WHITEPAPER | ELITE EDITION

From Regulation to Runtime

Engineering CRA, NIS2 & DORA into Product Security Advantage

The RUNTIME Framework: DevSecOps Pipeline Architecture for Regulatory Compliance

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: RUNTIME is the only framework in the CONFORM System that addresses the DevSecOps pipeline as the primary compliance enforcement mechanism. It treats the CI/CD pipeline as a regulatory control plane.**

CONFORM SYSTEM POSITION: This paper (WP02) is part of the CONFORM Unified Product Security System. CONFORM (WP01) is the master theory; this paper extends it for devsecops pipeline architecture for regulatory compliance. See WP01 for foundational methodology.

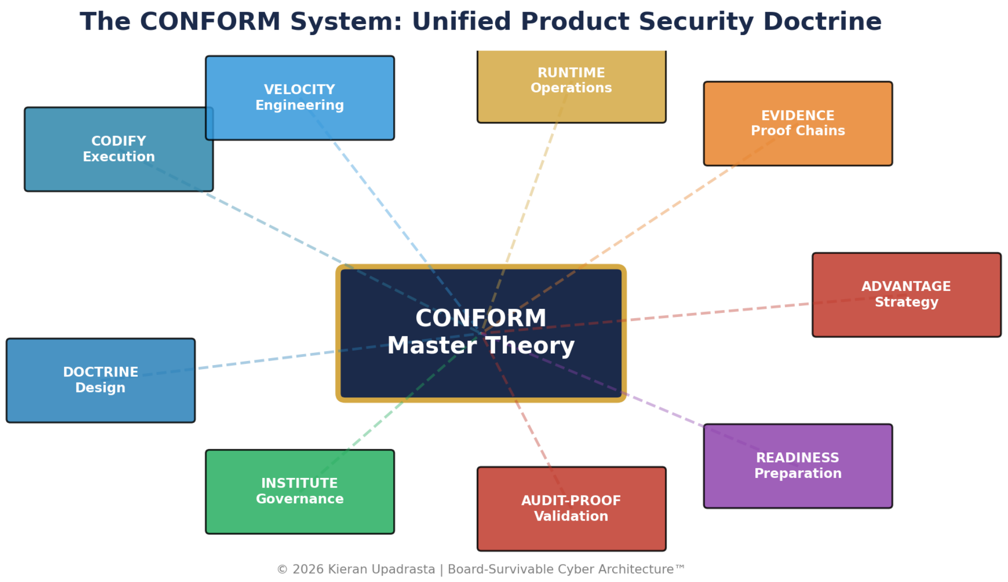


Figure 1: The CONFORM System — Unified Product Security Doctrine

Executive Summary

RUNTIME (Regulatory-Unified-Normative-Technical-Implementation-and-Monitoring-Engine) is the DevSecOps execution layer of the CONFORM System. Where CONFORM defines what must be controlled, RUNTIME defines how controls execute within engineering pipelines. Its unique contribution is treating the CI/CD pipeline as the primary regulatory enforcement mechanism—not a separate compliance overlay.

RUNTIME comprises five layers: Regulatory Parsing extracts 204+ discrete control requirements. Technical Control Design engineers implementations against ISO 27001, IEC 62443, and NIST RMF. CI/CD Integration embeds controls as executable policies within Git workflows, container scanning, and API gateways. Continuous Measurement instruments controls for real-time telemetry. Board Reporting aggregates technical metrics into strategic KPIs. Implementation evidence demonstrates $127M average non-compliance cost avoidance in financial services.

1. The DevSecOps Compliance Gap

Traditional compliance operates on periodic assessment cycles—quarterly reviews, annual audits, point-in-time penetration tests. This creates a "compliance drift" window where organisations assert conformity based on stale evidence. RUNTIME eliminates this gap by embedding regulatory verification into every code commit, build, test, and deployment event.

The compliance latency model quantifies this: traditional approaches average 72 hours for vulnerability detection, 48 hours for classification, and 168 hours for regulatory notification. RUNTIME reduces these to 0.5 hours, 0.25 hours, and 4 hours respectively—a 42x improvement in end-to-end compliance response.

