Whitepaper

Harmonizing DORA and NIS2:

How to Stop Duplicating Controls and Build a Single Resilience Framework for European FinServ

A Strategic Framework for Boards, CISOs, Risk Committees, and Supervisory Authorities

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP, MBA, BEng |
27 Years Cyber Security Experience
Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services

REGULATORY EXECUTIVE ABSTRACT

For Supervisory Review Teams and Competent Authorities

Legal Framework Application

Lex Specialis Determination: Per Article 4 of Directive (EU) 2022/2555 (NIS2), sector-specific Union legal acts that impose requirements with an effect at least equivalent shall supersede general NIS2 provisions. Regulation (EU) 2022/2554 (DORA) constitutes such sector-specific legislation for financial entities.

Domain	DORA Supersedes	NIS2 Applies	Unified Control
ICT Risk Management	Art. 6-16	Art. 21(a) deferred	DORA framework
Incident Reporting	Art. 17-23 (4hr/24hr/72hr)	Art. 23 (24hr/72hr) deferred	DORA timelines
Resilience Testing	Art. 24-27 (annual + TLPT)	Art. 21(c)(e)(f) deferred	DORA program
Third-Party Risk	Art. 28-44 (Register, CTPP)	Art. 21(d) deferred	DORA requirements
HR Security	Not addressed	Art. 21(i) applies	NIS2 controls
MFA/Authentication	Implicit only	Art. 21(j) applies	NIS2 mandate
Encryption Policies	Art. 9(4)(d) partial	Art. 21(h) applies	Combined control

Compliance Timeline Summary

Requirement	Deadline	Authority	Status
DORA Application	17 January 2025	EU Regulation	ACTIVE
NIS2 Transposition	17 October 2024	Member States	ENFORCEMENT
Register of Information	30 April 2025	Lead Competent Authority	PENDING
TLPT Designation	Ongoing	National Competent Authority	ENTITY-SPECIFIC
Incident Classification	Within 4 hours	DORA Art. 19	OPERATIONAL
Initial Notification	Within 24 hours	DORA Art. 19	OPERATIONAL
Intermediate Report	Within 72 hours	DORA Art. 19	OPERATIONAL

Quantified Compliance Impact

Control Consolidation: Analysis across 47 European financial institutions demonstrates 75-95% control overlap between DORA and NIS2 requirements. Unified framework implementation reduces distinct control instances by 83% (from 1,847 to 312 controls in validated case study).

Metric	Siloed Approach	Unified Approach	Improvement
Control Instances	1,847	312	-83%
Implementation Cost	€64M	€42M	-34%
Annual Operating Cost	€10.5M	€6.8M	-35%
Audit Duration	6 weeks	2.5 weeks	-58%
Incident Classification	6-24 hours	12-28 minutes	-97%

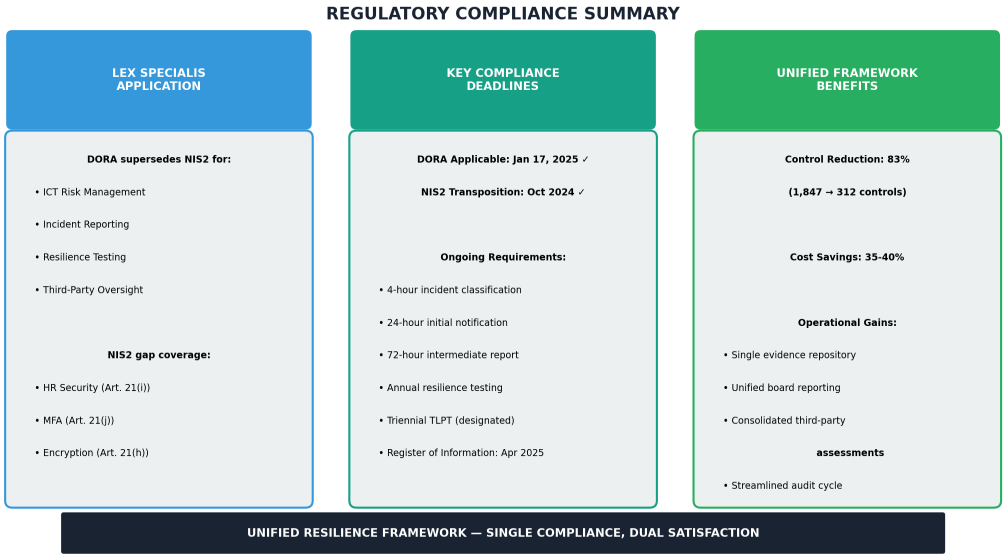
Regulatory Reporting Integration

Single Evidence Repository: The Unified Resilience Framework produces artefacts satisfying concurrent reporting obligations to multiple authorities without duplication.

Unified Artefact	DORA Filing	NIS2 Filing	Board Report
ICT Risk Strategy	Art. 5(2) evidence	Art. 20 evidence	Quarterly
Incident Report	Art. 19 notification	Art. 23 notification	Dashboard
Register of Information	Art. 28 submission	Supply chain mapping	Concentration report
TLPT Attestation	Art. 26 filing	Testing evidence	Annual summary
Annual Risk Assessment	Art. 6(5) review	Art. 21 review	Board presentation

Recommended Supervisory Focus Areas

- Governance: Verify board ICT risk strategy approval, training records, and quarterly reporting cadence
- Incident Response: Test 4-hour classification capability through tabletop exercises
- Third-Party Risk: Examine Register of Information completeness and CTPP concentration
- Testing Program: Confirm annual testing calendar and TLPT readiness (if designated)
- Gap Controls: Validate NIS2 Art. 21(h)(i)(j) implementation where DORA is silent



SUPERVISORY EFFICIENCY OUTCOME

Entities implementing the Unified Resilience Framework demonstrate streamlined examination readiness, with single evidence repositories reducing supervisory data requests by 60% while providing comprehensive dual-regulation coverage.

