assessments. Staff are encouraged and funded to attend conferences, join associations, and share insights from peers to detect emerging trends. Horizon scanning is most structured in the geopolitical risk framework, but also happens informally through networks and supplier forums. This mix of structured intelligence and relationship-based awareness supports foresight, early detection, and preparedness for new or evolving risks.
3. Case Study Three: Multinational Corporate – uses early detection mechanisms and dedicated monitoring teams across operational domains. A specialised Geopolitical Risk Team continuously scans global developments and produces an annual forward-looking risk report. This is updated as necessary throughout the year. These insights feed into crisis management planning and inform strategic discussions, ensuring awareness of both immediate and longer-term risks. Horizon scanning typically looks about a year ahead, integrating scenario analysis and early warnings to anticipate potential crises before they materialise, helping resilience teams prepare proactively.
4. Case Study Four: North American Insurance Company – has a functioning but short-term focused risk radar, with horizon scanning typically covering only one to three years. Risk Management leads structured assessments, while Enterprise Resilience provides operational input. Threat intelligence is drawn from sources such as cross-functional department meetings, covering geopolitical, cyber, and health risks.
5. Case Study Five: Global Bank – risk radar and horizon scanning are interpreted as forward-looking risk management, but the organization is clear about their practical limits. Instead of five to ten years, this organization's focus is usually on a one to two-year horizon, since risks evolve too quickly for longer forecasts to be reliable. The organization views longer-term horizon scanning as speculative, preferring pragmatic monitoring that supports resilience planning, while avoiding over-reliance on uncertain predictions.
6. Case Study Six: Global Logistics Company – horizon scanning is seen as relevant but a lower priority compared with other immediate resilience needs. It is in place but only looks one to three years ahead, depending on the area being explored. The interviewee cautions that risk radar activities can be distorted by biases or misread signals, leading to unnecessary distractions from current vulnerabilities. In today's volatile environment – marked by rapid global change, misinformation, and transformational technologies such as AI – the risk landscape is shifting too quickly for long-range forecasts to be fully reliable. Instead, the focus should balance foresight with responsiveness, ensuring that resilience remains grounded in current realities rather than overcommitting resources to uncertain future scenarios.
7. Case Study Seven: Global Aerospace Company – integrates risk radar and horizon scanning through its Anticipate and Detect resilience model brick. Traditional risk identification is mature, with quarterly risk assessments across the organization. The company has also expanded its focus

into emerging threats that may not yet qualify as direct risks. Previously fragmented across silos, this work is now coordinated through biannual high-level meetings involving senior leaders to review a consolidated threat landscape. Risk awareness has also been built into the organizational culture, with employees encouraged to report concerns. This approach emphasises foresight, detecting signals before risks materialise, and building a structured rhythm for threat monitoring, while embedding scanning into overall enterprise risk management.

Overall outcome

Each interviewee agreed that Risk Radar is a fundamental principle of resilience. The majority also agreed that having an Exceptional Risk Radar provides advantages. Every organization had a risk assessment capability in place and some level of horizon scanning, but the maturity and scope of these activities vary. A recurring point made was that risk radar cannot be relied on beyond a short-term (one to three year) period. Decisions will need to be made by individual organizations on whether they react early to mitigate longer-term emerging risks or whether to simply maintain a watching brief. Executive leadership will need to either lead or be included in this decision-making process.

Flexible and Diversified Resources and Assets

Resilient organizations maintain resources and assets that are flexible and diversified. Where resources are insufficient, they must be strengthened to fully capitalise on technological advancements and other opportunities. The aim is to ensure that resources are adaptable, robust, and aligned with organizational purpose and risk appetite.

1. Case Study One: Global Energy Manufacturer – this principle is not yet fully realised although progress has been made, particularly in value chain resilience. However, supplier choices are often made in silos without resilience criteria, limiting diversification opportunities. Power resilience has been strengthened at the new gigascale facility by securing three independent feeds.
2. Case Study Two: Global Professional Services Firm – this principle is seen as essential to resilience. The organization avoids single points of failure by creating Business Response Teams (BRTs) for critical suppliers, supported with playbooks and exercises. Scenario-based exercises have been used to help identify weak areas, and investments in alternative options have been made where needed. Beyond suppliers, investment has been made in organizational capability, through application tiering and backup systems.
3. Case Study Three: Multinational Corporate – links Flexible and Diversified Resources and Assets directly to resilience-by-design. The interviewee stressed that embedding redundancy and alternatives from the outset makes operations inherently adaptable. Examples include call centres split across buildings or countries, and warehouses designed with resilience input from day one. Such structures allow continuity during disruption, avoiding reliance on post-incident recovery. The organization accepts that not everything can be replicated in full, but building in failover and alternative suppliers ensures business continuity, even if at reduced capacity.
4. Case Study Four: North American Insurance Company – COVID-19 forced a rapid shift to remote working: staff without laptops physically moved desktop equipment home to continue operations. Since then, desktops have been replaced with laptops, greatly improving flexibility. Additional resilience measures include contracts with mobile recovery vendors to deploy units on site, annual testing of these capabilities, moving data centres to hardened third-party facilities, and migrating applications to the cloud. Flexibility now spans both day-to-day operations and crisis scenarios, ensuring adaptability and business continuity.
5. Case Study Five: Global Bank – the interviewee explained that resilience must be by design and built into systems, processes, and third-party arrangements rather than bolted on afterwards. The bank's global structure demands – and creates – flexibility. The focus on Critical Business Services drives prioritisation of resources, ensuring that IT assets, contracts, and recovery strategies align to client impact. Cloud adoption, backup and restore strategies, and diversification of suppliers all support adaptability. Flexibility is framed as proactive, client-focused, and embedded into governance.

