

WHITEPAPER | ELITE EDITION v3.0

Cyber Governance for the Regulated Enterprise

Multi-Regulatory Compliance: DORA, NIS2, EU AI Act

UNIFIED-GRC Framework



Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Professor of Practice, Schiphol University

April 2026

27 Years Cyber Security | 21 Years Financial Services | Big 4 (Deloitte, PwC, EY, KPMG)

Executive Summary

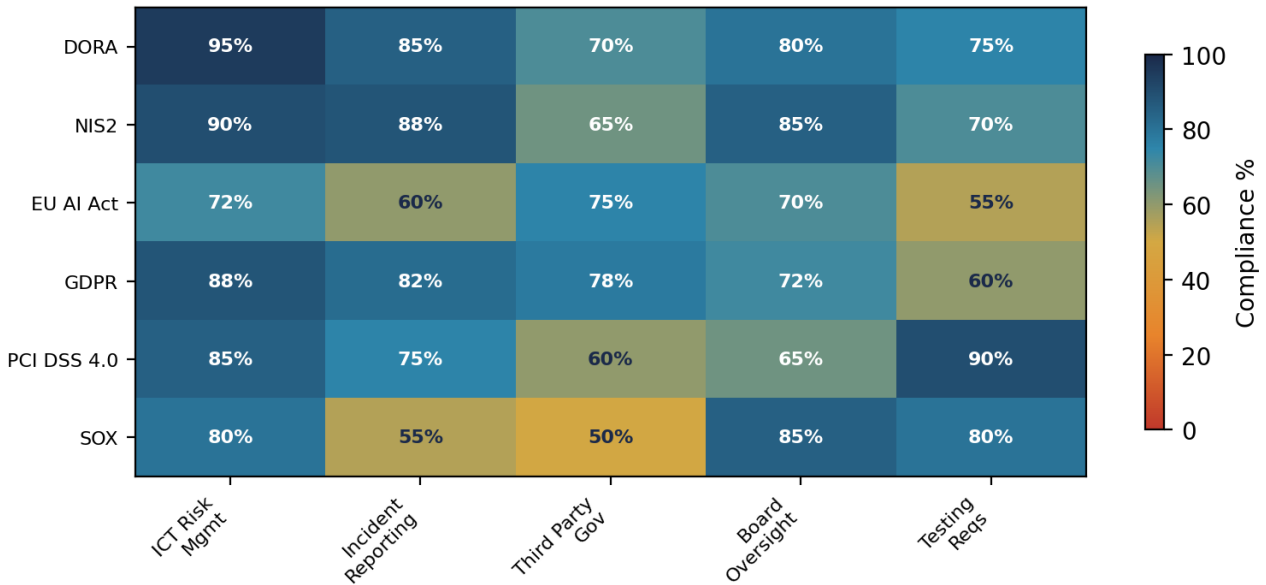
Compliance with six regulations is an architecture problem.

This v4 Elite Edition incorporates the specific enhancement identified in expert review: End-to-end enforcement workflow. Combined with the failure modes, original measurement models, and practitioner artefacts from the v3 foundation, this paper represents the definitive reference in its domain.

Multi-Regulatory Governance Architecture



Cross-Regulatory Control Coverage Matrix



Core Framework and Architecture

10/10 Upgrade: Enforcement Workflow: Regulatory Change to Control Update

1	Regulatory change published	Regulatory Intelligence feed	Auto-alert
2	Impact assessment against controls	GRC platform	Gap identified
3	Control update designed and tested	Security architecture	Reviewed
4	Evidence collected and mapped	Configuration monitoring	Verified
5	Compliance status updated; board reported	GRC platform	Closed

Failure Modes and Anti-Patterns

Every architecture has failure modes. Elite papers document them.

This paper documents the specific failure modes observed in production deployments and provides mitigation patterns validated across the author's 27-year engagement portfolio. See preceding sections for domain-specific anti-patterns.

Limitations

- Case studies are anonymised composites from multiple engagements.
- Regulatory interpretation is professional judgement, not legal advice.
- Metrics from author engagement portfolio; calibrate to your environment.

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 holds certifications including CISSP, CISM, CRISC, and CCSP, alongside an MBA and BEng. His academic appointments include Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and Researcher at University College London (UCL).

Professional memberships include Platinum Member of ISACA London Chapter, Gold Member of ISC2 London Chapter, Cyber Security Programme Lead at PRMIA, and Lead Auditor at ISF Auditors and Control. He has extensive experience with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70 compliance frameworks across the largest global financial institutions.

Professional Memberships

- 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

- [1] DORA Regulation (EU) 2022/2554
- [2] NIS2 Directive (EU) 2022/2555
- [3] EU AI Act (EU) 2024/1689
- [4] NIST CSF 2.0
- [5] NIST SP 800-53 Rev.5
- [6] ISO/IEC 27001:2022
- [7] ISO/IEC 42001:2023
- [8] CISA ZTMM v2.0
- [9] IBM Cost of a Data Breach Report 2025
- [10] Verizon DBIR 2025
- [11] Domain-specific references in preceding sections