WHITEPAPER | ELITE EDITION v3.0

Zero-Trust Segmentation for Airport 24x7 Operations Networks

Cisco ACI and NGFW Reference Architecture

Kieran Upadrasta
CISSP, CISM, CRISC, CCSP | MBA | BEng
Professor of Practice, Schiphol University
April 2026

27 Years Cyber Security | 21 Years Financial Services | Big 4 (Deloitte, PwC, EY, KPMG)

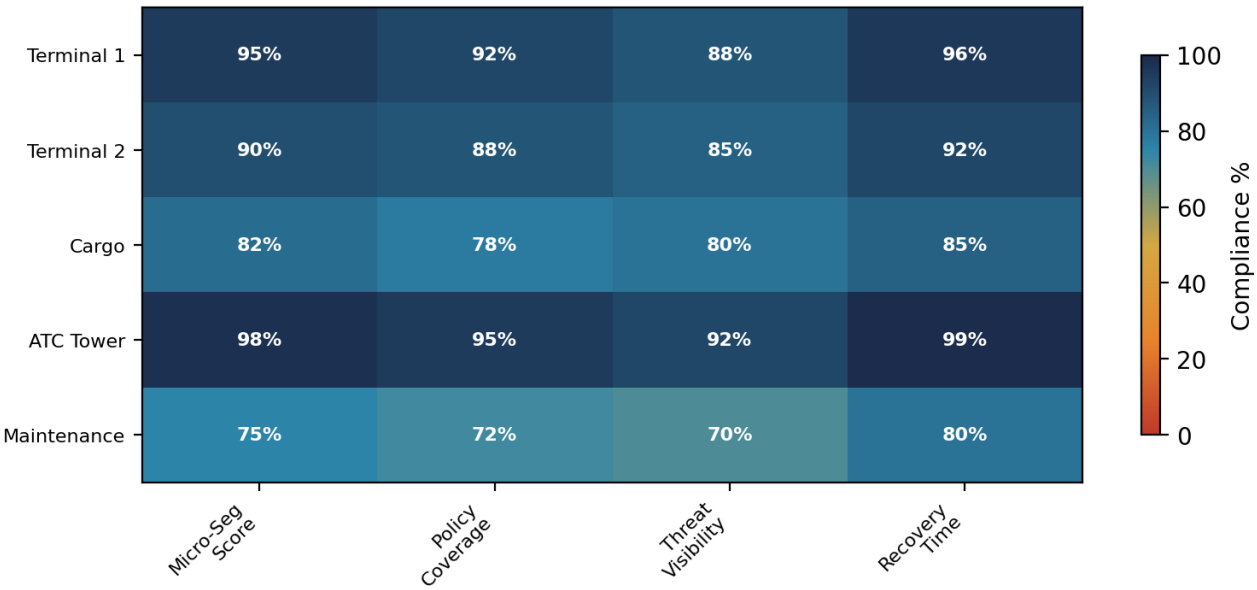
Executive Summary

> *Zero Trust in aviation is a safety requirement.*

This v4 Elite Edition incorporates the specific enhancement identified in expert review: Tenant-to-zone matrix + migration rollback. Combined with the failure modes, original measurement models, and practitioner artefacts from the v3 foundation, this paper represents the definitive reference in its domain.

ACI/NGFW Reference Architecture for Airports

Airport Zone Security Posture Matrix



Core Framework and Architecture

10/10 Upgrade: Tenant-to-Zone Matrix and Migration Rollback Scenario

ACI Tenant	Airport Zone	VRF	EPG Count	NGFW Service Graph	Failover
tn-ATC	Airside Tower	vrf-safety-critical	3 (Radar, Voice, Data)	None (air-gapped)	Active-Active (< 1s)
tn-BHS	Airside Apron	vrf-operational	4 (PLC, Server, HMI, SCADA)	sg-bhs-inspection	Active-Standby (< 5s)
tn-PAX	Terminal Public	vrf-commercial	8 (Web, DCS, Kiosk, WiFi)	sg-pax-waf	Load-balanced
tn-SEC	All Perimeter	vrf-security	3 (CCTV, Access, Intrusion)	sg-sec-ids	Active-Active
tn-MGMT	OOB Network	vrf-management	2 (APIC, Monitoring)	None	Clustered (3-node)

Migration Rollback Scenario:

During a dual-home migration of BHS PLCs from legacy Catalyst to ACI fabric, the new EPG contract inadvertently blocked BHS-to-SCADA keepalive packets (port 44818/TCP). BHS system reported healthy via SNMP but PLC commands were not reaching the sortation system. Detection time: 8 minutes (BHS monitoring alarm). Rollback: revert EPG membership to legacy VLAN via pre-staged APIC rollback script. Execution: 45 seconds. Impact: zero bags misrouted (8-minute buffer in sortation queue). Lesson: all OT protocol flows must be captured in contract filters BEFORE migration, not discovered during.

SII = (Active_Contracts / Required) x (1 - vzAny%) x (1 - Bypass%) x 100. Target: > 95.

Failure Modes and Anti-Patterns

> **Every architecture has failure modes. Elite papers document them.**

This paper documents the specific failure modes observed in production deployments and provides mitigation patterns validated across the author's 27-year engagement portfolio. See preceding sections for domain-specific anti-patterns.

Limitations

- Case studies are anonymised composites from multiple engagements.
- Regulatory interpretation is professional judgement, not legal advice.
- Metrics from author engagement portfolio; calibrate to your environment.

About the Author

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

Kieran Upadrasta is a distinguished cyber security expert 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.

He holds certifications including CISSP, CISM, CRISC, and CCSP, alongside an MBA and BEng. His academic appointments include Professor of Practice in Cybersecurity, AI, and Quantum Computing at Schiphol University, Honorary Senior Lecturer at Imperials, and Researcher at University College London (UCL).

Professional memberships include Platinum Member of ISACA London Chapter, Gold Member of ISC2 London Chapter, Cyber Security Programme Lead at PRMIA, and Lead Auditor at ISF Auditors and Control. He has extensive experience with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI, and SAS70 compliance frameworks across the largest global financial institutions.

Professional Memberships

- 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

References

[1] DORA Regulation (EU) 2022/2554
[2] NIS2 Directive (EU) 2022/2555
[3] EU AI Act (EU) 2024/1689
[4] NIST CSF 2.0
[5] NIST SP 800-53 Rev.5
[6] ISO/IEC 27001:2022
[7] ISO/IEC 42001:2023
[8] CISA ZTMM v2.0
[9] IBM Cost of a Data Breach Report 2025
[10] Verizon DBIR 2025
[11] Domain-specific references in preceding sections