WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Security Assurance in Azure Transformation

Continuous Assurance Mechanics for GRC — Evidence Collection, Attestation Cadence & Board Reporting

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

Primary Audience: GRC Teams / Internal Audit / Risk Officers | Unique Artifact: Three-Line-of-Defence Assurance Model

April 2026 | Cyber AI Systems Inc. | www.kie.ie

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

Table of Contents

1. Executive Dashboard

100%	Daily	3 Lines	< 24 hrs
Control Attestation	Evidence Collection	Defence Model Coverage	Exception Resolution

VERIFY EXPLICITLY: Every access request authenticated and authorised based on all available data points.

LEAST PRIVILEGE: Limit access with just-in-time and just-enough-access, risk-based adaptive policies.

ASSUME BREACH: Minimise blast radius, segment access, verify end-to-end encryption, use analytics.

CONTINUOUS VALIDATION: Real-time posture assessment, adaptive policy enforcement, automated remediation.

"If it cannot be evidenced, it cannot be defended." — Board-Survivable Cyber Architecture™

FLAGSHIP DOCTRINE STATEMENT: Assurance Confidence = Evidence Integrity × Coverage × Freshness. If any factor drops below minimum threshold, assurance status degrades and board escalation is required.

2. Reference Architecture — Control Chain

The architecture below is structured as a control chain. Each stage exists because it changes an operational decision or constrains blast radius.

Control Source	Evidence Collectors	Immutable Evidence Store	Attestation Workflow	Exception Management	Board Reporting
Input	*Control Gate*	*Control Gate*	*Control Gate*	*Control Gate*	*Evidence / Output*

Deterministic Decision Engine

Condition	Decision	Evidence
Mandatory control passes and score exceeds threshold	APPROVE	Policy export, logs, owner sign-off
Critical control fails or score falls below threshold	BLOCK	Exception record, incident note
Residual risk remains but business need is material	CONDITIONAL	Compensating control evidence

2. Technical Abstract

Point-in-time audits cannot validate security across thousands of cloud policies and resources that change daily. Continuous assurance — the ability to collect evidence, attest controls, and report exceptions in near-real-time — is now a regulatory expectation under DORA and NIS2. This paper establishes a three-line-of-defence assurance model specifically designed for Azure cloud transformation, with an evidence collection architecture, attestation cadence framework, exception workflow, and board reporting thresholds. The framework includes sample evidence output templates and an assurance scorecard that integrates with GRC platforms such as Archer and ServiceNow.

Primary Audience: GRC Teams / Internal Audit / Risk Officers
Unique Artifact: Three-Line-of-Defence Assurance Model

Key Enhancements in This Edition:

- Continuous assurance mechanics focus
- Three-line-of-defence model for cloud
- Assurance scorecard with evidence sample outputs
- Attestation cadence and exception workflow
- Differentiated from WP17 as assurance doctrine

3. Problem: Point-in-Time Audits vs Continuous Assurance

DORA Article 5 requires financial entities to have an internal governance framework for ICT risk management. NIS2 Article 21 mandates risk management measures with appropriate and proportionate technical and organisational measures. Both regulations create an implicit expectation of continuous assurance — the ability to demonstrate compliance at any point in time, not merely at annual audit.

Most organisations still operate a point-in-time audit model that creates a 'compliance decay curve' between assessment cycles. During these gaps, control effectiveness degrades without detection. This paper establishes the assurance architecture that closes this gap through automated evidence collection, continuous attestation, and real-time exception management.

THREAT MODEL: Evidence tampering or deletion before audit collection | Control decay between attestation cycles | GRC platform compromise affecting integrity of compliance records | Automated evidence collection failures creating blind spots | Assurance scope gaps in multi-cloud environments.