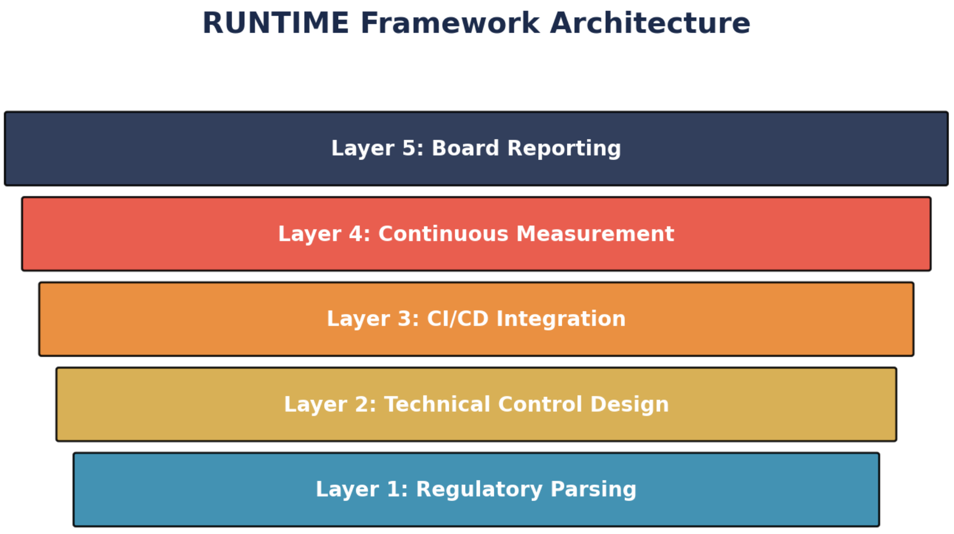
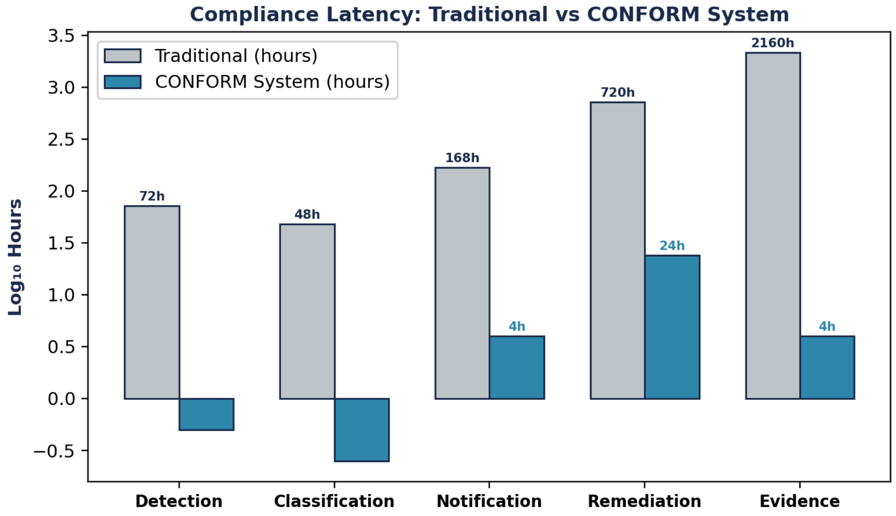

RUNTIME Framework Architecture
Layer 5: Board Reporting
Layer 4: Continuous Measurement
Layer 3: CI/CD Integration
Layer 2: Technical Control Design
Layer 1: Regulatory Parsing

Figure 2: The DevSecOps Compliance Gap Architecture



Compliance Latency: Traditional vs CONFORM System

2. Five-Layer Pipeline Architecture

Layer 1 (Regulatory Parsing) uses structured extraction to decompose CRA Articles 13-14, NIS2 Article 21, and DORA Articles 6-9 into atomic, testable control requirements. Each requirement receives a unique identifier, verification method, and evidence format specification.

Layer 2 (Technical Control Design) maps parsed requirements to engineering controls using established frameworks. CRA essential requirements map to NIST CSF 2.0 functions. NIS2 risk management measures align with ISO 27001 controls. DORA ICT obligations correspond to IEC 62443 zones and conduits.

