Adaptive Cyber Resilience in the Age of AI

Ensure sovereignty and trust at AI speed

ATOS GROUP Accelerating intelligence

C-Suite brief

Cybersecurity has reached an inflection point, driven by a fundamental change in its operating conditions.

The erosion of traditional security perimeters has been underway for years – driven by mobility, remote work, globalization, cloud, and digital ecosystems. What has changed is **speed and scale.**

Threats now operate at **machine speed,** outpacing defense models shaped largely around human-led responses. AI is reshaping both offense and defense. Regulations demand continuous, provable execution, not periodic assurance. And sovereignty has moved from policy debate to operational requirement.

Cyber risk is now the number one global business risk, placing it firmly at the top of the board agenda*. Yet even as cybersecurity budgets increase, scrutiny is intensifying because risks, costs, and expectations are outpacing investment. The question for leadership is no longer whether cybersecurity activity is increasing, but whether the organization can regain control quickly when disruption occurs, and prove it.

The principles of cybersecurity remain. The operating model must change. It must execute with machine-speed discipline.

The cybersecurity architectures most enterprises rely on today are built on sound principles, but were designed for execution at human speed, across fragmented environments, and proven largely through documentation. That model is no longer sufficient as IT and OT converge, AI and data pipelines become operational dependencies, ecosystems expand, and disruption propagates across dependencies faster than humans can coordinate.

Adding tools and controls hasn't solved the execution gap; what closes it is a change in operating discipline. Closing the gap requires shifting cybersecurity from prevention-first control accumulation to a resilience operating discipline that assumes disruption and focuses on limiting impact and recovering fast.

Atos Group calls this **Adaptive Cyber Resilience.**

It reframes cybersecurity as an **adaptive operating discipline** that is focused on maintaining control, recovering fast, and continuously proving resilience under pressure rather than proposing yet another framework, checklist, or product stack. This model brings together four inseparable shifts:

- AI embedded at the core of security operations
- Sovereignty treated as a design principle
- Security measured by business outcomes rather than tool counts
- Human accountability retained even when execution operates at machine speed

Adaptive Cyber Resilience is where speed meets discipline. Through a continuous cycle of **prepare, respond, and adapt,** it turns resilience from a goal into a governed operating discipline. **Prepare** builds readiness before disruption. **Respond** contains impact and enables engineered, demonstrable recovery at speed. **Adapt** ensures security evolves faster than the environment it protects. A governance control layer connects board-level intent with operational execution, closing the fragmentation that too often separates strategy from reality.

This paper outlines what has changed, the questions leaders must confront, and a concrete path to regaining control through disciplined execution. It is written for executives accountable for outcomes, not experimentation.

Atos Group brings more than 25 years of experience operating in mission-critical environments, sovereign infrastructure, and industries where systems must operate under pressure, fail safely, and withstand scrutiny. Through Atos Cyber Services and Eviden Cyber Products, this experience operates as one integrated system at scale, under pressure, and over time.

Cybersecurity is being redefined. Organizations will either shape that future through disciplined resilience or react to it under pressure.

*Allianz Risk Barometer 2026

The shift: Why the old model breaks

Every board recognizes cybersecurity as a strategic risk. Fewer can answer a simple question: **If something goes wrong tomorrow, how quickly do we regain control, and can we prove it?**

That gap between recognition and readiness is not a failure of effort. Controls still matter. Compliance still matters. But static controls and periodic assurance no longer match today's operating reality.

Business now runs through constantly changing dependencies across cloud, IT, OT, partners, APIs, data flows, and AI systems. This extends exposure beyond the boundaries most security models were designed to manage, while creating an opportunity to rethink controls for greater efficiency. The result is compounding risk that is often invisible, rarely owned end-to-end, and increasingly difficult to contain.

The traditional perimeter has faded. Today's effective perimeters are identities, APIs, and increasingly the models and agents that operate across ecosystems. Control is distributed, dependencies run deep, and many organizations no longer fully map the environments they must secure. Here's why:

1. AI changes the equation - permanently

AI does not simply accelerate cybersecurity; it changes the control model. As attacks move faster and weaknesses surface sooner, human-led operations struggle to absorb the pace. At the same time, agentic systems introduce delegated authority into digital operations, making a compromised agent more than a data risk: it becomes a digital insider threat with the power to act.

2. Geopolitical tension has made cybersecurity a sovereignty issue

State-sponsored threat actors, supply chain weaponization, and fragmentation of the global technology landscape have made cybersecurity inseparable from sovereign control. Organizations operating across jurisdictions now face a threat environment shaped not only by criminal actors but by nation-state objectives, economic coercion, and information warfare. Who holds the data, controls the infrastructure, and supplies the technology now shapes the organization's cyber risk in real time.

