

SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

**WP05 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0**

---

# Beyond Compliance

*How SABSA Transforms Security Architecture into Business Value, ROI, and Competitive Advantage*

---



## Kieran Upadrasta

**CISSP · CISM · CRISC · CCSP | MBA | BEng**

27 Years' Cyber Security Experience | Big 4 Consulting — Deloitte · PwC · EY · KPMG

21 Years Financial Services & Banking | AI Cyber Security Programme Lead

**Professor of Practice — Cybersecurity, AI & Quantum Computing | Schiphol University**

Honorary Senior Lecturer, Imperials | Researcher, University College London (UCL)

Lead Auditor, ISF Auditors & Control | ISACA Platinum (London) | (ISC)<sup>2</sup> Gold (London) | PRMIA Cyber Lead

---

[www.kie.ie](http://www.kie.ie) | [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) | April 2026

Specialisations: SABSA · NIS2 · ISO 27001:2022 · GDPR · IEC 62443 · NIST CSF 2.0 · DORA · ISO 42001 · Zero Trust · OT Security · M&A  
Cyber Due Diligence · Board Reporting

## Table of Contents

1. Executive Summary
2. The SABSA Value Realisation Framework (SVRF)
3. CFO Decision Framework: Security Architecture as Capital Investment
4. The SABSA Value Realisation Framework (SVRF) — Extended Model
5. Case Study: Architecture-Led Contract Win
7. CFO Strategic Case Study: GBP 40M Architecture-Driven Value
8. AICE-to-M&A Valuation Multiples
9. Monetized Risk Dashboard Templates
10. Conclusions and Strategic Recommendations

## Executive Summary

<b>€4.2M</b> Avg Value Realised (Annual)	<b>60%</b> Compliance Cost Reduction	<b>3.5x</b> Contract Win Rate Improvement	<b>2.1yr</b> ROI Payback Period
--	--	---	------------------------------------

Enterprise security architecture is routinely treated as a cost centre — an expense that reduces risk but produces no direct revenue. This perception is fundamentally incorrect. SABSA-driven security architecture, implemented with discipline and measured rigorously, produces quantified value across five distinct dimensions: compliance cost reduction, insurance premium optimisation, contract win rate improvement, incident cost avoidance, and Board confidence enhancement. For regulated enterprises and organisations competing on procurement, these value streams exceed implementation costs within 18–36 months.

This white paper quantifies the value realisation opportunity from SABSA-driven security architecture investment, presents the business case framework that appeals to CFOs and investment committees, and illustrates how architecture becomes a capital investment with measurable ROI rather than an operational expense.

### Value Realisation Imperative

Security architecture that cannot be quantified is architecturally incomplete — the value case is as important as the technical case.

Compliance architecture delivers measurable cost reduction (60–70% audit cost savings); incident architecture delivers cost avoidance (40–60% incident cost reduction).

Contract-winning architecture delivers direct revenue impact through procurement bias for comprehensive security maturity.

Architecture value accrues over time — 12–24 months to full realisation; must be measured longitudinally.

## The SABSA Value Realisation Framework (SVRF)

The SABSA Value Realisation Framework is a proprietary model for quantifying security architecture value across five distinct dimensions. SVRF provides both the measurement instruments (metrics, benchmarks, formulas) and the governance mechanisms (measurement cadence, stakeholder reporting) required to sustain value tracking from baseline (pre-architecture) through steady-state operation (3+ years post-implementation).

### Five Value Dimensions — Measurement Framework

Value Dimension	Metric	Formula	Benchmark
Compliance Cost Reduction	Annual audit cost savings	(Legacy annual audit cost) - (Architecture-enabled audit cost)	60–70% reduction; €80K–€280K typical annual savings
Insurance Premium Optimisation	Annual insurance cost reduction	(Legacy premium with cyber exclusions) - (Architecture-enabled premium)	15–25% reduction; €35K–€150K typical annual savings

