WHITEPAPER | ELITE EDITION

The Regulatory Readiness Playbook

Turning CRA and NIS2 into Engineering Control

The READINESS Framework: Formal Scoring Model and Continuous Assessment

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services | AI Cyber Security Programme Lead
Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University
Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

UNIQUE CONTRIBUTION: READINESS provides a weighted scoring rubric, sample assessment output, Regulatory Exposure Index, and Continuous Readiness concept.

CONFORM System Position: This paper (WP10) extends the CONFORM master theory (WP01) for formal scoring model and continuous assessment. See WP01 for foundational methodology.

Executive Summary

READINESS is the assessment and planning layer of the CONFORM System. v10.0 adds the formal scoring model with weights, a sample assessment output, and the Continuous Readiness concept linking point-in-time assessment to ongoing monitoring.

1. Formal Readiness Scoring Model

Readiness Score = sum of (Dimension_Weight x Implementation_Level) across six dimensions. Each dimension is scored 1-5 with defined criteria:

Dimension	Weight	Score 1 (Gap)	Score 3 (Partial)	Score 5 (Met)
Regulatory Analysis	20%	No requirement mapping exists	Partial mapping; gaps unquantified	Complete 204-req catalogue mapped
Engineering Architecture	25%	No CI/CD pipeline; manual deployment	Basic pipeline; no security gates	Full pipeline with automated gates
Documentation & Evidence	20%	No evidence infrastructure	Manual evidence; incomplete records	Cryptographic evidence chains
Integration & Automation	15%	No policy-as-code; manual controls	Partial automation; some OPA policies	Full CODIFY deployment
Normative Assessment	10%	No maturity model; ad hoc processes	Informal maturity; basic metrics	Instrumented maturity (L3+)
Executive Governance	10%	No board reporting; no oversight	Annual reporting; limited oversight	Quarterly + real-time with signed records

Table 1: Readiness Scoring Rubric — Six Dimensions with Weighted Criteria

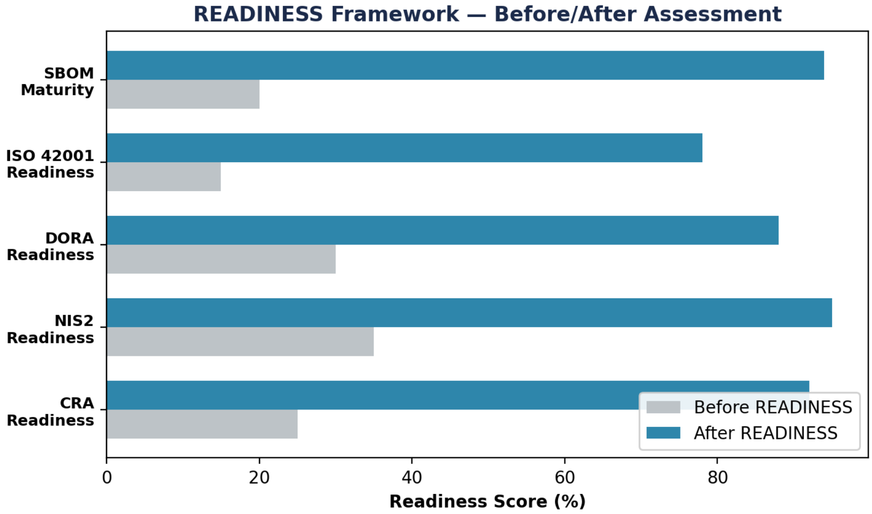

Figure: Readiness Assessment — Before/After

2. Sample Assessment Output

The following illustrates a completed readiness assessment for a mid-market technology company:

Dimension	Score	Weight	Weighted	Priority
Regulatory Analysis	2.5	20%	0.50	HIGH — gaps in DORA mapping
Engineering Architecture	3.0	25%	0.75	HIGH — no security gates
Documentation & Evidence	1.5	20%	0.30	CRITICAL — no evidence chain
Integration & Automation	2.0	15%	0.30	HIGH — manual controls
Normative Assessment	3.5	10%	0.35	MEDIUM — informal maturity
Executive Governance	2.0	10%	0.20	HIGH — annual reporting only
TOTAL READINESS SCORE	—	100%	2.40 / 5.00	48% — significant gaps

Table 2: Sample Readiness Assessment — Mid-Market Technology Company

Interpretation: 48% readiness score indicates significant gaps. Priority remediation: Documentation & Evidence (CRITICAL), then Regulatory Analysis and Engineering Architecture (HIGH). Estimated 12-month programme to reach 80%+ readiness.