3. Complexity has outpaced control

More tools do not guarantee control. More alerts do not guarantee better decisions. As AI accelerates attacks and connected OT expands the control gap, security must be judged by its ability to detect, contain, and recover at speed. The issue is no longer technology alone. It is an operating model that is no longer fit for purpose.

4. The boardroom reality

Cybersecurity now defines business continuity, regulatory exposure, and is inseparable from digital sovereignty. Executives face growing accountability for risks they cannot always fully observe or control. Across jurisdictions, regulatory expectations are converging: controls must operate continuously, effectively, and under pressure. With assumed breach as the baseline, security is judged by outcomes. They need to detect fast, contain impact, recover quickly, and demonstrate it.

5. The innovation dilemma

Every digital, cloud, and AI transformation initiative expands the attack surface. Every new application brings a software stack, a supply chain, and a dependency chain. Every new data flow and agentic workflow creates new exposure. Treating security as a late-stage gate guarantees constant catch-up. Security must become embedded, continuous, and adaptive from design through operations.

The old model breaks because it treats cybersecurity as a collection of controls applied to a relatively stable system. Today's enterprise is adaptive, distributed, interdependent, and under pressure from adversaries, regulators, and its own transformation agenda, all at once.

Security can no longer sit at the edge as a specialist function. It must move into the business, with explicit ownership by business leaders and executive accountability for outcomes.

That shift is no longer optional. It is the condition for operating securely in the world as it is.

The new imperative: What must change

Knowing the model must evolve is not enough. The harder question is what must replace it. And the answer is not about refinement, extension, or incremental progress. It is about redefining how cybersecurity operates in practice.

What is required is a fundamental shift in how cybersecurity is conceived, governed, and operated, from a static, control-based discipline to a dynamic, resilience-driven operating model aligned with business outcomes.

The primary change is leadership and governance; technology enables it but does not drive it. For some organizations, this shift is already underway; for others, it sets the direction for how cybersecurity leadership must evolve. Let's take a closer look at what this entails.

1. From more controls to continuous control

The shift is not about doing more of the same, but faster. It is about changing what security is designed to achieve.

Security operations are drowning in signals, but more alerts don't create more control. The priority is to move from alerts to intelligence-led decisions, converting signals into actions prioritized by business impact, enriched by context, and executed at speed.

2. From human-only security to human-AI operations

Modern threats now move with a volume, velocity, and sophistication that human teams cannot absorb alone. Machine-speed security requires AI-augmented detection, triage, and response, not as a replacement for judgment but as a way to extend it. AI must be embedded into a governed operating model where every automated action is explainable, reversible, and accountable. Human ownership remains non-negotiable.

The average eCrime breakout time fell to just 29 minutes in 2025, with the fastest observed breakout occurring in only 27 seconds.

- 2026 CrowdStrike Global Threat Report

3. From generic security to contextual, sovereign, outcome-driven security

One-size-fits-all frameworks cannot address the diversity of risks that modern enterprises face. Risk tolerance and prioritization vary by context, so security must be shaped by each organization's business model, regulatory obligations, sovereignty requirements, and dependency landscape, and then measured by outcomes boards can understand and act on. A regulated bank and a multinational managing sovereign data do not share the same priorities or acceptable levels of risk.

4. Cybersecurity as a core business function

Cybersecurity can no longer be governed as a technical function inside IT. It is a core business discipline shaping revenue protection, partner trust, regulatory license to operate, and technology adoption. That requires board-level governance, business-level measurement, clearer ecosystem accountability, and integration into strategic decisions on transformation, cloud, AI, M&A, human-machine delegation, and sovereignty requirements.

5. From protection to adaptive resilience

Prevention remains necessary but is no longer sufficient on its own. Cybersecurity must operate on the assumption that disruption will occur and be ready to detect what matters, contain impact, sustain critical operations, and recover at speed. This is the shift from protection to adaptive resilience, an operating posture built, tested, measured, and continuously improved under pressure.

The hard questions boards must ask

The shift to adaptive resilience begins with different questions, not technical questions, but leadership ones. These questions define whether cybersecurity is truly under control or merely documented.

They give leadership a common test of readiness: whether cybersecurity is governed as an operating discipline connected to control, continuity, sovereignty, and business outcomes.