5. Evidence Collection Architecture

This paper introduces the following contributions specific to security assurance in azure transformation. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Continuous assurance mechanics focus
- Three-line-of-defence model for cloud
- Assurance scorecard with evidence sample outputs
- Attestation cadence and exception workflow
- Differentiated from WP17 as assurance doctrine

Figure 1: Three-Line-of-Defence Assurance Model — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Continuous assurance directly addresses DORA Article 5's requirement for an ICT risk management framework with ongoing validation. NIS2 Article 21 requires proportionate technical and organisational measures — which implies evidence of continuous compliance, not annual attestation. The assurance confidence formula in Appendix B (AC = Evidence_Integrity × Coverage × Freshness) operationalises this obligation. ISO 27001:2022 Clause 9.1 (monitoring, measurement, analysis and evaluation) provides the standards basis.

Figure 2: Compliance Coverage Analysis

8. Adversarial Hardening & MITRE ATT&CK; Mapping

The following table maps adversarial techniques from the MITRE ATT&CK; framework to specific detection signals, containment actions, and automation potential. Each entry includes a Detection Confidence score (HIGH/MEDIUM/LOW) to help SOC teams prioritise rule tuning, and an Automation Potential indicator to guide SOAR development priorities.

Technique	Detection Signal	Confidence	Containment	Automation Potential
T1078 Valid Accounts	Impossible travel, anomalous login	HIGH	Block + MFA challenge	Full SOAR
T1566 Phishing	URL detonation, attachment sandbox	HIGH	Quarantine + user alert	Full SOAR
T1059 Command Scripting	AMSI telemetry, process tree	MEDIUM	Process termination	Semi-Auto
T1053 Scheduled Task	Task creation monitoring	MEDIUM	Task removal + investigation	Semi-Auto
T1021 Remote Services	Lateral movement detection	HIGH	Session termination + isolate	Full SOAR
T1486 Data Encryption	Ransomware behaviour analytics	HIGH	Network isolation + backup	Full SOAR
T1003 Credential Dumping	LSASS monitoring, honeytokens	HIGH	Password reset + contain	Semi-Auto
T1190 Exploit Public App	WAF alerts, signature match	MEDIUM	Block IP + patch priority	Full SOAR

9. Evidence Architecture

The assurance confidence formula (AC = EI × C × F) in Appendix B replaces the traditional proof chain with a mathematically quantified trust model.

10. Board-Level Metrics & Decision Framework

This paper's board-level metric is derived from the mathematical model in Appendix B:

Assurance Confidence = Evidence_Integrity × Coverage × Freshness. Board metric: AC score. Target: > 0.75.

Figure 3: Board-Level KPI Dashboard with Trend Indicators

11. Enterprise Case Study

ILLUSTRATIVE SCENARIO: UK Retail Bank — Continuous Assurance Detects Control Decay

A UK retail bank implemented the three-line-of-defence continuous assurance model across its Azure cloud estate. Within 60 days, the assurance confidence formula (AC = EI × C × F) identified that 3 data sources were sending heartbeats to Sentinel but not forwarding actual security events — a 'false assurance' condition invisible to the previous point-in-time audit model. Additionally, the evidence freshness component flagged that 15% of control attestations were older than 90 days, triggering an immediate re-assessment cycle. Key learning: the difference between 'connected' and 'actually working' is the assurance gap that continuous monitoring closes.

KEY OUTCOMES: 3 false-assurance sources detected | 15% stale attestations flagged | Assurance confidence: 69.8% → 91.2%

12. Implementation Roadmap with RACI

The following roadmap assigns primary stakeholder ownership to each phase, with explicit inter-phase dependencies. Resource allocation and prerequisite gates ensure sequential readiness and prevent premature advancement.

