

+WhitePaper:

# Sharpening Your Business Resilience Strategy

The guide to secure  
operations now and in the  
future



# Executive Summary\_

**From cyberattacks and climate volatility to geopolitical instability and systemic digital dependencies, business resilience is now an imperative for executive leadership. In many sectors, where operational continuity is mission-critical, the ability to absorb, anticipate, and react to disruption defines organisational viability and even a licence to operate. Beyond that, resilience is also a business accelerator, helping to assess opportunities and respond quickly in order to adapt and improve.**

This whitepaper explores how resilience has evolved from a narrow focus on disaster recovery and standard contingency planning into a strategic, enterprise-wide capability that prioritises long-term stability by anticipating and preparing for a broad spectrum of potential threats.

Faced with an uncertain environment, leaders must navigate complex challenges: how to align strategies with new threats, clarify risk governance and optimise investments, all with a comprehensive and consistent view. This white paper proposes a concrete approach to building corporate resilience that integrates all its dimensions: cybersecurity, operational dependencies, physical risks, governance and human readiness.

Given the growing complexity of threats and regulatory expectations, many organisations are turning to expert partners for support. Airbus Protect draws on decades of experience in safety-critical systems and cybersecurity to deliver embedded expertise, personalised assessments, and integrated solutions that scale with complexity and regulation.

When treated as a strategic leadership priority rather than a compliance requirement, resilience empowers organisations to effectively navigate volatility, recover stronger from future disruptions, and maintain business continuity, in turn, upholding stakeholder confidence and protecting brand reputation.





# Table of Contents

<b>Executive summary</b>	<b>003</b>
<b>Introduction – The need for business resilience</b>	<b>007</b>
<b>What does resilience mean for today’s businesses?</b>	<b>008</b>
<b>The biggest challenges businesses face today</b>	<b>009</b>
<b>What it takes to build resilience</b>	<b>012</b>
<b>How business can boost resilience</b>	<b>014</b>
<b>Putting resilience to the test</b>	<b>017</b>
<b>Strong frameworks in action: The story of a resilience transformation</b>	<b>018</b>
<b>The human touch in business resilience</b>	<b>019</b>
<b>Future-ready resilience: safeguarding from tomorrow’s threats</b>	<b>020</b>
<b>Conclusion</b>	<b>022</b>



Business resilience is defined as an organisation's capacity to anticipate, prepare for, respond to, and adapt to incremental change and sudden disruptions, ensuring continuity under both expected and unforeseen circumstances.

# Introduction

## The need for business resilience

The frequency and severity of business disruptions are rising, resulting in greater costs. In IBM's 2024 Cost of a Data Breach Report, it was revealed that the **global average cost of a data breach has reached USD 4.9 million, representing a 10% increase over 2023 and the highest level since reporting began.**

Furthermore, Check Point Research found that the average number of weekly cyberattacks in Europe surged by 22% in Q2 2025, marking the most significant increase across all global regions. This escalation demands a more robust and forward-looking approach to resilience.

Where operating environments are more volatile than ever, business resilience is imperative.

More than just a defensive shield, true resilience provides the operational confidence and agility for an organisation to take calculated risks and seize strategic opportunities that might otherwise be out of reach in a volatile environment.

High-reliability industries, such as aviation, energy, healthcare, and defence, face a long and growing list of complex and evolving threats. Whether it is the cascading effects of global supply chain failures, extreme weather events, or the escalating sophistication of cyberattacks, maintaining secure and adaptable operations across physical systems and the digital space has become an urgent board-level priority.

Compounding this challenge is the emergence of powerful new technologies. Agentic AI has emerged with significant disruptive potential, embodied in autonomous systems capable of reasoning and executing complex actions. While these offer immense operational capability, they also create new attack surfaces and regulatory uncertainties, accelerating the urgency to invest in secure, adaptable solutions for resilient, future-ready frameworks.

