WHITEPAPER | ELITE EDITION

Institutionalising Product Security

The Operating Model for CRA, NIS2 and Audit-Ready Delivery

The INSTITUTE Framework: Cryptographic Accountability for Enterprise Governance

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: INSTITUTE makes governance accountability cryptographically provable through signed governance action records and dynamic escalation triggers.**

CONFORM System Position: This paper (WP05) extends the CONFORM master theory (WP01) for cryptographic accountability for enterprise governance. See WP01 for foundational methodology.

Executive Summary

INSTITUTE is the organisational architecture layer of the CONFORM System. Its unique upgrade in v10.0: every governance action is now cryptographically signed and enters the AUDIT-PROOF evidence chain, making accountability provable — not just documented.

1. The Institutional Gap

Most organisations treat product security as a project with an end date. CRA, NIS2, and DORA require ongoing compliance — a permanent institutional capability. INSTITUTE reframes security governance as an institution: permanent roles, defined processes, clear accountability chains, and measurable maturity.

2. Cryptographic Accountability Model

Every governance action — approval, escalation, override, delegation — generates a signed record that enters the evidence chain. This makes accountability cryptographically provable.

Field	Type	Example	Purpose
action_id	UUID	gov-2026-0128	Unique governance event
actor_id	String	ciso@org.com	Accountable individual
role	Enum	CISO | ARCHITECT | BOARD_MEMBER	RACI role classification
action_type	Enum	APPROVE | ESCALATE | OVERRIDE | DELEGATE	Governance action taken
linked_control	String	CRA-13.6-03	Related regulatory control
risk_score	Float	42.5	Risk context at decision time
timestamp	RFC 3339	2026-03-28T09:15:00Z	Immutable action time
payload_hash	BLAKE3	blake3:8f3a...d2c1	Content integrity hash
signature	Ed25519	ed25519:Qw7R...Ab==	Accountability signature

Table 1: Governance Action Record — Cryptographic Accountability Schema

3. Dynamic Governance Engine

Governance is event-driven, not calendar-driven. Automated triggers escalate decisions based on risk thresholds, regulatory deadlines, and control status changes.

Trigger Condition	Threshold	Automated Action	Escalation Target
Risk score exceeds tolerance	Risk > 50	Block deployment; alert CISO	CISO within 1 hour
Critical vulnerability unpatched	> 48h past SLA	Escalate to Design Authority	DA Chair within 4h
Board reporting metric RED	Any KPI in RED for > 7 days	Generate board alert package	Board Committee within 24h
Third-party risk rating change	Provider drops below threshold	Suspend provider access; alert	CISO + Legal within 4h
Regulatory deadline approaching	< 90 days to enforcement date	Activate readiness programme	Programme Director immediate

Table 2: Dynamic Governance Triggers — Automated Escalation Rules

4. Instrumented Maturity Model

Maturity levels are defined by quantitative KPIs derived from pipeline telemetry (RUNTIME) and evidence chain data (AUDIT-PROOF), not subjective assessment.

Maturity Level	% Controls Automated	Mean Time to Evidence	% Decisions Signed	Board Reporting
L1 Ad Hoc	< 10%	> 30 days	0%	Annual or none
L2 Informal	10-30%	14-30 days	< 25%	Semi-annual
L3 Defined	30-60%	3-14 days	50-75%	Quarterly
L4 Integrated	60-85%	4-72 hours	75-95%	Monthly + alerts
L5 Optimised	> 85%	< 4 hours	> 95%	Real-time dashboard