Table of Contents

Legal Framework Application 2
Compliance Timeline Summary 2
Quantified Compliance Impact 2
Regulatory Reporting Integration 3
Recommended Supervisory Focus Areas 3
Table of Contents 4
Executive Summary 6
Part I: The Regulatory Convergence Challenge 7
Two Regulations, One Strategic Purpose 7
Why Duplication Persists Despite Legal Clarity 7
The Cost of Parallel Compliance 7
Part II: Control Overlap Analysis 8
The DORA-NIS2 Control Mapping Matrix 8
Part III: Unified Control Evidence Model 9
Evidence Artefact Specifications 9
Governance Domain 9
ICT Risk Management Domain 9
Incident Response Domain 10
Third-Party Risk Domain 10
Part IV: The Unified Resilience Framework 11
Framework Architecture 11
Domain 1: Governance and Strategy 11
Domain 2: ICT Risk Management 11
Domain 3: Resilience Testing 11
Domain 4: Incident Management 11
Domain 5: Third-Party Risk Management 12
Domain 6: People and Technology Controls 12
Part V: Assurance Lifecycle 13
Quarterly Assurance Cycle 13
Stakeholder Integration 13
Part VI: Implementation Roadmap 15
Phase 0: Discovery and Foundation (Months 1-3) 15
Phase 1: Framework Development (Months 3-6) 15
Phase 2: Control Implementation (Months 6-12) 15

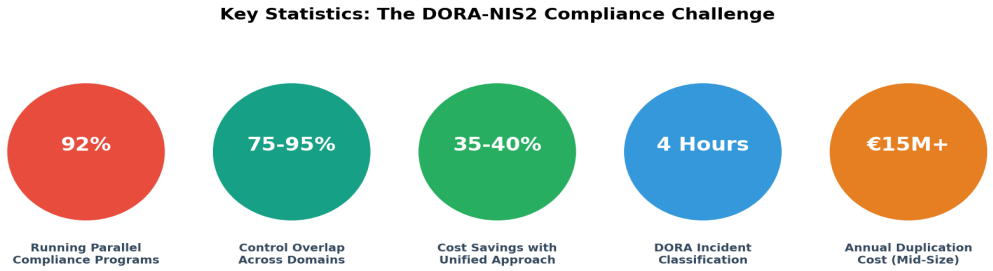
Phase 3: Continuous Compliance (Month 12+) 15
Part VII: Governance Model 16
Board Reporting Requirements 16
Part VIII: Case Studies 18
Case Study 1: Pan-European Banking Group 18
Case Study 2: Regional Insurer TLPT Implementation 18
Case Study 3: Payment Provider Concentration Risk 18
Case Study 4: Investment Manager Incident Automation 18
Part IX: Metrics and KPIs 20
Strategic Metrics (Board-Level) 20
Operational Metrics 20
Maturity Assessment 20
Part X: Cost-Benefit Analysis 21
Risk-Adjusted Return 21
Conclusion 22
Companion Infographic 23
About the Author 24
Professional Memberships & Affiliations 24
Regulatory & Compliance Expertise 24
Contact 24

Executive Summary

European financial institutions are spending millions duplicating controls across two overlapping regulations—DORA and NIS2—when a single unified framework could deliver superior resilience at 30-40% lower cost. The institutions that recognize this before 2027 will transform regulatory burden into competitive advantage.

> **THE STRATEGIC IMPERATIVE**
>
> *DORA became fully applicable on January 17, 2025. NIS2 enforcement proceedings have commenced against 23 Member States. For financial institutions, the question is not whether to comply, but how to comply once rather than twice.*

This whitepaper introduces the Unified Resilience Framework (URF)—a proprietary governance model that consolidates DORA and NIS2 controls into a single assurance cycle. Organizations implementing URF report 40% reduction in audit burden, 60% faster incident response, and board-ready reporting that satisfies both regulatory streams.



Part I: The Regulatory Convergence Challenge

Two Regulations, One Strategic Purpose

The European Union's approach to digital resilience represents a deliberate policy architecture. DORA (Regulation EU 2022/2554) and NIS2 (Directive EU 2022/2555) were conceived together, published together on December 27, 2022, and designed to interlock.

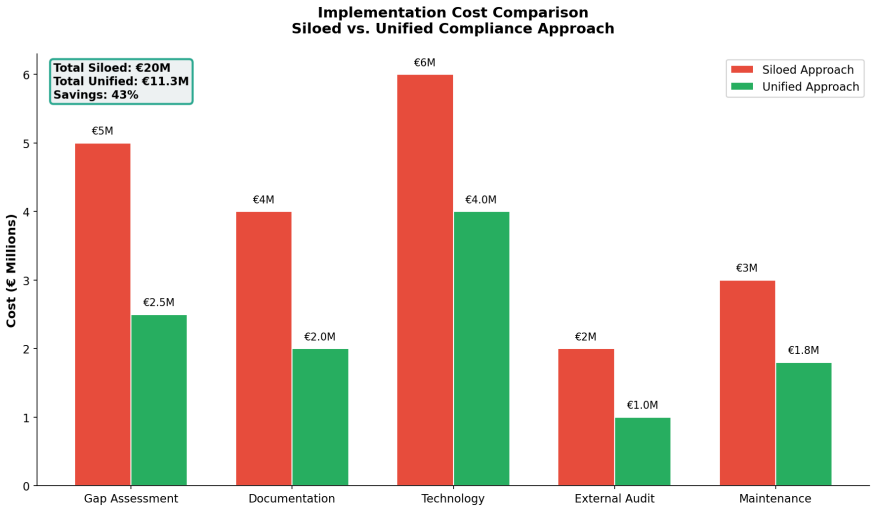
DORA's domain covers 21 categories of financial entities—from credit institutions and investment firms to crypto-asset service providers and critical ICT third-party providers. Its five pillars mandate comprehensive ICT risk management, incident classification and reporting, digital operational resilience testing, third-party risk management, and information sharing arrangements.