Many organisations are at risk of discovering the limitations of short-term contingency planning the hard way, as they continue to rely on reactive approaches to resilience. A recent report from The World Economic Forum's unveiled that **over 70% of business leaders believe their organisations are not adequately prepared for the next major disruption.** That's why it is absolutely essential for businesses to implement future-ready resilience frameworks, practices and training programmes, especially in an increasingly complex environment. Not only to anticipate the next crisis, but to build the capacity to adapt and evolve in response to shifting environmental, geopolitical, and technological challenges in the years to come.

In this guide, we explore how organisations in aviation and critical sectors can sharpen their resilience strategies by understanding today's threats, identifying capability gaps, and deploying advanced but pragmatic solutions.



*Allianz reports that cyber incidents, business interruptions and natural catastrophes remain the top three global business risks for the third consecutive year.*

White Paper

**What does resilience mean for today's businesses?**

# What does resilience mean for today's businesses?

In the past five years, the notion of resilience has moved away from the disaster recovery and business continuity narrative and shifted toward a forward-looking, proactive strategy embedded across enterprise functions. For C-suite leaders, resilience intersects with financial performance, brand trust, stakeholder expectations, and regulatory compliance.

## The threat landscape

Companies now operate in a dual-threat environment – facing both cyber and geopolitical risks – as ransomware attacks and supply chain intrusions grow more sophisticated, and global tensions increasingly destabilise critical markets and infrastructure.

Now more than ever, cyber threats pose a significant and escalating business risk. Cyber attacks, motivated by financial gain, leverage exposed edge devices and public-facing applications for intrusion. According to CrowdStrike's 2024 Global Threat Report, over half [\(55%\) of all active cyber threat groups](#) tracked in 2024 were financially driven. Compounding the challenge, adversaries now exploit vulnerabilities quickly, taking advantage of delayed patching cycles and inadequate monitoring.

On the other hand, 'traditional' threats long considered manageable, such as geopolitical tensions, natural disasters and infrastructure failures, are returning with increased frequency and intensity due to climate change, complex diplomatic relations and technological sophistication. In fact, United Nations Disaster Risk Reduction (UNDRR) revealed in a 2025 report that disaster costs now exceed [over \\$2.3 trillion annually](#), when cascading and ecosystem costs are taken into account, exerting a substantial macroeconomic toll.

This context amplifies risk convergence and exposes supply chains and physical infrastructure to disruption risks, in the same way that pressures to accelerate time to market introduce digital vulnerabilities. In aviation and other safety-critical sectors, these overlapping threats can lead to cascading failures across digital and physical domains.

However, viewing resilience solely through the lens of threat mitigation is incomplete.

## Why resilience matters

Cyberattacks, power outages, system failures, or geopolitical disruption – all the above have the potential to halt operations across digital and physical domains. The resulting consequences of a disaster, including prolonged service outages, reputational harm, regulatory non-compliance, and even human safety risks, have rendered the reactive approach increasingly untenable.

As such, resilience must be built into the fabric of operations to:

- > **Preserve mission-critical functions under stress**
  - Supports the continuation of critical operations (such as manufacturing execution systems (MES) and safety-critical OT controls) during a cyberattack or power failure, mitigating downtime.
- > **Ensure systemic integrity**
  - Even under partial failure, where a system does not collapse entirely under stress, businesses can maintain safe operational output until the system is restored, preserving customer trust and regulatory standing.
- > **Maintain compliance during incidents**
  - Many sectors, aviation in particular, are governed by strict regulatory regimes. As such organisations must ensure compliance obligations are still being fulfilled during operational crises to avoid fines and potential licence suspension.

# The biggest challenges businesses face today

A resilient organisation, confident in its ability to manage disruptions, is better positioned to innovate and pursue growth. It can enter new markets or adopt new technologies with the assurance that it can withstand unexpected setbacks. In this sense, resilience becomes a strategic enabler – a foundation upon which the business can build, adapt, and ultimately, thrive.

Once an area handled by IT, disaster recovery planning (DRP) is now a primary leadership role in which C-suite executives are more directly involved. Where incidents have an immediate operational and reputational impact on companies, business continuity planning (BCP) must be aligned across technical, operational, and leadership functions.

This alignment, however, is a developing challenge. According to a 2024 resilience survey, only [31% of surveyed organisations](#) have fully integrated resilience programmes across functions. This misalignment often results in duplicated controls, unclear responsibilities during crises, and slower recovery times.

