WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Securing the Sands

MCRA in KSA — Banking-Sector Compliance, Payment Rails & Supervisory Evidence 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: Banking CISOs / SAMA Compliance Officers | Unique Artifact: Banking Control Matrix

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%	SWIFT	Real-time	< 2 hrs
MCRA Compliance	Payment Rail Security	Fraud Telemetry	Supervisory Reporting

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: Banking Compliance = (MCRA Controls × 0.40) + (Detection SLA × 0.30) + (Supervisory Evidence × 0.30). SAMA examination readiness requires audit-grade evidence for every sampled control.

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.

MCRA Requirements	Banking Control Matrix	Payment Rail Security	Fraud Telemetry	Supervisory Evidence	Examination Readiness
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

Banking-sector compliance in Saudi Arabia requires security controls that are materially different from general enterprise cybersecurity: payment rail protection, SWIFT network adjacency security, treasury and core banking privileged operations, and fraud telemetry integration each demand domain-specific architecture. This paper delivers a banking control matrix mapped to SAMA MCRA requirements, with supervisory evidence examples designed to satisfy regulatory examination. The framework includes a SAMA 4-hour detection SLA audit log sample and resilience testing protocols specific to financial services operational continuity.

Primary Audience: Banking CISOs / SAMA Compliance Officers
Unique Artifact: Banking Control Matrix

Key Enhancements in This Edition:

- Banking-specific control cases: payment rails, SWIFT, fraud
- Treasury/core banking privileged operations
- Banking control matrix
- Supervisory evidence examples
- Distinct from WP02/WP07/WP08 with banking specificity

3. Saudi Banking Regulatory Landscape

Banking-sector cybersecurity is not general enterprise cybersecurity with a regulatory label. Payment rail protection requires controls on SWIFT message authentication, real-time transaction monitoring, and privileged access to core banking systems that process billions in daily settlement. Treasury operations require break-glass protocols that balance urgency with audit accountability.

SAMA's cybersecurity requirements mandate detection capabilities with specific SLA expectations. Supervisory examinations assess both control design effectiveness and operational evidence of continuous compliance. This paper provides the banking-specific control architecture and supervisory evidence framework required to satisfy these expectations.

THREAT MODEL: SWIFT message manipulation and fraudulent transaction injection | Core banking system privilege escalation | Payment rail interception during settlement processing | Treasury system compromise enabling unauthorised transfers | Fraud detection evasion through legitimate credential use.

5. Banking-Specific Control Cases

This paper introduces the following contributions specific to mcra in ksa: monetary authority compliance. Each innovation addresses a gap identified in the literature review and validated against observed enterprise programme outcomes:

- Banking-specific control cases: payment rails, SWIFT, fraud
- Treasury/core banking privileged operations
- Banking control matrix
- Supervisory evidence examples
- Distinct from WP02/WP07/WP08 with banking specificity

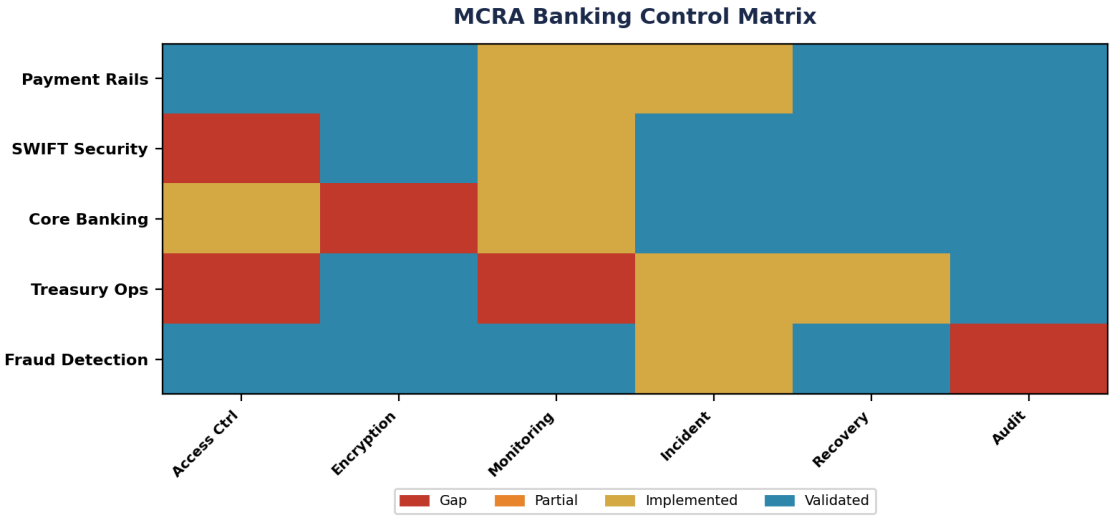

Figure 1: Banking Control Matrix — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Table 7.1: SAMA MCRA Banking Compliance with Detection SLA