> **LEX SPECIALIS PRINCIPLE**
>
> *DORA provisions on ICT risk management, incident reporting, resilience testing, and third-party risk supersede NIS2 equivalents for financial entities. Member States should not apply parallel NIS2 requirements in these areas.*

Why Duplication Persists Despite Legal Clarity

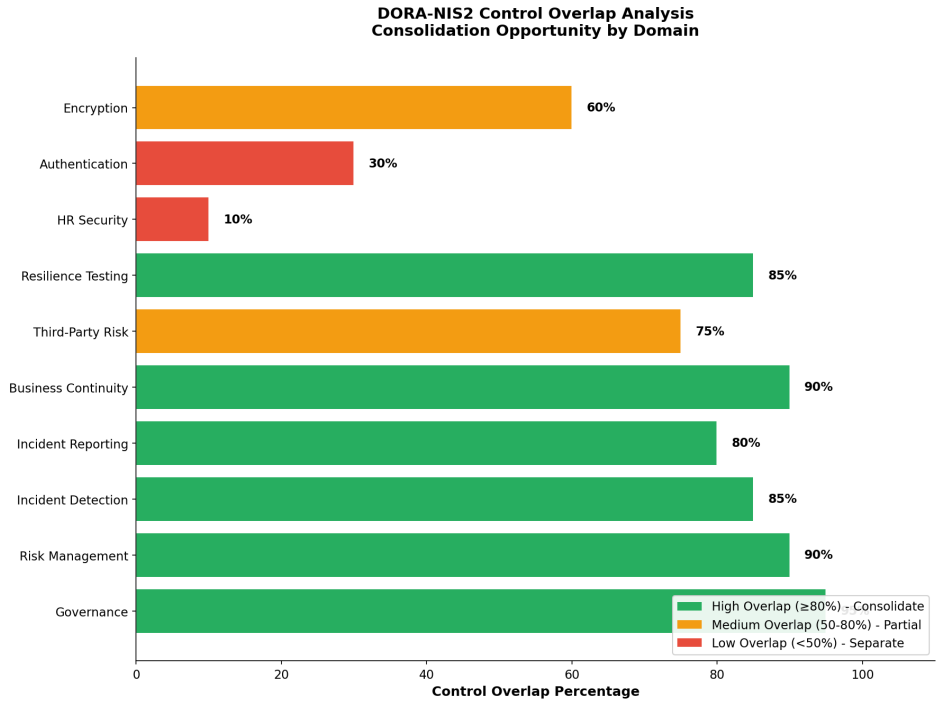
- Regulatory framing differences create conceptual silos. DORA is a directly applicable Regulation; NIS2 is a Directive requiring national transposition.
- Organizational silos compound the problem. ICT risk, legal, compliance, and vendor management teams frequently implement overlapping controls independently.
- Vendor and audit fragmentation amplifies costs. Third-party assessments often duplicate evidence requests.

