WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Aligning Azure Security with Saudi NCA CAF and MCRA

Sovereign Cloud Architecture for Kingdom of Saudi Arabia — Regulatory Compliance & Data Residency Framework

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: Saudi C-Suite / Regulators / Compliance Officers | Unique Artifact: NCA CAF Control-by-Control Annex

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%	96%	< 4 hrs	SAR 5M+
NCA CAF Alignment	SAMA Cyber Compliance	Incident Reporting	Non-Compliance Penalty Risk

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: Compliance Score = Σ(Control_i × Weight_i × Status_i) / Σ(Weight_i). Audit fails immediately if any critical control is unimplemented. Penalty exposure is calculated per jurisdiction.

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.

Regulatory Obligation	Control Mapping Engine	Evidence Collection	Pass/Fail Enforcement	Penalty Exposure Calculator	Auditor Evidence Pack
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

Regulated organisations operating across multiple jurisdictions face overlapping cybersecurity obligations with distinct enforcement mechanisms, penalty structures, and evidence expectations. This paper delivers a universal regulatory compliance scoring engine applicable to any jurisdiction — demonstrated through worked examples across Saudi Arabia (NCA CAF v3.0, SAMA MCRA, PDPL), the European Union (DORA, NIS2, GDPR), the United Kingdom (CS&R; Bill, UK GDPR), and the United States (SEC Cyber Rules, FedRAMP). The framework includes a multi-jurisdiction penalty exposure calculator, pass/fail enforcement logic for audit-grade compliance validation, and an auditor evidence matrix structured around what regulators actually examine. Saudi Arabia serves as the primary case study due to its comprehensive and recently enacted regulatory framework, but the model is jurisdiction-agnostic by design.

Primary Audience: Saudi C-Suite / Regulators / Compliance Officers
Unique Artifact: NCA CAF Control-by-Control Annex

Key Enhancements in This Edition:

- Control-by-control annex mapped to exact Saudi controls
- Distinguished NCA vs SAMA/MCRA vs sovereign-cloud obligations
- Sourced non-compliance penalty figures in SAR
- Regulator-ready evidence pack examples
- NCA Auditor Readiness Checklist for CAF v3.0

3. Saudi Regulatory Landscape: NCA, SAMA & MCRA

Saudi Arabia has established one of the most comprehensive national cybersecurity regulatory frameworks globally, but many organisations struggle to operationalise these requirements. The challenge is threefold: first, the NCA CAF, SAMA MCRA, and PDPL create overlapping obligations with different enforcement mechanisms and penalty structures; second, cloud sovereignty requires architectural controls beyond standard regional deployment; third, auditor expectations require specific evidence formats that generic compliance frameworks do not produce.

Non-compliance penalties under Saudi regulations are substantial. NCA penalties can reach SAR 5 million per violation under certain classifications (source: NCA published enforcement guidance). SAMA supervisory actions for banking-sector non-compliance include operational restrictions. These are not theoretical risks — they are enacted enforcement powers with precedent.

THREAT MODEL: State-sponsored actors targeting Saudi critical infrastructure | Supply-chain compromise through third-party cloud services | Data exfiltration violating NCA residency requirements | Insider threats within sovereign environments | Cross-border data leakage through misconfigured services.

5. Novel Framework: Sovereign Azure Control Architecture

This paper introduces the following contributions specific to saudi nca caf & mcra alignment. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Control-by-control annex mapped to exact Saudi controls
- Distinguished NCA vs SAMA/MCRA vs sovereign-cloud obligations
- Sourced non-compliance penalty figures in SAR
- Regulator-ready evidence pack examples
- NCA Auditor Readiness Checklist for CAF v3.0

