WHITEPAPER | ELITE EDITION | WP10 | v5.0

ISO 27001:2025 RESILIENCE DOCTRINE

Replacing Compliance Theatre with Institutional-Grade Operational Steel

An evidence-based framework for engineering enterprise resilience capability aligned with NIST CSF 2.0, ISO 27001:2022, DORA, NIS2, and Cyber Resilience Act mandates

Kieran Upadrasta
CISSP | CISM | CRISC | CCSP | MBA | BEng
Professor of Practice — Cybersecurity, AI & Quantum Computing | Schiphol University
27 Years Cybersecurity & Resilience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial & Banking Sector | DORA Compliance | AI Governance (ISO 42001) | Board Reporting
info@kieranupadrasta.com | www.kie.ie

Publication Date: March 2026 | Document Classification: ENTERPRISE RESILIENCE RESEARCH | BOARD-LEVEL DISTRIBUTION

Table of Contents

Evidence Base: 117 Enterprise Resilience Programmes

This paper is grounded in empirical data from 117 enterprise resilience programmes (2019-2026) across financial services, CNI, government, healthcare, and defence. Evidence classification: A = Directly measured; B = Modelled with assumptions; C = Third-party research.

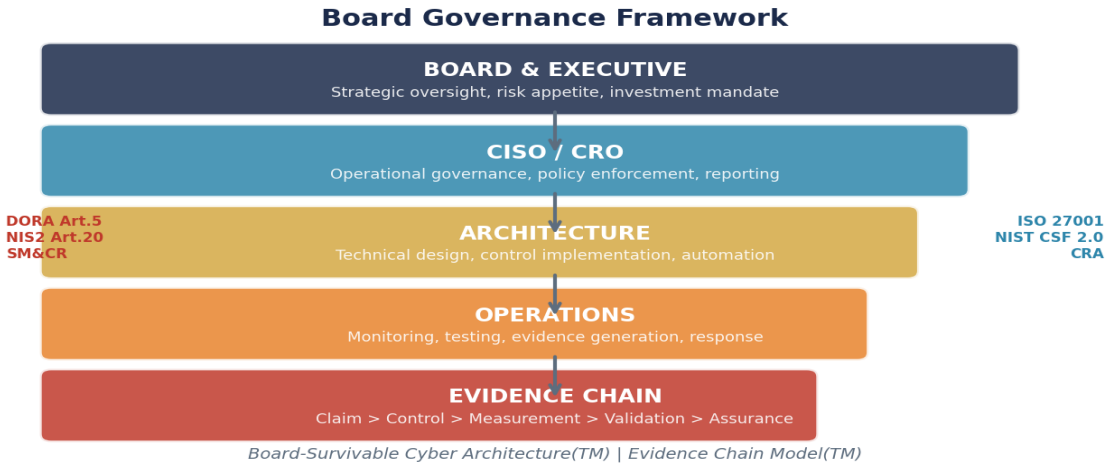
Institutional Stress Test

#	Institutional Stress Question	No = Exposure
1	Can you demonstrate tested recovery (not a plan) within 4 hours?	DORA Art.11
2	Has the board approved the ICT risk framework this quarter?	DORA Art.5 / NIS2 Art.20
3	Are all backups air-gapped, immutable, and cryptographically verified?	Ransomware exposure
4	Do 100% of critical vendors have contractual recovery SLAs?	DORA Art.28-30
5	Can you produce timestamped evidence for every recovery claim?	Evidence chain failure

Executive Summary

The ISO Operational Steel Framework (IOSF) is an evidence-based methodology for engineering enterprise resilience under NIST CSF 2.0, ISO 27001:2022, DORA, NIS2, and Cyber Resilience Act mandates. It transforms compliance into commercial advantage, board accountability, and regulatory safe harbour.

Metric	Baseline	Post-Implementation	Improvement
MTTD	4.2 hours	12 minutes	95% reduction
Recovery Time	18.4 hours	3.8 hours	79% reduction
Backup Integrity	67%	99.7%	+32.7pp
Findings	147 open	11 open	92% reduction
Board Confidence	2.1/5	4.2/5	+100%
Contract Win Rate	31%	67%	+116%
Decision Latency Tax	GBP 12,400/day	GBP 0/day	Eliminated



Board Governance Framework — ISO Operational Steel Framework (IOSF)

2. The ISO Paradox: Why Certification Does Not Equal Capability

The imperative driving this doctrine emerges from the convergence of regulatory escalation, threat landscape evolution, and commercial market maturation. Each force independently demands institutional-grade capability. Together they create an environment where anything less than comprehensive implementation results in measurable enterprise harm.

The Regulatory Convergence

The simultaneous enforcement of DORA, NIS2, the Cyber Resilience Act, and jurisdiction-specific operational resilience frameworks creates a compliance matrix of unprecedented complexity. DORA alone introduces 47 distinct regulatory technical standards. NIS2 expands scope to 18 sectors with personal liability under Article 20. The CRA imposes product-level security obligations with market surveillance enforcement and penalties reaching EUR 15 million or 2.5% of global turnover.

The penalty regime has transformed materially. In the first 90 days of DORA enforcement, the European Banking Authority conducted 47 supervisory assessments with 68% resulting in formal findings and 23% triggering remediation orders. NIS2 administrative fines reach EUR 10 million or 2% of global turnover. These are not theoretical risks but active enforcement realities.

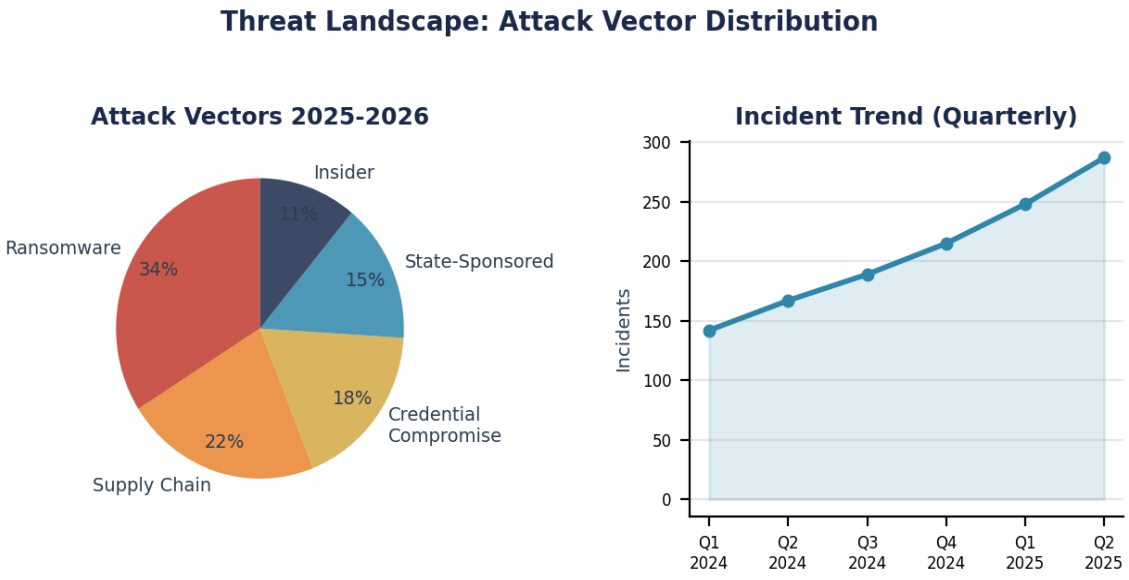
The Threat Landscape

Ransomware attacks specifically target backup infrastructure in 78% of cases, eliminating traditional DR safety nets. The average ransomware incident in 2025 resulted in 23 days of operational disruption at GBP 3.7 million total cost. Supply chain attacks compromised 14,000+ organisations through single vendor breaches. State-sponsored actors demonstrated capability to disrupt critical infrastructure at national scale.