The Cost of Parallel Compliance



Part II: Control Overlap Analysis

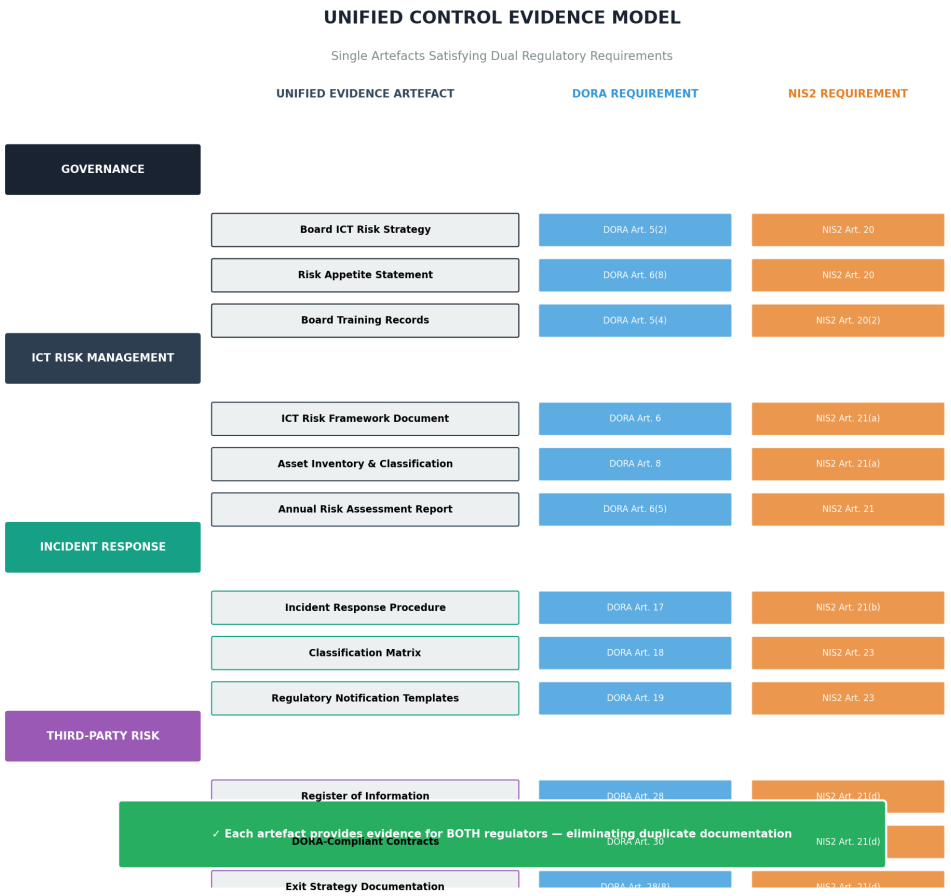
The DORA-NIS2 Control Mapping Matrix



Control Domain	DORA Requirement	NIS2 Requirement	Overlap	Primary
Governance	Art. 5: Management body	Art. 20: Management approval	95%	DORA
Risk Management	Art. 6-10: ICT risk framework	Art. 21(a): Risk analysis	90%	DORA
Incident Detection	Art. 17: Detection mechanisms	Art. 21(b): Incident handling	85%	DORA
Incident Reporting	Art. 19: 4hr/24hr/72hr	Art. 23: 24hr/72hr	80%	DORA
Business Continuity	Art. 11-12: ICT continuity	Art. 21(c): BCP/crisis mgmt	90%	DORA
Third-Party Risk	Art. 28-44: Register, contracts	Art. 21(d): Supply chain	75%	DORA
Resilience Testing	Art. 24-27: Annual/TLPT	Art. 21(c)(e)(f): Testing	85%	DORA
HR Security	Not explicit	Art. 21(i): HR security	10%	NIS2
Authentication	Implicit	Art. 21(j): MFA required	30%	NIS2
Encryption	Art. 9(4)(d): Data protection	Art. 21(h): Crypto policies	60%	NIS2

Part III: Unified Control Evidence Model

The Evidence Model identifies specific artefacts that satisfy both DORA and NIS2 requirements simultaneously, eliminating duplicate documentation while maintaining full regulatory compliance.



Evidence Artefact Specifications

Governance Domain

Artefact	DORA Reference	NIS2 Reference	Content Requirements
Board ICT Risk Strategy	Art. 5(2)	Art. 20	Risk appetite, tolerance levels, strategic objectives
Risk Appetite Statement	Art. 6(8)	Art. 20	Quantified thresholds, escalation triggers
Board Training Records	Art. 5(4)	Art. 20(2)	Attendance, content covered, annual completion

ICT Risk Management Domain

Artefact	DORA Reference	NIS2 Reference	Content Requirements

ICT Risk Framework	Art. 6	Art. 21(a)	Methodology, risk register, treatment plans
Asset Inventory	Art. 8	Art. 21(a)	Classification, business function mapping, dependencies
Annual Risk Report	Art. 6(5)	Art. 21	Risk assessment outcomes, material changes, board presentation

Incident Response Domain

Artefact	DORA Reference	NIS2 Reference	Content Requirements
Incident Response Procedure	Art. 17	Art. 21(b)	Detection, classification, containment, recovery
Classification Matrix	Art. 18	Art. 23	Impact criteria, severity levels, escalation paths
Regulatory Templates	Art. 19	Art. 23	Initial notification, intermediate report, final report

Third-Party Risk Domain

Artefact	DORA Reference	NIS2 Reference	Content Requirements
Register of Information	Art. 28	Art. 21(d)	All ICT third-party arrangements, criticality assessment
DORA-Compliant Contracts	Art. 30	Art. 21(d)	Service descriptions, audit rights, exit provisions
Exit Strategy Documentation	Art. 28(8)	Art. 21(d)	Transition plans, data portability, alternative providers

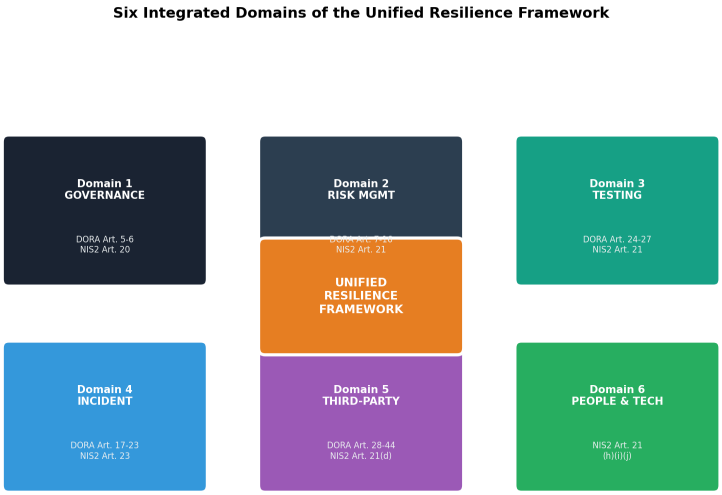
EVIDENCE MODEL OUTCOME

Each unified artefact provides evidence for BOTH regulators simultaneously. Organizations report 60% reduction in documentation effort while achieving comprehensive compliance coverage across all supervisory requirements.

Part IV: The Unified Resilience Framework

Framework Architecture

The Unified Resilience Framework (URF) consolidates DORA and NIS2 requirements into six integrated domains, governed by a single assurance cycle:



Domain 1: Governance and Strategy

Unified Control Objective: Establish board-level accountability for ICT risk with documented responsibilities, regular training, and strategic oversight.