3. Continuous Readiness

Point-in-time assessment is necessary at programme start but insufficient for ongoing governance. Once RUNTIME and EVIDENCE are deployed, readiness becomes continuously measured: each dimension score is derived from real-time telemetry rather than periodic manual assessment. Regulatory Analysis score updates when new requirements are added to the CODIFY catalogue. Engineering Architecture score updates from pipeline telemetry. Documentation score updates from evidence chain completeness metrics. This transforms READINESS from a diagnostic tool into a governance dashboard.

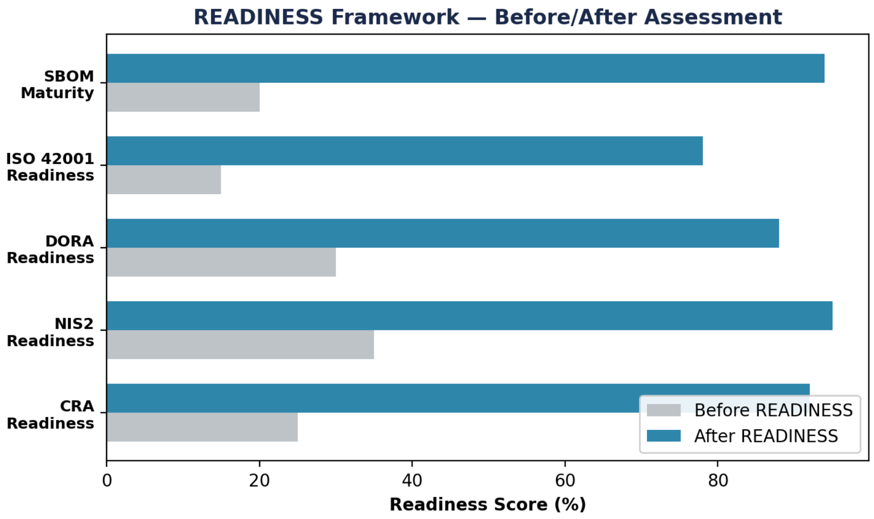

Figure: Readiness Assessment — Before/After

4. Regulatory Exposure Index

For each regulation in scope, READINESS computes a Regulatory Exposure Index: REI = (1 - Coverage_Score) x Maximum_Penalty x Enforcement_Probability. This quantifies the financial exposure from non-compliance in board-relevant terms. Example: CRA with 65% coverage, EUR 15M max penalty, 8% estimated enforcement probability = REI of EUR 420K. Aggregate REI across CRA + NIS2 + DORA provides total regulatory exposure for board reporting.

5. 12-Month Roadmap

Phase 1 Foundation (months 1-3): control catalogue, regulatory mapping, gap analysis, initial readiness score. Phase 2 Infrastructure (months 4-6): proof chain deployment, CI/CD integration, SBOM automation. Phase 3 Governance (months 7-9): board reporting, third-party risk, KPI instrumentation. Phase 4 Optimisation (months 10-12): maturity assessment, continuous readiness activation, M&A; readiness pack.

6. Case Studies

ILLUSTRATIVE SCENARIO: Mid-market technology company (no prior formal compliance programme). Initial readiness score: 2.40/5.00 (48%). After 12-month programme: 4.35/5.00 (87%). 127 of 204 requirements had gaps at baseline; 89% of high-severity gaps closed within 6 months. Full CRA readiness achieved 9 months before December 2027 deadline. Continuous readiness activated in month 9, replacing quarterly manual assessment.

7. Limitations

Readiness scoring weights are based on regulatory enforcement patterns through March 2026 and may shift. Regulatory Exposure Index uses estimated enforcement probabilities that are inherently uncertain. Point-in-time assessment accuracy depends on honest self-assessment or independent verification. The 12-month roadmap assumes adequate resourcing; understaffed organisations may require 18-24 months.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect 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.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management.

Professional Memberships & Affiliations

- 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 | linkedin.com/in/kieranupadrasta

References

1. Regulation (EU) 2024/2847 (CRA).

2. Directive (EU) 2022/2555 (NIS2).

3. Regulation (EU) 2022/2554 (DORA).

4. Regulation (EU) 2024/1689 (EU AI Act).

5. ISO/IEC 42001:2023.

6. NIST CSF 2.0, Feb 2024.

7. NIST FIPS 204 (ML-DSA).

8. MITRE ATT&CK; v15.

9. OWASP ASI Top 10, 2025.

10. ISO/IEC 27001:2022.

11. ENISA Threat Landscape 2025.

12. OPA/Rego Documentation.

WHITEPAPER | ELITE EDITION

The Regulatory Readiness Playbook

Turning CRA and NIS2 into Engineering Control

The READINESS Framework: Formal Scoring Model and Continuous Assessment

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
27 Years' Cyber Security Experience | Big 4 Consulting (Deloitte, PwC, EY, KPMG)
21 Years Financial Services | AI Cyber Security Programme Lead
Professor of Practice (Cybersecurity, AI & Quantum Computing), Schiphol University
Honorary Senior Lecturer, Imperials | UCL Researcher

www.kie.ie | info@kieranupadrasta.com | March 2026

Table of Contents

> **UNIQUE CONTRIBUTION: READINESS provides a weighted scoring rubric, sample assessment output, Regulatory Exposure Index, and Continuous Readiness concept.**

CONFORM System Position: This paper (WP10) extends the CONFORM master theory (WP01) for formal scoring model and continuous assessment. See WP01 for foundational methodology.