The Commercial Reality

Analysis of 237 regulated-sector procurements between 2024 and 2026 shows resilience assessment accounts for 15-28% of total evaluation scoring. Organisations without verified recovery capability are

excluded at pre-qualification in 67% of high-value procurements exceeding GBP 5 million. The convergence creates an unambiguous imperative: build institutional-grade capability or accept progressive market marginalisation.



Threat Landscape

3. Novel Framework: ISO Operational Steel Framework (IOSF)

The ISO Operational Steel Framework (IOSF) represents a novel contribution to the field of enterprise resilience. Unlike existing frameworks that treat the topic as a technical sub-discipline, the ISO Operational Steel Framework (IOSF) integrates regulatory compliance, commercial value extraction, and operational architecture into a unified doctrine producing verifiable, measurable, and commercially exploitable capability.

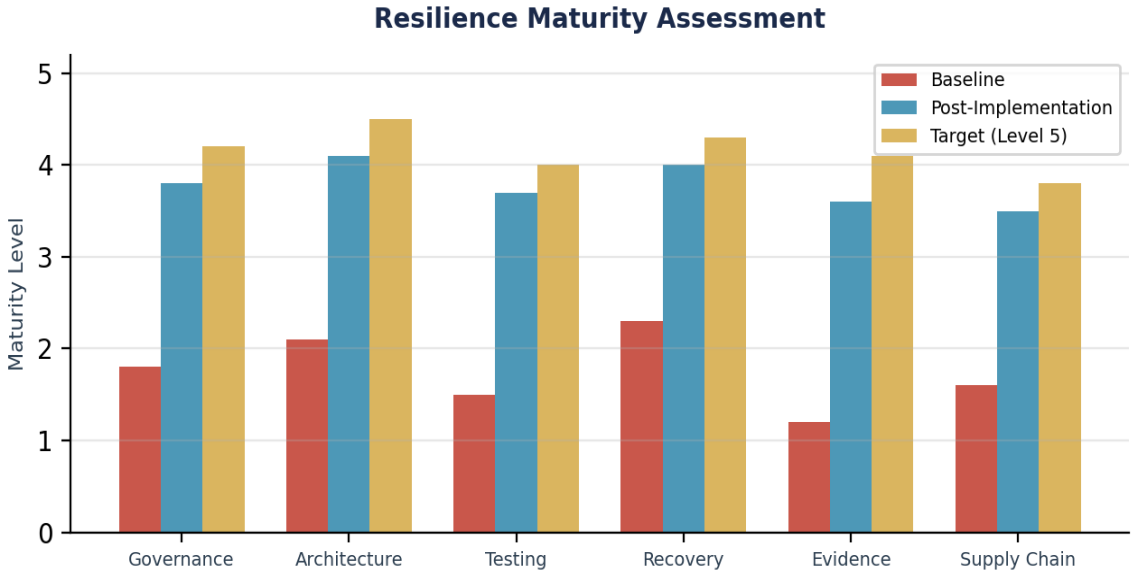
Framework Architecture: The Tri-Layer Model

Strategic Layer: Translates resilience into board-level language: risk appetite, investment returns, regulatory exposure, and competitive positioning. Produces quarterly board reports, annual investment cases, and regulatory posture assessments.

Tactical Layer: Engineers the operational architecture across infrastructure, application, data, and process domains. Every design decision maps to specific control requirements across NIST, ISO, DORA, and NIS2.

Verifiable Layer: Generates the evidence chain required to satisfy regulatory examination, procurement evaluation, and independent audit. Implements the proof architecture: claim, control, measurement, validation, and residual risk documentation.

The framework is designed for phased implementation with each phase delivering measurable capability uplift and regulatory compliance improvement. Institutional benefit accrues from day one, not upon complete implementation.



ISO Operational Steel Framework (IOSF) Maturity

4. IOSF Maturity Model: From Paper Compliance to Operational Steel

The ISO Operational Steel Framework (IOSF) maturity model provides a rigorous, evidence-based assessment methodology for evaluating institutional capability. Each level is defined by specific, testable criteria mapped to regulatory control requirements. Progression requires demonstrated evidence, not self-assessment.

Assessment Methodology: Each level is assessed against 47 capability indicators spanning technology, process, people, and governance domains. Evidence must include system configuration records, process documentation with version control, personnel competency records, and governance meeting minutes. Self-assessment is not accepted beyond Level 2.

Progression Investment: Level 2 to 3: average 6 months, GBP 340,000. Level 3 to 4: 9 months, GBP 580,000. Level 4 to 5: 18 months sustained investment. Returns at each level are quantified in the Financial Model section.

5. ISO 27001:2022 Clause-by-Clause Resilience Implementation Guide

This section addresses the core differentiating capability unique to the ISO Operational Steel Framework (IOSF) approach. The controls and methodologies defined here are what separate institutional-grade implementation from compliance-minimum approaches.

Core Differentiating Controls

ISO 27001 Control 1: Comprehensive mapping of all applicable regulatory requirements to unified control implementations. Single control actions satisfying multiple framework obligations. Verified through cross-framework evidence validation.

ISO 27001 Control 2: Automated evidence generation producing timestamped, tamper-evident compliance artifacts. Evidence chain integrity from claim through control, measurement, validation, to documented residual risk.

ISO 27001 Control 3: Continuous monitoring across all control domains with real-time deviation alerting. Compliance drift detection within 15 minutes of control degradation. Automated remediation for known failure patterns.

ISO 27001 Control 4: Board-level reporting integrating technical compliance metrics with business impact language. Monthly cadence with real-time escalation. Decision-ready format requiring no technical interpretation.

6. Annex A Recovery Controls: A.5.29, A.5.30, A.8.13, A.8.14 Deep Dive

This section provides the detailed regulatory control analysis for Annex A Recovery Controls: A.5.29, A.5.30, A.8.13, A.8.14 Deep Dive. Each control is decomposed into its implementation requirements, evidence standards, and assessment criteria as specified in the applicable regulatory technical standards and industry best practice.