Top 10 questions that every board should be asking right now

1. Are all business owners aware and accountable for cyber risk in their processes and products, with clear decision rights, metrics, and escalation paths?
2. Do we control a single, coherent view of identity, access rights, privilege escalation, and AI agent/ machine identities across our hybrid environment?
3. When something goes wrong tomorrow, are we at the right speed to detect, trace, and contain blast radius of an intrusion and rapidly recover if needed?
4. Is our data pipeline and AI agent platforms secured against data theft and AI manipulation?
5. Have we identified and protected the assets and processes that are critical to revenue, operations, and market trust?
6. Is our cyber ecosystem prepared for AI-driven attacks operating at machine speed?
7. Do we have a plan to balance the security and sovereignty risk of the platforms, data, and models we depend on?
8. Is our cybersecurity fit to support our business growth plans including market expansion, client trust, and the adoption of cloud, AI and other emerging technologies?
9. Do we know where our AI systems operate, under whose control, and with what guarantees?
10. What is our future-proof plan for when a Quantum Computer breaks traditional cryptography?

The organizations that ask these questions honestly, and act on the answers with discipline will close that gap. However, the ones that avoid them will discover the answers during an incident that will have lasting impacts on their business.

Our vision: How we respond

Cybersecurity does not need another framework. The demands of cybersecurity today call for a different operating model, built for growing complexity, speed, sovereignty, and accountability.

Atos Group calls this model **Adaptive Cyber Resilience.**

It is the shift:
From fragmented tools to coherent control.
From static defenses to adaptive resilience.
From periodic compliance to continuous demonstrability.
From prevention as an objective to continuity as an outcome.

Adaptive Cyber Resilience brings together four inseparable shifts:

1. AI at the core of security operations
2. Sovereignty translated into operating requirements
3. Security measured by business outcomes
4. Human accountability retained even when execution operates at machine speed

This is not a future vision. It is the operating model cybersecurity now requires.

AI for security. Security for AI

AI is reshaping cybersecurity in two ways at once: it accelerates how security operates, and it creates new AI systems that must be secured and governed.

On the defensive side, AI for security increases the speed, precision, and consistency of cybersecurity decisions, from risk prioritization and control assurances to protection, detection, and response. It must sit at the core of security operations, not as another tool, but as the operating engine. AI transforms security operations by enabling machine-speed detection, continuous monitoring of identities and cloud posture, and rapid response capabilities that activate in seconds rather than hours. These capabilities are powered by large-scale pattern recognition across millions of signals that no human team could process.

Used this way, AI transforms security operations from fragmented activity into continuous, intelligence-led decision-making.

But there is a second, equally critical dimension. As organizations deploy AI and agentic systems into their own business operations, those systems become assets that must be secured. AI models, training data, decision pipelines, and agentic workflows, all represent new attack surfaces that require new forms of governance, monitoring, and runtime control. As AI moves from generating outputs to initiating actions, the primary risks are no longer limited to data exposure or misuse, but extend to loss of control, goal drift, and unintended autonomous behavior.

Control must be enforceable at runtime, not implied at design time. This means bounding autonomy, making AI behavior observable, enforcing policies continuously, and retaining the ability to interrupt execution when behavior diverges from intended goals. Decisions and actions must remain traceable and auditable, with explicit human accountability.

Without this discipline, AI capability scales faster than an organization's ability to control risk. With it, AI becomes a governed, auditable, and trustworthy component of the enterprise even as autonomy increases.

Atos Group embeds AI at the core of cybersecurity, driven by a **dual mandate: accelerating security operations while securing AI systems themselves.**

Eviden's Foundations of Trust for AI

As AI systems move from experimentation to core business operations, trust in AI must be engineered, not assumed. **Eviden Cybersecurity Products provide the foundational cyber capabilities required to make AI trustworthy at scale.**

1. **Data protection** extends encryption beyond traditional IT to the AI pipeline, data in use, and retrieval augmented generation, ensuring confidentiality from data ingestion to inference.
2. **AI identity governance** manages rights, permissions, lifecycle, auditability, and continuous monitoring so access and actions remain controlled, explainable, and accountable.
3. **Digital identities for AI agents** uniquely identify and cryptographically bind autonomous agents through certificates or identity wallets, enabling authentication, trust, and traceability across ecosystems.

Together, these foundations help customers use AI confidently while retaining control, accountability, and trust as autonomy, scale, and regulation increase.

Sovereignty as an operational discipline

Sovereignty has become a strategic issue, yet it remains one of the least operationalized concepts in enterprise cybersecurity today.

For most organizations, sovereignty is treated as a compliance checkbox for data residency requirements, contractual clauses about jurisdiction, vendor questionnaires, the choice of a certified cloud provider, et al.

Necessary but insufficient.