6. Case Study Six: Global Logistics Company – this principle is a high priority area but is framed as adaptability and flexibility. Overly prescriptive plans undermine adaptability. The interviewee stressed that competence, authority, and psychological safety are more valuable than fixed recovery plans, as these foster improvisation when disruptions occur. The organization measures resilience confidence across IT and operations by assessing reliability, recoverability, and resource adequacy. This covers assets such as backup power, redundant networks, spare equipment, and people's capability to act. Some resources are centrally defined, while surveys ensure that local needs are captured.
7. Case Study Seven: Global Aerospace Company – this organization frames Flexible and Diversified Resources and Assets as twofold: avoiding single points of failure (SPoFs) and building adaptability. SPoFs are identified in the risk management cycle, encouraging awareness and mitigation. Adaptability is more challenging due to regulation and long production lead times, but is strongest in digital and human areas, where flexibility is greatest. Overall, resilience in this area relies on connecting silos and ensuring that resources can be reconfigured even within the constraints of a complex, regulated industry.

Overall outcome

Each organization see this principle as a core aspect of resilience, with similar approaches to supplier resilience and having strategies in place to maintain flexible and diversified assets and processes.

The importance of resilience-by-design is a theme that emerges. Designing resilience, failover, and agility into systems helps prevent issues and associated downtime. Some aspects of flexibility can only be designed in as a system is being built – retrofitting is not always an option. This is another strong justification for the need to integrate or communicate across silos – to support change and transformation teams and to ensure that resilience-by-design decisions are made at the appropriate point.

In addition, flexible assets are not only just about infrastructure, IT, or suppliers – Human Resources is another area where this principle is important. Enabling and training flexible, adaptable, and empowered people provides a strong framework for resilience.

Strong Relationships and Networks

Resilient organizations value and cultivate Strong Relationships and Networks, both within the organization and externally, including with suppliers, contractors, business partners, and customers.

1. Case Study One: Global Energy Manufacturer – internal collaboration has improved through the use of Risk Councils, but external communications (with regulators, customers, and communities) are fragmented and slow. Regulators are engaged directly and through lobbying.
2. Case Study Two: Global Professional Services Firm – the organization has a strong emphasis on relationships and networks as central to resilience. The interviewee highlighted the importance of maintaining close links with peers and critical suppliers, including conducting joint forums with other firms to review supplier performance and resilience. Internally, work is being done to break down silos by creating cross-functional forums, such as supplier resilience forums, where risks are assessed collaboratively. Deliberate structures, communication skills, and integration efforts strengthen existing networks. The interviewee stressed that relationships underpin both horizon scanning and operational resilience, providing early insight and collective action when disruptions occur.
3. Case Study Three: Multinational Corporate – Strong Relationships and Networks are built through structured policies and forums. Supplier relationships are managed with resilience requirements embedded in contracts. Internally, periodic forums bring together business continuity teams from different markets to share best practices, review incidents, and hear from experts across domains such as cyber and technology. This helps break down silos and promotes organizational

integration. Externally, the company participates in sector forums, exchanging lessons and planning joint simulations with peers. Overall, strong networks are supported through contractual controls, structured collaboration, cross-functional forums, and selective external information sharing.

