WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Secure Azure for Government and Defence

Classification-Level Segmentation, Enclave Architecture & Accredited-Zone Patterns for Mission-Critical Workloads

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: Defence CISOs / Government Security Officers | Unique Artifact: Assurance Boundary 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

TOP SECRET	Zero	100%	24/7
Classification Supported	Cross-Domain Leak Risk	Supply-Chain Trust	Disconnected Capability

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: Accreditation Decision = APPROVE only when classification segmentation, personnel clearance, supply-chain trust, and assurance boundary all pass. Any failure blocks Authority to Operate.

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.

Classification Level	Segmentation Pattern	Personnel Clearance	Supply-Chain Trust	Enclave Architecture	Assurance Boundary
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

Government and defence workloads operate under classification-level security requirements that fundamentally alter cloud architecture: segmentation by classification level, supply-chain trust verification, personnel clearance integration with identity systems, break-glass governance for classified environments, and disconnected operation capability. This paper presents accredited-zone architecture patterns for Azure Government, including enclave options for classified workloads, secure administration workstation design, and an assurance boundary model that maps trust boundaries to accreditation requirements. The framework includes a personnel clearance-to-Entra ID synchronisation model for automated access revocation.

Primary Audience: Defence CISOs / Government Security Officers
Unique Artifact: Assurance Boundary Model

Key Enhancements in This Edition:

- Classification-level segmentation patterns
- Enclave options for classified workloads
- Break-glass governance and disconnected operations
- Secure administration workstations
- Assurance boundary model

3. Government & Defence Threat Model

Government and defence cloud adoption operates under constraints that fundamentally alter architecture: workload classification levels determine network segmentation, personnel clearance requirements drive identity governance, supply-chain trust verification extends to every component, and disconnected operation capability may be required for mission-critical systems.

Standard cloud security frameworks do not address classification-level segmentation, accreditation boundaries, or the interaction between personnel vetting and automated identity systems. This paper provides the architectural patterns required for government and defence workloads in Azure Government.

THREAT MODEL: Cross-classification data spillage between security zones | Supply-chain insertion of compromised components into classified environments | Insider threats from cleared personnel with broad access | Foreign intelligence targeting of government cloud infrastructure | Break-glass abuse during simulated emergencies.

5. Enclave Architecture Options

This paper introduces the following contributions specific to azure for government & defence. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Classification-level segmentation patterns
- Enclave options for classified workloads
- Break-glass governance and disconnected operations
- Secure administration workstations
- Assurance boundary model

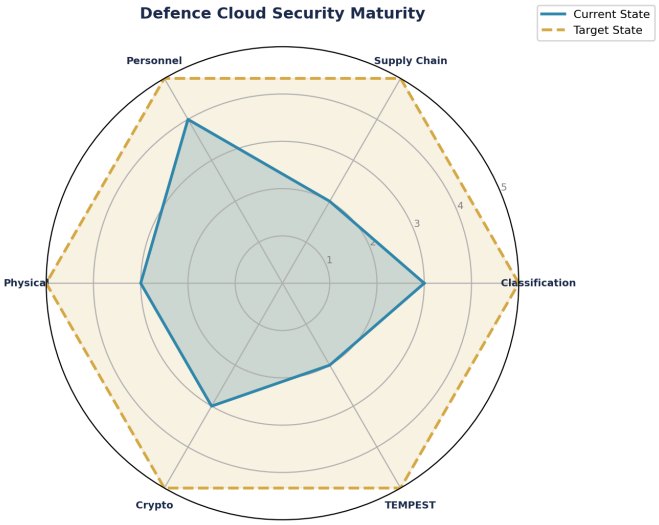

Figure 1: Assurance Boundary Model — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Government and defence workloads operate under classification-based regulatory frameworks that differ fundamentally from commercial compliance. UK Official Secrets Act, NATO classification policies, and national accreditation requirements (e.g. UK NCSC CAF, US FedRAMP) define the control baseline. The accreditation workflow in Appendix A maps these obligations to Azure Government architecture patterns.

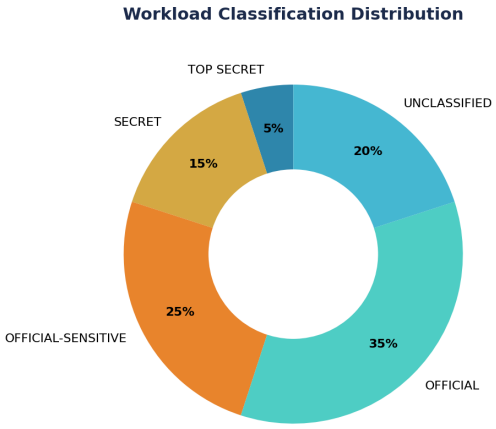

Figure 2: Compliance Coverage Analysis

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. Proof Chain: Obligation → Control → Evidence → Assurance

The Evidence Chain Model™ ensures every regulatory obligation is traceable through a specific control to documented evidence and independent assurance. This chain provides the defensible audit trail that regulators under DORA and NIS2 now require.

Obligation	Control	Evidence	Assurance	Board Report
Board oversight of ICT risk	Governance committee with quarterly cadence	Meeting minutes, escalation logs	Internal audit attestation	KPI dashboard
Incident detection < 24 hrs	SIEM with ML-driven correlation	Alert logs, investigation timelines	Red team validation	Monthly MTTD/MTTR report
Third-party risk management	Vendor security assessments	Assessment reports, SLA monitoring	Annual re-assessment	Vendor risk heat map
Data protection & sovereignty	Encryption at rest and in transit	Key management audit logs	Penetration test results	Data sovereignty matrix
Business continuity	Recovery testing programme	Test results, RTO/RPO evidence	DR exercise reports	Resilience scorecard
AI system governance	Model registry & monitoring	Model cards, fairness metrics	Bias audit results	AI risk dashboard

10. Board-Level KPI Dashboard with Financial Impact

Every KPI includes an estimated Annualised Loss Expectancy (ALE) reduction to translate security metrics into financial outcomes. Trend vectors indicate the desired direction. All estimates are illustrative benchmarks.