But synchronising BCPs and DRPs, which often reside in different departments with separate priorities, leaves many executives asking where to start. As such, they face the following challenges:

## Knowing what to protect

From digital transformation and cybersecurity to environmental disruption and aging infrastructure, many business leaders have struggled to understand where to focus their resilience investments. In World Economic Forum's [2025 Resilience Pulse Check](#), while executives tend to prioritise financial (56%) and digital (46%) resilience, foundational capabilities like crisis response (20%), strategic reorientation (20%), and foresight (18%) are significantly deprioritised, suggesting a strong bias toward short-term, measurable outcomes rather than long-term adaptability and systemic risk management

## Prioritising the right risks

As threat vectors evolve, choosing which risks to mitigate, at what level and at what cost, becomes more complex. Risk prioritisation must balance technical feasibility, regulatory obligations, stakeholder tolerance, and potential business impact. In safety-critical sectors, this often means weighing low-probability events against high-consequence outcomes.

## Understanding the cost of inaction

Many executives still view resilience as a costly expense, rather than a strategic necessity. However, historical large-scale disruptions, from ransomware attacks to climate-induced infrastructure failures, have repeatedly demonstrated that the cost of inaction far exceeds the investment in preparedness.

In April 2025, a large-scale power outage suddenly swept across the [Iberian Peninsula](#), affecting millions in Spain, Portugal, and parts of southern France. Critical infrastructure, including transport networks, hospitals, digital communications, and manufacturing plants, was forced offline for hours, and in some cases, it took days to recover to full capacity. The outage resulted in production delays, missed contract deadlines, significant financial losses, particularly for organisations that lacked backup power systems, redundant communications, or tested crisis protocols.

The grand total amounted to [1.6 billion](#) euros lost – much of which could have been mitigated through foresight, planning, and investment in resilient infrastructure.



*Resilience is the interconnection and synchronisation of multiple disciplines, which draw on complementary skills and involve continuous progress over time.*

## White Paper

**The biggest challenges businesses face today**

The greatest challenge for business resilience is not in identifying every possible disruption, but in striking the right balance between protection and recovery.

In practice, this means accepting that resources are finite and choosing wisely between investing in prevention and building capacity to recover, as illustrated in the graph below. Over time, protection becomes less efficient as costs increase, threats evolve, and rigid controls introduce operational friction.

Meanwhile, investment in recovery capabilities grows more efficient as organisations develop adaptive processes, real-time insights, and scalable response mechanisms. The intersection of these curves, where protection begins to deliver diminishing returns, and recovery begins to create strategic advantage, is the resilience threshold. It is here that business leaders must focus their decision-making.

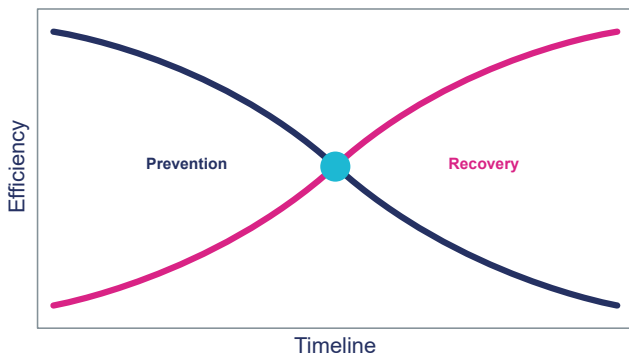


FIGURE 1: The right balance between prevention and recovery for effective corporate resilience

As such, C-suite executives must grapple with two fundamental questions:

> **What should be secured**

Beyond a basic, compliance-driven level, organisations must define a strategic boundary that protects the most vital elements of the business, such as assets, operations, and relationships. This means identifying mission-critical functions, understanding their dependencies, and prioritising protection where it will have the greatest impact.

> **How much protection is enough**

Complete risk elimination is impossible. The goal must be to reduce risk to an acceptable level that aligns with risk appetite and operational capacity.

This means determining the appropriate scope, depth, and duration of mitigation required to ensure resilience without overextending resources.