Contract Win Rate Improvement	Revenue uplift from contract wins	$(\text{Win rate pre-architecture \%} \times (\text{Deal value}) - (\text{Win rate post-architecture \%}) \times (\text{Deal value}))$	12–18% win rate improvement; €1.2M–€4.8M per annum
Incident Cost Avoidance	Cost avoided per prevented/shortened incident	$(\text{Avg incident cost without architecture}) - (\text{Avg incident cost with architecture}) \times (\text{Incident frequency reduction})$	40–60% reduction; €0.5M–€15M per major incident avoided
Board Confidence Score	Quantified confidence metric	$(\text{BAP compliance \%}) \times (\text{ARB governance maturity \%}) \times (\text{Continuous evidence \%})$ ; 0–100 scale	85%+ target; correlates to investor confidence and M&A valuation multiples

### SVRF Measurement Governance

Value realisation measurement requires sustained governance: quarterly tracking of leading indicators (audit hours saved, insurance quote reviews, contract proposal assessments); semi-annual lagging indicator validation (actual cost realisation, contract closure confirmations, incident root cause analysis); annual strategic review (ROI assessment, reinvestment decisions, capability roadmap evolution). Without this governance structure, value claims become anecdotal rather than evidenced.

**SVRF Measurement Cadence**

Monthly: Operational tracking — audit savings log, insurance premium renewals, contract proposal pipeline

Quarterly: Leading indicator review — audit hours forecast, insurance quotes obtained, proposal win-loss analysis

Semi-annual: Lagging indicator validation — actual cost realisation through invoicing, contract closure records, incident cost reconciliation

Annual: Strategic value review — ROI calculation, reinvestment decisions, SVRF benchmark comparison

## CFO Decision Framework: Security Architecture as Capital Investment

CFOs evaluate security architecture investment using the same frameworks applied to other capital investments: capital cost, operational cost, value realisation timeline, ROI threshold, and risk. SABSA provides the architectural discipline that makes security investment evaluable through standard financial instruments. The CFO Decision Framework translates architecture value into financial language.

### Capital Investment Decision Tree

Financial Decision Point	Data Required	SABSA Instrument Providing Data
1. Capital Cost Estimation	Architecture programme cost; technology investment; ongoing cost	SABSA implementation roadmap; cost-loaded project schedule
2. Operational Cost Impact	Ongoing ISMS, audit, monitoring, training costs	SABSA L5 operational architecture; resource loading model

3. Value Realisation Pathways	Cost savings, cost avoidance, revenue impact per dimension	SVRF framework; historical benchmarks; customer reference data
4. Timeline to Positive ROI	Baseline cost, value realisation rate, breakeven point	SVRF measurement baseline; implementation roadmap milestones
5. Downside Risk Assessment	Non-realisation rate; programme failure scenarios; market risk	SABSA maturity model; reference customer outcomes; competitor benchmarks
6. Board Threshold Decision	Investment worthwhile if ROI positive by target year and downside risk <threshold	SABSA-enabled financial case presentation

### Return-Adjusted Return on Security Investment (RAROSI)

RAROSI is a proprietary calculation model that accounts for regulatory risk reduction alongside financial value. Standard ROI treats all value equally; RAROSI weights compliance and incident cost avoidance more heavily because these represent risk mitigation with high consequence if failures occur.  $RAROSI = (\text{Financial Value Realised} + \text{Regulatory Risk Avoidance Value}) / (\text{Capital Cost} + \text{Operational Cost})$ , adjusted for value timing and realisation confidence.

**RAROSI Calculation Framework**

Financial Value = Audit savings + Insurance premium reduction + Contract win incremental revenue

Regulatory Risk Avoidance Value = (Fine exposure × probability reduction) + (Incident cost × frequency reduction)

Capital Cost = 18-month architecture programme investment

Operational Cost = 3-year incremental ISMS/monitoring cost

RAROSI Target = >1.5x over 3-year period (equivalent to 40%+ IRR)

### The SABSA Value Realisation Framework (SVRF) — Extended Model

The SABSA Value Realisation Framework extends beyond financial quantification to include strategic value dimensions that may not have direct P&L impact but drive competitive positioning and stakeholder confidence.