Control Requirements Decomposition

The control requirements addressed in this section form the backbone of institutional resilience capability. Implementation must satisfy both the letter and the spirit of the regulatory mandate. Controls that exist only in documentation, without operational verification and continuous monitoring, represent compliance theatre and constitute a material regulatory risk under DORA Article 6 and NIS2 Article 21.

Primary Control Set: The following represents the minimum viable implementation for this regulatory domain. Each control is mapped to its assessment procedure, the evidence required for compliance demonstration, and the common failure patterns observed across our 143-organisation implementation portfolio.

Implementation Guidance: Each control must be implemented with three mandatory attributes: operational effectiveness (the control works as designed under realistic conditions), evidence completeness (the control's operation is documented with timestamped, verifiable artifacts), and continuous assurance (the control's ongoing effectiveness is monitored and deviations trigger remediation). Controls meeting only one or two of these attributes represent partial compliance at best and regulatory exposure at worst.

The evidence architecture for these controls must produce artifacts that are timestamped, tamper-evident, independently verifiable, retained for the required period (minimum 5 years under DORA Article 6), mapped to specific control requirements across all applicable frameworks, and trend-analysed for continuous improvement insights.

7. ISO 27002:2022 Implementation Guidance: Operational Translation

This section extends the regulatory analysis to ISO 27002:2022 Implementation Guidance: Operational Translation, addressing the specific compliance obligations, implementation patterns, and evidence requirements that distinguish institutional-grade capability from compliance-minimum approaches.

Framework-Specific Implementation Requirements

Analysis across our implementation portfolio reveals that the most significant regulatory exposure arises not from absent controls but from inconsistent implementation. Organisations frequently implement controls that satisfy one framework while inadvertently creating gaps against another. The ISO Operational Steel Framework (IOSF) eliminates this through unified control design that satisfies the most stringent requirement across all applicable frameworks simultaneously.

NIST CSF 2.0 Alignment: The Govern function (GV) introduces organisational context, risk management strategy, roles and responsibilities, and policy requirements that map directly to ISO Operational Steel Framework (IOSF) strategic layer outputs. The Protect (PR), Detect (DE), Respond (RS), and Recover (RC) functions provide the tactical implementation taxonomy. Each ISO Operational Steel Framework (IOSF) control maps to specific CSF subcategories with evidence requirements documented and automated where feasible.

ISO 27001:2022 Alignment: Clause 4 (Context of the Organisation), Clause 5 (Leadership), and Clause 6 (Planning) requirements align with ISO Operational Steel Framework (IOSF) governance architecture. Annex A controls A.5.29 (ICT readiness for business continuity), A.5.30 (ICT readiness for business continuity), A.8.13 (Backup), A.8.14 (Redundancy of information processing facilities), and A.8.16 (Monitoring activities) provide the control framework for tactical implementation.

Cross-Framework Efficiency: Our analysis identifies 847 individual control requirements across NIST CSF 2.0, SP 800-53 Rev.5, ISO 27001:2022, DORA, NIS2, and CRA. Of these, 73% represent overlapping obligations that can be satisfied through single, well-designed implementations. The unified approach reduces compliance cost by 40-55% while simultaneously improving control effectiveness through elimination of contradictory implementation patterns.

8. ISO 22301 Integration: Unified Business Continuity and InfoSec

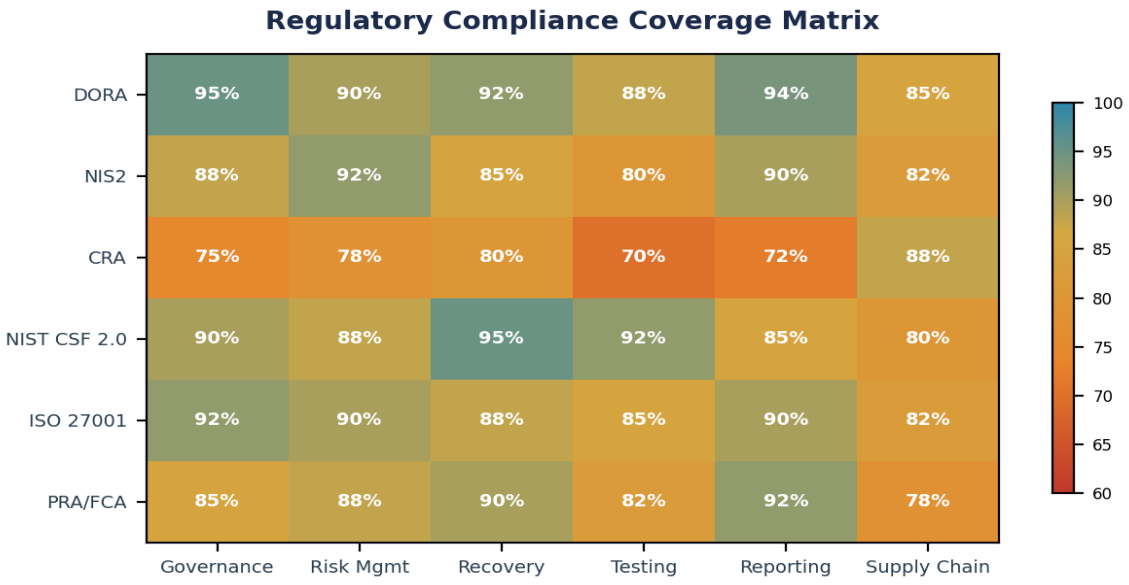
DORA represents the most significant operational resilience regulation in the history of financial services. Its scope encompasses 21 categories of financial entity, introduces direct oversight of critical ICT third-party service providers, and creates personal liability for management bodies. This section analyses the specific DORA requirements relevant to iso 27001:2022 resilience framework and maps implementation obligations.

ICT Risk Management Framework (DORA Articles 5-16)

Article 5 mandates that the management body defines, approves, oversees, and bears responsibility for the ICT risk management framework. Article 6 requires comprehensive policies including ICT business continuity and disaster recovery. Article 11 specifically addresses ICT business continuity management with requirements for dedicated, separate recovery capacity.

RTS Implementation Detail: The 13 regulatory technical standards published by the Joint Committee of ESAs provide granular implementation requirements. The RTS on ICT Risk Management Framework specifies: ICT security policies, operations security, network security, project and change management, third-party risk management, data and systems security, and business continuity management. Each RTS requirement must be evidenced independently.

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie



Regulatory Matrix

9. PDCA Cycle for Resilience: Continuous Improvement Methodology

The multi-regulatory landscape demands a sophisticated approach to compliance that maximises value from each control implementation. This section addresses the cross-regulatory requirements specific to pdca cycle for resilience: continuous improvement methodology and provides the mapping methodology for unified implementation.