Both questions must be answered in a context that is increasingly fluid. As it stands, there is no single 'normal' operating condition. Business models are changing rapidly, threats are multiplying in scale, speed and sophistication, and technology itself introduces as many risks as it mitigates.

This volatility demands comprehensive resilience strategies that are capable of sustaining core functions and protecting systemic integrity.

**For C-suite executives, resilience now means ensuring:**

- \* Integrated coverage of both digital and physical risks,
- \* Clear executive ownership of continuity planning,
- \* Coordination between IT disaster recovery and business-wide continuity strategies,
- \* Real-time visibility into operational dependencies and vulnerabilities.

**C-level leaders must now prioritise:**

- \* Safeguarding business continuity amid unpredictable conditions,
- \* Securing all critical assets against increasingly complex cyber threats,
- \* Ensuring operational and regulatory resilience across global supply chains,
- \* Adopting sustainable practices without compromising stability.

It is precisely to address these challenges and priorities that a structured plan is vital. That's why, at Airbus, our partnership always begins with a comprehensive maturity assessment. This gives us a clear picture of strengths and weaknesses and allows us to build a realistic and prioritised roadmap.



White Paper

**What it takes to build resilience?**

# What it takes to build resilience?

Disruption doesn't always arrive as a single, headline-grabbing event. Sometimes, it takes the form of a sustained accumulation of smaller, seemingly disconnected incidents. This could manifest as a cyber intrusion followed by a supply chain delay, compounded by an equipment malfunction or regional power outage.

Whether a shock is singular or layered, of internal or external origin, resilience boils down to the same core principle: the ability to adapt under stress without systemic failure.

## Embedding adaptability and fault tolerance – Three pillars of building resilience

A robust resilience programme rests on three critical pillars. Organisations must:

1

**Mitigate their most consequential risks**

Organisations must effectively mitigate risk through data-driven assessments and proportionate controls, grounded in a clearly defined risk appetite. Scenario planning is critical, not to predict every threat, but to expose the types of disruption that could cause systemic or existential failure.

2

**Secure the assets that matter most**

Effective protection begins with an up-to-date inventory of critical business services and their dependencies. Without clear visibility, resilience efforts risk being misdirected – either overprotecting non-essential assets or underestimating vulnerabilities that could prove catastrophic.

Once critical assets are identified, organisations must ensure they are defended in proportion to the impact their loss would have. The aim is to break the chain of escalation, so even if one component fails, essential functions remain intact.

3

**Determine needs in an unstable context – and adapt**

Continuous horizon scanning, threat intelligence and scenario testing keep plans relevant as technologies, geographies and regulations evolve. Advanced technology can act as an enabler as AI-enhanced monitoring platforms ingest telemetry from OT sensors, cloud workloads and identity systems, surfacing anomalies far faster than human analysts. Automation can isolate infected hosts or initiate fail-overs within seconds.

## AI and resilience

Yet Airbus Protect's own operating doctrine stresses that technology remains a tool, effective only when its outputs are understood and governed by informed humans. The integration of AI, automation, and cloud-based platforms undoubtedly expands an organisation's capabilities, but it also increases the surface area for potential disruption.

Effective resilience lies in managing this trade-off, harnessing innovation for its benefits, while actively governing the risks it introduces. That's why readiness cannot rely on tooling alone, but through iterative testing, cross-functional drills, and closed-loop lessons-learned cycles.



# How Businesses can boost their resilience

## The five resilience pillars

1

### **Risk/threat management: Build clarity around your threat landscape**

Resilience begins with understanding risk. Given the surge in exploitable vulnerabilities, with over 40,000 susceptibilities identified in the last year, a 30% increase from the previous year, it is crucial that organisations continuously assess potential threats and understand how those risks intersect across departments and systems. This ranges anywhere from cyberattacks and climate-related hazards to geopolitical instability and third-party failures.

Risk and threat management involves identifying threat scenarios, quantifying their potential impact across operational, reputational, and regulatory dimensions, and consistently refining treatment plans. Crucially, this function must be dynamic and forward-looking, leveraging threat intelligence, scenario simulation, and cross-domain collaboration to anticipate risk rather than simply respond to it.