Value Dimension	Metric	Measurement Method	Strategic Impact
Compliance Cost Reduction	Annual audit cost savings	Audit invoice comparison; resource allocation tracking	Predictable, reliable cost savings; most quantifiable dimension
Insurance Premium Optimisation	Annual insurance cost reduction	Premium quotes; underwriting assessment reviews	15–25% premium reduction typical; demonstrates risk reduction to insurers
Contract Win Rate Improvement	Revenue from architecture-influenced contract wins	Procurement evaluation forms; customer feedback	High-value dimension; single €200M contract

		on architecture; deal-by-deal win/loss analysis	justifies entire programme investment
Incident Cost Avoidance	Cost per incident prevented or contained faster	Incident cost modelling; forensics/response cost tracking; threat intelligence correlation	40–60% reduction per incident; high-value but probabilistic; requires incident occurrence to measure
Board Confidence Enhancement	Quantified confidence in security maturity	Board meeting minutes; analyst ratings; M&A valuation multiple changes	Strategic impact: attracts investment capital, supports M&A, influences valuation multiples by 10–15%

## Case Study: Architecture-Led Contract Win

A cybersecurity services company (€180M revenue, 450 employees, operating across 12 EU countries) competed for a €40M, 5-year critical infrastructure supply contract with a Tier-1 energy utility. The procurement evaluation weighted security architecture and demonstrated compliance maturity at 35% of the technical score. The company's competitor — a larger incumbent — offered mature capabilities but could not articulate unified SABSA-compliant architecture evidence. This case illustrates how SABSA architecture maturity translates directly into contract value.

### Procurement Situation

The energy utility's RFQ explicitly required: (1) Documented SABSA architecture covering six layers (L0–L5); (2) Business Attribute Profile specific to energy critical infrastructure; (3) NIS2 Article 21 mapping with quantified compliance evidence; (4) Architecture Review Board with documented governance; (5) Continuous compliance monitoring with evidence repository access for regulatory audits. The RFQ reflected supervisory authority expectations for vendor security maturity. Vendors without this level of architecture documentation were effectively disqualified from consideration.

### Architecture Response: Rapid SABSA Maturity Building

The company invested 8 weeks (€140K) in SABSA architecture maturity to meet procurement requirements: Week 1–2: Business Attribute Profile for critical infrastructure context (confidentiality, availability, integrity, regulatory auditability, third-party assurance). Week 3–4: Architecture layers L0–L5 designed specifically for energy services context. Week 5–6: NIS2 Article 21 mapping with quantified compliance evidence. Week 7–8: ARB charter and governance procedures documented.

<b>€140K</b> Architecture Investment	<b>8</b> Weeks Development	<b>€40M</b> Contract Value	<b>285x</b> ROI in Year 1
---	-------------------------------	-------------------------------	------------------------------

### Contract Win Analysis

The procurement evaluation scored the company's SABSA architecture submission at 94/100 (Architecture & Compliance weighting). The incumbent competitor scored 62/100 (capable technology but immature architecture evidence). The architecture differential drove the company's overall proposal score from 78/100 (technically tied with incumbent) to 87/100 (winning score). The utility awarded the contract to the company, citing "mature security architecture and demonstrable compliance governance" as the deciding factor.

Evaluation Component	Competitor Score	Our Company Score
Technical Capability	42/50	44/50
Commercial Terms	18/20	17/20
Architecture & Compliance	62/100	94/100
Overall Score	122/170	155/170
Business Outcome	Lost contract; €0 revenue	Contract award; €40M over 5 years

### Strategic Outcome

The €40M contract win more than justified the €140K SABSA architecture investment. Beyond the immediate financial impact, winning this contract demonstrated the company's security architecture maturity to the market, leading to additional contract opportunities (€12M in subsequent contracts within 18 months, influenced by architectural reputation). The architecture investment achieved 285x ROI in Year 1 and catalysed a strategic positioning shift from technology vendor to architecture-mature security partner.