Executive Summary

READINESS is the assessment and planning layer of the CONFORM System. v10.0 adds the formal scoring model with weights, a sample assessment output, and the Continuous Readiness concept linking point-in-time assessment to ongoing monitoring.

1. Formal Readiness Scoring Model

Readiness Score = sum of (Dimension_Weight x Implementation_Level) across six dimensions. Each dimension is scored 1-5 with defined criteria:

Dimension	Weight	Score 1 (Gap)	Score 3 (Partial)	Score 5 (Met)
Regulatory Analysis	20%	No requirement mapping exists	Partial mapping; gaps unquantified	Complete 204-req catalogue mapped
Engineering Architecture	25%	No CI/CD pipeline; manual deployment	Basic pipeline; no security gates	Full pipeline with automated gates
Documentation & Evidence	20%	No evidence infrastructure	Manual evidence; incomplete records	Cryptographic evidence chains
Integration & Automation	15%	No policy-as-code; manual controls	Partial automation; some OPA policies	Full CODIFY deployment
Normative Assessment	10%	No maturity model; ad hoc processes	Informal maturity; basic metrics	Instrumented maturity (L3+)
Executive Governance	10%	No board reporting; no oversight	Annual reporting; limited oversight	Quarterly + real-time with signed records

Table 1: Readiness Scoring Rubric — Six Dimensions with Weighted Criteria

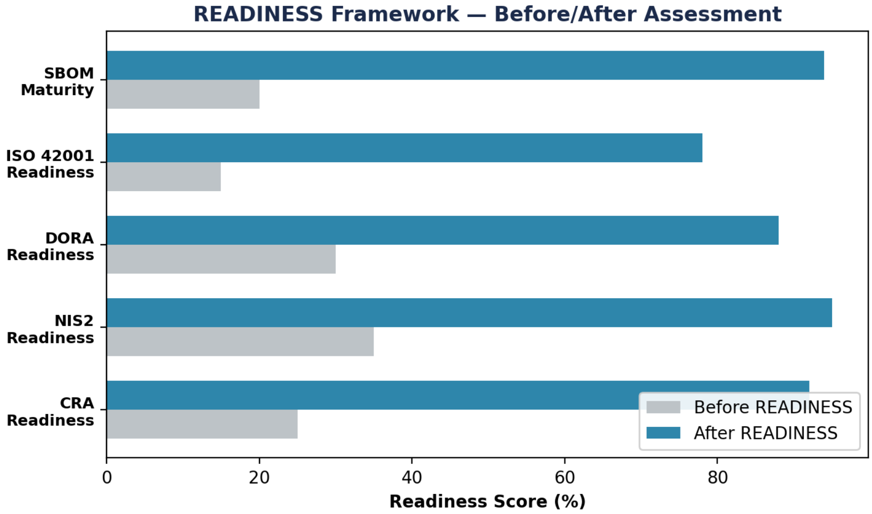

Figure: Readiness Assessment — Before/After

2. Sample Assessment Output

The following illustrates a completed readiness assessment for a mid-market technology company:

Dimension	Score	Weight	Weighted	Priority
Regulatory Analysis	2.5	20%	0.50	HIGH — gaps in DORA mapping
Engineering Architecture	3.0	25%	0.75	HIGH — no security gates
Documentation & Evidence	1.5	20%	0.30	CRITICAL — no evidence chain
Integration & Automation	2.0	15%	0.30	HIGH — manual controls
Normative Assessment	3.5	10%	0.35	MEDIUM — informal maturity
Executive Governance	2.0	10%	0.20	HIGH — annual reporting only
TOTAL READINESS SCORE	—	100%	2.40 / 5.00	48% — significant gaps

Table 2: Sample Readiness Assessment — Mid-Market Technology Company

Interpretation: 48% readiness score indicates significant gaps. Priority remediation: Documentation & Evidence (CRITICAL), then Regulatory Analysis and Engineering Architecture (HIGH). Estimated 12-month programme to reach 80%+ readiness.