The other pillars of resilience feed directly into this one, ensuring the risk picture reflects operational realities rather than theoretical assumptions.

2

### **Incident management: Strengthen your first line of response**

When disruption strikes, the effectiveness of the immediate response often determines the scale of its impact. Incident management is the first line of operational defence, tasked with containing threats before they escalate into broader crises. Its primary role is to ensure fast, structured intervention, backed by predefined escalation protocols and communication pathways.

Incident response must be executed with discipline and clarity. This capability demands clearly defined roles, trained response teams, and mechanisms for early detection and alerting. Incident management also acts as a trigger for the activation of other resilience functions, such as crisis coordination, continuity plans, and recovery workflows. Incident management should be planned, rehearsed, and continuously refined if it is to be effective.

3

### **Crisis management: Prepare for high-impact events**

Some events go beyond the remit of local containment. They have the potential to bring critical services to a screeching halt, undermining public trust and jeopardising the long-term viability of the organisation.

Crisis management exists to provide the governance structures, decision-making frameworks, and coordination mechanisms necessary to navigate high-impact, cross-functional disruptions. This includes defining leadership roles, managing external and internal communications, and coordinating with stakeholders across supply chains, regulatory bodies, and civil infrastructure.

Unlike incident management, which focuses on immediate operational containment, crisis management takes a macro view, prioritising strategic decision-making under uncertainty. It requires sound documentation and active leadership alignment to be able to expect the unexpected.

## The five resilience pillars

4

### **Business continuity management: Sustain core operations during disruption**

Where non-cyber risks remain prevalent, with climate-related threats such as floods, heatwaves and extreme storms increasing in frequency and intensity and posing a direct risk to critical infrastructure, data centres, transport hubs, and supply chains, business continuity must ensure critical operations remain functional when physical disruption hits. Business continuity management creates this capacity.

Continuity management defines an organisation's critical functions, maps their dependencies, and ensures the infrastructure, resources, and roles required to maintain them are available during a disruption. Continuity plans must be designed around realistic recovery objectives, regularly tested through scenario-based exercises, and updated to reflect evolving organisational and external risks. Rather than focusing solely on "getting back to normal," this function is primarily focused on maintaining an acceptable level of function until full recovery is possible.

5

### **Disaster recovery management: Restore systems with speed and integrity**

When the acute phase of disruption has passed, organisations must turn their attention to recovering quickly and safely. Disaster recovery focuses on restoring systems, data, infrastructure, and services with minimal disruption, ensuring the business can resume normal operations and meet contractual, legal, and reputational obligations.

A prolonged outage in data availability, production capacity, or customer services can have cascading impacts on reputation, regulatory standing, and commercial viability. DRM ensures that businesses can resume operations in line with both contractual obligations and regulatory requirements. Effective disaster recovery involves tested procedures, resilient architecture, and governance mechanisms that ensure accountability at every step.

In complex and highly regulated environments, this pillar involves oversight bodies such as resilience steering committees that report directly to the board. In this, compliance obligations like NIS2 or the SEC disclosure rule should be treated as minimum operating standards, as opposed to arduous catch-up exercises.

### **The balance between protection and recovery**

Protection involves building layered defences, robust governance, and predictive risk capabilities. Recovery demands tested systems, responsive coordination, and sustained capacity to absorb and rebound from shock. It is the interplay between these forces, proactive safeguarding and adaptive recovery, that defines great resilience.



*The objective is not to eliminate all risk. The goal is to ensure that, when disruption occurs, the organisation can protect what matters most, recover quickly, and emerge stronger.*

# Putting resilience to the test

## Our signature 360° Resilience approach

At Airbus Protect, resilience is never static, it's constantly evolving and developing. Our flagship 360° Resilience model provides a structured, three-year plan that transforms compliance-driven frameworks into a state of demonstrable readiness. Built around the needs of the five outlined pillars, we define, develop and implement capabilities, combined with rigorous measurement of key performance indicators and a clear governance and delivery model

To ensure progress is measurable and lasting, the plan follows an Annual Resilience Cycle.