In a world where AI models, cloud infrastructure, and agentic systems cross borders by design, sovereignty must become an operational discipline, consistently executed across the entire IT stack, not a legal afterthought.

This means making deliberate, informed decisions across the application, infrastructure, and supply chain, defining where data and execution reside, which models are trusted, and how autonomy is bounded. It means understanding that sovereignty is not binary. It is a spectrum of control that must be calibrated to the sensitivity of the asset, the regulatory context, and the business impact of a loss of control. Sovereignty defines who controls the data, models, and decisions. Security ensures that control is efficient, resilient, and enforceable. **Without sovereignty, security lacks accountability. Without security, sovereignty is merely an intention without assurance.**

Atos Group approaches sovereignty as a key design principle embedded from the start, where security is integral to architecture rather than imposed afterwards. This includes operating across public, hybrid, private, and sovereign infrastructure configurations. It includes ensuring governance, traceability, and control are maintained regardless of where workloads run and what the geopolitical context currently is. And it includes helping clients answer the questions that matter most: where do we need sovereign control, to what degree, and what are the operational implications of these intentional decisions?

From controls to measurable impact

The cybersecurity industry has spent decades measuring itself by inputs, tools deployed, controls implemented, audits passed, and certifications obtained. Boards are no longer satisfied with this. They are asking a different question.

What is the actual impact of our security investment on the outcomes that matter?

Those outcomes are specific and measurable: Mean time to detect (MTTD), mean time to contain (MTTC), mean time to recover (MTTR), business downtime avoided, data leakage circumvented, regulatory penalties prevented, customer trust preserved, and operational continuity maintained.

Outcome-driven security connects cybersecurity activity directly to business performance, in real time, not only in quarterly reports. It requires continuous measurement, transparent reporting, and the discipline to adjust posture based on what the data shows.

Atos Group designs its cybersecurity engagements around measurable business outcomes that are defined in business terms, tracked continuously, and aligned with what the board and the executive team are accountable for delivering.

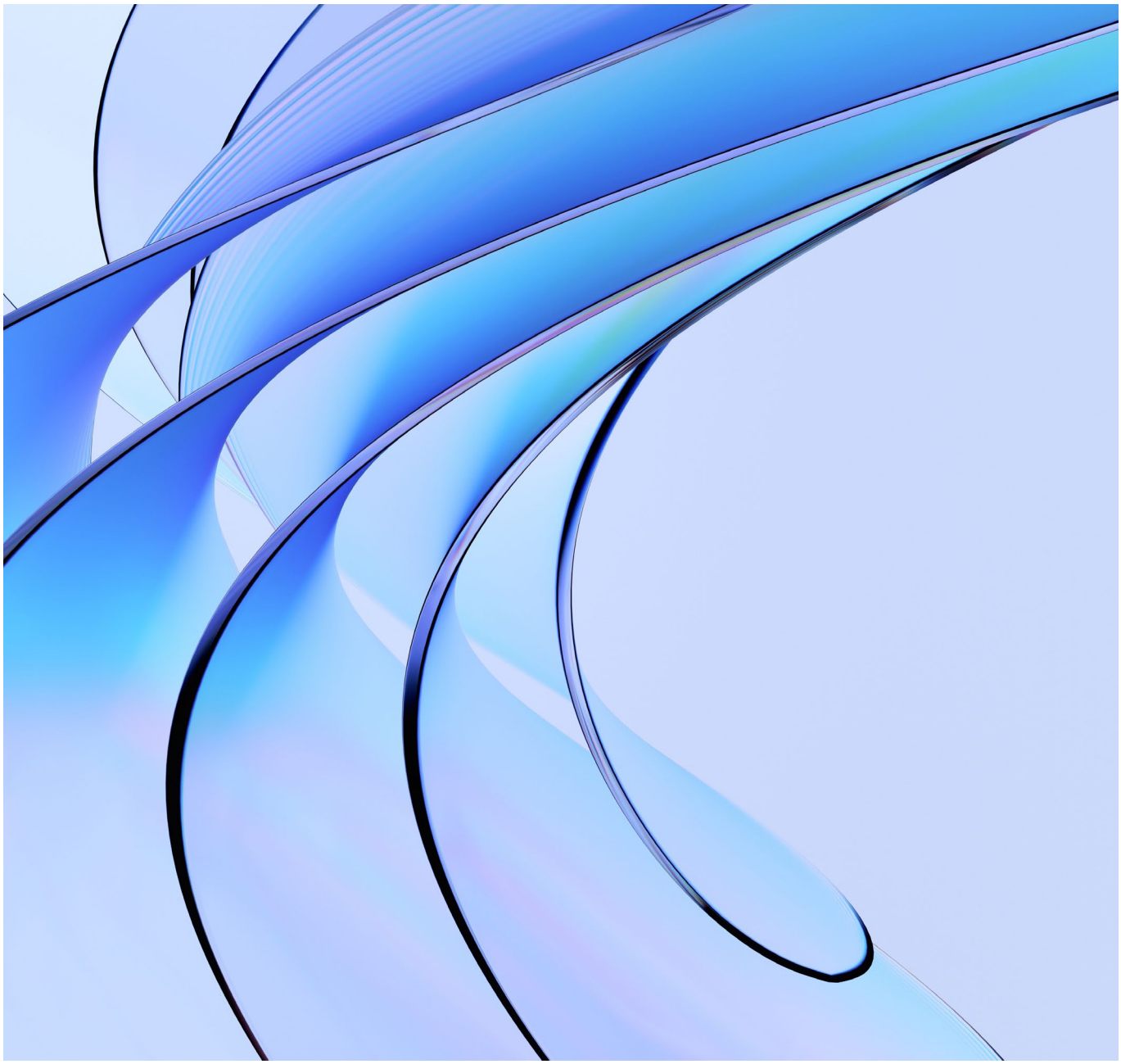
People, accountability, and the next generation of cyber leadership