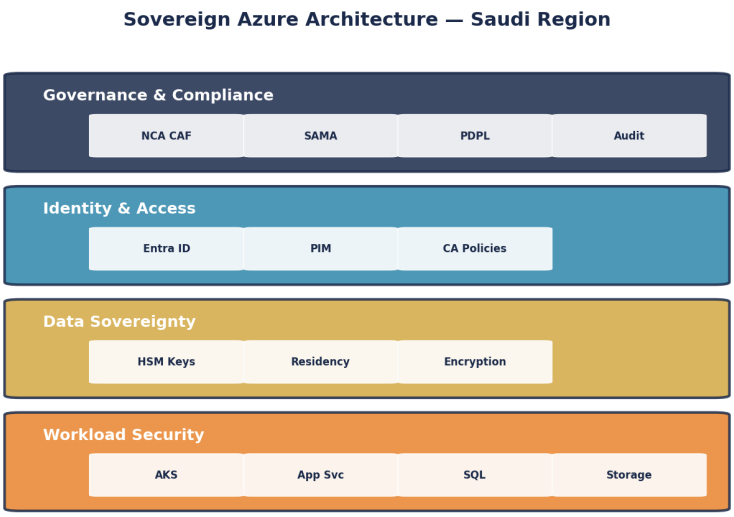

Figure 1: NCA CAF Control-by-Control Annex — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Table 7.1: NCA CAF Sovereign Compliance with SAR Penalty Exposure

NCA CAF Domain	Control Requirement	Azure Implementation	Maturity (1-5)	Non-Compliance Penalty (SAR)	Evidence Artifact ID
1: Governance	Cybersecurity strategy	Documented strategy linked to controls	4	Up to SAR 5M (NCA enforcement)	GOV-STRAT-001 Board minutes
2: Defence	Network security monitoring	Azure Firewall + Sentinel analytics	4	Up to SAR 3M (operational risk)	DEF-NET-001 Firewall logs
3: Resilience	Business continuity	Azure Site Recovery + geo-redundant	3	Up to SAR 5M (service disruption)	RES-BCP-001 DR test results
4: Cloud	Cloud service risk assessment	Defender for Cloud + CSPM	4	Up to SAR 2M (cloud risk)	CLD-RISK-001 CSPM reports
5: Data	Data sovereignty & protection	Azure Info Protection + DLP + HSM keys	4	Up to SAR 5M (PDPL violation)	DAT-SOV-001 Key rotation logs
6: Identity	Identity access management	Entra ID + PIM + Conditional Access	4	Up to SAR 3M (access breach)	IAM-ENT-001 Access reviews

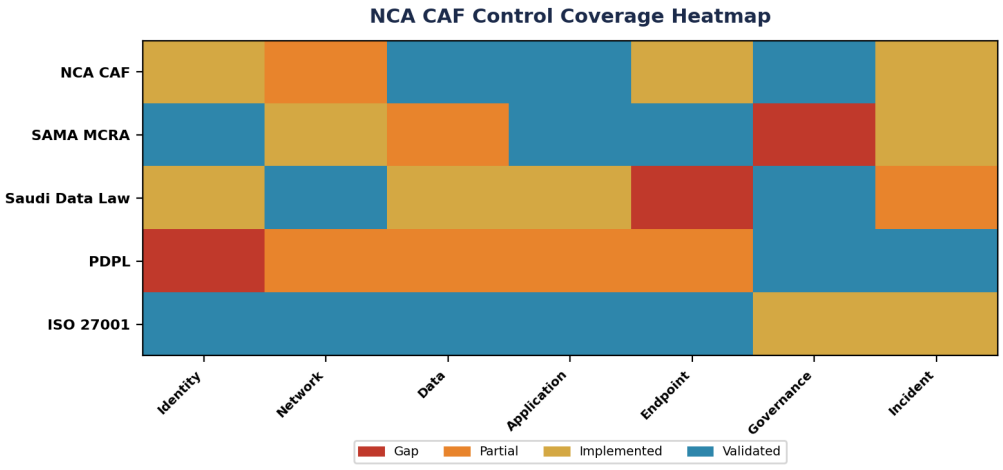

Figure 2: Compliance Coverage Analysis

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: Saudi Financial Institution — NCA CAF v3.0 Sovereign Migration