## The Annual Resilience Cycle:

- \* **Define:** Each year begins by setting a clear, measurable resilience target, for example, successfully managing a full-day simulated crisis exercise while maintaining critical operations.
- \* **Develop:** We build the necessary processes, plans, and technical measures to meet that objective, whether that's refining BCPs, enhancing DR frameworks, or delivering targeted awareness sessions.
- \* **Train:** The cycle culminates in a synthesis exercise that tests the entire resilience system, not just isolated functions, validating readiness across all five pillars and ensuring that improvements are embedded into practice.

Repeating this cycle annually allows organisations to progressively mature their resilience capabilities, combining immediate tactical wins with long-term strategic transformation

## Synthesis exercises and the Cyber Range

Exercises are at the heart of proving resilience. Airbus Protect's synthesis exercises validate the entire resilience system, testing leadership composure, technical containment, business adaptability, and recovery feasibility in a single, integrated scenario. Turning theoretical plans into demonstrated capabilities, these exercises reveal hidden weaknesses and strengthen cross-functional coordination.

To execute these in safe but realistic conditions, we leverage our state-of-the-art Cyber Range. This advanced simulation environment functions as a "digital twin" of the client's critical IT/OT assets, allowing technical teams to train, test, and rehearse incident response in conditions that mirror real operations, without risking live systems. The Cyber Range enables complex, collaborative scenarios that integrate both cyber and physical dimensions, from malware containment drills to operational failover testing, accelerating technical and human readiness alike.

Combined, synthesis exercises and Cyber Range training transform resilience from a documented intention into a proven capability, ensuring that when disruption occurs, every part of the organisation knows how to respond.



White Paper

**Strong frameworks in action: The story of a resilience transformation**

# Strong frameworks in action: The story of a resilience transformation

## Enhancing cyber resilience in a public transport infrastructure

### How Airbus Protect supported a mission-critical organisation in strengthening operational continuity

#### Sector context

Public sector organisations, tasked with cross-border service delivery, operate within a highly sensitive threat landscape. The critical nature of these services, often built upon tightly integrated OT systems, means that even a momentary disruption can have serious national and international repercussions. With the increasing convergence of IT and OT domains, combined with a growing volume of sophisticated, financially motivated cyber threats, the challenge was twofold: protect complex cyber infrastructures, while maintaining uninterrupted service.

#### Airbus Protect's approach

Airbus Protect delivered a customised, close-quarters engagement model, aligning directly with the client's internal teams and governance structure. With our deep heritage in industrial cybersecurity and safety, we embedded subject-matter experts within the organisation to provide continuous monitoring, threat detection and incident coordination tailored to OT-specific constraints. This proximity enabled us to respond rapidly to emerging incidents while also anticipating long-term strategic risks. Regular scenario-planning workshops, ongoing vulnerability analysis, and transparent communication frameworks ensured that our actions remained aligned with evolving operational and geopolitical priorities.

#### Outcomes and strategic value

The result has been a measurable improvement in the organisation's cyber resilience posture. Airbus Protect's sustained presence has enabled faster detection and resolution of security incidents, improved coordination between IT and OT security stakeholders, and strengthened business continuity planning across critical service domains. Following high satisfaction ratings in stakeholder feedback, the organisation formalised the partnership within Airbus Protect's strategic reference programme in an ongoing commitment to long-term resilience.



# The human touch in business resilience

Automated detection systems, AI-enabled analytics, and structured playbooks are invaluable to containment and mitigation, but they rely on human interpretation, decision-making, and coordination to function effectively.

In high-pressure scenarios, it is people who must assess incomplete information, weigh competing priorities, and take responsibility for critical actions. This human factor, ranging from executive leadership through to front-line responders, is central to how resilient organisations absorb, adapt to, and recover from disruption.

For this reason, resilience planning must account for the human element at every stage.

## Leadership

Resilience starts at the top. Executives should speak regularly and visibly about resilience to reinforce its strategic value and set the cultural tone for the workforce. More than just formal statements, leaders should show consistent, hands-on engagement in planning exercises, crisis reviews, and investment decisions to demonstrate that resilience is a shared organisational priority.