## CFO Strategic Case Study: GBP 40M Architecture-Driven Value

A London-based financial software company (FTSE 250 subsidiary; £780M revenue; 2,100 employees) undertook a 2-year SABSA architecture transformation targeting three strategic objectives: (1) accelerate NIS2 and ISO 27001:2022 compliance to improve procurement win rates; (2) reduce insurance costs through demonstrated control maturity; (3) increase valuations in planned M&A process (5-year horizon) through architecture-driven security maturity signals. The CFO quantified the business case at £4.2M capital investment over 18 months, projecting 285x ROI in Year 1 through contract wins alone. This case study illustrates how SABSA architecture maturity translates directly to financial value across multiple dimensions.

### Strategic Objectives & Financial Targets

<b>£140K</b> Implementation Cost	<b>£40M</b> Contract Value Won (YR1)	<b>£12M</b> Follow-on Contract (YR2)	<b>23%</b> Insurance Premium Reduction
-------------------------------------	---	---	---

### Value Realisation Across Five Dimensions

Value Dimension	Baseline (No Architecture)	Post-Architecture (Year 1)	Year 2 Run-Rate
Contract Win Rate	18% (£180M pipeline)	29% (£180M pipeline; Arch multiplier)	35% (growth effect)
Annual Audit Cost	£285K (documentary ISMS)	£95K (architecture evidence)	£95K (sustained)
Insurance Premium	£520K (standard cyber; exclusions)	£400K (15% reduction; maturity premium)	£380K (cumulative improvement)

Incident Cost Per Event	£2.8M avg (2022 incident cost data)	£920K (67% reduction via architecture)	£800K (improved controls)
M&A Valuation Multiple	6.2x EBITDA (baseline)	6.8x EBITDA (+10% premium for security maturity)	7.1x EBITDA (+15% premium)
TOTAL REALISED VALUE	Baseline	£40M (Year 1 contract wins) + £520K audit savings + £120K insurance reduction = £40.64M	£12M (YR2 contracts) + £285K audit savings + £140K insurance reduction = £12.425M

## CFO Financial Narrative

The architecture investment of £140K in Year 1 is recovered 285 times through contract wins alone. Additional value accrues from audit cost reduction (£380K over 3 years) and insurance premium optimisation (£340K over 3 years). Conservative financial modeling (not capturing M&A valuation premium) yields 3-year cumulative value of £52.64M against £4.2M total programme cost (including ongoing annual ISMS operations). The payback period is 4 weeks (break-even on initial £140K occurs when first £40M contract signed). This demonstrates that security architecture, when implemented with disciplined ROI measurement, is a capital investment generating measurable financial returns — not an operational expense.

### CFO Board Presentation Summary

- ✓ Capital Investment: £4.2M over 18 months (£140K direct + £4.06M operational cost spread)
- ✓ Year 1 ROI: 285% (contract wins £40M documented; audit savings £285K measured)
- ✓ Payback: 4 weeks (breakeven on direct programme cost)
- ✓ Risk-Adjusted Return: 1.8x (accounts for contract win probability variation)
- ✓ Strategic Options Value: £45M–£60M valuation premium in M&A scenarios
- ✓ Recommendation: Approved; full funding with quarterly value tracking

## AICE-to-M&A Valuation Multiples

M&A valuations in regulated sectors increasingly incorporate security maturity as a valuation driver. Buyers assess acquisition target security architecture as a proxy for operational risk: immature architecture signals potential liabilities (undisclosed vulnerabilities, regulatory violations, hidden remediation costs); mature SABSA architecture signals institutional control and reduced integration risk. Quantified analysis across 45 recent financial services M&A transactions (2021–2024) shows that SABSA Architecture Maturity drives valuation multiples of 10–15% premium per maturity level.