4. Case Study Four: North American Insurance Company – internally, efforts focus on breaking down silos and improving collaboration across departments. Externally, the company actively partners with local authorities, for example, running a joint exercise with the county to distribute medication in an anthrax scenario, ensuring employees and families could access resources. However, gaps remain, particularly around preparedness for active shooter situations and broader engagement with emergency responders, where further exercises and partnerships are needed. Supplier relationships are also being strengthened through enhanced third-party risk management and contractual resilience requirements.
5. Case Study Five: Global Bank – the interviewee noted that collaboration with peers and clients is a regular part of operational resilience, so strong ties exist with competitors, regulators, and industry forums. Community engagement is treated as a given since systemic impacts on clients are central to resilience planning. The organization participates in industry forums and client groups, fostering cross-sector learning and preparedness. However, challenges remain around balancing collaboration with data privacy restrictions, in particular in areas such as ransomware response, where regulatory barriers limit the extent of mutual support that can be entered into.
6. Case Study Six: Global Logistics Company – Strong Relationships and Networks are viewed as one of the top resilience priorities for this organization. The interviewee stressed that both internal and external engagement matter – building connections with colleagues, auditors, and regulators is vital. Locally, country coordinators nurture relationships with communities, though the level of engagement varies across regions. While global structures support connection, there is recognition that more could be done to foster and formalise community engagement consistently. Overall, the principle is fully endorsed, seen as fundamental to resilience, and embedded through ongoing dialogue with stakeholders, regulators, and international teams.
7. Case Study Seven: Global Aerospace Company – Strong Relationships and Networks are central to the resilience strategy. Internally, the focus is on connecting silos rather than breaking them down, ensuring collaboration and strong relationships across risk, business continuity, crisis, and cyber teams. Externally, the organization prioritises resilient supplier relationships, cascading resilience requirements throughout its supply chain, and strengthening engagement with governments in response to geopolitical and regulatory pressures. Significant investment is directed at ensuring contractual resilience obligations and robust supplier audits. Partnerships and joint ventures are also emphasised as resilience enablers.

Overall outcome

There was very strong consensus that Strong Relationships and Networks is one of the top resilience priorities, providing many advantages both internally and externally. This principle is at the core of removing siloes or connecting between them, as well as being essential to effective supply and value chain resilience. Relationships also underpin horizon scanning and early warning systems.

Other important networks that add to resilience include those with regulators, governments, and industry groups and forums. In some sectors, much work is done with competitors in the area of resilience, in particular sector exercising and informal benchmarking.

The area with the most variation seems to be community relationships and engagement, with a lack of consistency in this area seen in the case studies. Some of the organizations show strength in this area, while others highlight it as an area needing development.

Decisive and Rapid Response

Resilient organizations have the capability to carry out a rapid response to issues and incidents, and crises.

1. Case Study One: Global Energy Manufacturer – the interviewee emphasised crisis leadership, explaining that, in disruption, the leader becomes the focal point for decisions, avoiding 'decision by committee'. They described taking charge, with authority delegated from senior leadership, enabling quick, clear actions. Using a military-style OODA loop (observe, orient, decide, act), they make decisions with the information available, even if it is only partial, and continuously adapt. They also noted the need for rapid crisis communications, sometimes bypassing slow approval chains to issue timely messages. Overall, the principle is applied through clarity of command, speed, adaptability, and persistence. A lot relies on the character and experience of the crisis leader.
2. Case Study Two: Global Professional Services Firm – the interviewee highlighted the importance of small, empowered teams, stressing that fewer people in the room speeds decision-making. They described using Core Gold teams within crisis response, who are able to act quickly without waiting for large groups. Business Emergency Response Teams (BERTs) and Business Response Teams (BRTs) bring together cross-skilled experts on 24/7 rotation, supported by playbooks and scenario exercises. Escalation processes are clear, with comms integrated from the outset. This structure ensures quick decision-making, proactive incident detection, and fast, coordinated responses to disruption.
3. Case Study Three: Multinational Corporate – Decisive and Rapid Response is enabled by a strong incident management structure with clear escalation steps and a structured decision-making process. Incidents are first assessed by a small triage team, which includes the Resilience Director, domain lead, and the most impacted function lead. This group quickly decides whether to invoke crisis management. If escalation is needed, they brief the relevant executive member, who approves invocation and designates a crisis leader based on the nature of the disruption. The structure is designed to avoid delays, ensure swift escalation from incident to crisis management, and provide clear authority for rapid, informed decisions.
4. Case Study Four: North American Insurance Company – this principle is underpinned by a formal crisis management framework. Previously, executives acted informally, leading to confusion and siloed decisions. With support from external expertise, a structured model was introduced that clearly defines roles. This separation prevents duplication and delay, ensuring that decisions are made swiftly and coherently. Escalation processes and checklists allow incident teams to mobilise quickly, making responses proactive, cohesive, and collaborative.
5. Case Study Five: Global Bank – incidents are handled by business and technology together, through a clear, formalised, crisis management process. Full crisis activation automatically involves the COO or CTO as chair, depending on the disruption's nature. Impact tolerances are closely monitored, with breaches escalated quickly to senior levels. The organization avoids desktop tests, instead emphasising live and simulated exercises that reveal vulnerabilities and drive real-time learning. Escalation, board-level oversight, and joint ownership between business and technology ensure swift, well-informed decisions and rapid mobilisation when disruptions occur.
6. Case Study Six: Global Logistics Company – Decisive and Rapid Response is seen as essential but must balance speed with adaptability. The interviewee stressed that it is not only about making quick, well-informed decisions but also about pivoting when new information emerges. This is another case study organization that draws on the OODA loop as a strong structure for incident decision-making. The key is a culture that supports flexibility, iterative decision-making, and willingness to change course when evidence shifts.
7. Case Study Seven: Global Aerospace Company – Decisive and Rapid Response is embedded in this organization's crisis management culture, matching the React and Recover brick in its resilience framework. The organization is regarded as highly effective at 'firefighting', supported by crisis management teams at site and corporate levels. Crisis management teams at site and corporate level

are activated rapidly via mass-notification technology. Additionally, crisis anticipation groups meet monthly with the ERM team to pre-define escalation triggers and response options, ensuring that decisions can be made calmly in advance in many areas.

