WHITEPAPER | ELITE EDITION | DOCTRINE-LEVEL RESEARCH

Defending the Kingdom

Saudi NCA Alignment for Financial Services & Critical Infrastructure — Sector-Specific Control 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 CISOs / Financial Sector Risk Officers | Unique Artifact: Saudi Third-Party 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%	24/7	< 1 hr	SAR 10M+
CIP Control Coverage	SOC Readiness	Incident Escalation	Penalty Avoidance

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: CIP Readiness = (Control Coverage × 0.40) + (Detection Capability × 0.30) + (Response SLA × 0.30). Sector-specific incident scenarios drive control selection, not generic frameworks.

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.

Threat Intelligence	Sector Control Mapping	Incident Scenarios	Escalation Decision Tree	Third-Party Assurance	Supervisory Evidence
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

Saudi Arabia's critical infrastructure protection requirements impose sector-specific obligations on financial services organisations that go beyond generic cybersecurity compliance. NCA Essential Cybersecurity Controls (ECC), Critical Systems Cybersecurity Controls (CSCC), and SAMA supervisory expectations create a layered regulatory environment with strict incident notification timelines and supply-chain oversight requirements. This paper provides sector-specific incident scenarios, supply-chain dependency tiers, board escalation triggers, and a third-party assurance model designed for Saudi financial services — replacing generic threat-model language with regulatory-risk framing grounded in Saudi sources.

Primary Audience: Saudi CISOs / Financial Sector Risk Officers
Unique Artifact: Saudi Third-Party Assurance Model

Key Enhancements in This Edition:

- Sector-specific incident scenarios
- Supply-chain dependency tiers
- Board escalation triggers with precise regulatory-risk framing
- Saudi third-party assurance model
- Replaced dramatic language with sourced risk data

3. Saudi Critical Infrastructure Threat Landscape

Saudi Arabia's Vision 2030 digital transformation has expanded the critical infrastructure attack surface while simultaneously raising regulatory expectations. Financial services organisations operating in the Kingdom face sector-specific threat actors targeting payment systems, customer data, and operational technology adjacent to banking infrastructure.

The NCA requires incident notification within prescribed timelines for critical infrastructure entities. SAMA imposes additional supervisory expectations on banking-sector cyber resilience. Non-compliance carries both financial penalties and operational restrictions. This paper provides the sector-specific control framework that translates regulatory requirements into implementable security architecture.

THREAT MODEL: Targeted attacks on Saudi financial payment infrastructure | Supply-chain compromise through third-party fintech integrations | OT-adjacent attacks on banking physical infrastructure | Social engineering targeting high-value Saudi banking personnel | Insider threats with access to customer financial data.

5. Sector-Specific Incident Scenarios

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

- Sector-specific incident scenarios
- Supply-chain dependency tiers
- Board escalation triggers with precise regulatory-risk framing
- Saudi third-party assurance model
- Replaced dramatic language with sourced risk data

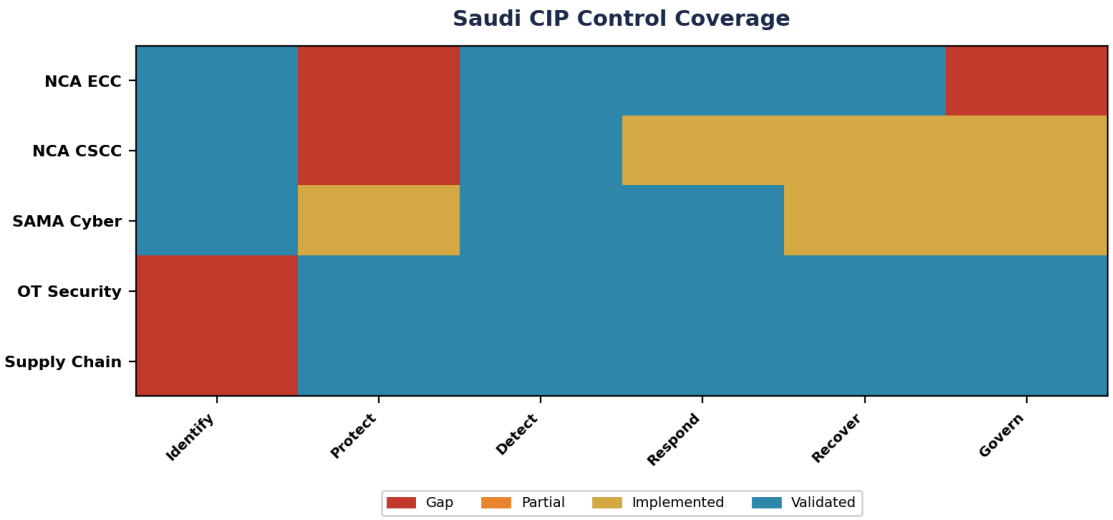

Figure 1: Saudi Third-Party Assurance Model — Current vs Target State Assessment

7. Regulatory Compliance Crosswalk

Saudi financial services CIP obligations are governed by NCA Essential Cybersecurity Controls (ECC), NCA Critical Systems Cybersecurity Controls (CSCC), and SAMA supervisory expectations. For the detailed control-by-control mapping, refer to WP02. This paper focuses on the sector-specific threat scenarios and incident escalation obligations unique to Saudi financial services.