No operating model, however advanced, removes the need for human judgment, accountability, and leadership. But the profile of that leadership is changing.

Cybersecurity professionals must become AI-fluent, operationally minded, and able to make risk decisions at speed. They must understand how AI reasons, where it fails, when to override it, and how to translate machine-generated intelligence into board-level decisions.

This shift goes beyond an incremental upgrade in skills and reflects a generational change, where the cybersecurity workforce is defined less by the volume of alerts it processes and more by how effectively it leads AI-augmented operations while retaining human authority.

Atos Group is actively building this next generation through AI-first training programs, security leadership development, and human-AI operating models that govern security at machine speed without losing human accountability.

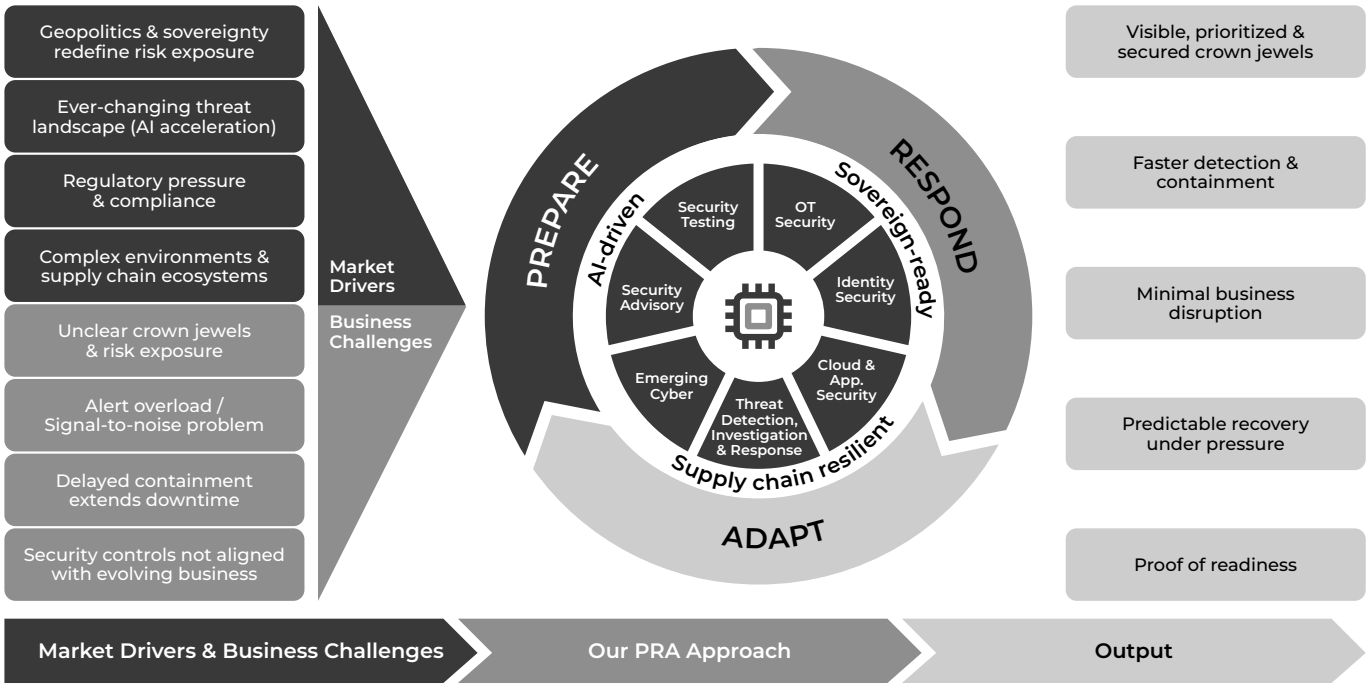


From a vision to reality: How enterprises operationalize cyber resilience

Turning Adaptive Cyber Resilience into reality requires more than intent. It requires an operating model that can function continuously, under pressure, and across a fragmented ecosystem.