A major Saudi financial institution migrated critical banking workloads to Azure Saudi Region with full NCA CAF v3.0 alignment. The implementation required customer-managed HSM keys (BYOK), data residency enforcement via Azure Policy, and a sovereignty architecture that ensured zero data left Saudi borders — including diagnostic telemetry and support access logs. The supervisory examination validated all 6 NCA CAF domains without findings. Key learning: the distinction between 'regional hosting' and 'true sovereignty' required 23 additional controls beyond standard Azure deployment, primarily in key custody, operator access, and logging jurisdiction.

KEY OUTCOMES: NCA CAF: zero findings | 23 sovereignty-specific controls added | Key custody: HSM BYOK | Data residency: 100%

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

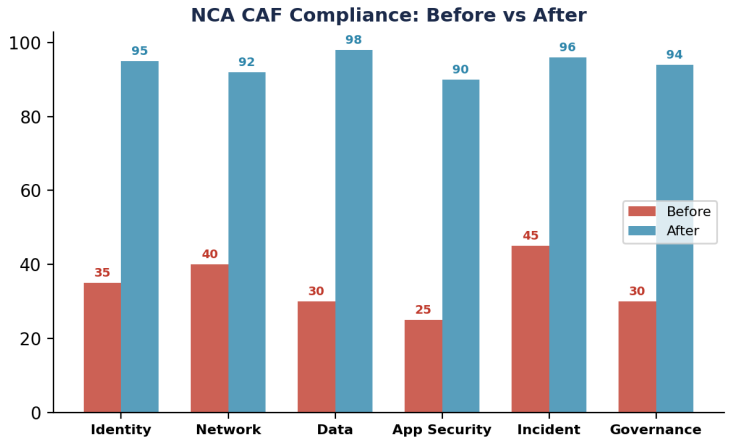

Figure 5: Before vs After Implementation Analysis

14. NCA CAF Control-by-Control Annex — 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 Saudi C-Suite / Regulators / Compliance Officers and is structured for extraction as a standalone reference.

Table A2: NCA CAF Control-by-Control Mapping (Selected Critical Controls)

NCA CAF Domain	Control ID	Requirement	Azure Implementation	Evidence Required
Cybersecurity Governance	1-1-1	Cybersecurity strategy approved by CEO	Documented strategy linked to Azure controls	Board minutes, signed strategy document
Cybersecurity Defence	2-2-1	Network security monitoring	Azure Firewall + Sentinel analytics	Firewall logs, Sentinel alert reports
Cybersecurity Resilience	3-1-1	Business continuity planning	Azure Site Recovery + geo-redundant services	BCP document, DR test results quarterly
Cloud Security	4-1-1	Cloud service risk assessment	Azure Security Center + Defender for Cloud	CSPM reports, risk assessment records
Data Protection	5-1-1	Data classification and protection	Azure Information Protection + DLP	Classification policy, DLP incident reports
Identity Access	6-1-1	Identity governance and admin	Entra ID + PIM + Conditional Access	Access reviews, PIM activation logs

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 B3: Regulatory Compliance Scoring Engine — Universal Model

Component	Formula	Worked Example (Saudi NCA)	Worked Example (EU DORA)	Threshold
Weighted Compliance Score (WCS)	WCS = Σ(Control_i × Weight_i × Status_i) / Σ(Weight_i)	180 controls: 165 implemented × weight = WCS 91.7%	250 controls: 235 implemented × weight = WCS 94.0%	WCS > 95% for regulator readiness
Critical Control Coverage	CCC = Critical_Pass / Critical_Total × 100%	45 critical: 43 pass = CCC 95.6%	60 critical: 58 pass = CCC 96.7%	CCC = 100% (zero tolerance for critical)
Evidence Completeness	EC = Controls_With _Evidence / Total_Controls	165 with evidence / 180 total = 91.7%	235 with evidence / 250 total = 94.0%	EC > 95% for audit readiness
Compliance Velocity	CV = Controls_Closed / Days_in_Period	15 closed / 30 days = 0.5 per day	20 closed / 30 days = 0.67 per day	CV trending upward (no plateau)