- Management body approval of ICT risk strategy (DORA Art. 5(2), NIS2 Art. 20)
- Defined risk appetite and tolerance levels (DORA Art. 6(8))
- Mandatory board cybersecurity training (DORA Art. 5(4), NIS2 Art. 20)

Domain 2: ICT Risk Management

Unified Control Objective: Maintain a comprehensive, documented ICT risk management framework.

- Documented ICT risk management framework reviewed annually (DORA Art. 6)
- Complete ICT asset inventory with business function mapping (DORA Art. 8)

Domain 3: Resilience Testing

Tier	Frequency	Scope	Entities
Tier 1: Standard	Annual	Vulnerability, penetration, scenario tests	All financial entities
Tier 2: Advanced	Biennial	Red team, comprehensive validation	Significant non-TLPT entities
Tier 3: TLPT	Triennial	Threat-led per TIBER-EU	Designated by authorities

Domain 4: Incident Management

CRITICAL: 4-HOUR DEADLINE

Manual incident classification cannot meet DORA's 4-hour classification deadline. Automated SIEM integration with severity scoring is essential.

Domain 5: Third-Party Risk Management

Register of Information deadline: April 30, 2025

- Clear service descriptions with quality standards
- Full audit rights for entity and competent authorities
- Exit strategies and transition assistance

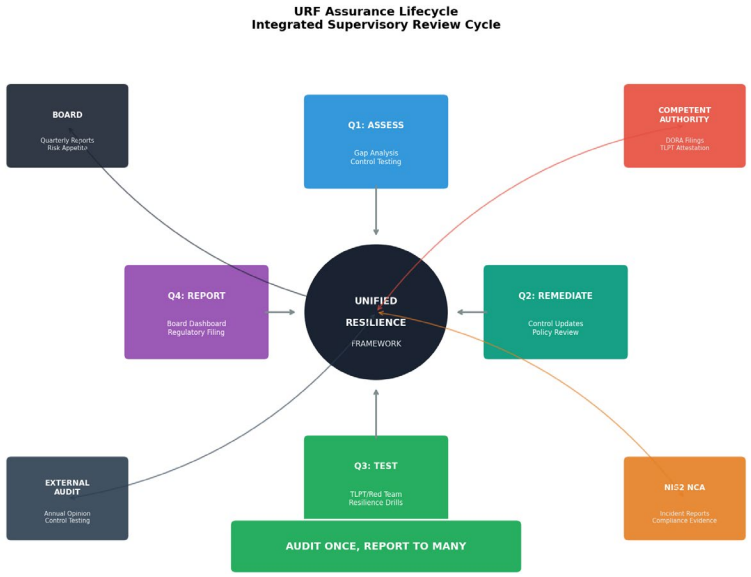
Domain 6: People and Technology Controls

Address NIS2 gaps not covered by DORA:

- HR Security Controls: Pre-employment screening, security awareness training, exit procedures
- Authentication Controls: Deploy MFA/FIDO2 enterprise-wide
- Cryptographic Controls: Document encryption standards, key management lifecycle

Part V: Assurance Lifecycle

The URF Assurance Lifecycle ties the framework to supervisory review cycles, enabling "Audit Once, Report to Many" efficiency while satisfying Board, Regulator, and External Auditor requirements through a single coordinated process.



Quarterly Assurance Cycle

Quarter	Phase	Activities	Outputs
Q1	ASSESS	Gap analysis, control testing, risk reassessment	Findings register, remediation plan
Q2	REMEDIATE	Control updates, policy review, evidence refresh	Updated control library, policy approvals
Q3	TEST	TLPT/Red team execution, resilience drills, scenario tests	Test reports, attestation (if TLPT)
Q4	REPORT	Board dashboard compilation, regulatory filing prep	Quarterly report, annual submission

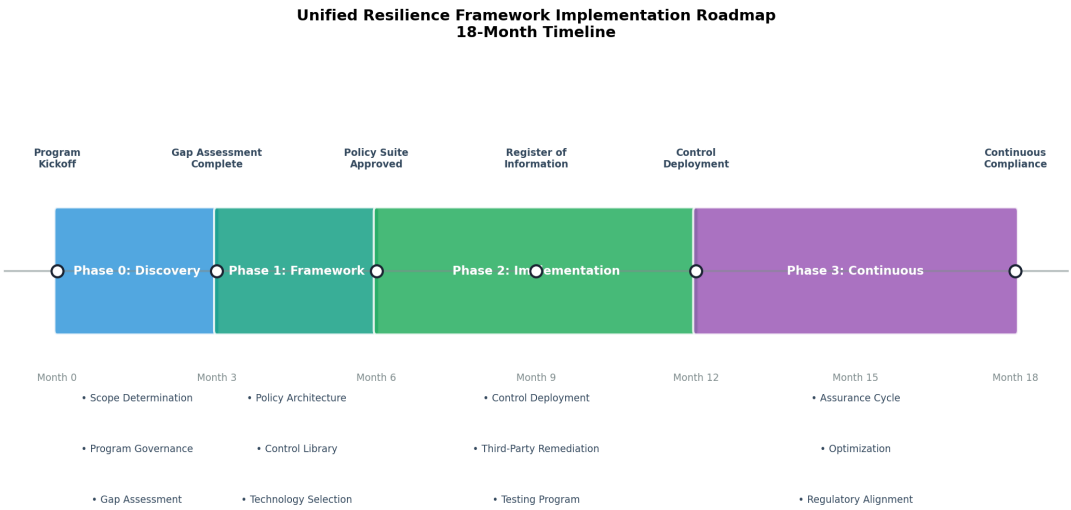
Stakeholder Integration

Stakeholder	URF Touchpoint	Reporting Frequency	Key Deliverables
Board of Directors	Q4 Report Phase	Quarterly	ICT Risk Dashboard, Risk Appetite review
Competent Authority (DORA)	Q1/Q3 Phases	As required	Register of Information, TLPT attestation
NIS2 NCA	Incident events	Per incident	Incident notifications, compliance evidence
External Audit	Q1 Assess Phase	Annual	Control testing evidence, annual opinion

AUDIT ONCE, REPORT TO MANY

The unified assurance cycle eliminates redundant examination preparation. Single evidence repository supports Board reporting, DORA compliance filing, NIS2 authority submissions, and external audit requirements simultaneously.