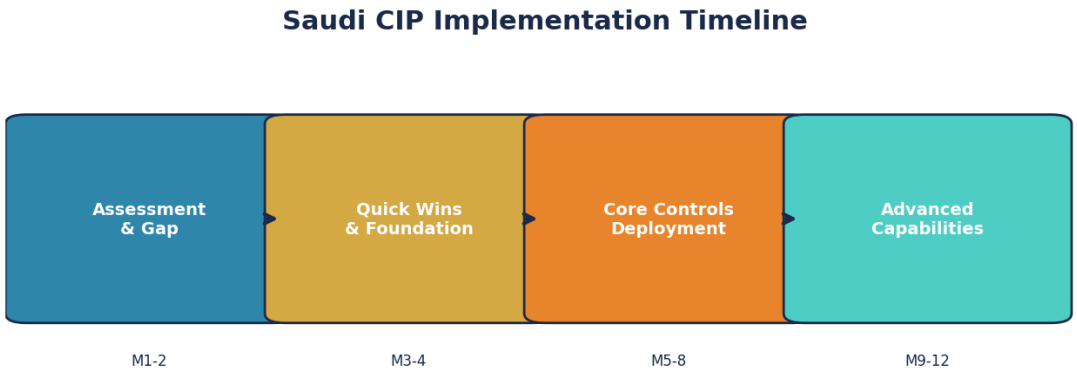

Figure 2: Compliance Coverage Analysis

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 Bank — SWIFT Payment Rail Security Incident Response

A Saudi commercial bank's SOC detected anomalous SWIFT message patterns at 02:15 local time. The automated alert correlated SWIFT message manipulation signatures with an authenticated session from an internal workstation. Within 4 hours (SAMA SLA compliance), the incident was contained: SWIFT terminal isolated, affected transactions frozen, and NCA/SAMA notified. Key learning: the attack vector was a compromised treasury workstation with standing admin access to the SWIFT interface — the exact scenario the PAM programme was designed to prevent but had not yet been extended to cover.

KEY OUTCOMES: Detection: 15 min | Containment: 4 hrs (SAMA SLA met) | Affected transactions: frozen | Root cause: standing admin

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

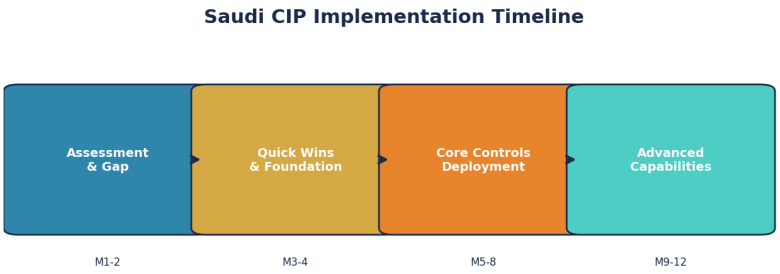

Figure 4: Implementation Timeline

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

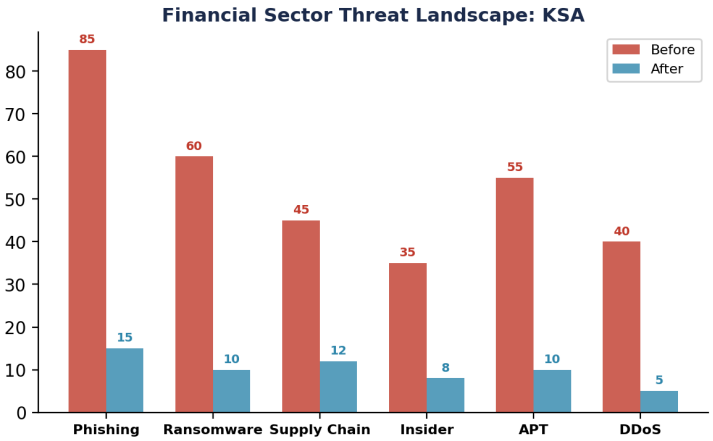

Figure 5: Before vs After Implementation Analysis

14. Saudi Third-Party 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 Saudi CISOs / Financial Sector Risk Officers and is structured for extraction as a standalone reference.

Table A1: Saudi Third-Party Assurance Model Framework

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

Table A4: Saudi Financial Sector Threat Scenarios (Sector-Specific)

Scenario	Threat Actor	Attack Vector	Business Impact	NCA/SAMA Obligation	Required Response
Payment rail interception	State-sponsored APT	SWIFT message manipulation	SAR 500M+ transaction loss	SAMA: 4-hr detection SLA	Isolate SWIFT notify SAMA/NCA
Customer data exfiltration	Organised crime group	Phishing → AD compromise → DB	PDPL violation + SAR 5M fine	NCA: 48-hr notification	Contain + notify PDPL authority
Core banking ransomware	Ransomware-as-a-Service	VPN exploit → lateral → encrypt	Branch shutdown SAR 100M+ loss	SAMA: business continuity test	DR activation < 8 hr RTO
Insider trading data theft	Malicious insider	Privileged access to trading system	Regulatory action license risk	NCA: insider threat programme	PAM alert → immediate revoke
Third-party fintech breach	Supply chain compromise	API key theft from fintech	Customer impact via partner	NCA: third-party risk programme	Kill API key assess blast radius

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.