This is where intent becomes discipline.

A continuous model of AI-powered Cyber Resilience



Prepare. Respond. Adapt.

Cyber resilience cannot be built as a linear program or a one-time transformation. It must operate as a continuous cycle. The Prepare-Respond-Adapt (PRA) approach enables organizations to step in at any point, strengthen security where it matters most, and continuously improve resilience over time.

PRA is not a framework, checklist, or maturity ladder. It is an adaptive operating model that turns established cybersecurity standards and frameworks into sustained execution under machine-speed threats, AI-driven systems, systemic dependencies, and continuous regulatory pressure.

Prepare is about reducing risk and elevating trust before disruption occurs. It focuses on continuously understanding exposure, identifying business-critical assets, and designing security and sovereignty into architectures, platforms, and processes by default. This includes exposure management, compliance by design, secure foundations with recovery as a core capability, and human-centric defenses.

Prepare does not assume perfection. It assumes continuous change, validation, and readiness under pressure.

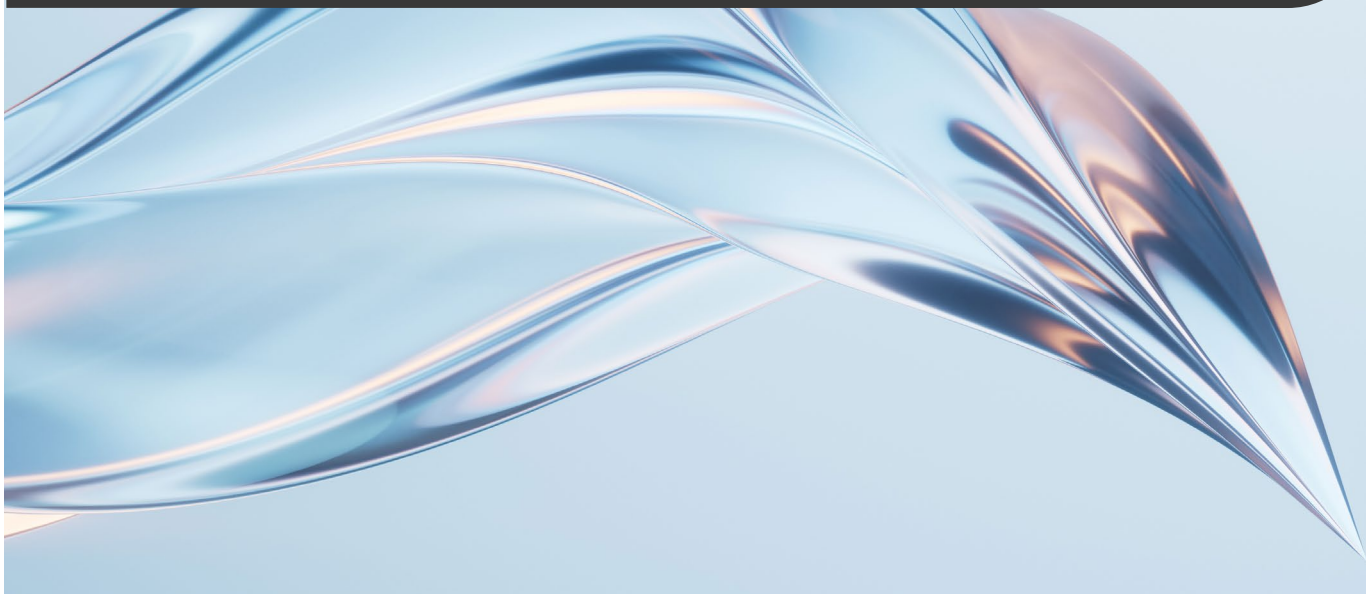
The goal is to reduce the probability and impact of disruption while creating a posture that can absorb shock without collapse. Preparation answers a fundamental question: if something happens tomorrow, are we ready today?

Threat Detection and Incident Response (TDIR)

TDIR is Atos's end to end cyber protection capability, supporting organizations across the full PRA incident lifecycle.