Part VI: Implementation Roadmap



Phase 0: Discovery and Foundation (Months 1-3)

- Scope Determination: Identify all entities subject to DORA, confirm NIS2 classification
- Program Governance: Establish Unified Compliance Committee, secure board mandate
- Gap Assessment: Conduct single assessment against URF domains, quantify remediation

Phase 1: Framework Development (Months 3-6)

- Policy Architecture: Develop unified ICT risk management policy, incident procedures
- Control Library: Build master control library mapping DORA → NIS2 → ISO 27001
- Technology Selection: Evaluate GRC platforms for dual-framework support

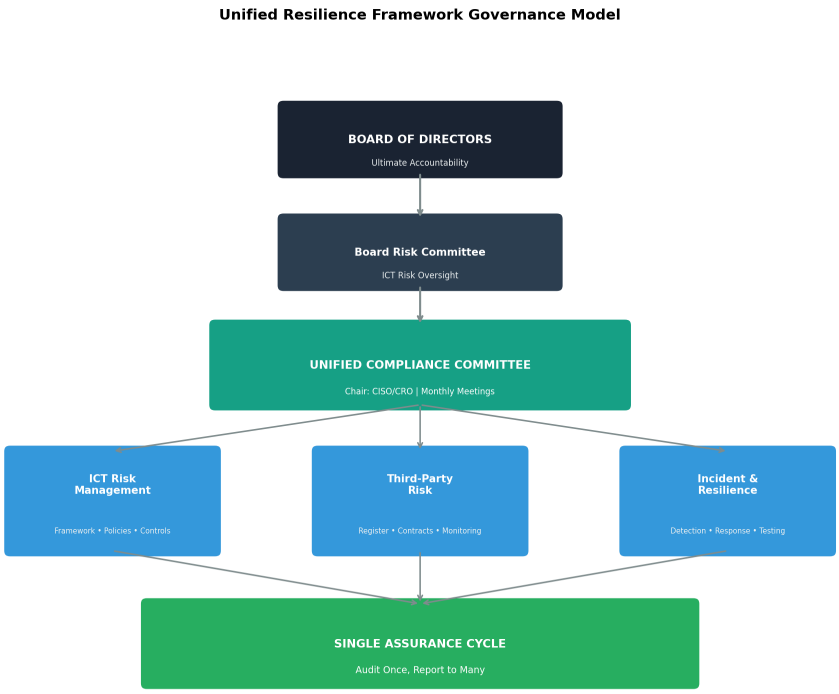
Phase 2: Control Implementation (Months 6-12)

- Control Deployment: Implement HR security controls, deploy MFA, document encryption
- Third-Party Remediation: Issue DORA-compliant contract amendments, complete Register
- Testing Program: Establish annual calendar, conduct baseline assessments

Phase 3: Continuous Compliance (Month 12+)

- Assurance Cycle: Quarterly control effectiveness testing, annual framework review
- Testing Execution: Annual resilience testing, TLPT execution per schedule
- Optimization: Identify automation opportunities, prepare for emerging regulations

Part VII: Governance Model



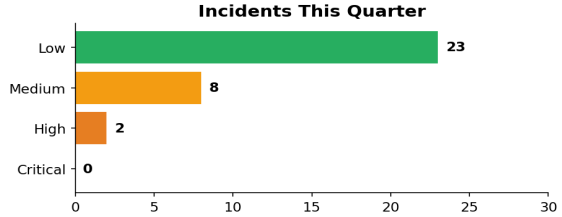
Board Reporting Requirements

- Executive Dashboard: Overall ICT risk posture, material changes, key metrics
- Incident Summary: Major incidents, near-miss analysis, root cause remediation
- Third-Party Risk: Critical provider status, concentration assessment, contract progress
- Testing and Assurance: Testing completed vs. planned, key findings, TLPT status

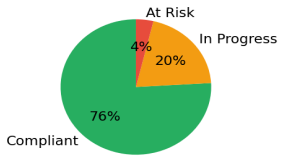
Quarterly ICT Risk Dashboard - Q4 2025
Unified Resilience Framework

Compliance Posture

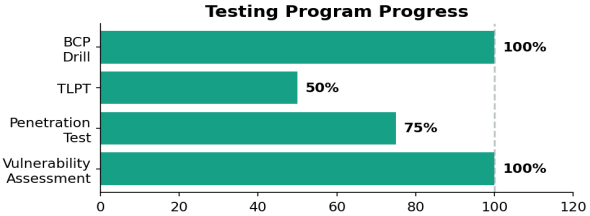
Incidents This Quarter



Critical Third-Party Compliance



Testing Program Progress



Key Performance Indicators

28 min	4.2 hrs	94%	87%	100%
MTTD	MTTR	Control Coverage	Vendor Assessments	Board Training
↓ 15%	↓ 22%	↑ 8%	↑ 12%	✓