Overall outcome

There was ubiquitous agreement that Decisive and Rapid Response is a vital principle for resilience and this was reflected in each case study showing strong structures in place for incident and crisis management. Themes that emerged include the understanding that small leadership teams are more effective for rapid and decisive decision-making, with either direct input from executive level or pre-empowerment to make decisions on behalf of the executive. The OODA loop (observe, orient, decide, act) was apparent in two of the case studies as a useful structure for incident decision-making. Where organizations took time to pre-consider crisis actions and document how and when to escalate, or had built playbooks to assist in decision-making, this was seen as helpful. The use of notification technologies to rapidly pass messages to crisis teams was also a factor in ensuring effectiveness in this area.

Review and Adapt

This principle requires organizations to review and analyse events and adapt their strategies based on the information gathered, as well as using lessons learned from what went well and what did not do so.

1. Case Study One: Global Energy Manufacturer – while engineering and quality functions rigorously use tools such as root cause analysis, A3, and the 5 Whys, disruption management lacks similar processes. The interviewee stressed that learning from events is critical to avoid repeat failures and to become more predictive, although this is an immature area for the organization and completely under-resourced.
2. Case Study Two: Global Professional Services Firm – Review and Adapt is embedded through structured post-incident reviews and continuous learning. There is a strong process of writing Post-Incident Reports (PIRs) for every incident, including exercises. Lessons learned are escalated to the board when necessary. This creates accountability and drives change. External audits, such as ISO certification, add another layer of review by providing independent perspectives. The aim is to capture lessons systematically, avoid repeat issues, and improve resilience practices over time.
3. Case Study Three: Multinational Corporate – post-incident reviews are mandatory and are produced for both local and group-level events. They are shared with stakeholders and used to identify lessons and close gaps. External consultants may be brought in to run independent reviews after complex incidents, ensuring objectivity. The main aim is continuous learning and improvement, with open actions tracked to ensure implementation. This structured process of review, feedback, and adaptation reinforces a culture of learning, while also aligning with governance expectations and international standards, embedding resilience into everyday practice.
4. Case Study Four: North American Insurance Company – this principle is recognised as important but is not yet fully mature. After-action reports are produced for exercises, incidents, and crises, and lessons are captured. However, the process is inconsistent: significant issues may be escalated to governance groups, but minor lessons are not always systematically addressed. The organization sometimes struggles to collate and evaluate all observations, has no centralised repository, and does not always integrate those observations into risk management. A key gap is quantifying the financial impacts of disruptions, which limits awareness and prioritisation.
5. Case Study Five: Global Bank – a continuous learning culture is in place, with after-action reviews centralised and tracked. In addition, resilience policies are regularly reviewed to ensure they are not out of date. Regulatory feedback loops are also in place, which help to ensure adaptation.
6. Case Study Six: Global Logistics Company – this area is strongly emphasised in this organization. The interviewee stressed that after-action reviews must be non-judgemental and psychological safety must underpin learning processes. The focus must not be on blaming

individuals but on understanding the context, culture, and environment that shaped decisions and actions. By treating after-action reviews as opportunities to learn, rather than mechanisms for blame, organizations can foster real improvement. The aim is to adjust systems and environments so that future outcomes are better, rather than simply remediating isolated issues. This mindset sees Review and Adapt as a cultural enabler of resilience as well as a method to improve processes.

7. Case Study Seven: Global Aerospace Company – the Review and Adapt principle is deeply embedded in the organization's resilience framework, within both the React and Recover and Transform and Thrive bricks. The organization's three lines of defence support the sharing of lessons and coordination of improvements. Every CMT activation and major incident triggers structured debriefs, and lessons learned feed into design and process improvements. As well as being a resilience good practice, this is a regulatory requirement for this organization.

Overall outcome

The principle of Review and Adapt is seen as a central aspect of resilience improvement and adaptation in all the case study organizations. It is a continuous cycle that is vital for developing and improving resilience. Again, there are different levels of maturity shown, but where there are gaps, the interviewees are aware of this and are working to address these. Areas of practice in more mature organizations include escalating lessons learned to the board where appropriate, using external consultants to provide independent challenge and expertise, having a strong focus on psychological safety to encourage openness and honesty, and seeing the Review and Adapt principle as an enabler of resilience culture as well as an organizational learning requirement.