Table 3: Instrumented Maturity Model — Quantitative Progression Criteria

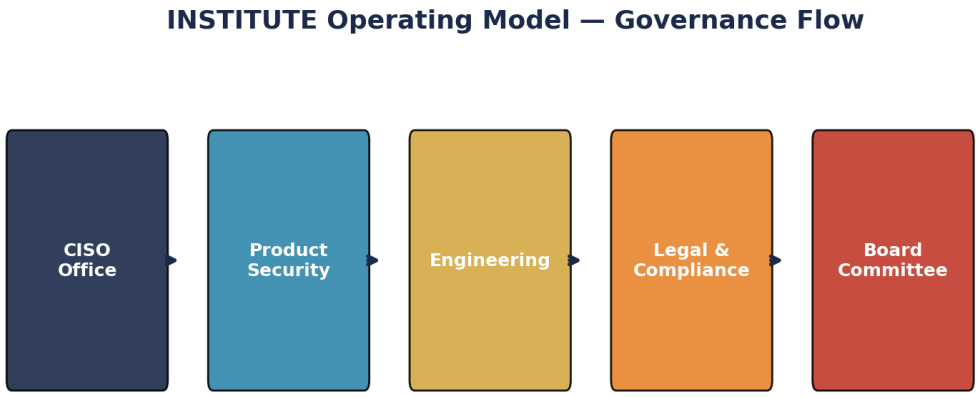

Figure: Operating Model Governance Flow

5. Operating Model Architecture

Five governance levels: Board Committee (strategic oversight, liability management), CISO Office (policy, standards, risk tolerance), Product Security Team (framework implementation, evidence chain management), Engineering Teams (control execution, pipeline compliance), Legal/Compliance (regulatory interpretation, incident notification). Each level has RACI responsibilities for every CRA, NIS2, and DORA requirement.

6. Cultural Change Programme

Security champions network (target: 1 per 30 engineers), developer security training aligned to CRA essential requirements, gamified compliance metrics with team leaderboards, executive security briefings quarterly. Cultural metrics: security awareness score (target >85%), developer engagement rate (target >60%), time-to-report for vulnerabilities (target <24h).

7. Case Studies

ILLUSTRATIVE SCENARIO: Global technology company (4,000 engineers, 8 product lines). 18-month INSTITUTE deployment: maturity Level 1 to Level 3, 65% fewer critical vulnerabilities, 120-engineer champion network, board reporting from annual to quarterly with real-time alerts. All governance actions cryptographically signed from month 6 onwards.

8. Limitations

Organisational change requires 12-18 months for meaningful maturity advancement. Cultural metrics are context-dependent. Cryptographic accountability requires HSM infrastructure. Dynamic governance triggers need calibration per organisation to avoid alert fatigue. This paper addresses organisational model only; technical enforcement is in WP02 (RUNTIME).

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

Institutionalising Product Security

The Operating Model for CRA, NIS2 and Audit-Ready Delivery

The INSTITUTE Framework: Cryptographic Accountability for Enterprise Governance

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: INSTITUTE makes governance accountability cryptographically provable through signed governance action records and dynamic escalation triggers.**

CONFORM System Position: This paper (WP05) extends the CONFORM master theory (WP01) for cryptographic accountability for enterprise governance. See WP01 for foundational methodology.

Executive Summary

INSTITUTE is the organisational architecture layer of the CONFORM System. Its unique upgrade in v10.0: every governance action is now cryptographically signed and enters the AUDIT-PROOF evidence chain, making accountability provable — not just documented.

1. The Institutional Gap

Most organisations treat product security as a project with an end date. CRA, NIS2, and DORA require ongoing compliance — a permanent institutional capability. INSTITUTE reframes security governance as an institution: permanent roles, defined processes, clear accountability chains, and measurable maturity.

2. Cryptographic Accountability Model

Every governance action — approval, escalation, override, delegation — generates a signed record that enters the evidence chain. This makes accountability cryptographically provable.

Field	Type	Example	Purpose
action_id	UUID	gov-2026-0128	Unique governance event
actor_id	String	ciso@org.com	Accountable individual
role	Enum	CISO | ARCHITECT | BOARD_MEMBER	RACI role classification
action_type	Enum	APPROVE | ESCALATE | OVERRIDE | DELEGATE	Governance action taken
linked_control	String	CRA-13.6-03	Related regulatory control
risk_score	Float	42.5	Risk context at decision time
timestamp	RFC 3339	2026-03-28T09:15:00Z	Immutable action time
payload_hash	BLAKE3	blake3:8f3a...d2c1	Content integrity hash
signature	Ed25519	ed25519:Qw7R...Ab==	Accountability signature

Table 1: Governance Action Record — Cryptographic Accountability Schema

3. Dynamic Governance Engine

Governance is event-driven, not calendar-driven. Automated triggers escalate decisions based on risk thresholds, regulatory deadlines, and control status changes.