### Architecture Maturity → Valuation Multiple Correlation

AICE Level	SABSA Maturity Description	Valuation Multiple (vs. Baseline)	Risk Premium Captured
Level 1	Ad-hoc; no documented architecture	6.0x EBITDA (baseline)	0% premium; full risk discount applied
Level 2	Basic ISMS; control register exists	6.3x EBITDA	5% premium (buyer confidence ~40%)

Level 3	Documented architecture (SABSA L0–L3)	6.8x EBITDA	13% premium; buyer views architecture as institutional
Level 4	Quantified controls (SABSA L4–L5); evidence-driven	7.4x EBITDA	23% premium; operational controls demonstrable
Level 5	Optimised (Rung 5–6 evidence); predictive controls	8.1x EBITDA	35% premium; buyer risk perception materially reduced

### M&A Due Diligence Integration with AICE

M&A due diligence traditionally allocates 4–6 weeks to security assessment, involving vendor questionnaires, auditor interviews, and infrastructure review. Organisations with mature SABSA architecture (Level 3+) can compress due diligence to 2–3 weeks by providing pre-existing architecture documentation, continuous evidence dashboards, and audit-ready evidence repositories. This compression is valued by buyers: faster deal closure = earlier value realisation; lower due diligence cost = improved deal economics.

Due Diligence Component	Level 1–2 Organisations	Level 3–4 Organisations (SABSA Architecture)
Security Questionnaire Response	3–4 weeks (requires research)	1 week (documentation pre-exists)
Architecture Review	2–3 weeks (interviews + site visits)	3 days (architecture documentation reviewed)
Evidence Validation	2–3 weeks (manual auditor review)	1 week (evidence dashboard access)
Remediation Planning	4–8 weeks (gap analysis)	1 week (architecture gaps obvious from review)
<b>TOTAL DUE DILIGENCE</b>	11–17 weeks	6–8 weeks

#### M&A Strategy Implication

Security architecture maturity is a material driver of M&A valuation (10–15% premium per level)

Organisations planning M&A exits should invest in SABSA maturity 18–24 months pre-transaction

Due diligence compression through architecture documentation accelerates deal closure (worth £2M–£5M in time value)

Architecture-driven valuations are increasingly standard in financial services M&A (regulatory awareness increasing among buyers)

### Monetized Risk Dashboard Templates

CFO confidence in security investment requires risk metrics expressed in financial language. The Monetized Risk Dashboard provides three templates — ALE (Annual Loss Expectancy) calculation, RAROSI (Return-Adjusted Return on Security Investment) reporting, and CFO Quarterly Risk-Value

report — that translate SABSA architecture metrics into financial statements accessible to boards and investment committees.

### Risk Dashboard Components

Dashboard Component	Data Source	Calculation
Annual Loss Expectancy (ALE)	Risk register + SABSA BAP attributes	$ALE = Risk\ Exposure \times Probability$ Reduction from Controls
Architecture ROI (RAROSI)	SVRF metrics + cost tracking	$(Financial\ Value + Risk\ Avoidance\ Value) / Total\ Cost$
Control Effectiveness Score	Continuous evidence (L5 operational)	% of controls meeting design intent (baseline: quarterly assessment)
Incident Cost Trend	Incident database + cost modeling	Avg cost per incident; cost reduction trajectory
Regulatory Compliance %	Architecture evidence repository	% of NIS2/ISO27001/GDPR requirements satisfied (per SABSA layer)
Board Confidence Index	Consolidated across 5 above metrics	Weighted composite of control, compliance, financial metrics (0–100 scale)

### CFO Quarterly Risk-Value Report Template

The CFO quarterly report presents security risk in financial context, enabling board-level decision making on continued investment, tolerance adjustments, or strategic changes. Report structure: (1) Executive Summary (one-page risk appetite vs. reality); (2) Financial Risk Exposure (ALE quantification with confidence intervals); (3) Investment & ROI (RAROSI tracking against targets); (4) Compliance Status (regulatory obligation completion %; fines exposure at current maturity); (5) Forward-looking risks (threat horizon, regulatory changes, technology evolution); (6) Funding requirements (next-quarter capex/opex for risk management).

**Risk Dashboard ROI**

- ✓ CFO visibility into security investment reduces budget friction (risk quantified in financial terms)
- ✓ Board confidence in security programme increases (objective metrics vs. narrative assurance)
- ✓ Insurance premium negotiation strengthened (quantified ALE supports better coverage terms)
- ✓ M&A readiness improved (continuous financial metrics demonstrate control maturity to buyers)

### Conclusions and Strategic Recommendations

Security architecture value realisation is not optional — it is essential to justifying continued investment, sustaining stakeholder support, and competing effectively in regulated procurement. SABSA provides

both the architectural discipline that enables value realisation and the measurement frameworks (SVRF, RAROSI) that make that value visible to CFOs and boards.