Redesign Processes

This principle is about using the capability to adapt to strategically rethink and restructure organizational processes in response to resilience requirements, as well as to fully exploit new technologies and opportunities.

1. Case Study One: Global Energy Manufacturer – the Redesign Processes principle was strongly recognised as part of resilience by this interviewee, who emphasised that organizations should exploit new technologies and capabilities to enhance resilience and gain competitive advantage. They expressed some frustration that this view is not yet held by the wider organization, but they are working to change this dynamic.
2. Case Study Two: Global Professional Services Firm – this principle is clearly evident in this organization. The interviewee gave a practical example of moving away from bureaucracy and hundreds of disjointed BIAs across jurisdictions, instead focusing on the organization's 15 to 20 truly critical processes, aligned to business strategy and client value. The organization has willingness to change processes when no workaround exists. Redesigning processes in this way has resulted in reduced duplication and sharpened focus, and has enabled resilience to be embedded in strategy, operations, and key supplier organizations.
3. Case Study Three: Multinational Corporate – this principle is highlighted as vital to resilience by this organization, which sees the ability to adapt as a cornerstone. The interviewee noted that resilience-by-design helps strengthen flexibility, making processes more adaptable during disruption. Adaptation is seen as both strategic and cultural, requiring leadership, awareness, and continuous adjustment to evolving conditions.
4. Case Study Four: North American Insurance Company – this principle is recognised but not yet fully realised. There have been small but impactful examples, such as moving from paper to digital signatures, which cut turnaround times from days to minutes and improved efficiency and resilience.
5. Case Study Five: Global Bank – this principle is embedded in this organization's resilience. The bank continually reviews and adapts its organizational and technological processes as part of its operational resilience cycle. This involves learning from incidents and identifying weak points, then adjusting processes to reduce the chance of failure. The bank has overhauled templates, business continuity plans, and testing strategies to simplify frameworks and make them more

dynamic. Redesigning processes is seen as ongoing, practical adaptation – which is central to strengthening resilience.

6. Case Study Six: Global Logistics Company – this principle is seen as an outcome of culture rather than procedure. The interviewee stressed that resilience depends on whether an organization has the environment and freedom to rethink and restructure processes without bureaucracy. They supported the idea that redesigning processes enables faster responses to disruptive events, whether from new competitors, emerging technologies such as AI, or crises. The ability to adapt organizational processes quickly and efficiently strengthens resilience by embedding flexibility. Ultimately, successful redesign depends less on formal steps and more on fostering a culture of adaptability and innovation.
7. Case Study Seven: Global Aerospace Company – organizational leaders recognise the need to simplify and streamline processes, reducing complexity where possible, but admit it is 'complex to be simple' sometimes. While there is strong management intention to pursue the ability to redesign and adapt processes, progress is at an early stage. The aim is to reduce the number of processes and embed resilience into existing frameworks, making operations more efficient, integrated, and adaptable over the coming years.

Overall outcome

Again, there was consensus that this is an important resilience principle. There is clear correlation between redesign and adaptation. Capabilities in this area varied across the organizations studied, with the wider current and historical business culture having a large impact on how willing organizations are to review their processes and invest in redesign and adaptation. Where this principle is strongly embedded in resilience, there are clear benefits – simplification of complex business systems, improving resilience operational areas such as business continuity, and strengthening resilience by enhancing flexibility and agility. This principle is also at the heart of digital transformation processes and the approach that organizations are taking to the uptake of AI and associated areas such as digital twins.

Retain Stakeholders

The ability to Redesign Processes will not bring benefits unless the organization also retains stakeholders through the process, but retaining stakeholders is also a wider resilience principle.

1. Case Study One: Global Energy Manufacturer – the Retain Stakeholders principle is recognised, but this organization has struggled with this area. Communication with stakeholders, regulators, communities, and employees is somewhat disjointed. There is a culturally-driven over-reliance on historic relationships with stakeholders rather than actively working with them to ensure retention.
2. Case Study Two: Global Professional Services Firm – this principle is strongly evident in this case. The interviewee emphasised that resilience depends on building trust, confidence, and ongoing dialogue with clients, regulators, suppliers, and employees. The organization achieves this through integrated forums, supplier resilience assessments, and clear communication channels such as emergency hotlines accessible to all staff. Strong legal and contractual frameworks align expectations with both clients and suppliers, reducing risk and helping retention. Senior leadership involvement, regular reporting, and transparency reinforce accountability. These measures ensure stakeholders remain engaged, informed, and supportive, embedding resilience into relationships and sustaining the organization's reputation and performance.
3. Case Study Three: Multinational Corporate – this principle is reflected through structured policies, strong governance, and active communication with employees, regulators, suppliers, and sector peers. Regular forums, simulations, and industry-wide exercises strengthen external collaboration and relationships, while internal communities share lessons and best practice. By combining contractual requirements, cultural embedding, and transparent reporting, the organization sustains confidence and engagement, ensuring stakeholders remain aligned and committed.