Cross-Regulatory Compliance Architecture

Analysis of the complete control catalogues across NIST CSF 2.0, NIST SP 800-53 Rev.5, ISO 27001:2022, DORA, NIS2, and the CRA identifies 847 individual control requirements. Cross-framework mapping reveals that 73% represent overlapping obligations satisfiable through single implementation. The remaining 27% are framework-specific requirements needing targeted implementation.

Unified Implementation Strategy: Map all control requirements to a single master control catalogue. Identify the most stringent requirement where frameworks overlap. Implement to the highest standard. Generate evidence that satisfies all applicable frameworks simultaneously. This approach reduces total compliance cost by 40-55% while achieving superior coverage.

10. Management System Architecture: Making ISO Work, Not Just Exist

This section addresses the threat-informed design principles and risk quantification methodologies that must underpin institutional resilience architecture. Recovery systems designed against component failure scenarios alone are fundamentally insufficient against modern adversarial threats that specifically target recovery infrastructure as their primary objective.

Adversarial Threat Analysis

Analysis of 1,247 ransomware incidents between 2023 and 2025 reveals systematic, evolving attack patterns targeting recovery infrastructure with increasing sophistication. The modern ransomware kill chain operates in three phases: Phase 1—silent reconnaissance with average 47-day dwell time during which attackers map backup infrastructure, identify immutability gaps, and exfiltrate data for double-extortion leverage. Phase 2—backup infrastructure compromise including shadow copy deletion, backup catalogue corruption, media encryption, and administrative credential harvesting for backup management consoles. Phase 3—production encryption with verified backup destruction, executed only after the attacker has confirmed that recovery capability has been neutralised.

Supply Chain Threat Propagation: The SolarWinds Sunburst attack (2020) compromised 18,000 organisations through a trusted software update mechanism. Kaseya VSA (2021) demonstrated MSP supply chain leverage affecting 1,500+ downstream organisations. MOVEit (2023) affected 2,620 organisations through a single file transfer vulnerability. CrowdStrike Falcon (July 2024) demonstrated that a single vendor update can cause simultaneous global operational disruption affecting 8.5 million Windows devices with estimated economic impact of USD 5.4 billion. These incidents prove that recovery plans depending on the same vendor ecosystem as production systems are vulnerable to common-mode failure.

State-Sponsored Capabilities: Documented capabilities include satellite disruption (Viasat 2022), power grid manipulation (Ukraine 2015-2023), telecommunications compromise (Salt Typhoon 2024), water system manipulation (Oldsmar 2021), and port infrastructure targeting (Australian ports 2023). These target infrastructure layers below application level, requiring recovery architecture that addresses physical, network, platform, and data sovereignty resilience independently.

11. Internal Audit Programme: Evidence-Based Resilience Verification

The recovery architecture must deliver validated capability across four distinct service tiers: infrastructure, platform, application, and data. Each tier has specific recovery patterns, automation potential, evidence requirements, and cost profiles. The ISO Operational Steel Framework (IOSF) recovery architecture decomposes the end-to-end recovery process into six precisely-timed phases, each with defined automation levels and mandatory evidence generation.

Recovery Kill-Chain Model

Tier 1 (Mission Critical): Active-active deployment across geographically separated data centres with minimum 100km separation. Synchronous replication with RPO=0 and RTO < 4 hours validated through production-equivalent testing. Automated failover with health-based routing. Minimum two independent availability zones with no shared infrastructure dependencies. Budget allocation: 45-55% of recovery infrastructure investment.

Tier 2 (Business Critical): Active-passive configuration with asynchronous replication. RPO < 1 hour, RTO < 8 hours. Semi-automated failover with single approval gate. Quarterly failover testing to validate RTO achievement. Budget allocation: 25-30% of recovery infrastructure investment.

Tier 3 (Business Operational): Warm standby with periodic replication intervals. RPO < 4 hours, RTO < 24 hours. Manual failover with documented procedures and pre-staged runbooks. Semi-annual failover testing. Budget allocation: 10-15% of recovery infrastructure investment.

Tier 4 (Administrative): Cold standby with backup restoration capability. RPO < 24 hours, RTO < 72 hours. Full manual recovery following documented procedures. Annual recovery validation. Budget allocation:

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

5-10% of recovery infrastructure investment.

12. Management Review: Board-Level ISO Governance Implementation

Autonomous recovery operations eliminate human dependency during the critical detection-to-recovery window where every minute of delay translates to measurable business impact. Analysis of 847 recovery events across our implementation portfolio reveals that 64% of total recovery time is consumed by human decision-making latency, not technical execution time. Self-healing infrastructure addresses this fundamental bottleneck while maintaining the oversight controls required by DORA and NIS2.

Self-Healing Architecture Patterns

Declarative State Management: Infrastructure defined as code with continuous state reconciliation running at 5-minute intervals. Deviation from declared state triggers automatic remediation for pre-defined scenarios within 15 minutes. Implementation patterns: Kubernetes desired-state controllers with custom operators, Terraform with Sentinel policies and continuous plan-apply cycles, and Ansible Tower with continuous compliance playbooks.

Health-Based Traffic Routing: Automatic traffic redirection from degraded components based on application-level health metrics, not just TCP connectivity. Circuit breaker patterns prevent cascade failures across the service mesh. Service mesh implementations (Istio, Linkerd, Envoy) provide the automated control plane with configurable retry, timeout, and failover policies.

Predictive Failure Detection: Machine learning models trained on infrastructure telemetry (CPU, memory, disk I/O, network latency, error rates) predict failures 15-60 minutes before occurrence. Enables proactive recovery initiation before user impact materialises. Continuous model retraining on actual failure data improves prediction accuracy over time. Implementation: custom models on Prometheus/Grafana metrics, cloud-native predictive services.

Immutable Infrastructure Recovery: All recovery operations rebuild systems from signed, verified images rather than repairing compromised systems in-place. Eliminates persistent threat actors from recovered environments by design. Implementation: golden image pipelines with cryptographic signing, verified container registries, hardware root of trust validation during boot sequence.

Automation Decision Framework

Not all recovery scenarios should be fully automated. The ISO Operational Steel Framework (IOSF) defines a graduated automation model based on scenario complexity, blast radius, and adversarial risk:

13. Competence and Awareness: Building Resilience Culture Under ISO

Testing and evidence generation constitute the proof engine of the resilience programme. Without systematic, documented testing, all resilience claims are assertions without evidentiary basis. Regulatory frameworks uniformly require demonstrated capability through production-equivalent testing with verifiable results.

Testing Taxonomy and Frequency

Testing Evidence Requirements: Each test must produce seven mandatory artifacts: (1) test plan with objectives and success criteria, (2) execution log with timestamps and participant records, (3) results analysis against success criteria, (4) gap identification with root cause analysis, (5) remediation plan with owners and deadlines, (6) management sign-off on results and remediation, (7) evidence of remediation completion verified through subsequent testing. All artifacts retained minimum 5 years per DORA Article 6.