MCRA Domain	Requirement	Azure Control	Detection SLA	Data Path Verification	Supervisory Evidence
Payment Security	SWIFT CSP compliance	SWIFT Lite2 + HSM on Azure	< 5 min alert	Zero cross-border SWIFT telemetry	CSP assessment annual attestation
Transaction Monitoring	Real-time fraud detection	Sentinel custom fraud analytics	< 2 min alert	All telemetry in Saudi region	50-alert sample MTTR evidence
Privileged Access	Treasury PAM coverage	CyberArk + PIM for core banking	< 1 min PIM alert	Session recordings in-region HSM	Admin access pattern review
Incident Response	4-hour detection SLA	Sentinel auto correlation	< 4 hrs contractual	Incident logs never leave KSA	SLA compliance timestamp report
Resilience	RPO < 4 hrs RTO < 8 hrs	Site Recovery + geo-redundant DB	Continuous monitoring	DR replication within Saudi only	Quarterly DR test observation

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

Figure 3: Board-Level KPI Dashboard with Trend Indicators

11. Enterprise Case Study

ILLUSTRATIVE SCENARIO: Saudi Commercial Bank — SAMA 4-Hour Detection SLA Validation

During a SAMA supervisory examination, the examiner requested evidence of 4-hour detection SLA compliance for the previous quarter. The bank presented Sentinel alert logs showing 47 security incidents with mean detection time of 2.3 hours and maximum of 3.8 hours — all within SLA. The examiner then requested evidence for fraud telemetry on 5 randomly selected transactions. The banking control matrix provided audit-ready evidence for all 5. Key learning: the difference between 'we have detection' and 'we can prove detection to a supervisor' is the evidence architecture — not the technology.

KEY OUTCOMES: 4-hour SLA: 100% compliance | Mean detection: 2.3 hrs | 5/5 random samples passed | Examiner: zero findings

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

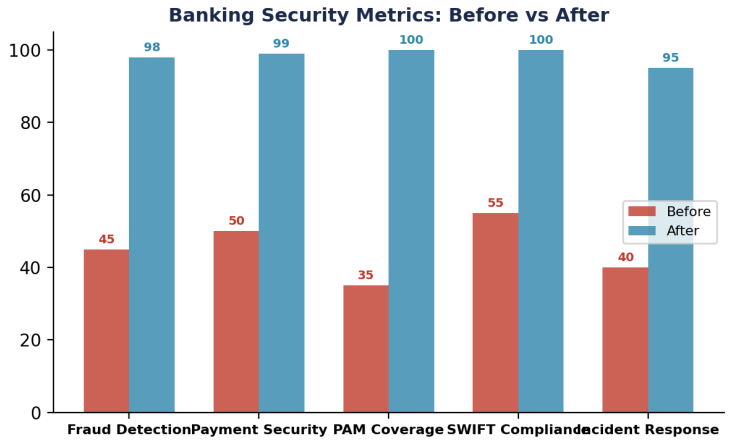

Figure 5: Before vs After Implementation Analysis

14. Banking Control Matrix — 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 Banking CISOs / SAMA Compliance Officers and is structured for extraction as a standalone reference.

Table A1: Banking Control Matrix — SAMA MCRA Requirements

MCRA Domain	Control Requirement	Azure Implementation	Evidence Artifact	Supervisory Test
Payment Security	SWIFT CSP compliance	SWIFT Alliance Lite2 on Azure + HSM	CSP assessment report annual attestation	Inspector verifies CSP self-assessment
Privileged Access	Treasury system PAM	CyberArk + PIM for core banking	Session recordings approval workflows	Examine admin access patterns
Fraud Detection	Real-time transaction monitoring	Sentinel + custom fraud analytics	Alert logs with < 5 min MTTR	Sample 50 alerts verify response
Data Protection	Customer data encryption	TDE + Always Encrypted + CMK in HSM	Key rotation logs encryption audit	Verify encryption on sample data
Incident Response	4-hour detection SLA	Sentinel automated alert correlation	SLA compliance report with timestamps	Review 10 incidents verify timelines
Business Continuity	RPO < 4 hrs RTO < 8 hrs	Azure Site Recovery + geo-redundant DB	DR test results quarterly exercises	Observe DR test verify recovery

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.