4. Case Study Four: North American Insurance Company – this principle is partially evident in this case. The organization maintains functional stakeholder engagement through compliance with state regulators, structured crisis communication, and partnerships such as county health collaborations on emergency preparedness. Vendor resilience is improving, with a strong recent focus on this area. Employees are engaged via awareness campaigns, training, and wellbeing initiatives, supporting retention and trust. However, strategic stakeholder alignment is weaker: board engagement is minimal, customer-facing resilience is limited, and external partnerships (e.g. law enforcement, emergency responders) remain underdeveloped, leaving stakeholder retention dependent on the resilience team rather than organizational strategy.
5. Case Study Five: Global Bank – this principle is strongly embedded in this organization. It maintains close ties with regulators, competitors, clients, and communities as part of its operational resilience framework. Engagement is structured through industry forums, client groups, and collaborative initiatives that emphasise systemic stability. With communities, the focus is on protecting client interests and minimising systemic impact, which are seen as integral to resilience. While collaboration with other banks is limited, the organization recognises the need for industry-wide initiatives to address third-party and systemic vulnerabilities. Retaining stakeholders is linked to transparency, shared preparedness, and protecting collective trust.
6. Case Study Six: Global Logistics Company – this principle was described as a top priority, with relationships and networks seen as central to resilience. The interviewee stressed that dealing with people – employees, auditors, regulators, and communities – must be the foundation of any resilience programme. At the local level, coordinators maintain relationships with communities, ensuring that engagement is grounded in local context. The organization recognises that stakeholder trust relies on open conversations and consistent contact with both internal and external groups. Retaining stakeholders is therefore about prioritising people, fostering dialogue, and embedding relationships across all levels.
7. Case Study Seven: Global Aerospace Company – this organization stresses the importance of both internal and external relationships. Externally, strong engagement with suppliers, governments, regulators, and joint venture partners is prioritised. The company invests heavily in cascading requirements across its supply chain and works to strengthen networks shaped by political and regulatory dynamics. Stakeholder retention is therefore achieved through collaboration, transparency, and long-term trust-building.

Overall outcome

Another principle which is accepted across the board, the Retain Stakeholders principle emphasises maintaining trust and engagement with key stakeholders during times of disruption, but also during business as usual. It is particularly important when change and transformation are taking place to ensure that stakeholders understand what is occurring and why. Involving stakeholders in decision-making helps gain commitment to change programmes. Case studies highlight that effective communication and transparency are central to retention, and proactive engagement with regulators, customers, suppliers, and employees helps sustain confidence and loyalty. Retaining stakeholders requires deliberate structures, consistent dialogue, and alignment with expectations. It also depends on creating an organizational culture based on trust, openness, and people-first approaches. Retaining stakeholders is seen as essential to preserving reputation, enabling collaboration, and ensuring long-term resilience.

Reinventing Purpose

This principle emphasises the need for organizations to constantly consider whether their purpose should evolve or adapt.

1. Case Study One: Global Energy Manufacturer – the interviewee linked the Reinventing Purpose principle to embedding resilience into corporate identity and strategy, stressing that resilience is often missing from high-level visions, despite being essential for long-term

sustainability. The interviewee had been working to take the organization with them in this area.

2. Case Study Two: Global Professional Services Firm – the interviewee viewed this principle as the highest level of organizational resilience. It is evident in this company, which has significantly reviewed its purpose under new leadership – a pivot specifically linked to resilience by the CEO. This reframing of organizational purpose demonstrates how resilience can be central to long-term strategy and cultural renewal, rather than a narrow compliance function. By embracing a new direction and embedding resilience as part of leadership vision, the organization shows that reinventing purpose is a key driver for organizational growth and stakeholder confidence.
3. Case Study Three: Multinational Corporate – the Reinventing Purpose principle is strongly recognised in this case study – it is seen as a critical part of resilience, shaped by priorities such as climate risk and the shift towards sustainability. This organization has embedded the principle into governance through committees and executive-level discussions, aligning corporate purpose with resilience goals such as net-zero targets and renewable energy adoption. As a fast-moving company, it must constantly redefine its mission to remain relevant, and resilience plays a central role in this reinvention – ensuring that purpose evolves with environmental, technological, and societal change.
4. Case Study Four: North American Insurance Company – this principle is not yet fully embedded in this organization, with resilience mainly framed as meeting regulatory requirements, with limited strategic vision. Without this, resilience remains operational rather than purpose-driven, limiting its transformative potential.
5. Case Study Five: Global Bank – resilience is not framed as Reinventing Purpose in this organization. The interviewee acknowledged that while resilience could be linked to reviewing business direction, markets, and products, the organization does not currently approach it this way. The interviewee saw the idea as overly ambitious. The organization focuses more on compliance and operational processes, making it difficult to integrate resilience into higher-level strategic reinvention.
6. Case Study Six: Global Logistics Company – the interviewee rejected this principle. Purpose and values should remain stable; failure usually results from clinging to outdated processes, not from inappropriate values.
7. Case Study Seven: Global Aerospace Company – this organization sees the Reinventing Purpose principle as essential to long-term resilience. Leaders link it directly to strategic adaptation, such as the company's net-zero trajectory and technological transformation programme. The interviewees stressed that resilience goes beyond crisis management and business continuity to redefining corporate direction so the business can thrive in future markets. Climate change, regulation, and shifting economic conditions are driving this reinvention. Resilience is seen as both a mindset and a strategic necessity: embedding purpose into culture, operations, and governance to ensure the organization adapts before external shocks make it obsolete.

