ZERODUO

From Compliance to Resilience.

Designing trust. Delivering Confidence.

Notable breaches impacting organisations across the Globe

Selected incidents that impacted manufacturing, regulators, wholesalers, or patient-support services.

2017 — Equifax
Major consumer PII breach; widely attributed to unpatched Apache Struts (CVE-2017-5638) and control breakdowns.

2020 — SolarWinds (Orion)
Trusted updates weaponized; ~18,000 customers potentially exposed, with targeted follow-on intrusions.

2021 — Colonial Pipeline
Single incident triggered fuel supply disruption; highlights cascading impact from IT compromise into real-world operations.

2023 — MOVEit Transfer (Progress)
CL0P exploited CVE-2023-34362 against internet-facing MFT; webshells planted; data stolen across hundreds of orgs.

2024 — OpenAI / ChatGPT
Redis client bug caused some users to see others' chat titles; limited payment-related data exposed for some Plus users.

2024 — Change Healthcare (UnitedHealth)
Attack rooted in missing MFA on remote access; major healthcare payment/claims disruption and sensitive data exposure risk.

ZERODUO

Most incidents start the same way

The difference is how quickly impact spreads.

Attack Types

Ransomware + double extortion:

Encrypt + steal + leak: operational disruption + reputational pressure (Colonial, Change Healthcare).

Supply chain compromise:

Attackers poison trusted software/update channels to scale access (SolarWinds-style).

Mass exploitation of internet-facing systems:

Zero-days and misconfigurations in exposed apps/MFT/APIs → webshells → bulk data theft (MOVEit-style).

AI-era data leakage:

Bugs, misconfigurations, or unsafe AI usage can leak data cross-user or outside the org (service bugs, prompt/data leakage).

Most common root-causes

- **Patch/asset blind spots:** known vulns stay open too long.
- **Weak IAM:** missing MFA, over-privilege, stale accounts.
- **Third-party risk gaps:** vendors, SaaS, and build pipelines.
- **Exposed services:** internet-facing apps/MFT/APIs without hardening.
- **Insufficient monitoring:** attackers dwell too long before detection.
- **Weak data governance + AI guardrails:** no classification, retention, DLP, or safe AI rules.

These incidents show a consistent pattern: attackers exploit trust, weak identity controls, exposed internet services, and software/AI failures, then monetize with extortion, fraud, or regulatory pain.

ZERODUO

Why this matters for Greece-based pharma?

Data + trust are the prize

PII, credentials, operational access, and models — monetized fast, at scale.

Business-wide blast radius

When cyber hits: revenue stops, regulators show up, customers lose trust, and execs own the fallout.

Regulatory + AI governance pressure

Privacy regimes + sector rules + emerging AI standards raise the bar: evidence, accountability, resilience.

ZERODUO

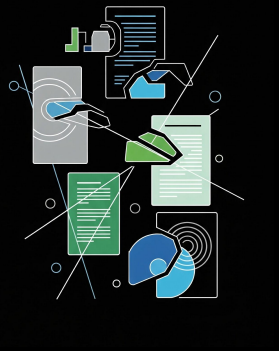
Risks are multiplying, Regulations are accelerating, Frameworks are out of control

The next decade belongs to organizations that can answer with confidence.

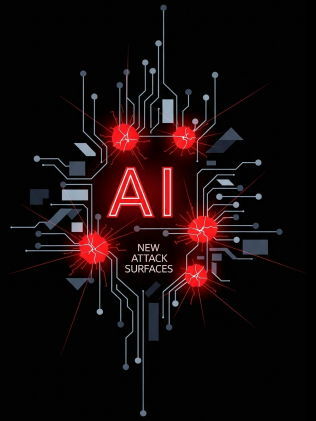
ZERODUO

Compliance keeps you safe, Resilience keeps you ahead

Most organizations treat compliance as a one-time checklist. But the real challenge lies in maintaining readiness across changing laws, technologies, and teams.



Fragmented compliance efforts.



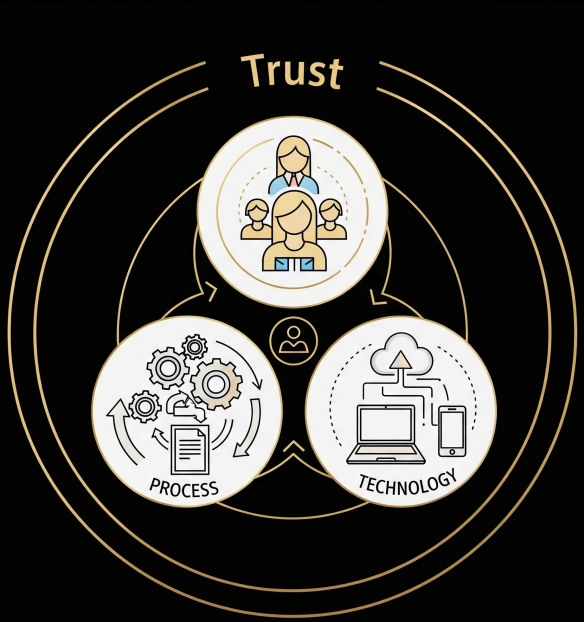
AI systems introducing new attack surfaces.