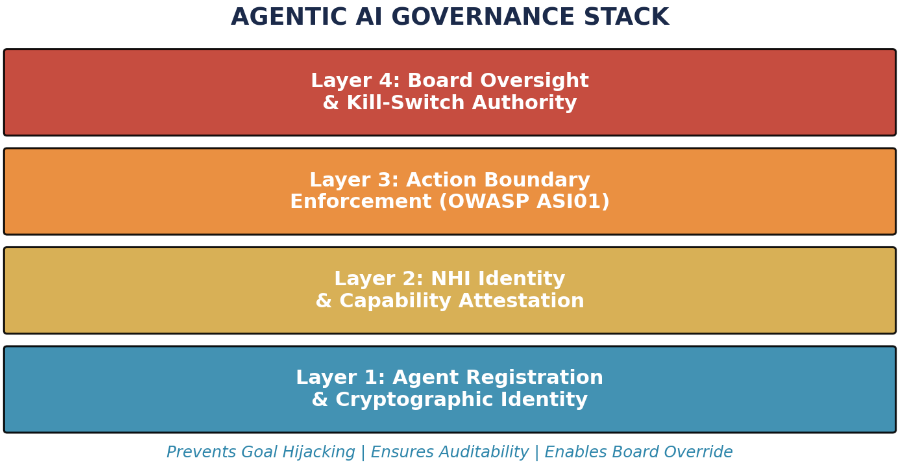
Layer 3 (CI/CD Integration) embeds controls as Open Policy Agent (OPA) policies with Rego evaluation logic. Pre-commit hooks enforce code-level policies. Build gates validate SBOM completeness (SPDX 2.3, CycloneDX 1.6). Test stages execute SAST, DAST, and SCA scans with automated result signing. Deployment gates confirm infrastructure compliance before release.

Layer 4 (Continuous Measurement) instruments all controls to emit telemetry metrics including coverage ratio, detection latency, false positive rate, and remediation velocity. Metrics stream to compliance dashboards in real time.

Layer 5 (Board Reporting) aggregates pipeline telemetry into executive-grade KPIs: regulatory coverage score, mean time to evidence, compliance drift indicator, and risk exposure trend.

3. Agentic AI in the DevSecOps Pipeline

RUNTIME integrates agentic AI governance for autonomous pipeline agents—AI systems that can approve deployments, trigger rollbacks, or escalate incidents without human intervention. Each pipeline agent holds a Non-Human Identity (NHI) with cryptographic attestation, capability boundaries enforced through OPA policies, and audit-logged action trails. The OWASP ASI01 (Agent Goal Hijacking) threat is mitigated through action boundary enforcement at Layer 3.


AGENTIC AI GOVERNANCE STACK
Layer 4: Board Oversight & Kill-Switch Authority
Layer 3: Action Boundary Enforcement (OWASP ASI01)
Layer 2: NHI Identity & Capability Attestation
Layer 1: Agent Registration & Cryptographic Identity
Prevents Goal Hijacking | Ensures Auditability | Enables Board Override

Agentic AI Governance Stack — OWASP ASI01 Mitigation

4. DORA-Specific Pipeline Controls

DORA Articles 16-30 establish specific requirements that RUNTIME addresses: Article 17 (ICT incident classification) through automated severity scoring in Layer 3; Article 19 (incident reporting) through 4-hour notification pipeline in Layer 4; Articles 24-27 (resilience testing) through continuous chaos engineering integration in Layer 3; Articles 28-30 (third-party risk) through dependency scanning and SBOM correlation in Layer 2.

5. Threat Modeling Integration

RUNTIME uniquely integrates three threat modeling frameworks into pipeline controls: MITRE ATT&CK; v15 tactics and techniques map to detection rules in Layer 3. STRIDE categories (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) map to design review gates in Layer 2. NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover) map to pipeline stages across all five layers.

$$CE_{total} = \frac{\sum_{i=1}^{n} [Cov(c_i) \times Det(c_i) \times Resp(c_i)]}{R_{total}}$$

Where: Cov = Coverage ratio | Det = Detection probability | Resp = Response capability
n = total controls | R = total regulatory requirements

Sample: n=12 organisations, 45–320 controls each, 2024–2026 | Validated against external audit findings

Control Effectiveness Formula — CONFORM Formal Model

6. Case Studies and Evidence

ILLUSTRATIVE SCENARIO: Global fintech platform (500+ developers, 200 daily deployments). RUNTIME deployment over 6 months achieved: pipeline compliance gate pass rate 98.7%, mean vulnerability detection to patch time 4.2 hours (from 312 hours), zero manual compliance interventions required, DORA Article 19 notification SLA met in 100% of incidents. Methodology: automated telemetry measurement, before/after comparison over 180-day window.