When preparedness and adaptability are embedded into values and daily operations, a resilient culture is built. Executives should focus on transparency and supporting continuous improvement to maintain effective resilience.

## Training

Resilience comes down to facilitating a skills-rich, response-ready environment, equipped with prepared and empowered people. With active training programmes, policy becomes muscle memory. Multi-disciplinary crisis simulations, which combine cyber responders, business continuity leads, operational managers, and communications teams, expose coordination gaps and help embed roles and responsibilities in a low-risk setting. In this, staff gain the opportunity to practise critical recovery procedures, such as isolating a compromised OT workstation or executing manual fallback. As a result of practical training, the workforce becomes prepared and ready to respond calmly and efficiently when real alarms sound.

## Technology

Technology is a critical enabler of resilience, but only when designed to enhance human decision-making. In high-pressure environments, the value of data lies in relevance, and as such, monitoring systems should be designed and deployed with humans in mind. Instead of overwhelming analysts with unfiltered logs, dashboards should surface actionable intelligence in an intuitive way that supports timely intervention. Visualisation tools should adapt to the operational roles of their users, helping them focus on the most urgent data, such as anomalies, dependencies, or recovery metrics.



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

White Paper

**Future-ready resilience: safeguarding from tomorrow's threats**

# Future-ready resilience: safeguarding from tomorrow's threats

Threat environments are not static. In fact, their sophistication and impact grow more with each technological cycle. According to European Union Agency for Cybersecurity (ENISA), advanced persistent threats and AI-generated attacks have seen a [138% increase over the past year](#).

Offensively deployed AI can now automate phishing, vulnerability discovery, and deep-fake-powered disinformation at scale. Furthermore, hyper-connectivity deepens systemic risk, increasing interdependence between cloud-based systems, APIs and therefore creating the potential to trigger cascading failures across global platforms through one compromised entry point. Meanwhile geopolitical fragmentation raises the likelihood of sanctions, export-control shocks and state-backed cyber sabotage of critical infrastructure.

Resilience planning must therefore look beyond static, pre-defined runbooks. Future-ready organisations should institutionalise continuous threat intelligence ingestion, integrating feeds from open-source platforms, industry-specific ISACs, and national threat exchanges. This intelligence must be contextualised and operationalised for real-time risk triage, prioritisation, and escalation procedures. Regular tests should be taken to identify emergent threats and challenge the reliability of existing continuity plans.

Crucially, this intelligence must feed directly into enterprise risk registers and capital allocation cycles, ensuring that resilience measures receive sustained investment proportional to their strategic importance. Regulatory foresight is equally vital with frameworks such as the EU Digital Operational Resilience Act (DORA) and the SEC's cyber incident disclosure rules inside the current planning cycle.

## Third-party support

Business resilience is a tough journey to manage alone. There is a great amount to consider in establishing business resilience in a way that accounts for all critical factors: cybersecurity posture, operational dependencies, physical risk, governance structures, and human readiness.

Third party support from expert teams, well-versed in cybersecurity, operational risk, safety engineering, and legislation, can lift the weight of complex risk mapping and systems integration across enterprise functions. These teams can run various assessments, build robust resilience frameworks, and support training initiatives, while maintaining compliance. Bringing technical depth and sector-specific insights, they can bridge the gap between tools and outcomes, enabling organisations to prepare, respond, and seamlessly recover from disruption with minimised impact.

At Airbus Protect, we recognise that resilience doesn't stop at framework deployment. True resilience is grounded in addressing ongoing threat evolution and continuous improvement. As a trusted partner in high-reliability sectors, including aerospace, defence, and public infrastructure, we combine our heritage in safety-critical engineering with cutting-edge capabilities in cybersecurity, operational safety, and compliance strategy. Through ongoing assessment and cross-functional collaboration, businesses build resilience that is robust and constantly improving to meet the demands of an uncertain future.

Our teams are embedded across client operations, delivering forward-looking threat modelling, tailored governance architectures, and integrated resilience solutions that scale with complexity. By anticipating tomorrow's risks today, we help organisations embed agility and continuity into the core of their operations, ensuring they remain mission-ready, regardless of what's ahead.