Overall outcome

Reinventing Purpose was the only principle where one of the interviewees rejected the principle rather than agreed with it. Another saw it as overly ambitious. Across the case studies, there was a wide range of approaches to the principle, with some seeing it as of central and pivotal importance to long-term resilience and others believing that it had no relevance. Of those who accepted the principle, for some, it is a personal professional understanding, rather than an organizational reality. For others, though, it is a capability that is in place, with those organizations seeing it as a strategic imperative.

CONCLUSION

This project set out to explore the four Business Enablers for resilience and the eight Principles of Resilience through seven in-depth case studies. The Business Enablers and Principles of Resilience were developed a number of years ago, so one of the aims was to assess whether these are still appropriate in today's organizational climate.

Another aim was to provide practical assistance to resilience professionals around the world, who often struggle to find real-life case studies showing how resilience is practically expressed, governed, and managed. Governance, vision, and strategy were key aspects of the case studies conducted for this document, as guidance in these areas is a particular weakness in the global resilience body of knowledge.

The case studies reinforce a clear and consistent message: organizational resilience is no longer a peripheral or technical discipline – it is becoming a core strategic capability.

Across sectors and geographies, resilience is evolving from:

- A compliance-driven function to a strategic enabler,
- A siloed set of activities to an integrated organizational capability, and
- A reactive posture to a proactive, adaptive mindset.

However, the case studies also reveal that this transition is underway, but not complete. Many organizations remain constrained by fragmented governance, misaligned incentives, limited resources, and a persistent tension between short-term performance pressures and long-term resilience investment. These constraints are systemic features of modern organizational life and, in many cases, are outside the current control of resilience leaders.

Looking forward, several implications have emerged for the next phase of organizational resilience:

- Resilience must continue to move 'upwards' into strategy, not just 'across' into functions. The most resilient organizations are those that treat resilience as a central lens through which overall strategy is informed and developed. This requires boards and executives to shift from asking 'Are we resilient?' to asking 'How is resilience shaping our strategic choices?'
- The role of the Chief Resilience Officer (or equivalent) is likely to become increasingly important. Across multiple case studies, the absence of unified executive ownership emerged as a limiting factor. A senior leader with authority, cross-functional remit, and board access provides not just coordination, but leadership narrative – helping organizations understand resilience as a coherent strategic story rather than a collection of technical activities.
- Resilience must be designed into systems, not bolted on afterwards. The recurring theme of missed resilience-by-design opportunities suggests that too many organizations sacrifice long-term resilience capabilities for short-term cost-control. In an era of systemic risk and increasing technological dependency, resilience must be a central element considered at the design and build stage for organizational systems and processes. It must be embedded into infrastructure, technology, operating models, supply chains, and transformation programmes from the outset.
- Culture and people determine resilience outcomes. While frameworks, technology, and governance are essential, the case studies repeatedly demonstrate that culture is the true multiplier. Psychological safety, leadership behaviours, learning mechanisms, and the empowerment of individuals and teams ultimately determine whether resilience practices are genuinely bought into and practised, or whether they are merely documented and given lip-service. The organizations that will thrive in the next decade will be those that invest deliberately in the human foundations of resilience.
- Finally, resilience must be understood as a permanently evolving capability, not a destination. There is no end state of 'being resilient'. Instead, resilience is a dynamic condition, shaped by changes in technology, geopolitics, climate risk, regulation, and social expectations. The organizations that succeed will be those that treat resilience as a continuous process of understanding, building, adapting, learning, and redesigning – not as a one-off programme or maturity target.

Overall, the case studies show that, while the language of resilience is now widely recognised in organizations, the way in which it is put into practice varies considerably between

organizations. Some view resilience primarily as compliance, while others embrace it as a strategic advantage and even a driver of purpose and cultural renewal.