According to Verizon DBIR report around 20% of cyberattacks originate from the exploitation of known vulnerabilities, while time to exploit has shrunk from months to days or even hours, making continuous visibility essential.

Through Continuous Threat Exposure Management, TDIR identifies exposed assets and realistic attack paths, enabling proactive risk reduction before exploitation occurs. When incidents happen, speed is decisive. TDIR combines AI assisted Managed Detection and Response with a Virtual SOC Analyst to accelerate investigations and containment. Internal Atos benchmarks show up to 60% faster investigations for AI ready alerts and up to 90% reduction for phishing related cases, delivering measurable improvements in MTTD and MTTR. Complemented by crisis simulations and tabletop exercises, TDIR strengthens organizational resilience in an increasingly complex threat environment.



Respond is about detecting, containing, mitigating, and recovering when disruption occurs.

It combines AI augmented detection, rapid containment, coordinated crisis management, and engineered, rehearsed, and demonstrable recovery capabilities. Response must operate at machine speed while preserving human decision authority. Recovery should be engineered into the response phase with tested paths and controlled restoration, even while the incident unfolds. Every action must be traceable, auditable, and reversible.

Resilience is ultimately proven under pressure. Response is successful when business impact is limited, services are restored quickly, and control can be demonstrated, not just declared.

Adapt is the continuous adjustment of cybersecurity to changes in the environment, whether driven by new regulations, emerging threats, technology shifts, or business transformation. Adapt ensures security does not drift out of alignment as the enterprise evolves.

This includes adjusting controls to new regulatory requirements, integrating learnings from threat intelligence and simulations, refining detection and response based on emerging attacker behavior, and anticipating future risks such as post quantum cryptography or agentic AI exposure.

Adapt turns experience, change, and foresight into improved readiness. The objective is simple: ensure the same incident never happens in the same way, and that security remains effective even as the landscape shifts.

Prepare-Respond-Adapt is the operational backbone of cyber resilience. Prepare builds the foundation. Respond protects continuity under stress. Adapt keeps security relevant over time.

This continuous improvement loop allows Atos to support clients at any stage of their resilience journey, meeting them where they are today and enabling them to build toward where they need to be.

Post Quantum Cryptography (PQC): A resilience imperative

Post Quantum Cryptography (PQC) migration is no longer a future consideration. It is an immediate necessity, driven by tangible advances in quantum computing and increasingly explicit guidance from national authorities worldwide.

Digital trust relies on core elements like identity, secure communications, software integrity, and data protection, all built on cryptography that won't stay reliable forever. Data harvested now can be decrypted later by cryptographically relevant quantum computers, expected by around 2035.

PQC migration will take years, and must start now, beyond the CISO function alone. Once cryptography fails, trust cannot be restored at speed, and business continuity, regulatory exposure, and market confidence are simultaneously impacted.

Migrating to new algorithms is not sufficient.

Crypto agility must be implemented across the entire cryptographic stack to enable easy evolution over time. In this journey, **Eviden Cybersecurity Products provides PQC ready European cryptographic foundations**, enabling end to end use cases for digital certificates, data protection, and secure communications.

What makes PRA executable

Governance as the cyber control layer

Most organizations have capabilities; what's missing is coherence across them. A governance control layer translates board-level risk appetite into enforceable priorities, accountability, and investment decisions. It aligns security architecture with business strategy and ensures the PRA cycle, technology stack, partner ecosystem, and leadership team operate as one system, not as disconnected initiatives.

Security aligned to business transformation

Cyber resilience cannot be retrofitted. Security must be designed into digital, cloud, and AI initiatives from the start, shaping architecture choices, data flows, sourcing models, partner ecosystems, and human-AI responsibilities before systems go live or operating models scale. When resilience is embedded early, security accelerates transformation. When added late, it becomes a constraint, and risk accumulates silently.

Ecosystem orchestration makes resilience scalable

No single organization can deliver cyber resilience alone. Modern security depends on hyperscalers, specialist technologies, enterprise platforms, partners, and internal capabilities. What matters is the ability to orchestrate the ecosystem coherently through a single governance and operating model. Atos Group combines ecosystem choice with architectural independence, ensuring controls, sovereignty requirements, compliance obligations, and outcome metrics apply consistently across providers.

The CISO's agenda for the next 24 months

Delivering cybersecurity outcomes requires aligning strategy with execution. Over the next 24 months, the most effective CISOs will focus on a defined set of priorities to strengthen resilience and ensure measurable impact.

The organizations that act on these priorities with discipline will be materially more resilient in 24 months. Those who defer them will spend those 24 months reacting to the consequences of inaction.