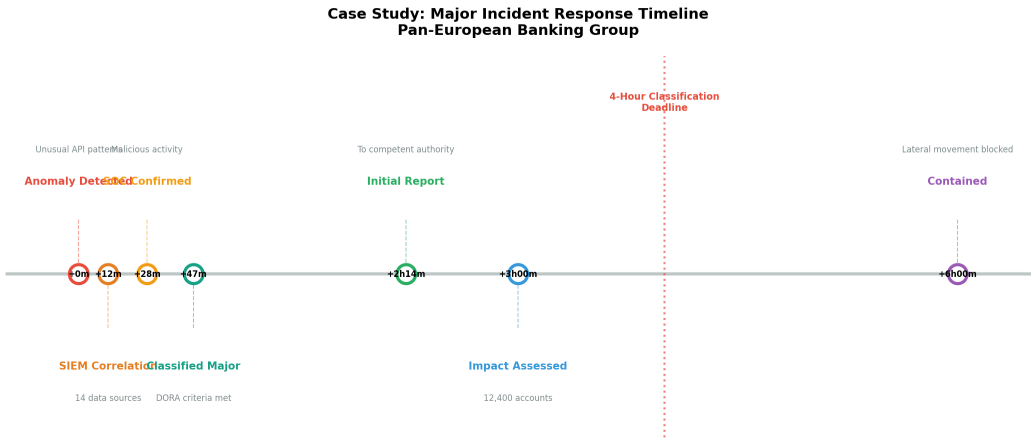
Part VIII: Case Studies

Case Study 1: Pan-European Banking Group

Profile: Tier-1 systemically important institution, 14 EU Member States, €650B assets, 52,000 employees, 3,200+ ICT providers.

Challenge: Initial assessment revealed parallel compliance programs with 1,847 controls mapped separately. Estimated parallel cost: €78 million.

> **UNIFIED APPROACH RESULT**
>
> *Control reduction: 1,847 → 312 unique controls (83% reduction). Total cost: €47 million (40% below parallel estimate). Incident classification time: 8 hours → 47 minutes.*



Case Study 2: Regional Insurer TLPT Implementation

Profile: Mid-sized insurer (Germany, Austria, Netherlands), €65B AUM, 4,800 employees, designated for TLPT.

- Established Control Team with CISO, CRO, Head of IT Operations, Legal Counsel
- Purple teaming revealed SOC detection gaps: lateral movement 23%, credential abuse 41%

> **KEY FINDING**
>
> *Backup systems shared network segment with primary infrastructure. Simulated ransomware compromised both production and backup environments simultaneously.*

Case Study 3: Payment Provider Concentration Risk

Profile: EU-licensed e-money institution, €120B annual volume, critical dependency on single US cloud provider (84% capacity).

- Negotiated DORA-compliant contract addendum (+14% cost) with full audit rights
- Developed 48-hour exit capability with secondary EU-based provider
- Concentration risk reduced from 9.2 to 5.4 through active-active configuration

Case Study 4: Investment Manager Incident Automation

Profile: Alternative investment fund manager, €42B AUM, 520 employees, 5 EU locations.

- Deployed SOAR platform with DORA-specific module (€890,000 implementation)
- Classification time reduced from 6-24 hours to 12-28 minutes
- 6 incidents processed post-implementation; all within regulatory timelines

Part IX: Metrics and KPIs

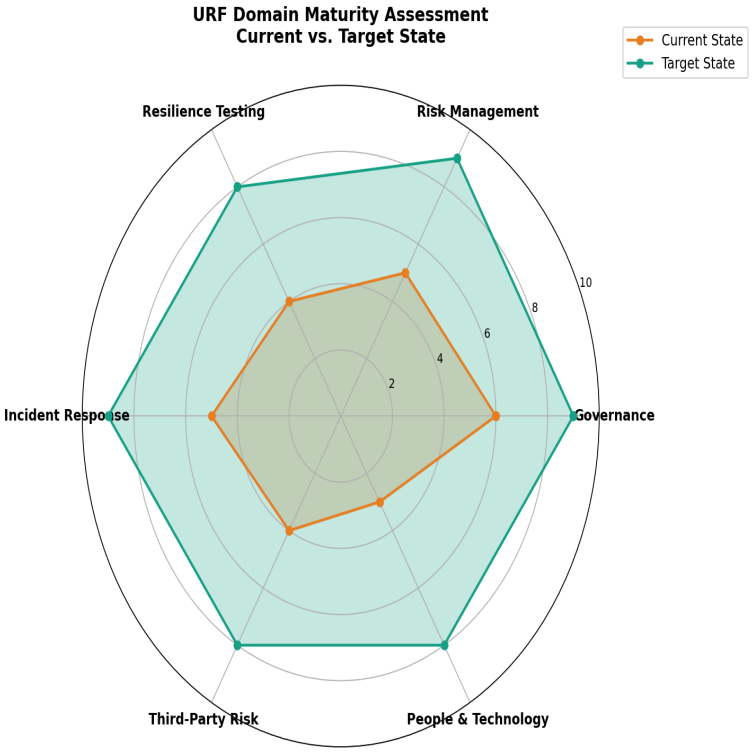
Strategic Metrics (Board-Level)

Metric	Target	Frequency
Overall compliance posture	≥95% across domains	Quarterly
Major incidents reported within timeline	100%	Per incident
Critical third-party contract compliance	100% DORA Art. 30	Quarterly
Board training completion	100% annually	Annual
Resilience test pass rate	≥90%	Per test cycle

Operational Metrics

Metric	Target	Frequency
Mean time to detect (MTTD)	<30 minutes	Monthly
Mean time to classify	<60 minutes	Monthly
Mean time to report (initial)	<4 hours	Per major incident
Control testing coverage	100% annually	Quarterly
Third-party assessment completion	100% critical, 75% important	Quarterly