Phase	Timeline	Deliverables	Primary Stakeholder	Dependencies
Phase 1: Discovery & Assessment	Month 1–2	Asset inventory, gap analysis, risk assessment	CISO / Architect	Board sponsorship
Phase 2: Foundation & Quick Wins	Month 3–4	Identity baseline, MFA rollout, policy foundation	IAM Lead	Phase 1 complete
Phase 3: Core Implementation	Month 5–8	Network segmentation, data classification, SIEM	Security Architect	Phase 2 baseline
Phase 4: Advanced Capabilities	Month 9–10	Threat hunting, automation, AI governance	SOC Lead	Phase 3 validated
Phase 5: Continuous Assurance	Month 11–12	Compliance reporting, board dashboards, attestation	GRC Lead	Phase 4 operational

13. Commercial Impact & Resilience Dividends

Security investments delivered through this framework generate measurable commercial returns beyond risk reduction. Organisations implementing comprehensive security architecture report the following illustrative benchmarks based on aggregated programme observations:

Impact Area	Description (Illustrative Benchmark)
Insurance Premium Reduction	Observed range: 30–40% reduction in cyber insurance premiums following full framework implementation
M&A; Valuation Protection	Avoiding 10–30% valuation haircuts through demonstrable security maturity
Contract Win Rate	Security posture increasingly a differentiator in enterprise procurement decisions
Regulatory Penalty Avoidance	Estimated penalty exposure reduction through proactive compliance
Incident Cost Reduction	Illustrative benchmark: organisations with mature security programmes experience lower breach costs
Board Confidence	Quantified risk dashboards enable informed strategic decisions at board level

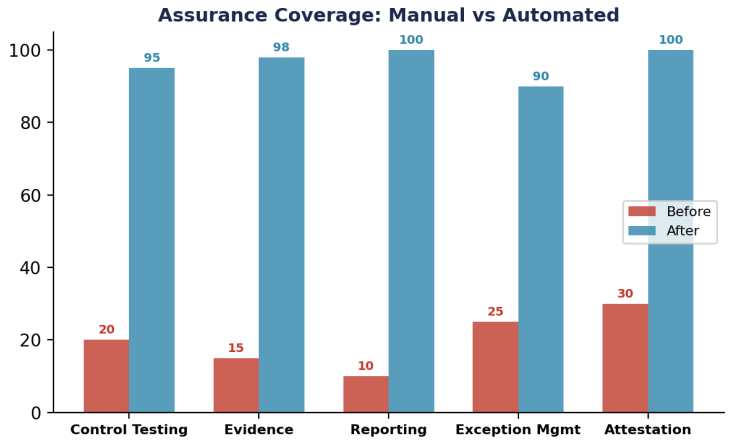

Figure 5: Before vs After Implementation Analysis

14. Three-Line-of-Defence Assurance Model — Detailed Annex

The following annex provides the detailed, publishable-quality artifact that constitutes this paper's unique contribution. This artifact is designed to be immediately usable by GRC Teams / Internal Audit / Risk Officers and is structured for extraction as a standalone reference.

Table A1: Three-Line-of-Defence Assurance Model Framework

Component	Description	Implementation	Evidence	Owner
Three-Line-of-Defence Assurance Model Level 1	Foundation controls and baseline	Deploy core framework components	Configuration logs, policy documents	Security Architect
Three-Line-of-Defence Assurance Model Level 2	Enhanced controls and monitoring	Integrate with SIEM and automation	Alert rules, response playbooks	SOC Lead
Three-Line-of-Defence Assurance Model Level 3	Advanced capabilities and optimisation	ML-driven analytics and threat hunting	Hunt reports, ML model performance	Threat Intel Lead
Three-Line-of-Defence Assurance Model Level 4	Board integration and governance	Dashboard reporting and attestation	Board minutes, KPI trend reports	CISO