Atos Group: Credibility that scales under pressure

Adaptive cyber resilience cannot be delivered through vision alone. It requires experience, scale, and the ability to operate in environments where failure is not an option.

As the European leader in cybersecurity, Atos Group brings together long-standing expertise, industrial-grade operations, and trusted security foundations to make resilience executable in the real world, combining Atos cybersecurity services for execution, Eviden cybersecurity products as trust anchors and Atos Amplify for advisory and transformation.

A plethora of experience that shapes execution

Atos Group has more than 25 years of experience delivering cybersecurity for large enterprises, public sector organizations, and mission critical environments. Over that time, the Group has evolved alongside every major structural shift in cybersecurity — from perimeter centric models to cloud and hybrid architectures, from IT only environments to IT and OT convergence, from human speed security operations to AI augmented, intelligence driven defense.

These evolutions were addressed early, driven by operational necessity rather than trends. This depth of experience matters when cybersecurity must function continuously, under regulatory scrutiny, and during crisis situations.

Cyber services built to operate continuously

Atos Cyber Services are designed for continuous operation across industries and geographies. They combine advisory and governance, security architecture, threat intelligence, security operations, incident response, crisis management, and recovery capabilities. These services operate through a global network with strong local execution, enabling proximity to clients, regulators, and critical infrastructure realities.

This model allows Atos to support organizations throughout the full Prepare-Respond-Adapt cycle, not as isolated activities, but as a coordinated operating discipline aligned with business impact, regulatory expectations, and leadership decision making.

Eviden Cybersecurity products as trust anchors and deep expertise on crypto and data protection

Through Eviden, Atos delivers cyber products that provide durable, security by design foundations made in Europe.

These products address core trust mechanisms such as identity, cryptography, access control, and data protection. They are designed for environments where demonstrability, assurance, and longevity are essential criteria.

Eviden Cybersecurity products support the highest levels of certification and clearance required in sensitive and regulated sectors. They provide stable security anchors that enable services to function reliably over long system lifecycles and evolving threat landscapes.

A pragmatic approach to Digital Sovereignty

Sovereignty is treated by Atos as an operational capability embedded in how systems are designed and managed.

Through Eviden cybersecurity products and Atos cyber services, sovereignty is embedded into intentional choices and architectures that control where data resides and is accessed, how identities are managed, and how critical processes are protected. This is combined with a global footprint and strong local delivery capabilities that reflect regulatory, sector specific, and operational realities.

This approach enables organizations to retain control, autonomy, and resilience in their entire IT and OT stacks, even as regulations, dependencies, or geopolitical conditions change.

Embedding AI in cyber operations

AI has been part of Atos cybersecurity operations for many years, adapted to address scale, speed, and complexity rather than as a recent acceleration trend.

Across Atos's Cyber Services, AI supports signal correlation, risk prioritization, and faster detection and response, while keeping human accountability explicit. Through Eviden, security for AI is treated as a dedicated discipline, covering governance, runtime observability, and demonstrable control.

This allows organizations to use AI as a force multiplier for resilience without compromising trust, compliance, or sovereignty.

One Mission. Two Engines.

Atos Group has one mission: to make **Adaptive Cyber Resilience** executable in the real world. That mission is powered by two engines working as one system: **Atos's Cyber Services** and **Eviden's Cybersecurity Products,** designed to work together under a single resilience operating model that integrates AI capabilities, enforces sovereignty by design, reduces fragmentation, and supports continuous adaptation.

This is how adaptive cyber resilience moves from concept to operating reality.

At speed. At scale. Under pressure. Over time.

Let's talk!

As the threat landscape accelerates through AI and digital environments grow more complex and interconnected, adaptive cyber resilience has become essential to business continuity.

Wherever you are on the journey, we invite you to connect with us to:

Prepare - Gain clarity across assets and dependencies to prioritize exposure and deliberately build security where it matters most for your business continuity.

Respond - Detect, contain, and recover fast to minimize business disruption and maintain continuity under pressure.

Adapt - Continuously reassess priorities and evolve posture as threats, technologies, regulations, and business conditions change.

Connect with us at atoscybersecurity@atos.ai

About Atos Group

Atos Group is a global leader in digital transformation with c. 56,000 employees and annual revenue of c. €7.2 billion (at the go-forward perimeter), operating in 54 countries under two brands - Atos for services and Eviden for products and systems. European number one in cybersecurity and a leader in cloud, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE listed on Euronext Paris.

107696-SY+ST-F Whitepaper-LetsTalk-AtosGroup-Cys-WEB