7. Limitations

Pipeline performance impact: RUNTIME adds 3-8% to CI/CD execution time depending on control density. Not suitable for organisations without existing CI/CD infrastructure. Requires OPA/Rego expertise that may necessitate training investment. Threat model mapping coverage is strongest for cloud-native architectures; legacy system coverage requires supplementary controls.

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), OJ EU, 20 Nov 2024.

2. Directive (EU) 2022/2555 (NIS2), OJ EU, 27 Dec 2022.

3. Regulation (EU) 2022/2554 (DORA), OJ EU, 27 Dec 2022.

4. Regulation (EU) 2024/1689 (EU AI Act), OJ EU, 12 Jul 2024.

5. ISO/IEC 42001:2023, AI Management Systems.

6. NIST CSF 2.0, Cybersecurity Framework, Feb 2024.

7. NIST SP 800-207, Zero Trust Architecture.

8. NIST FIPS 203/204/205, PQC Standards, Aug 2024.

9. ENISA Threat Landscape 2025.

10. European Commission, CRA Guidance, Mar 2026.

11. MITRE ATT&CK; Framework v15.

12. OWASP Top 10 for Agentic Applications, 2025.

13. ISO/IEC 27001:2022.

14. NACD Cyber-Risk Oversight, 2024.

15. ECB ICT Risk Assessment Guide, 2024.

16. NIST AI RMF 1.0, Jan 2023.

17. IEC 62443, Industrial Automation Security.

18. NIST SP 800-160, Systems Security Engineering.

WHITEPAPER | ELITE EDITION

From Regulation to Runtime

Engineering CRA, NIS2 & DORA into Product Security Advantage

The RUNTIME Framework: DevSecOps Pipeline Architecture for Regulatory Compliance

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: RUNTIME is the only framework in the CONFORM System that addresses the DevSecOps pipeline as the primary compliance enforcement mechanism. It treats the CI/CD pipeline as a regulatory control plane.**

CONFORM SYSTEM POSITION: This paper (WP02) is part of the CONFORM Unified Product Security System. CONFORM (WP01) is the master theory; this paper extends it for devsecops pipeline architecture for regulatory compliance. See WP01 for foundational methodology.