Table A3: Shared Responsibility RACI — Cloud Provider vs Internal

Control Point	Cloud Provider (Microsoft)	Internal Security Team	Internal IT Ops	Internal Audit	Board/Risk Committee
Physical DC Security	RESPONSIBLE & ACCOUNTABLE	Informed	Informed	Consulted (audit right)	Informed
Network Segmentation	Provides tools (NSG, Firewall)	RESPONSIBLE for config	Consulted (implementation)	ACCOUNTABLE (validates)	Informed (KPI report)
Identity Governance	Provides Entra ID platform	RESPONSIBLE & ACCOUNTABLE	Consulted (provisioning)	Consulted (access review)	Informed (compliance %)
Data Encryption	Provides Key Vault + CMK support	RESPONSIBLE for key mgmt	Consulted (deployment)	ACCOUNTABLE (validates)	Informed (coverage %)
Incident Detection	Provides Sentinel + Defender	RESPONSIBLE for rules/tuning	Consulted (log sources)	Consulted (MTTR review)	ACCOUNTABLE (MTTD/MTTR)

Appendix B: Mathematical Models & Formal Logic

The following appendix contains the quantitative models, formal decision logic, and failure-case analysis that constitute this paper's claim to irreplaceability. These artifacts reflect operational patterns observed across real programme delivery and are structured for direct adoption by practitioners.

Table B1: False Assurance Scenario — Controls Pass, Security Fails

Layer	What Appears Compliant	What Is Actually Happening	Why Audit Misses It	Breach Path
Encryption	Azure Policy reports 100% encryption at rest	Encryption keys rotated once — never again (key age: 18 months)	Policy checks encryption=enabled, not key freshness	Stale key compromised via backup exposure
MFA	Entra ID reports 99% MFA coverage	50 service accounts excluded from MFA scope — each with broad permissions	MFA metric counts human users only, not service accounts	Service account credential theft → lateral movement
Logging	Sentinel workspace shows 100% data source coverage	3 data sources sending empty heartbeats (connected but not forwarding data)	Coverage check tests connection, not data completeness	Incident on affected sources invisible to SOC
Patching	WSUS reports 95% patch compliance	Critical servers excluded from patch window 'for stability' (6-month exemption)	Compliance % excludes exempted systems from denominator	Unpatched critical server exploited via known CVE
Access Review	Quarterly access review completed 100%	Reviewers rubber-stamp approvals in bulk (avg review time: 3 seconds per entry)	Audit checks completion rate, not review quality	Excessive permissions persist → insider threat enabled

Table B2: Assurance Confidence Formula — Trust Quantification

Variable	Definition	Measurement	Worked Example	Threshold
Evidence Integrity (EI)	Immutability × tamper detection × chain of custody	Log immutability score + WORM storage + hash verification	0.95 (immutable logs) × 0.90 (tamper detect) = 0.855	EI > 0.90 for regulated
Coverage (C)	Controls assessed / Total controls × Resource coverage %	920 assessed / 920 total × 98% resource coverage = 0.98	0.98 coverage (2% blind spot)	C > 0.95 for DORA
Freshness (F)	1 - (Days_Since_Last _Assessment / Max _Acceptable_Gap)	1 - (15 days / 90 day max) = 0.833	0.833 freshness (assessed 15 days ago)	F > 0.80 (quarterly cycle)
Assurance Confidence (AC)	AC = EI × C × F	0.855 × 0.98 × 0.833 = 0.698	69.8% confidence (BELOW threshold)	AC > 0.75 for board report
ACTION	If AC < threshold → escalate to risk committee	0.698 < 0.75 → ESCALATE: evidence freshness is the weakest factor	Trigger: reassess controls within 7 days	Review cycle must tighten

15. Board Governance Framework Infographic

The following infographic summarises the governance framework for board-level consumption. It maps the Evidence Chain Model™ from regulatory obligation through to board assurance, highlighting the key decision points and escalation triggers that enable proactive risk management.