Cyber threats eroding trust faster than regulations can adapt.

ZERODUO

We help organizations move from Compliance to Resilience

ZeroDuo is an AI & Cyber Resilience advisory firm helping leaders embed trust, governance, and security across their people, processes, and technology.



Outcome-focused, business-centric, holistic & collaborative approach

ZERODUO

Beyond frameworks and audits, resilience by design

Our advisory model aligns the three pillars of organizational strength:

People Enablement

Building awareness, culture, and confidence.

- Role-based experiential learning
- Scenario-based decision simulations labs

Process Enablement

Creating adaptive governance and controls.

- Regulatory readiness for GDPR, DPDP, NIS2, ISO, SOC2, DORA
- Industry-specific blueprints (FinTech, SaaS, MedTech, Industrial)
- Benchmarking engine for “resilience maturity”
- Adaptive compliance controls that evolve with laws

Technology Enablement

Embedding secure, compliant design in systems.

- AI Governance & Risk assessments
- Secure Product & DevSecOps assessments
- Cloud & OT Security assessments

Enablement programs are designed to turn compliance intent into resilient capability.

ZERODUO

The Exposure-To-Resilience Model

True resilience is achieved at the intersection of your **Domains** and your **Maturity**

The new era belongs to organizations that treat resilience as a competitive strategy.

ZERODUO

We are Your Strategic Partner for AI & Cyber Resilience

Our strength lies in the intersection of strategy and execution.

Holistic Enablement

We address the full spectrum: People × Process × Technology × Ecosystem. True resilience requires orchestration across all dimensions.

Cross-Regulation Intelligence

Navigate complex regulatory landscapes with confidence. Our expertise spans GDPR, DPDPA, NIS2, DORA, AI Act, and emerging frameworks worldwide.

Future-Ready Frameworks

Leadership-backed methodologies designed not just for today's compliance, but for tomorrow's competitive advantage and sustained resilience.

Strategic Advisory DNA

Combining deep technical expertise with strategic business acumen, we deliver solutions that align with your organizational objectives and drive measurable outcomes.

We don’t advise from the sidelines, we help teams operationalize resilience.

ZERODUO

Transforming compliance into strategic advantage.

ZeroDuo Case Study 1 | Healthcare | AI & Cyber Resilience Enablement

A regional healthcare network deploying AI for diagnostics & patient management. Struggled with fragmented data privacy (local + GDPR), unsegmented cloud/OT links, and board unpreparedness for cyber incidents.

People Enablement

- Board-level simulations
- vCISO-led risk workshops
- Leadership crisis playbooks

Process Enablement

- AI Governance framework
- GDPR + local compliance mapping
- Defined cyber risk appetite

Technology Enablement

- Multi-cloud IAM hardening
- Segmented OT systems
- DevSecOps-secured AI pipelines

Business Impact Created

- Full regulatory audit clearance in 120 days.
- 70% reduction in AI/data incidents.
- Board approved new cyber risk appetite.
- Secured 5 government contracts citing compliance maturity.

ZERODUO

Transforming compliance into strategic advantage.

ZeroDuo Case Study 2 | Fintech | AI & Cyber Resilience Enablement

Fintech scaling AI in credit scoring & fraud detection. Facing fragmented compliance (GDPR, EU AI Act, DORA), cloud sprawl, and zero board visibility.

People Enablement

- Board-level simulations, embedded vCISO
- Audit defence enablement
- Leadership crisis playbooks, risk qualification workshops

Process Enablement

- AI Governance framework (risk reg, asset map etc.)
- Unified GDPR / AI Act / DORA compliance strategy
- Defined cyber risk appetite & review cadence
- Adaptive governance controls and maturity benchmarking

Technology Enablement

- Zero Trust & IAM hardening
- Secured SDLC & CI/CD pipelines
- GenAI guardrails and DevSecOps enablement

Business Impact Created

- Audit-ready in 90 days.
- 60% fewer AI incidents.
- €25M funding unlocked.
- 8 new enterprise clients citing trust & compliance maturity.

ZERODUO

Let’s design your resilience journey

Start with a ZeroDuo AI Resilience Snapshot, a 4-week diagnostic that identifies blind spots, benchmarks your readiness, and builds your roadmap to trust.

Delzad Mirza
The Bearded CISO

Vaibhav Tikekar
The Strategist

Get in touch

Our strength lies in the intersection of strategy and execution.

We don’t advise from the sidelines, we help teams operationalize resilience.

ZERODUO

ZERODUO

From Compliance to Resilience.

Designing trust. Delivering Confidence.