3. Continuous Readiness

Point-in-time assessment is necessary at programme start but insufficient for ongoing governance. Once RUNTIME and EVIDENCE are deployed, readiness becomes continuously measured: each dimension score is derived from real-time telemetry rather than periodic manual assessment. Regulatory Analysis score updates when new requirements are added to the CODIFY catalogue. Engineering Architecture score updates from pipeline telemetry. Documentation score updates from evidence chain completeness metrics. This transforms READINESS from a diagnostic tool into a governance dashboard.

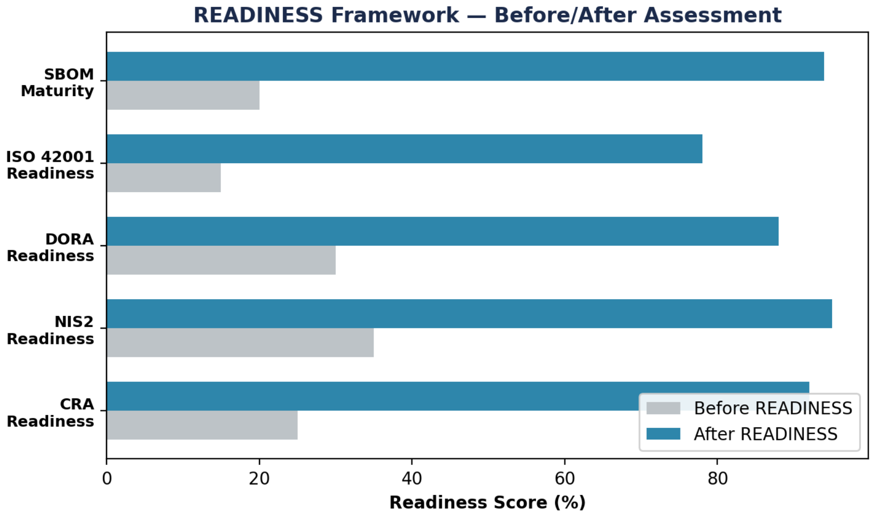

Figure: Readiness Assessment — Before/After

4. Regulatory Exposure Index

For each regulation in scope, READINESS computes a Regulatory Exposure Index: REI = (1 - Coverage_Score) x Maximum_Penalty x Enforcement_Probability. This quantifies the financial exposure from non-compliance in board-relevant terms. Example: CRA with 65% coverage, EUR 15M max penalty, 8% estimated enforcement probability = REI of EUR 420K. Aggregate REI across CRA + NIS2 + DORA provides total regulatory exposure for board reporting.

5. 12-Month Roadmap

Phase 1 Foundation (months 1-3): control catalogue, regulatory mapping, gap analysis, initial readiness score. Phase 2 Infrastructure (months 4-6): proof chain deployment, CI/CD integration, SBOM automation. Phase 3 Governance (months 7-9): board reporting, third-party risk, KPI instrumentation. Phase 4 Optimisation (months 10-12): maturity assessment, continuous readiness activation, M&A; readiness pack.

6. Case Studies

ILLUSTRATIVE SCENARIO: Mid-market technology company (no prior formal compliance programme). Initial readiness score: 2.40/5.00 (48%). After 12-month programme: 4.35/5.00 (87%). 127 of 204 requirements had gaps at baseline; 89% of high-severity gaps closed within 6 months. Full CRA readiness achieved 9 months before December 2027 deadline. Continuous readiness activated in month 9, replacing quarterly manual assessment.

7. Limitations

Readiness scoring weights are based on regulatory enforcement patterns through March 2026 and may shift. Regulatory Exposure Index uses estimated enforcement probabilities that are inherently uncertain. Point-in-time assessment accuracy depends on honest self-assessment or independent verification. The 12-month roadmap assumes adequate resourcing; understaffed organisations may require 18-24 months.

About the Author

Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a distinguished cyber security architect 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.

Mr. Upadrasta has worked with the largest corporations to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70. His expertise spans business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments, and risk management.

Professional Memberships & Affiliations

- 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 | linkedin.com/in/kieranupadrasta

References

1. Regulation (EU) 2024/2847 (CRA).

2. Directive (EU) 2022/2555 (NIS2).

3. Regulation (EU) 2022/2554 (DORA).

4. Regulation (EU) 2024/1689 (EU AI Act).

5. ISO/IEC 42001:2023.

6. NIST CSF 2.0, Feb 2024.

7. NIST FIPS 204 (ML-DSA).

8. MITRE ATT&CK; v15.

9. OWASP ASI Top 10, 2025.

10. ISO/IEC 27001:2022.

11. ENISA Threat Landscape 2025.

12. OPA/Rego Documentation.