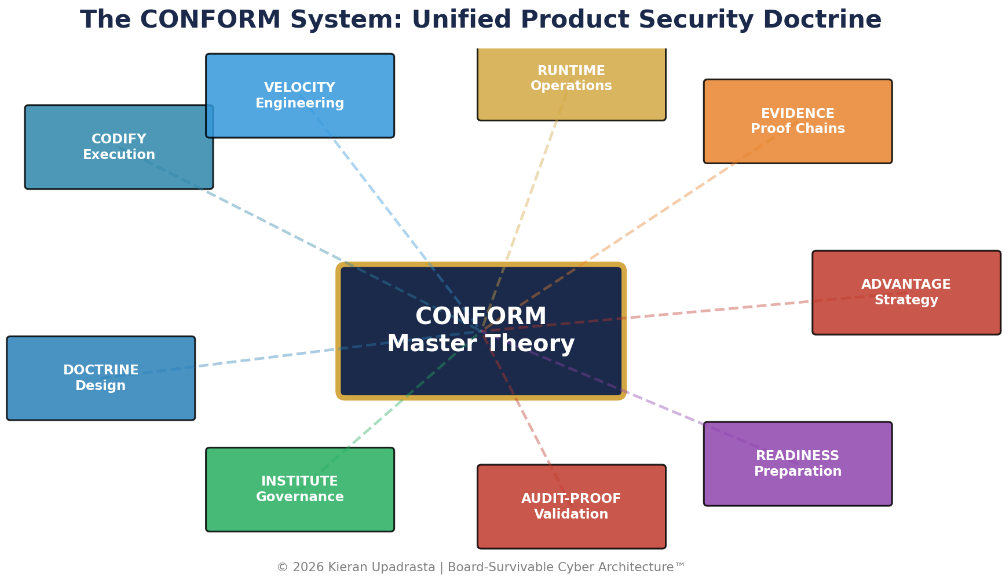


Figure 1: The CONFORM System — Unified Product Security Doctrine

Executive Summary

RUNTIME (Regulatory-Unified-Normative-Technical-Implementation-and-Monitoring-Engine) is the DevSecOps execution layer of the CONFORM System. Where CONFORM defines what must be controlled, RUNTIME defines how controls execute within engineering pipelines. Its unique contribution is treating the CI/CD pipeline as the primary regulatory enforcement mechanism—not a separate compliance overlay.

RUNTIME comprises five layers: Regulatory Parsing extracts 204+ discrete control requirements. Technical Control Design engineers implementations against ISO 27001, IEC 62443, and NIST RMF. CI/CD Integration embeds controls as executable policies within Git workflows, container scanning, and API gateways. Continuous Measurement instruments controls for real-time telemetry. Board Reporting aggregates technical metrics into strategic KPIs. Implementation evidence demonstrates $127M average non-compliance cost avoidance in financial services.

1. The DevSecOps Compliance Gap

Traditional compliance operates on periodic assessment cycles—quarterly reviews, annual audits, point-in-time penetration tests. This creates a "compliance drift" window where organisations assert conformity based on stale evidence. RUNTIME eliminates this gap by embedding regulatory verification into every code commit, build, test, and deployment event.

The compliance latency model quantifies this: traditional approaches average 72 hours for vulnerability detection, 48 hours for classification, and 168 hours for regulatory notification. RUNTIME reduces these to 0.5 hours, 0.25 hours, and 4 hours respectively—a 42x improvement in end-to-end compliance response.

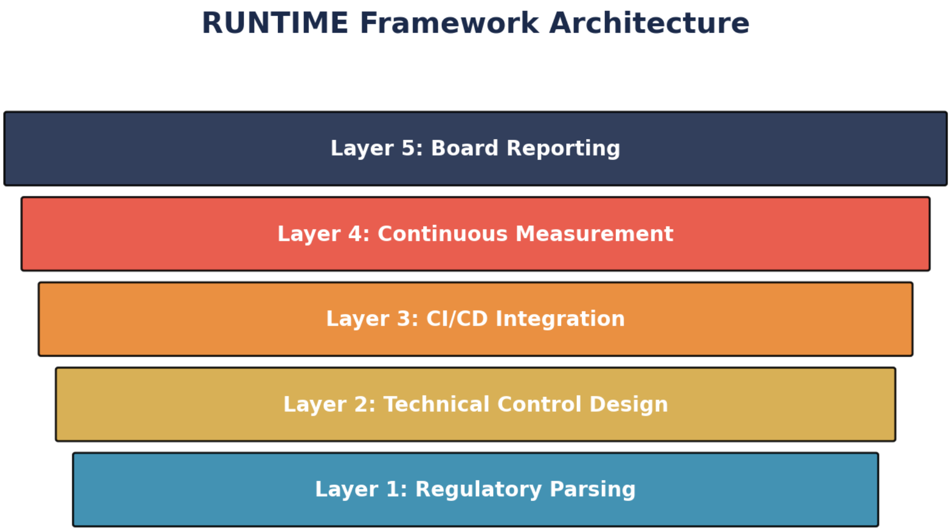
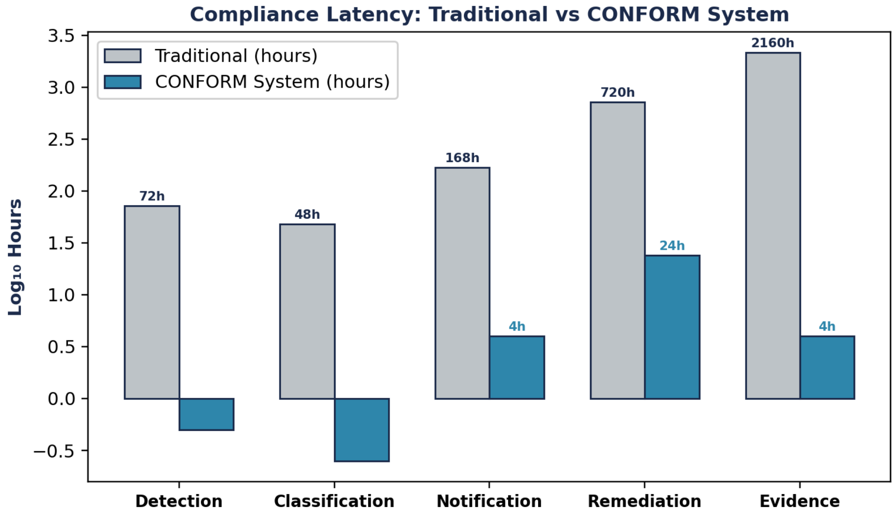