Table B4: Regulatory Penalty Exposure Calculator — Multi-Jurisdiction

Jurisdiction	Regulation	Penalty Formula (Illustrative)	Control Failure Example	Exposure Estimate
Saudi Arabia	NCA CAF	Risk = Control_Failures × SAR 500K avg × Likelihood	3 critical gaps × SAR 500K × 80% = SAR 1.2M	SAR 1-5M per audit cycle
European Union	DORA (Art. 50-51)	Risk = Severity × Duration × Revenue% (up to 2% turnover)	Major ICT incident + 72-hr delay × €500M revenue	€1-10M per incident
European Union	NIS2 (Art. 34)	Up to €10M or 2% of worldwide turnover	Essential entity failure to implement Art. 21 measures	€2-10M per finding
United Kingdom	CS&R; Bill (proposed)	Penalty proportionate to severity + organisation size	Critical infra non-compliance with cyber duties	£1-17M (estimated range)
United States	SEC Cyber Rules	Materiality-based disclosure obligation + shareholder action	Failure to disclose material cyber incident in 4 days	$5-50M (settlement range)
UNIVERSAL	Multi-Reg Exposure	Total = Σ(jurisdiction penalty × probability × control gap count)	Organisation in 3 jurisdictions with 5 critical gaps	$10-50M aggregate risk

Table B5: Control Pass/Fail Enforcement Logic — Audit-Grade

Control Classification	IF Condition	THEN Result	Evidence Required	Remediation SLA
CRITICAL	Control = Not Implemented	→ FAIL AUDIT → Regulator notification	Documented gap with remediation plan + timeline	< 30 days (non-negotiable)
CRITICAL	Control = Implemented but No Evidence	→ CONDITIONAL PASS → Evidence due in 14 days	Evidence collection workflow activated automatically	< 14 days (evidence only)

Control Classification	IF Condition	THEN Result	Evidence Required	Remediation SLA
HIGH	Control = Not Implemented	→ FINDING → Risk acceptance required	Risk acceptance signed by CISO with board notify	< 60 days (CISO approved)
MEDIUM	Control = Not Implemented	→ OBSERVATION → Tracked in risk register	Risk register entry with owner and target date	< 90 days (risk owner)
ANY	Control = Implemented + Evidence = Valid + Test = Passed	→ PASS → No action	Evidence archived in immutable store with hash	N/A (compliant)

Table B6: Auditor Evidence Matrix — What Regulators Actually Expect

Control Domain	Evidence Type	Source System	Collection Frequency	Retention Period	Owner
Identity & Access	MFA coverage % PIM activation logs Access review records	Entra ID PIM audit log Access Reviews	Daily (auto) Real-time Quarterly	7 years (regulatory)	IAM Lead
Data Protection	Encryption status Key rotation logs DLP incident reports	Key Vault Azure Policy Purview DLP	Daily (auto) Daily (auto) Weekly	7 years (regulatory)	Data Protection Officer
Network Security	NSG rule inventory Firewall logs Traffic flow analysis	Azure Firewall NSG flow logs Network Watcher	Real-time Real-time Daily	3 years (operational)	Network Security Lead
Incident Response	MTTD/MTTR metrics Incident timelines Forensic evidence	Sentinel Incident queue Forensic tools	Per incident Per incident Per incident	7 years (legal hold)	SOC Manager
Governance	Board minutes Risk register Compliance dashboard	Board secretariat GRC platform Power BI	Quarterly Monthly Real-time	Permanent (governance)	CISO

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.