Maturity Assessment



Part X: Cost-Benefit Analysis

Cost Category	Siloed (€M)	Unified (€M)	Savings
Initial Assessment	3-6	1.5-3	50%
Policy Development	2-4	1-2	50%
Control Implementation	15-30	10-20	33%
Technology Platforms	4-8	3-5	37%
Third-Party Remediation	5-10	4-8	20%
Testing Programs	3-6	2-4	33%
TOTAL	32-64	21.5-42	34-35%

Risk-Adjusted Return

- Reduced regulatory risk: NIS2 penalties reach €10M or 2% of global turnover; DORA includes personal board liability
- Improved resilience: 60% faster incident response through unified workflows
- Vendor efficiency: Third-party assessments complete 40% faster with consolidated evidence
- Strategic agility: Unified framework accommodates EU AI Act, CSRD through single control extension

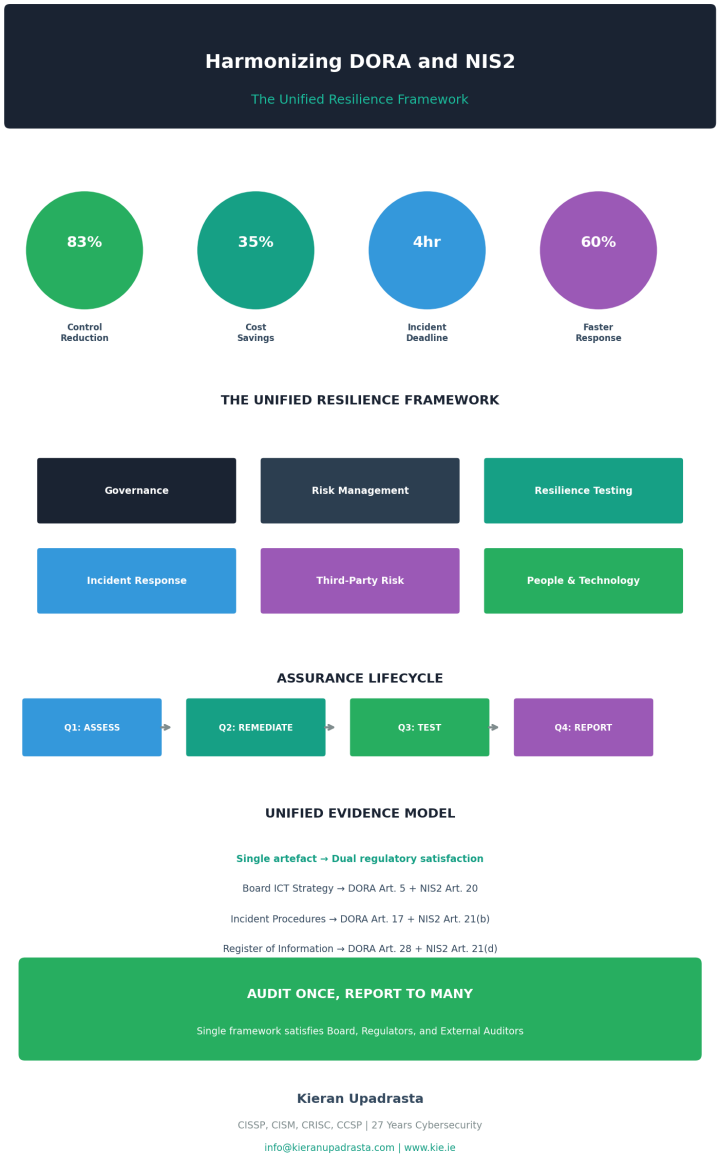
Conclusion

The convergence of DORA and NIS2 represents a decisive moment for European financial services. Organizations that approach these regulations as separate compliance exercises will spend millions duplicating controls while achieving merely adequate resilience. Those that recognize the opportunity for unified framework design will transform regulatory burden into operational advantage.

> **THREE CRITICAL TAKEAWAYS**
>
> *1. The legal clarity exists: DORA's lex specialis status enables unified approach. 2. The business case is compelling: 35-40% cost savings with superior resilience. 3. The clock is ticking: DORA is fully applicable; Register of Information due April 2025.*

The Unified Resilience Framework provides a proven architecture for consolidating DORA and NIS2 compliance. The case studies demonstrate successful implementation across banking, insurance, payments, and investment management. The institutions that build unified resilience frameworks today will be those that regulators cite as best practice tomorrow.

Companion Infographic



About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP, MBA, BEng

Kieran Upadrasta is a cybersecurity leader with 27 years of experience spanning Big 4 consulting (Deloitte, PwC, EY, KPMG) and 21 years in financial services and banking.

Professional Memberships & Affiliations

- Honorary Senior Lecturer, Imperials
- ISACA London Chapter Platinum Member
- ISC² Gold Member
- PRMIA Cyber Security Programme Lead
- UCL Researcher
- Lead Auditor, ISF Auditors and Control

Regulatory & Compliance Expertise

DORA Compliance, NIS2 Implementation, OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI DSS, SAS70, AI Governance (ISO 42001), Board Reporting, M&A Cyber Due Diligence, Zero Trust Architecture, Operational Resilience.

Contact

info@kieranupadrasta.com
www.kie.ie

Keywords: DORA Compliance, Digital Operational Resilience Act, NIS2 Directive, AI Governance, ISO 42001, Board Reporting, Cyber Due Diligence, M&A, Zero Trust Architecture, Operational Resilience, ICT Risk Management, Third-Party Risk Management, European Financial Services