White Paper

**Executive Checklist for Accelerated Resilience**

---

# Executive Checklist for Accelerated Resilience

This questionnaire is a strategic management tool, designed to quickly assess your organisation's posture and identify priority areas for action to turn resilience into a true performance asset.

## Strategic Anchoring and Executive Steering

- Do we view resilience as a strategic investment that protects our value and enables innovation, or is it still treated as a cost centre and a regulatory burden?
- Does our executive leadership visibly own resilience, ensuring unified governance that transcends the traditional silos between business functions and IT?
- Are our investment decisions actively managed to find the optimal balance between preventive protection and our ability to recover from a major crisis?

## Protecting Critical Functions and Operational Continuity

- Do we know precisely which of our functions are vital, and do we have a clear map of their dependencies to focus our protection efforts where the impact would be greatest?
- Do we have orchestrated response plans that allow for a smooth escalation from a local incident to global crisis management, activating the right continuity plans without delay?
- Is our technology designed to enhance human decision-making under stress, by providing actionable intelligence rather than an overload of information?

## A Culture of Preparedness and Validation Through Practice

- Do we go beyond theoretical plans by validating our resilience capability through large-scale synthesis exercises that simulate real-world conditions and test the entire response chain?
- Is our approach dynamic, with a continuous improvement process to adapt our defences and recovery plans to the constantly evolving threat landscape?
- Does our leadership drive a genuine culture of preparedness, where regular training turns procedures into reflexes, making the organisation more adaptable in the face of the unexpected?

**\_enabling a [trusted future]**

## Conclusion

Resilience has emerged as the essential prerequisite for sustainable performance in aviation and every other critical sector. As this whitepaper has explored, addressing these threats requires more than static planning or reactive recovery measures. Instead, resilience should take a comprehensive, end-to-end, and ongoing approach that unifies risk governance, technical hardening, and human enablement. Resilient organisations are those that can anticipate disruption, absorb impact, and recover with speed, while maintaining compliance, operational continuity, and stakeholder trust.

Given the volatile environment businesses operate in today, both digitally and physically, ongoing and proactive planning, testing, and refining will offer a competitive advantage. The benefits speak for themselves: enhancing operational stability, reducing exposure to reputational or regulatory harm, and the ability to protect long term value.

By embedding resilience into the core of the enterprise, leadership transforms it from a necessary safeguard into a strategic asset. An asset that not only protects the organisation but also empowers it to confidently navigate both risks and opportunities, ensuring sustainable performance in an uncertain future.



*We're there to support C-level leaders in embedding resilience into the core of their enterprise.*

At Airbus Protect, we understand the strategic weight of this challenge. That's why, drawing on decades of securing safety-critical aerospace operations, deep cybersecurity research, and environmental-risk expertise, we provide executive-level advisory, technical implementation and managed resilience services tailored to your context.

We don't just build frameworks; we build proven preparedness. Our resilience partnership is a collaborative journey that takes your organisation from paperwork to a state of demonstrable confidence, ready to face disruption and emerge stronger. Our expertise lies in helping high-reliability organisations like yours build the practices and capabilities to withstand today's threats, and tomorrow's unknowns.

Our team is ready to assess your resilience maturity and help you plan for what's next. Request a consultation today to explore how Airbus Protect can safeguard your operations. For additional insight into our end-to-end resilience philosophy, please visit our [Cyber Resilience](#) page on the Airbus Protect website.



*Airbus Protect stands ready to partner with you on that journey.*



# AIRBUS

Airbus Protect, 31700 Blagnac, France  
© Airbus Protect, 2024 - All rights reserved.  
Airbus Protect, its logo and the product names  
are registered trademarks. This document is  
not contractual. Subject to change without  
notice.  
[www.protect.airbus.com](http://www.protect.airbus.com)



**GET IN TOUCH TO DISCOVER  
HOW WE CAN SUPPORT YOU:**

[protect@airbus.com](mailto:protect@airbus.com)  
[www.protect.airbus.com](http://www.protect.airbus.com)