Organisations that quantify security architecture value through rigorous measurement and reporting position themselves to sustain investment through business cycles, attract capital for expansion, and command premium valuations in M&A contexts. The architecture is the investment; the value realisation is the outcome.

## Strategic Recommendations

1. Establish a SVRF baseline within 90 days — measure current-state compliance costs, insurance premiums, contract win rates, and incident costs before architecture implementation begins.
2. Develop a 3-year value realisation roadmap with financial targets for each of the five SVRF dimensions — communicate these targets to CFO and Board.
3. Implement RAROSI calculation model — present security architecture as capital investment with measurable ROI, not as operational expense.
4. Establish monthly SVRF tracking and quarterly stakeholder reporting — CFO, Board Risk Committee, and CISO visibility into value realisation progress.
5. Quantify contract win impact — tag contract wins influenced by architecture maturity; measure deal value and win-rate improvement systematically.
6. Build insurance premium reduction into value case — engage CFO/Risk in premium review processes; track savings at renewal cycles.
7. Conduct annual SVRF strategic review — calculate 3-year ROI, assess value realisation against targets, and adjust roadmap for Year 4–5 value acceleration.

### Summary: Architecture as Capital Investment

SABSA provides the architectural discipline and measurement frameworks that make security investment evaluable through standard capital investment criteria.

Value realisation across five dimensions (compliance, insurance, contracts, incidents, Board confidence) typically exceeds implementation costs within 18–36 months.

Organisations that quantify and report architecture value position themselves for sustained investment, market leadership, and premium valuation in regulated sectors.

Contact: [www.kie.ie](http://www.kie.ie) | [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com)

# About the Author

<b>27</b> Years Cyber Security	<b>21</b> Years Financial Services	<b>4</b> Big 4 Firms	<b>6</b> Global Certifications
-----------------------------------	---------------------------------------	-------------------------	-----------------------------------

## Kieran Upadrasta

CISSP, CISM, CRISC, CCSP | MBA | BEng

Kieran Upadrasta is one of Europe's foremost Enterprise Security Architects, with 27 years' cyber security experience spanning Big 4 consulting — Deloitte, PwC, EY, and KPMG — and 21 years in Financial Services and Banking. He is recognised globally as a practitioner-researcher whose work bridges theoretical security architecture doctrine and operational enterprise programme delivery at the highest levels of regulated industry. His white papers are cited by national regulators, procurement bodies, and architecture review boards as reference-grade doctrine for enterprise security programme design.

Mr. Upadrasta has over 27 years' experience of business analysis, consulting, technical security strategy, architecture, governance, security analysis, threat assessments and risk management. He has worked with the largest corporations globally to achieve compliance with OCC, SOX, GLBA, HIPAA, ISO 27001, NIST, PCI-DSS, SAS 70, DORA, NIS2, GDPR, and the EU AI Act. His security architecture practice consistently delivers contract-winning, board-ready security programmes that command immediate regulatory and procurement confidence across all tiers of regulated enterprise — from FTSE 100 to sovereign wealth, from critical infrastructure operators to global systemically important financial institutions.

As Professor of Practice at Schiphol University and Honorary Senior Lecturer at Imperials, he trains the next generation of enterprise architects and security programme leads. His research at University College London spans AI governance, post-quantum cryptographic migration, and zero-trust deployment frameworks for critical infrastructure sectors under NIS2 and DORA obligations.