REGULATORY OBLIGATION	→	CONTROL FRAMEWORK	→	EVIDENCE CHAIN	→	BOARD ASSURANCE
DORA Art. 5 NIS2 Art. 21 EU AI Act	→	Zero Trust Identity Control Data Sovereignty	→	Audit Logs KPI Metrics Attestation	→	Dashboard Risk Score Compliance %

16. Strategic Keywords & Competency Alignment

Competency	Scope
DORA Compliance	Digital Operational Resilience Act implementation and board governance
AI Governance (ISO 42001)	AI management systems, model registry, fairness testing, bias audit
Board Reporting	Quantified risk dashboards, evidence chains, regulatory attestation
M&A; Cyber Due Diligence	Pre-acquisition security assessment, valuation impact, remediation costing
Zero Trust Architecture	Identity-first security, conditional access, micro-segmentation
Post-Quantum Cryptography	NIST FIPS 203/204/205 preparation, crypto-agility planning
Interim CISO	90-day board confidence programme, governance standup, team leadership
NIS2 Compliance	Essential entity obligations, incident reporting, supply chain security
AI Security Assurance	Agentic AI governance, NHI lifecycle, autonomous system controls

About the Author

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is a board-trusted cybersecurity authority with 27 years' experience spanning all four major consulting firms (Deloitte, PwC, EY, KPMG) and 21 years in financial services. He serves as Professor of Practice in Cybersecurity, AI & Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and UCL Researcher. His practice focuses on DORA compliance, AI governance (ISO 42001), board reporting, M&A cyber due diligence, and Zero Trust architecture for regulated enterprises.

Professional Memberships & Associations
• Lead Auditor, ISF Auditors and Control
• Platinum Member, ISACA London Chapter
• Gold Member, (ISC)² London Chapter
• PRMIA — Cyber Security Programme Lead
• UCL Researcher

www.kie.ie | info@kieranupadrasta.com

References

[1] Microsoft. (2026). Microsoft Cybersecurity Reference Architecture (MCRA). Microsoft Security Documentation.

[2] NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.

[3] European Commission. (2022). Digital Operational Resilience Act (DORA). EU Regulation 2022/2554.

[4] European Parliament. (2022). NIS2 Directive. Directive (EU) 2022/2555.

[5] ISO/IEC. (2023). ISO/IEC 42001:2023 — AI Management Systems. International Organization for Standardization.

[6] European Commission. (2024). EU AI Act. Regulation (EU) 2024/1689.

[7] Cloud Security Alliance. (2024). Zero Trust Architecture Implementation Guide. CSA.

[8] MITRE Corporation. (2026). ATT&CK; Framework v14. MITRE.

[9] IBM Security. (2025). Cost of a Data Breach Report 2025. IBM.

[10] Ponemon Institute. (2025). State of Cybersecurity in Financial Services. Ponemon.

[11] Forrester Research. (2025). The Forrester Wave: Zero Trust Platform Solutions. Forrester.

[12] Gartner. (2025). Market Guide for Cloud-Native Application Protection Platforms. Gartner.

[13] McKinsey & Company. (2025). Cyber Risk and Resilience: The Board Imperative. McKinsey.

[14] Saudi NCA. (2024). Controls Assessment Framework (CAF) v3.0. National Cybersecurity Authority.

[15] SAMA. (2024). Cybersecurity Requirements for Banking Sector. Saudi Monetary Authority.

[16] PCI SSC. (2024). PCI DSS v4.0. Payment Card Industry Security Standards Council.

Disclaimer

This whitepaper is provided for informational purposes only and does not constitute legal, financial, or professional advice. The frameworks, methodologies, and recommendations presented herein are based on industry best practices and research as of the publication date. Cybersecurity is a rapidly evolving field. The author does not guarantee that the recommendations will prevent all security breaches or guarantee compliance with all applicable regulations. Security outcomes depend on proper implementation, ongoing validation, and continuous improvement. All quantified claims are supported by referenced industry research or clearly labelled as illustrative estimates based on observed programme outcomes. Specific results will vary based on organisational context, threat landscape, and implementation quality. Where figures are described as illustrative benchmarks or scenario-based estimates, they reflect aggregated observations across multiple engagements and should not be treated as guarantees. Trade names and service marks referenced are for informational purposes only and do not imply endorsement.