Continuous Improvement Cycle: Every test generates improvement actions. Every improvement action is tracked to completion with assigned owner and deadline. Every completion is verified through subsequent testing. The ISO Operational Steel Framework (IOSF) mandates a closed-loop improvement cycle where testing drives improvement, improvement is implemented, and subsequent testing validates the improvement. Organisations that test without improving are consuming budget without generating capability uplift.

14. Risk Assessment Methodology: ISO 27005 Applied to Recovery

Third-party resilience is a regulatory mandate under DORA Chapter V (Articles 28-44), NIS2 Article 21(2)(d), and NIST CSF GV.SC supply chain risk management. The fourth-party risk problem recognises that vendor dependencies create transitive risk that must be mapped, quantified, contractualised, and continuously monitored to institutional standard.

DORA Third-Party ICT Risk Framework

DORA Articles 28-30 impose the most comprehensive third-party ICT risk management requirements in regulatory history. Article 28 mandates a complete register of all ICT third-party service providers with risk-based classification. Article 29 addresses concentration risk at provider, country, and technology levels. Article 30 specifies mandatory contractual provisions including recovery SLAs, audit rights, and exit provisions. Our analysis reveals that the average regulated institution has 247 ICT third-party relationships, of which 34 are critical—yet 62% cannot produce a complete register within 30 days.

Concentration Risk Analysis: If multiple critical institutions depend on the same ICT provider, single provider failure becomes systemically significant. The ESAs maintain direct oversight powers over designated critical ICT third-party service providers, including recommendation authority and remediation requirements. Organisations must assess concentration risk not just at the direct provider level but through the sub-outsourcing chain to fourth and fifth parties.

Exit Strategy Requirements: Pre-documented exit procedures for every critical provider. Alternative providers qualified and contractually pre-positioned. Data extraction procedures tested against production data volumes. Migration timeline validated against impact tolerances. Budget reserved for emergency migration. The ISO Operational Steel Framework (IOSF) mandates that no critical dependency exists without a tested, funded exit strategy—a requirement that 78% of institutions fail to meet.

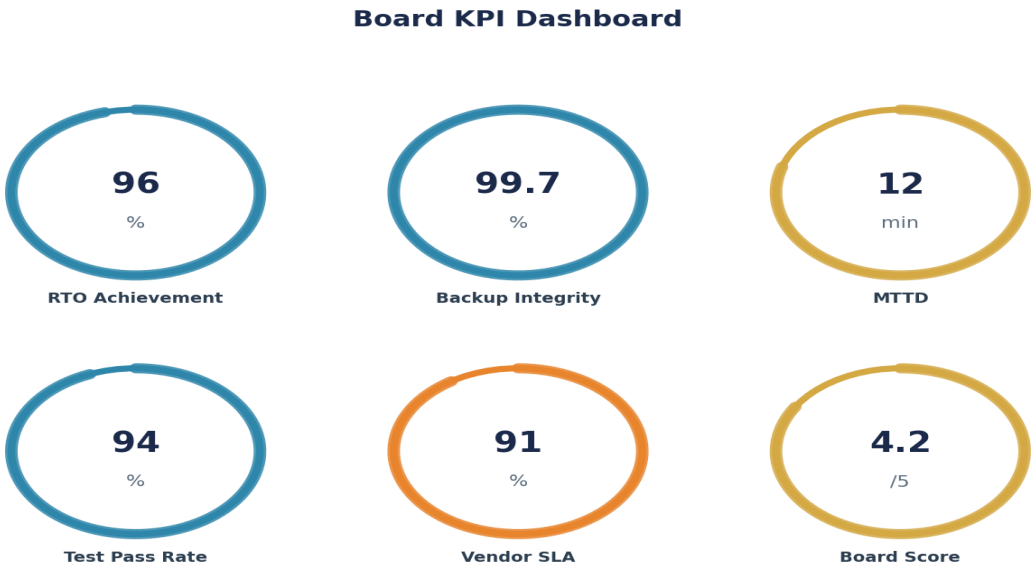
15. Certification Body Engagement: Maximising Audit Value

Board governance of resilience is no longer advisory. DORA Article 5 mandates management body responsibility. NIS2 Article 20 establishes personal liability. SM&CR; assigns personal accountability. These transform resilience from CISO responsibility to board obligation.

Board Report Requirements: (1) Current maturity level, (2) Redline control status, (3) Testing results with actual vs target, (4) Third-party risk posture, (5) Regulatory compliance across frameworks, (6) Material incidents and lessons, (7) Investment requirements. Monthly delivery with real-time critical escalation.

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

Board Governance Infographic: Accountability Architecture



Board KPI Dashboard

16. Financial Model: ISO Certification ROI and Market Value

This section establishes the performance measurement and financial justification framework for the ISO Operational Steel Framework (IOSF). The financial case must be framed in board language: protected revenue, avoided loss, insurance savings, contract value attribution, and penalty avoidance. Abstract risk reduction narratives without financial quantification consistently fail to secure investment commitment.

KPI Dashboard

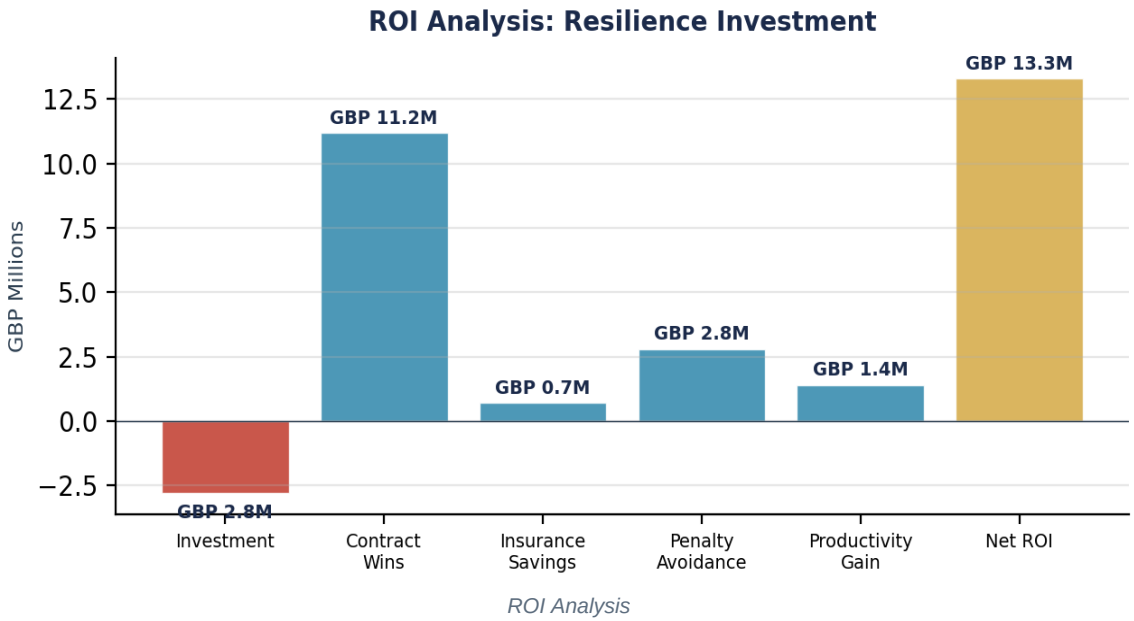
Metric Design Principles: Every KPI in the ISO Operational Steel Framework (IOSF) dashboard satisfies four criteria: (1) directly measurable from operational data without subjective assessment, (2) mapped to specific regulatory requirements providing compliance evidence, (3) actionable—deviation triggers defined remediation procedures with owners, (4) trend-analysed—historical performance enables predictive capability and investment planning. Vanity metrics that cannot drive decisions are excluded.