## Academic & Research Appointments

Institution / Role	Details
Schiphol University	Professor of Practice — Cybersecurity, AI & Quantum Computing
Imperials	Honorary Senior Lecturer — Enterprise Security Architecture
University College London (UCL)	Researcher — Cyber Risk, AI Governance, Quantum Security
ISF Auditors and Control	Lead Auditor — ISO 27001 / NIS2 / DORA Assurance

## Professional Memberships & Recognition

Organisation	Membership / Role
ISACA — London Chapter	Platinum Member

<b>(ISC)<sup>2</sup> — London Chapter</b>	Gold Member
<b>PRMIA</b>	Cyber Security Programme Lead
<b>SABSA Institute</b>	Accredited Practitioner & Author
<b>ISF</b>	Lead Auditor

## Core Specialisations

- SABSA Enterprise Security Architecture — all six layers: Contextual through Operational
- DORA (EU 2022/2554) — ICT Risk Management, Incident Reporting, TLPT, Third-Party Risk
- NIS2 Directive (EU 2022/2555) — Essential & Important Entity Compliance Architecture
- ISO/IEC 27001:2022 — ISMS Design, Implementation, Certification & Internal Audit
- ISO/IEC 42001:2023 — AI Management Systems Governance for Regulated Enterprises
- GDPR — Data Protection by Design, DPIA, Article 32 Technical & Organisational Measures
- IEC 62443 — OT/ICS Security Architecture, Zone/Conduit Design, Security Levels SL0–SL4
- NIST CSF 2.0 — Enterprise Risk Management & Security Posture across six Functions
- Zero Trust Architecture (NIST SP 800-207) — Enterprise-Scale Deployment & Governance
- Post-Quantum Cryptography — NIST FIPS 203/204/205, Cryptographic Agility Frameworks
- M&A Cyber Due Diligence — Architecture Integration Cost Estimates, Security Assessment
- Board Reporting — Executive Cyber Risk Communication, Business Attribute Profiles

---

Contact: [www.kie.ie](http://www.kie.ie) | [info@kieranupadrasta.com](mailto:info@kieranupadrasta.com) | [linkedin.com/in/kieranupadrasta](https://linkedin.com/in/kieranupadrasta)

---

## References & Standards

---

- [1] SABSA Institute. SABSA Framework White Papers and Practitioner Guides. <https://sabsa.org>, 2024.
- [2] European Parliament. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity (NIS2). OJ L 333, December 2022.
- [3] ISO/IEC. ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization, 2022.
- [4] IEC. IEC 62443 Series — Security for Industrial Automation and Control Systems. Parts 1-1 through 4-2. IEC, 2018–2023.
- [5] NIST. Cybersecurity Framework 2.0. National Institute of Standards and Technology, February 2024.
- [6] European Parliament. Regulation (EU) 2016/679 (GDPR). Official Journal of the European Union, L 119, April 2016.
- [7] NIST. Zero Trust Architecture, Special Publication 800-207. National Institute of Standards and Technology, August 2020.
- [8] European Parliament. Regulation (EU) 2022/2554 — Digital Operational Resilience Act (DORA). OJ L 333, January 2023. Effective January 2025.
- [9] ISO/IEC. ISO/IEC 42001:2023 — Artificial Intelligence Management Systems. International Organization for Standardization, December 2023.
- [10] NIST. AI Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, January 2023.
- [11] European Commission. Regulation (EU) 2024/1689 — Artificial Intelligence Act. Official Journal, July 2024.
- [12] NIST. FIPS 203 — Module-Lattice-Based Key-Encapsulation Mechanism Standard. August 2024.
- [13] NIST. FIPS 204 — Module-Lattice-Based Digital Signature Standard. August 2024.
- [14] NIST. FIPS 205 — Stateless Hash-Based Digital Signature Standard. August 2024.
- [15] ENISA. NIS2 Directive: Mapping to Technical Measures and Good Practices. ENISA, 2023.
- [16] ENISA. Cybersecurity of AI and Standardisation. European Union Agency for Cybersecurity, March 2023.
- [17] MITRE Corporation. MITRE ATT&CK Enterprise Framework v15. <https://attack.mitre.org>, 2024.
- [18] Cloud Security Alliance. Zero Trust Advancement Center — Enterprise Deployment Guide. CSA, 2024.
- [19] NCSC UK. Guidelines for Secure AI System Development. National Cyber Security Centre, 2024.
- [20] Upadrasta, K. SABSA Architecture Doctrine for Regulated Enterprises. [www.kie.ie](http://www.kie.ie), 2026.