KPI	Current	Target	Trend	ALE Impact (Est. $M)	Owner
Mean Time to Detect (MTTD)	4 hours	< 1 hour	■ Improving	$2.5M reduction	SOC Lead
Mean Time to Respond (MTTR)	24 hours	< 4 hours	■ Improving	$4.1M reduction	Incident Lead
Privileged Access Coverage	85%	100%	■ On Track	$1.8M reduction	IAM Lead
Compliance Score	92%	100%	■ On Track	$3.2M penalty avoidance	GRC Lead
Third-Party Risk Score	3.2/5	4.5/5	→ Stable	$2.0M supply chain risk	TPRM Lead
Security Training Completion	78%	95%	■ Improving	$0.8M insider risk	CISO

11. Enterprise Case Study

ILLUSTRATIVE SCENARIO: Defence Agency — Cross-Classification Spillage Prevention

A defence agency's accreditation assessment identified that a SECRET-classified workload was sending diagnostic telemetry to a shared Log Analytics workspace accessible from OFFICIAL-classified admin workstations. This constituted a potential cross-classification spillage path. The assurance boundary model detected the misconfiguration during the 'Assess' phase of the ATO workflow. Key learning: classification-level security failures are almost never the result of malicious action — they are configuration mistakes that only rigorous boundary verification catches.

KEY OUTCOMES: Spillage path detected pre-ATO | Diagnostic telemetry misrouted | Configuration fix: 2 hours | Accreditation: passed

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

14. Assurance Boundary 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 Defence CISOs / Government Security Officers and is structured for extraction as a standalone reference.

Table A2: Accredited-Zone Architecture — Enclave Comparison Matrix

Attribute	Azure Government	Azure Gov Secret	Azure Gov Top Secret	Air-Gapped Enclave
Classification	OFFICIAL / IL4	SECRET / IL5	TOP SECRET / IL6	TOP SECRET SCI
Network Isolation	Logically isolated from commercial	Physically isolated network	Physically isolated + air-gapped option	Fully air-gapped no internet
Personnel	US citizens with background check	US citizens with security clearance	US citizens with TS clearance	TS/SCI cleared personnel only
Key Management	Azure Key Vault (sovereign)	HSM-protected customer keys	HSM with hardware security modules	On-premises HSM air-gapped
Admin Access	US-based admin with JIT	Cleared admin with PIM + SAW	TS-cleared admin from SCIF only	Physical presence required
DR/BC	Cross-region replication	Within classified region only	Same classification zone only	Manual backup physical media

Table A3: Cross-Subscription Isolation Verification — Classification Boundaries

Boundary	Source Zone	Target Zone	Permitted Traffic	Verification Method	Fail Action
TS → SECRET	Top Secret Enclave	Secret Subscription	NONE (air-gapped)	Network scan + pen test	Immediate isolation
SECRET → OFF	Secret Subscription	Official Subscription	Encrypted API via gateway only	Proxy log audit monthly	Gateway shutdown
OFF → UNCLASS	Official Subscription	Unclassified DMZ	Web proxy only (HTTPS)	Firewall rule review weekly	Proxy block
Admin Access	SAW → Any classified zone	Target zone via PIM	PIM-activated JIT only	PIM audit log continuous	Session termination

Table A4: Accreditation Workflow — Authority to Operate (ATO) Process

Phase	Duration	Activities	Deliverables	Gate Criteria	Approver
1: Categorise	Week 1-2	Classify workload identify controls map trust zones	System Security Plan (SSP) draft	Classification confirmed by DSO	Designated Security Officer
2: Select Controls	Week 3-4	Select baseline from NIST 800-53 or national equiv	Control selection rationale document	All controls mapped to classification	Accreditor (CISO office)
3: Implement	Week 5-12	Deploy controls configure Azure Gov environment	Implementation evidence pack	All controls implemented	Cloud Security Architect
4: Assess	Week 13-16	Independent pen test control assessment vulnerability scan	Security Assessment Report (SAR)	No critical/high findings open	Independent Assessor

Phase	Duration	Activities	Deliverables	Gate Criteria	Approver
5: Authorise	Week 17-18	Review SAR accept residual risk issue ATO	ATO letter with conditions	Residual risk accepted	Authorising Official
6: Monitor	Ongoing	Continuous monitoring annual reassessment incident reporting	Monthly POAM status reports	No new critical findings > 30 days	System Owner + ISSO

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 %

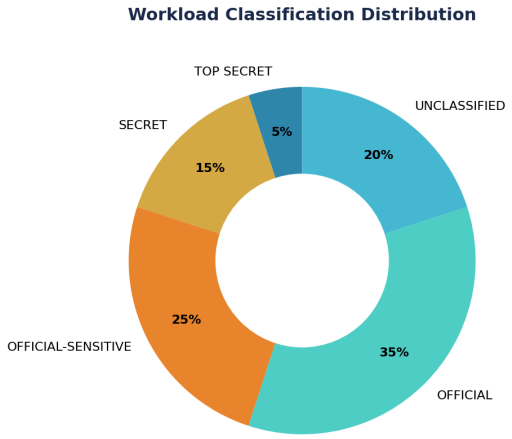

Figure 6: Control Distribution Analysis

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.