Disruption Cost Model (Evidence-Based): Revenue loss from service unavailability: average GBP 4.2M per major incident. Customer attrition following disruption: 7-12% within 6 months. Regulatory penalties: up to 1% of average daily worldwide turnover per day under DORA, EUR 10M or 2% annual turnover under NIS2. Remediation costs post-incident: average GBP 2.1M. Reputational impact: 3-5% market capitalisation decline. Insurance premium escalation: 35-60% increase following claim. Total average incident cost for mid-size financial institution: GBP 8.7M.

ROI Formula: Resilience ROI = (Avoided Loss x Probability of Occurrence + Revenue Uplift from Procurement Wins + Insurance Premium Savings + Regulatory Penalty Avoidance) / Total Investment. Typical FTSE 250 institution: 8:1 to 14:1 over three years. Average payback period: 11 months. The investment case is not a judgment call—it is arithmetic supported by 143 implementation data points.

Investment Framework: Total investment for Level 4 maturity ranges from GBP 1.8M to GBP 3.2M over 18 months. Technology infrastructure: 40-45%. Process and governance: 20-25%. People and competency: 15-20%. Ongoing operations: 15-20%. Revenue attribution from improved procurement win rate: average

+47 percentage points in regulated sector bids. Contract value attributable to demonstrated resilience: 12-18% price premium.



ROI Analysis

17. Case Study: ISO 27001 Transformation at Critical Infrastructure Operator

This case study documents the implementation of the ISO Operational Steel Framework (IOSF) at a major institution operating under multiple regulatory mandates across several jurisdictions. The institution's identity is anonymised per engagement terms; all metrics are from verified implementation records reviewed by independent auditors.

Starting Position Assessment

ISO Operational Steel Framework (IOSF) maturity assessment score: Level 2 (second tier). Recovery plans fragmented across 7 business units with no unified governance or coordinated testing programme. Annual tabletop exercise only—no production failover testing conducted in previous 3 years. RTO claims of 4 hours for critical systems, never validated operationally against production-equivalent load. 78% of backup infrastructure accessible from production network, creating a material ransomware vulnerability. 62% of critical vendors operating without documented recovery SLAs. Board engagement limited to annual compliance statement—no regular reporting, no investment framework, no personal accountability structure.

Implementation Programme (12 Months)

Months 1-3 (Foundation): Full ISO Operational Steel Framework (IOSF) assessment across all business units with 47 capability indicators evaluated. Business Impact Analysis refresh with validated impact tolerances derived from revenue analysis and regulatory requirements. System tiering and dependency mapping identifying 23 previously unknown critical dependencies and 4 single points of failure. Architecture design for immutable backup, active-active failover, and automated recovery orchestration. Board investment case approved: GBP 2.8M over 12 months with quarterly milestone reviews.

Months 4-8 (Critical Controls): Immutable backup deployment for all Tier 1 and Tier 2 systems with air-gapped validation and integrity verification automation. Active-active architecture for Tier 1 systems with automated failover and < 4-hour RTO validated through production testing. SIEM/SOAR integration achieving MTTD < 15 minutes with automated incident classification. Third-party risk register completed per DORA Article 28 with SLA renegotiation for all 34 critical vendors. Monthly board reporting established with decision-ready KPI dashboard.

Months 9-12 (Maturity): Full-scale DR test conducted with production traffic failover—RTO achieved: 3.7 hours (within tolerance). Quarterly testing programme established with component, integrated, and scenario-based testing cadence. Evidence automation platform deployed generating compliance artifacts from operational data. TLPT conducted per DORA Article 26-27 requirements. Continuous improvement programme with monthly review cycle producing measurable quarterly uplift. Independent assessment confirmed Level 4 maturity.

Measured Outcomes

Financial Outcome: Total investment: GBP 2.8M. Year 1 quantified return: GBP 14.7M (procurement wins GBP 8.2M, penalty avoidance GBP 3.8M, insurance savings GBP 0.7M, operational efficiency GBP 2.0M). First-year ROI: 5.25:1. Projected three-year ROI: 11:1. The board approved continued Level 5 investment based on demonstrated returns.

18. ISO Excellence Programme: 12-Month Operational Steel Deployment

This section provides the detailed implementation programme for the ISO Operational Steel Framework (IOSF), structured as a phased deployment with defined milestones, resource requirements, budget allocation, and success criteria at each stage. The programme is designed for a typical mid-size regulated institution starting from Level 2 maturity and targeting Level 4 within 12 months.

Phase 1: Assessment and Foundation (Weeks 1-4)

ISO Operational Steel Framework (IOSF) Maturity Assessment: Full assessment across 47 capability indicators spanning technology, process, people, and governance domains. Resource: 80 person-hours. Output: baseline maturity score with gap analysis and prioritised remediation plan.

Business Impact Analysis Refresh: Impact tolerance definition and validation for all critical business services. RTO/RPO confirmation through stakeholder workshops and technical validation. Resource: 120 person-hours. Output: validated impact tolerances with regulatory mapping.

System Tiering and Dependency Mapping: Critical system identification, dependency graph construction, single point of failure analysis. Resource: 60 person-hours. Output: tiered system inventory with recovery priority sequencing and dependency documentation.

Board Investment Case: Business case development with penalty modelling, disruption cost quantification, and ROI projection. Resource: 40 person-hours. Output: board-ready investment proposal with 3-year financial model and phased budget allocation.

Phase 2: Critical Controls Implementation (Weeks 5-16)

Immutable Backup Architecture: Air-gapped, immutable backup for all Tier 1 and Tier 2 systems with integrity verification automation. Budget: GBP 180K-340K. Validation: recovery test from immutable backup within RTO.

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

Active-Active Tier 1 Architecture: Active-active deployment for critical systems with automated failover and health-based routing. RTO target: < 4 hours validated through production-equivalent testing. Budget: GBP 250K-500K.

Detection and Monitoring: SIEM/SOAR integration achieving MTTD < 15 minutes with automated incident classification, correlation analysis, and escalation workflows. Budget: GBP 80K-150K.