Trigger Condition	Threshold	Automated Action	Escalation Target
Risk score exceeds tolerance	Risk > 50	Block deployment; alert CISO	CISO within 1 hour
Critical vulnerability unpatched	> 48h past SLA	Escalate to Design Authority	DA Chair within 4h
Board reporting metric RED	Any KPI in RED for > 7 days	Generate board alert package	Board Committee within 24h
Third-party risk rating change	Provider drops below threshold	Suspend provider access; alert	CISO + Legal within 4h
Regulatory deadline approaching	< 90 days to enforcement date	Activate readiness programme	Programme Director immediate

Table 2: Dynamic Governance Triggers — Automated Escalation Rules

4. Instrumented Maturity Model

Maturity levels are defined by quantitative KPIs derived from pipeline telemetry (RUNTIME) and evidence chain data (AUDIT-PROOF), not subjective assessment.

Maturity Level	% Controls Automated	Mean Time to Evidence	% Decisions Signed	Board Reporting
L1 Ad Hoc	< 10%	> 30 days	0%	Annual or none
L2 Informal	10-30%	14-30 days	< 25%	Semi-annual
L3 Defined	30-60%	3-14 days	50-75%	Quarterly
L4 Integrated	60-85%	4-72 hours	75-95%	Monthly + alerts
L5 Optimised	> 85%	< 4 hours	> 95%	Real-time dashboard

Table 3: Instrumented Maturity Model — Quantitative Progression Criteria

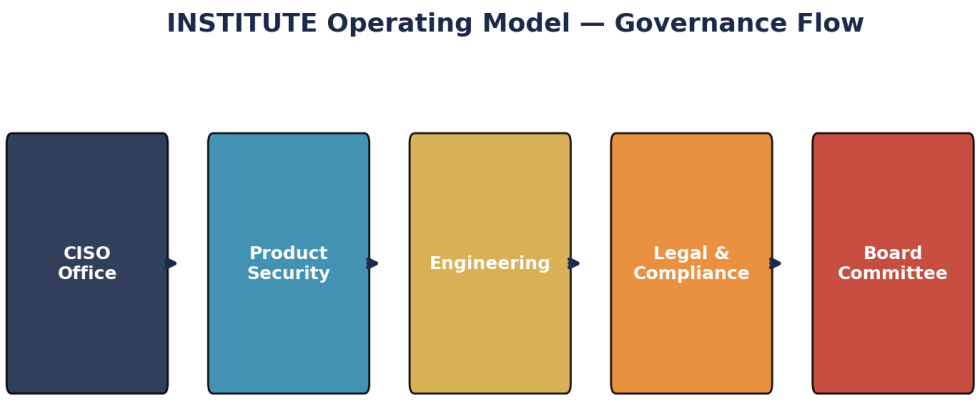

Figure: Operating Model Governance Flow

5. Operating Model Architecture

Five governance levels: Board Committee (strategic oversight, liability management), CISO Office (policy, standards, risk tolerance), Product Security Team (framework implementation, evidence chain management), Engineering Teams (control execution, pipeline compliance), Legal/Compliance (regulatory interpretation, incident notification). Each level has RACI responsibilities for every CRA, NIS2, and DORA requirement.

6. Cultural Change Programme

Security champions network (target: 1 per 30 engineers), developer security training aligned to CRA essential requirements, gamified compliance metrics with team leaderboards, executive security briefings quarterly. Cultural metrics: security awareness score (target >85%), developer engagement rate (target >60%), time-to-report for vulnerabilities (target <24h).

7. Case Studies

ILLUSTRATIVE SCENARIO: Global technology company (4,000 engineers, 8 product lines). 18-month INSTITUTE deployment: maturity Level 1 to Level 3, 65% fewer critical vulnerabilities, 120-engineer champion network, board reporting from annual to quarterly with real-time alerts. All governance actions cryptographically signed from month 6 onwards.

8. Limitations

Organisational change requires 12-18 months for meaningful maturity advancement. Cultural metrics are context-dependent. Cryptographic accountability requires HSM infrastructure. Dynamic governance triggers need calibration per organisation to avoid alert fatigue. This paper addresses organisational model only; technical enforcement is in WP02 (RUNTIME).

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.