Across the case studies, the Business Enablers were consistently identified as critical foundations: without strong leadership, integrated structures, alignment between strategy and operations, and a culture that empowers people, the Resilience Principles cannot be sustained.

The Resilience Principles themselves remain highly relevant and are being increasingly embedded. Even when this has not yet proved to be possible, given the organizational context, the resilience professionals who were interviewed personally recognised and supported the principle in question. The only notable exception was the principle of Reinventing Purpose, which somewhat divided opinion – with some organizations seeing it as essential and others rejecting it as unrealistic, or even inappropriate.

For organizations, the implication is clear: resilience cannot be treated as a narrow technical discipline. It requires governance at the highest level, a clear vision, deliberate investment in people and culture, and continuous adaptation of strategy and operations. For the resilience profession, the findings from this document reinforce the need to work across disciplines, to frame resilience as both protection and opportunity, and to develop common ways of measuring and demonstrating progress.

Ultimately, resilience is not an operational end state but a strategic capability based on a cycle of continuous assessment and improvement. It is much more than the ability to prevent or recover from a crisis; organizations that embed resilience into leadership, purpose, and culture will not only withstand disruption but also use it as a platform, an enabler, and a catalyst for innovation, transformation, and long-term sustainability.

Notes and references

(1) Organizational Resilience – BCI Position Statement, 2016, https://www.thebci.org/thought-leadership/bci-statement-on-organizational-resilience.html

(2) The Resilience Framework, BCI, 2024, https://www.thebci.org/certification-training/resilience-framework.html

(3) BCI Resilience Vision 2030 Report, 2025, https://www.thebci.org/resource/bci-resilience-vision-2030-report-.html

(4) The launch of ISO 22316, *Organizational resilience – Principles and attributes*, in 2017 (5) was the first step in formalising an international approach to developing resilience within businesses and other organizations. However, according to the BCI's *2022 Horizon Scan Report* (6), conducted five years after publication of ISO 22316, only 3.5% of surveyed organizations were planning to move towards using or implementing ISO 22316 as their preferential resilience standard. 2024 saw the introduction of a second organizational resilience standard, ISO 22336, *Organizational resilience – Guidelines for resilience policy and strategy* (7). This focuses on the strategic aspects of organizational resilience, including how to "establish a cooperative and coordinated capability to enhance resilience". There is seemingly no research available yet into ISO 22336 usage, but given that it builds upon ISO 22316, it appears unlikely that there has been a large uptake of this standard either.

(5) ISO 22316, *Organizational resilience – Principles and attributes*, 2017, https://www.iso.org/standard/50053.html

(6) *BCI Horizon Scan Report 2022*, BCI, https://www.thebci.org/resource/bci-horizon-scan-report-2022.html

(7) ISO 22336, *Organizational resilience – Guidelines for resilience policy and strategy*, 2024, https://www.iso.org/standard/50073.html

(8) *Roads to Resilience*, Cranfield School of Management and Airmic, 2014, https://www.airmic.com/sites/default/files/technical-documents/Roads-to-Resilience-full-report.pdf

(9) *Roads to Revolution*, Cass Business School and Airmic, 2018, https://www.airmic.com/sites/default/files/technical-documents/Roads-to-revolution.pdf

(10) ISO 22301, *Security and resilience – Business continuity management systems – Requirements*, 2019, https://www.iso.org/standard/75106.html

(11) ISO 27001, *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, 2022, https://www.iso.org/standard/27001

(12) SOC2: System and Organization Controls (SOC) 2 is a framework developed by the American Institute of Certified Public Accountants (AICPA) that assesses an organization's controls for protecting customer data.

Glossary

This publication follows the terms and definitions related to resilience as set out in ISO 22300:2025 *Security and resilience – Vocabulary*, https://www.iso.org/standard/85749.html

Acknowledgements

Airmic and the BCI would like to gratefully acknowledge the assistance of the following people in the development of this publication:

- All the case study participants
- Editor and project lead: David Honour
- The technical working group who guided the development of the publication:
  - Julia Graham, FCII, Chartered Insurance Risk Manager, FBCI, CEO, Airmic
  - David Thorp, Executive Director, BCI
  - Daren Evans, CEng FIMechE, ChPP RPP FAPM, MBCI, Operational Framework Manager, BAE Systems plc
  - Isaac Wheatley BSc, MBCI Senior Business Continuity Analyst, CMS – Cameron McKenna Nabarro Olswang LLP
  - Hoe-Yeong Loke, Head of Research, Airmic

Airmic
Marlow House
1a Lloyd's Avenue
London
EC3N 3AA

Tel: +44 207 680 3088
Fax: +44 207 702 3752
Email: enquiries@airmic.com
Web: www.airmic.com

BCI
9 Greyfriars Road
Reading, Berkshire
RG1 1NU, UK

Email: bci@thebci.org
Web: www.thebci.org