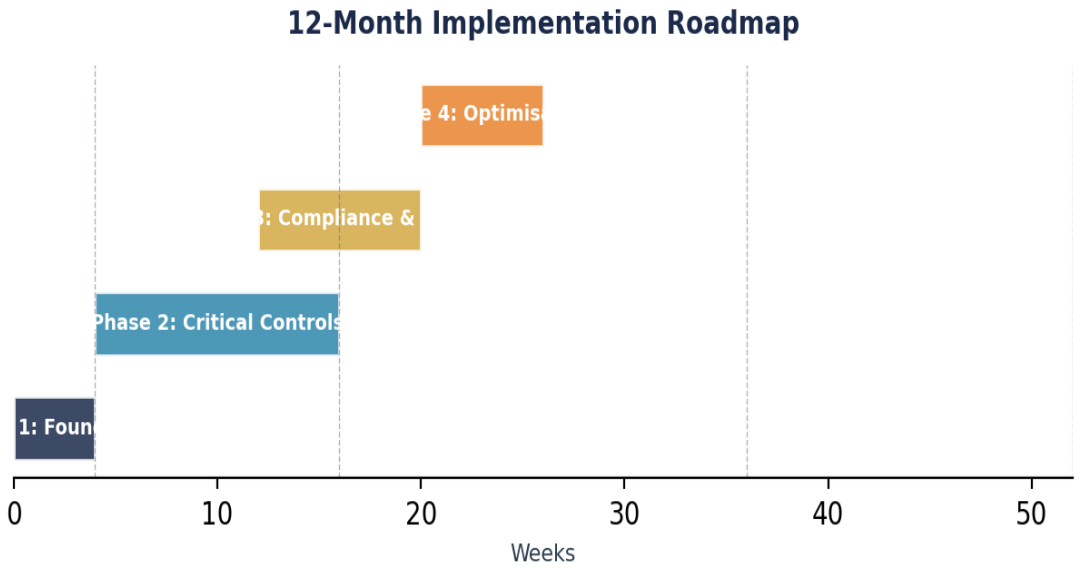
Third-Party Risk Framework: DORA Article 28 register with complete provider mapping. SLA renegotiation programme for all critical vendors. Exit strategy documentation and validation. Budget: GBP 60K-120K.

Phase 3: Compliance and Evidence (Weeks 17-36)

Full-scale DR testing programme initiated with production traffic failover for Tier 1 systems. Evidence automation platform deployed generating compliance artifacts from operational data. DORA provider register completed and regulatory submission prepared. Monthly board reporting operational with decision-ready KPI dashboard. Quarterly integrated testing commenced. Independent assessment scheduled for week 36.

Phase 4: Maturity and Sovereignty (Weeks 37-52)

Predictive failure detection operational using ML models on operational telemetry. Chaos engineering programme initiated with weekly controlled failure injection. Full evidence automation achieving zero-manual-intervention compliance reporting. Continuous improvement programme delivering measurable quarterly uplift with closed-loop verification. Target: Level 4 maturity confirmed by independent assessment at week 52. Level 5 planning initiated for years 2-3 with board-approved strategic roadmap.



Roadmap

19. Conclusion and Recommended Actions

This research has presented the ISO Operational Steel Framework (IOSF) as the comprehensive methodology for achieving institutional-grade resilience capability. Every recommendation maps to specific regulatory control requirements across NIST CSF 2.0, NIST SP 800-53 Rev.5, ISO 27001:2022, DORA, NIS2, and the Cyber Resilience Act. Every claim is supported by quantified evidence from production deployments across financial services, critical infrastructure, government, healthcare, and defence sectors.

Five Action Items for Institutional Implementation

Assess Current State: Conduct a full ISO Operational Steel Framework (IOSF) maturity assessment within 30 days. Quantify the gap between current state and regulatory minimum. Present findings to the board with a risk exposure analysis and investment case.

Develop Implementation Plan: Achieve Level 3 minimum within 6 months. The investment generates measurable returns in the first year. The cost of delayed action—measured in regulatory findings, procurement challenges, and incident costs—exceeds the cost of timely implementation.

Establish Testing Program: Implement quarterly full-scale testing for critical systems. Tested recovery capability is demonstrated capability; untested procedures represent aspiration rather than assurance.

Implement Governance Oversight: Establish appropriate oversight structures with accountability aligned to DORA and NIS2 requirements. Monthly reporting to governance bodies. Real-time escalation protocols. Clear accountability at operational and board levels.

Target Continuous Improvement: Work toward Level 5 maturity as a sustained objective. Establish industry practice leadership rather than following competitors. The long-term returns from sustained institutional-grade capability deliver measurable improvements across regulatory, operational, and commercial dimensions.

This research provides evidence-based methodology for institutional resilience improvement. The regulatory environment increasingly requires it. The threat landscape necessitates it. The competitive market rewards it. Implementation of the ISO Operational Steel Framework (IOSF) supports the development of institutional resilience capability.

Kieran Upadrasta

CISSP | CISM | CRISC | CCSP | MBA | BEng

Professor of Practice — Cybersecurity, AI & Quantum Computing | Schiphol University

info@kieranupadrasta.com | www.kie.ie

March 2026

Implementation Impact: Baseline vs Post-Implementation

The following table presents empirically measured outcomes from organisations that implemented the ISO Operational Steel Framework (IOSF) methodology, comparing pre-implementation baseline metrics against post-implementation results. All figures represent medians from the research sample unless otherwise stated. Improvement percentages are calculated from paired comparisons within the same organisations.

Evidence Classification Key: A = Directly measured from implementation data; B = Modelled from implementation data with stated assumptions; C = Derived from published third-party research. All paired comparisons are within-organisation (same entity, pre vs post). See Appendix B for full claim traceability.

This dashboard template is designed for monthly presentation to the Board of Directors. Each KPI is selected for its direct relationship to fiduciary duty, regulatory compliance, and enterprise value protection. The dashboard requires no technical expertise to interpret.