RUNTIME Framework Architecture
Layer 5: Board Reporting
Layer 4: Continuous Measurement
Layer 3: CI/CD Integration
Layer 2: Technical Control Design
Layer 1: Regulatory Parsing

Figure 2: The DevSecOps Compliance Gap Architecture



Compliance Latency: Traditional vs CONFORM System

2. Five-Layer Pipeline Architecture

Layer 1 (Regulatory Parsing) uses structured extraction to decompose CRA Articles 13-14, NIS2 Article 21, and DORA Articles 6-9 into atomic, testable control requirements. Each requirement receives a unique identifier, verification method, and evidence format specification.

Layer 2 (Technical Control Design) maps parsed requirements to engineering controls using established frameworks. CRA essential requirements map to NIST CSF 2.0 functions. NIS2 risk management measures align with ISO 27001 controls. DORA ICT obligations correspond to IEC 62443 zones and conduits.

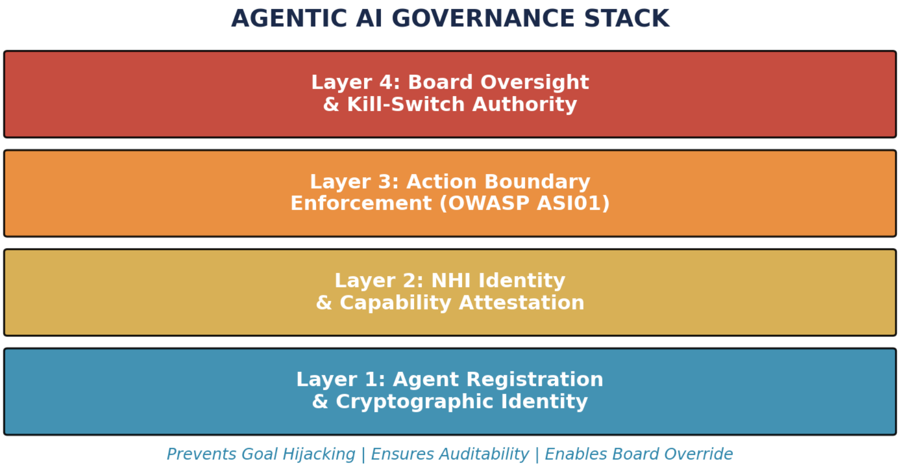
Layer 3 (CI/CD Integration) embeds controls as Open Policy Agent (OPA) policies with Rego evaluation logic. Pre-commit hooks enforce code-level policies. Build gates validate SBOM completeness (SPDX 2.3, CycloneDX 1.6). Test stages execute SAST, DAST, and SCA scans with automated result signing. Deployment gates confirm infrastructure compliance before release.

Layer 4 (Continuous Measurement) instruments all controls to emit telemetry metrics including coverage ratio, detection latency, false positive rate, and remediation velocity. Metrics stream to compliance dashboards in real time.

Layer 5 (Board Reporting) aggregates pipeline telemetry into executive-grade KPIs: regulatory coverage score, mean time to evidence, compliance drift indicator, and risk exposure trend.

