Mission-Ready Cyber Resilience

Keep critical services operational—anticipate, withstand, adapt, recover.

Why Cyber Resilience Matters?

Cyber incidents are no longer rare, isolated IT events. They are a fundamental business risk that can interrupt operations, erode trust, and trigger regulatory scrutiny. Leading organizations recognize that **prevention alone is not enough**—resilience is what determines whether the business survives and thrives under pressure.

Cyber resilience is the ability to **anticipate, withstand, adapt to, and recover from cyber incidents while maintaining critical business services.** It moves organizations beyond fragmented security controls toward measurable operational continuity and executive confidence.

Our Value Proposition

We help organizations move beyond tool-centric security and tick-the-box compliance to measurable, outcome-driven cyber resilience—focused on outcomes that matter when systems are under attack.

Our approach integrates prevention, detection, response, and recovery into a single, coherent operating model designed to:

- Sustain critical business services during cyber incidents, not just protect systems
- Reduce impact and recovery time through disciplined response and tested recovery capabilities
- Provide board-level assurance through clear, business-relevant resilience metrics

We position cyber resilience as a strategic capability, not a technical expense—directly aligned with operational continuity, regulatory expectations, and enterprise risk management.

A Board-Level Imperative

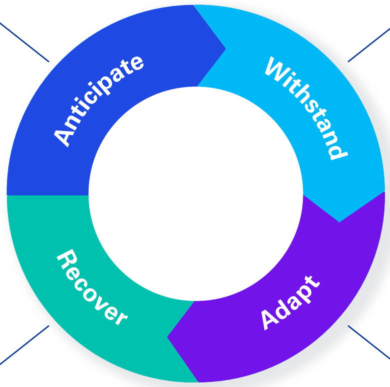
Cyber resilience is no longer a technical or operational concern—it is a regulated board responsibility. Across Europe and globally, regulators are explicitly linking cyber resilience to governance, accountability, and personal liability for boards and senior management.

Frameworks and regulations such as NIS2, DORA (Digital Operational Resilience Act), sector-specific supervisory expectations, and widely adopted standards (e.g. ISO 22301, ISO/IEC 27001, NIST, and operational resilience frameworks) require organizations to demonstrate not only strong preventive controls, but the ability to continue critical services during cyber incidents and recover within defined tolerances.

As a result, cyber resilience has become inseparable from business continuity, operational resilience, and enterprise risk management. Boards and executives need credible assurance that the organization can withstand cyber disruption, make disciplined decisions under pressure, and restore critical operations rapidly—while demonstrating compliance, control, and accountability to regulators and stakeholders.

Our Cyber Resilience Model

Our approach is built on a proven, end-to-end cyber resilience model that aligns technology, governance, and people around what matters most to the business. At its core are Business Impact Assessment (BIA) and Digital Crown Jewels (DCJ) analysis, ensuring that resilience investments protect the services and assets that truly matter.



Anticipate

Understand the threat landscape, assess cyber risk, and prepare the organization through informed governance and awareness.

Withstand

Design resilient architectures and controls that limit disruption and keep critical services running, even when defenses are challenged.

Recover

Restore operations rapidly using tested response and recovery plans, validated through realistic simulations and exercises.

Adapt

Respond dynamically to evolving threats through coordinated decision-making, technical flexibility, and operational readiness.

Our Cyber Resilience Services

We deliver end-to-end cyber resilience services that help organizations prepare for, withstand, respond to, and recover from cyber disruption. Our services span strategy, governance, architecture, and execution, and are tailored to each organization's risk profile, regulatory obligations, and critical business services.

Cyber Resilience Maturity Assessment & Roadmap

A structured assessment of cyber resilience capabilities across governance, technology, people, and operations. We identify gaps against leading practices and regulatory expectations, define critical business services, and develop a prioritized, multi year resilience roadmap with clear ownership, milestones, and KPIs. Targeted analysis of cyber resilience requirements under NIS2, DORA, and applicable sector-specific supervisory expectations as well as international standards such as ISO/IEC 27001, ISO 22301, and NIST, translating regulatory requirements into practical, implementable actions.

Policy, Governance & Framework Implementation

Design and implementation of cyber resilience-related strategies, policies, standards, and operating frameworks. This includes cyber resilience strategies, incident response and crisis management governance, escalation and decision-making models, and integration with enterprise risk management and operational resilience programs.

Board-Level & Executive Education

Targeted education and working sessions for boards and senior executives to strengthen oversight of cyber resilience. Topics include regulatory obligations, decision making during cyber crises, roles and responsibilities, and interpretation of resilience metrics to support informed governance and accountability.

Business Continuity, Cyber Recovery & Disaster Recovery Design

Design and enhancement of Business Continuity Plans (BCPs), Cyber Response & Recovery Plans (RRPs), and Disaster Recovery Plans (DRPs). Plans are cyber-aware, scenario-driven, and aligned to critical business services, recovery time objectives (RTOs), recovery point objectives (RPOs), and regulatory tolerances.

Resilient Architecture Review & Improvement

Assessment and improvement of IT / OT and security architectures to support resilience by design. This includes identity and access management, network segmentation, Zero Trust design, backup and recovery architecture, logging and detection engineering, and reduction of single points of failure to limit blast radius during incidents.

Threat Intelligence & Threat Hunting

Proactive, threat led services that provide insight into relevant threat actors, tactics, techniques, and procedures. This includes contextual cyber threat intelligence (CTI), mapping threats to business impact, and hypothesis driven threat hunting to identify advanced or stealthy threats before they result in material business impact.

Security Testing & Adversary Simulation

Validation of detection and response capabilities through vulnerability assessments (VA), penetration testing, and red teaming / purple teaming. Testing is threat led and focused on realistic attack paths, critical assets, and business impact rather than isolated technical findings.

Tabletop Exercises & Cyber Wargames

Design and facilitation of executive level and operational tabletop exercises and cyber wargames to test decision making, escalation, coordination, and communications under realistic attack scenarios. Exercises build organizational muscle memory and validate plans, roles, and recovery assumptions.

Cyber Incident Response & Digital Forensics

Incident response preparedness and on demand support during cyber incidents, including containment, investigation, and recovery coordination. Services include crisis coordination and decision support, digital forensics, root cause analysis, regulatory and legal support, and post incident reviews to capture lessons learned and strengthen future resilience.

Why Leading Organizations Choose Us

We combine global cyber resilience expertise with deep local insight, delivering practical, business-aligned solutions. Our focus is not on perfect prevention, but on the discipline of sustaining operations when prevention fails—helping organizations remain resilient, compliant, and trusted in an increasingly hostile digital environment.

Cyber Ready. Business Steady.

Because resilience is not just about surviving cyber incidents—it's about sustaining confidence, continuity, and growth when it matters most.

Contact us:

Constantinos Gavardinas
Partner, CIO Advisory &
Cyber Resilience
KPMG in Greece
E: kgkavardinas@kpmg.gr

Spyridon Papageorgiou
Partner,
Cybersecurity
KPMG in Greece
E: spyridonpapageorgiou@kpmg.gr

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

e-mail: info@kpmg.gr
kpmg.com/gr

kpmg.com/socialmedia

General Electronic Commercial Registry 003467701000

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.