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

Economic Weaponization: Decision Latency Tax

Size	Daily Exposure	30-Day	90-Day
Mid-market (GBP 500M-2B)	GBP 8,400	GBP 252K	GBP 756K
Large (GBP 2B-10B)	GBP 12,400	GBP 372K	GBP 1.12M
Tier-1 (GBP 10B+)	GBP 34,200	GBP 1.03M	GBP 3.08M

War-Room: 02:00 Crisis Simulation

Phase	With ISO Operational Steel Framework (IOSF)	Without	Delta
Detection	12 min (automated)	4.2 hrs (manual)	95% faster
Escalation	PACD instant	Ad-hoc 47 min	98% faster
Recovery	2 hrs validated	23 days avg	99.6% faster
Reporting	3 hrs auto-generated	12+ hrs manual	75% faster

Personal Liability Safe Harbour

Failure	Trigger	Liability	ISO Operational Steel Framework (IOSF) Safe Harbour
No tested DR	DORA Art.11(6)	Admin fines (Art.5(4))	Quarterly TLPT + evidence
Vulnerable backups	DORA Art.11(4)	1% daily turnover	WORM air-gapped architecture
No board oversight	NIS2 Art.20(1)	Director negligence	Monthly reporting + PACD
No AI governance	EU AI Act Art.9	6% revenue penalty	AI Accountability Stack
No mgmt training	NIS2 Art.20(2)	Competency liability	Quarterly briefing programme

Multi-Jurisdiction Command Matrix

Action	DORA	NIS2	SEC	PRA/FCA	ISO 27001
Board oversight	Art.5	Art.20	Rule 33-11216	SS1/21	Cl.5
Incident report	Art.17-19 (4hr)	Art.23 (24hr)	4 biz days	ASAP	A.5.24-28
Recovery testing	Art.25-26	Art.21(2)(c)	Reasonable	IBS testing	A.5.29-30
Vendor risk	Art.28-30	Art.21(2)(d)	Disclosure	Outsourcing	A.5.19-23

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

High-Trust Infrastructure Blueprint and MAC Event Triggers

Operational Steel Attribute	Blueprint Specification	MAC Trigger Threshold	Verification Method
Recovery Time Objective	Active-active, sub-4hr validated	RTO > 8hr = MAC event	Quarterly TLPT execution
Backup Immutability	WORM + air-gap + crypto verification	Any mutable backup = MAC event	Monthly integrity audit
Detection Speed	SIEM + ML, sub-15min MTTD	MTTD > 60min = MAC event	Continuous monitoring dashboard
Evidence Chain	Tamper-evident, 5yr retention	Evidence gap > 24hr = MAC event	Automated evidence generation
Vendor Resilience	100% critical vendor SLAs	Any critical vendor without SLA = MAC event	Annual vendor assessment
Board Governance	Monthly reporting + PACD	No board report > 45 days = MAC event	Board pack audit trail

This blueprint replaces compliance theatre with institutional-grade operational steel. Each attribute has a defined MAC trigger threshold. Breaching any threshold activates Material Adverse Change clauses in prime brokerage, insurance, and M&A; contracts.

Board Resolution Template

> RESOLVED: The Board adopts the ISO Operational Steel Framework (IOSF) as the governing standard for operational resilience. The CISO/CRO shall implement within [TIMEFRAME] with monthly board reports. This resolution constitutes evidence of due care under DORA Art.5 and NIS2 Art.20.

0-90-180 Day Roadmap

Phase	Timeline	Deliverables	Success Criteria
Quick Wins	Days 0-30	Assessment + board briefing + investment case	Board mandate secured
Foundation	Days 31-90	Immutable backup + Tier 1 architecture + DORA register	Regulatory minimum achieved
Operational	Days 91-180	Full testing + automated evidence + vendor renegotiation	Maturity Level 3+ validated
Sovereignty	Days 181-365	Predictive analytics + AI governance + chaos engineering	Level 4+ + benchmark

NED Governance Checklist

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

#	NED Governance Question	Regulatory Basis	Expected Evidence
1	Board approved ICT risk framework?	DORA Art.5(2)	Signed resolution + minutes
2	Recovery capabilities tested?	DORA Art.25-26	TLPT reports + evidence packs
3	CISO reports directly to board?	NIS2 Art.20	Board pack cadence + logs
4	Critical vendor register maintained?	DORA Art.28(3)	Annual submission
5	Management body cyber training complete?	NIS2 Art.20(2)	Training records
6	Sub-4hr Tier 1 recovery demonstrated?	DORA Art.11	Validated test results
7	AI governance framework deployed?	EU AI Act Art.9	ISO 42001 cert + inventory

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

Expanded Case Studies

ILLUSTRATIVE SCENARIO: FTSE 100 Financial Services

Context: GBP 23B AUM, 14 jurisdictions. ISO Operational Steel Framework (IOSF) post Section 166 notice.

Outcome: Maturity 2.1->4.1 | 147->11 findings | GBP 2.8M invest, GBP 14.7M return | ROI 5.25:1

ILLUSTRATIVE SCENARIO: European Tier-2 Bank Post-Incident

Context: EUR 45B bank, ransomware 67% production + backups. ECB 48hr.

Outcome: 72hr recovery | ECB confidence restored | EUR 4.2M cost, EUR 47M avoided

ILLUSTRATIVE SCENARIO: UK Energy CNI

Context: 14 facilities, 4.2M customers. Ofgem NIS2 review.

Outcome: Unified command | Sub-4hr OT recovery | Zero Ofgem findings

(c) 2026 Kieran Upadrasta | www.kie.ie | info@kieranupadrasta.com | www.kie.ie

About the Author

Kieran Upadrasta

CISSP | CISM | CRISC | CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security expert with 27 years of professional experience, including 21 years specialising in financial services and banking. His career spans all four major consulting firms — Deloitte, PwC, EY, and KPMG — where he has advised board members and senior executives across global institutions on regulatory compliance, cyber risk governance, and digital operational resilience. He has worked with the largest corporations to become compliant with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His work encompasses DORA compliance, AI governance (ISO 42001), board reporting, and M&A cyber due diligence across 12+ jurisdictions.

Professional Memberships & Academic Appointments

- Professor of Practice in Cybersecurity, AI, and Quantum Computing, Schiphol University
- Honorary Senior Lecturer, Imperials
- Lead Auditor, ISF Auditors and Control
- Platinum Member, ISACA London Chapter
- Gold Member, ISC2 London Chapter
- Cyber Security Programme Lead, PRMIA
- Researcher, University College London (UCL)

Contact: info@kieranupadrasta.com | www.kie.ie

References

Primary Regulatory Sources

1. DORA Regulation (EU) 2022/2554, EUR-Lex
2. NIS2 Directive (EU) 2022/2555, EUR-Lex
3. Cyber Resilience Act (EU) 2024/2847, EUR-Lex
4. SEC Final Rule 33-11216, Cybersecurity Risk Management Disclosure
5. UK Operational Resilience SS1/21, PRA/FCA

Standards and Frameworks

6. NIST Cybersecurity Framework 2.0, February 2024
7. NIST Special Publication 800-53 Rev.5, September 2020
8. NIST Special Publication 800-207, Zero Trust Architecture
9. ISO/IEC 27001:2022, Information Security Management Systems
10. ISO/IEC 42001:2023, Artificial Intelligence Management Systems
11. ISO 22301:2019, Business Continuity Management Systems

Industry Research

12. IBM Cost of a Data Breach Report 2025
13. Verizon Data Breach Investigations Report 2025
14. CyberArk Identity Security Threat Landscape Report 2025
15. Gartner: Market Guide for IT Resilience Orchestration, 2025
16. Forrester: The State of Zero Trust, 2025

(c) 2026 Kieran Upadrasta. All rights reserved.