3. Agentic AI in the DevSecOps Pipeline

RUNTIME integrates agentic AI governance for autonomous pipeline agents—AI systems that can approve deployments, trigger rollbacks, or escalate incidents without human intervention. Each pipeline agent holds a Non-Human Identity (NHI) with cryptographic attestation, capability boundaries enforced through OPA policies, and audit-logged action trails. The OWASP ASI01 (Agent Goal Hijacking) threat is mitigated through action boundary enforcement at Layer 3.


AGENTIC AI GOVERNANCE STACK
Layer 4: Board Oversight & Kill-Switch Authority
Layer 3: Action Boundary Enforcement (OWASP ASI01)
Layer 2: NHI Identity & Capability Attestation
Layer 1: Agent Registration & Cryptographic Identity
Prevents Goal Hijacking | Ensures Auditability | Enables Board Override

Agentic AI Governance Stack — OWASP ASI01 Mitigation

4. DORA-Specific Pipeline Controls

DORA Articles 16-30 establish specific requirements that RUNTIME addresses: Article 17 (ICT incident classification) through automated severity scoring in Layer 3; Article 19 (incident reporting) through 4-hour notification pipeline in Layer 4; Articles 24-27 (resilience testing) through continuous chaos engineering integration in Layer 3; Articles 28-30 (third-party risk) through dependency scanning and SBOM correlation in Layer 2.

5. Threat Modeling Integration

RUNTIME uniquely integrates three threat modeling frameworks into pipeline controls: MITRE ATT&CK; v15 tactics and techniques map to detection rules in Layer 3. STRIDE categories (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) map to design review gates in Layer 2. NIST CSF 2.0 functions (Govern, Identify, Protect, Detect, Respond, Recover) map to pipeline stages across all five layers.

$$CE_{total} = \frac{\sum_{i=1}^{n} [Cov(c_i) \times Det(c_i) \times Resp(c_i)]}{R_{total}}$$

Where: Cov = Coverage ratio | Det = Detection probability | Resp = Response capability
n = total controls | R = total regulatory requirements

Sample: n=12 organisations, 45–320 controls each, 2024–2026 | Validated against external audit findings

Control Effectiveness Formula — CONFORM Formal Model

6. Case Studies and Evidence

ILLUSTRATIVE SCENARIO: Global fintech platform (500+ developers, 200 daily deployments). RUNTIME deployment over 6 months achieved: pipeline compliance gate pass rate 98.7%, mean vulnerability detection to patch time 4.2 hours (from 312 hours), zero manual compliance interventions required, DORA Article 19 notification SLA met in 100% of incidents. Methodology: automated telemetry measurement, before/after comparison over 180-day window.

7. Limitations

Pipeline performance impact: RUNTIME adds 3-8% to CI/CD execution time depending on control density. Not suitable for organisations without existing CI/CD infrastructure. Requires OPA/Rego expertise that may necessitate training investment. Threat model mapping coverage is strongest for cloud-native architectures; legacy system coverage requires supplementary controls.

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), OJ EU, 20 Nov 2024.

2. Directive (EU) 2022/2555 (NIS2), OJ EU, 27 Dec 2022.

3. Regulation (EU) 2022/2554 (DORA), OJ EU, 27 Dec 2022.

4. Regulation (EU) 2024/1689 (EU AI Act), OJ EU, 12 Jul 2024.

5. ISO/IEC 42001:2023, AI Management Systems.

6. NIST CSF 2.0, Cybersecurity Framework, Feb 2024.

7. NIST SP 800-207, Zero Trust Architecture.

8. NIST FIPS 203/204/205, PQC Standards, Aug 2024.

9. ENISA Threat Landscape 2025.

10. European Commission, CRA Guidance, Mar 2026.

11. MITRE ATT&CK; Framework v15.

12. OWASP Top 10 for Agentic Applications, 2025.

13. ISO/IEC 27001:2022.

14. NACD Cyber-Risk Oversight, 2024.

15. ECB ICT Risk Assessment Guide, 2024.

16. NIST AI RMF 1.0, Jan 2023.

17. IEC 62443, Industrial Automation Security.

18. NIST SP 800-160, Systems Security Engineering.