SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

WP03 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0

Auditing the SABSA Framework

Achieving ISO 27001 Compliance Through Architecture-Led Assurance

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)² Gold (London) | PRMIA Cyber Lead

www.kie.ie | 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. ISO 27001:2022 Control Framework — Organisational, People, Physical, Technology
3. Architecture Evidence Ladder — Six-Rung Framework for Audit-Ready Compliance
4. Case Study: ISO 27001 Stage 2 Audit — Architecture as Evidence
6. Certification Timeline Artefact & Audit Pack
7. AI-Driven Automated Audit Verification (Rung 6)
8. Monetized Audit ROI & Compliance Value
9. Conclusions and Strategic Recommendations

Executive Summary

114	6	2x	1
ISO 27001:2022 Controls	SABSA Architecture Layers	Audit Efficiency Gain	Integrated Framework

ISO 27001:2022 introduced a revised control framework with 11 new controls, restructured control taxonomy, and strengthened requirements for supply chain security, threat intelligence, and ICT continuity. Yet many organisations implement ISO 27001 as a documentation exercise — control registers, policies, and procedures — without ensuring that these controls actually operate as designed in the organisation's real information security architecture. SABSA provides the architecture-centric approach that makes ISO 27001 implementation operationally effective: every control maps to an architectural artefact that can be independently verified, continuously monitored, and improved through architecture change management.

This white paper demonstrates how SABSA's six-layer architecture model transforms ISO 27001 from a compliance framework into an operational reality, where every control is architected, evidence is continuous, and audit becomes validation of design intent rather than excavation of documentation. For organisations seeking genuine information security, not just compliance theatre, architecture-centric ISMS is the only sustainable approach.

Architecture-Centric ISMS Imperative

ISO 27001:2022 controls cannot be sustained through policy alone — they require architecture.

Audit evidence that is "continuous and automated" demands architecture-integrated monitoring, not retroactive documentation.

Every ISO 27001 control should map to a SABSA architectural layer and produce an independent evidence artefact.

Architecture Review Board governance ensures ISMS controls survive technology change cycles.

ISO 27001:2022 Control Framework — Organisational, People, Physical, Technology

ISO 27001:2022 reorganises controls into four themes: Organisational controls (strategy, policies, governance); People controls (competence, awareness, behaviour); Physical controls (perimeter, access, environmental); and Technological controls (identity, cryptography, monitoring, coding). This four-theme structure aligns naturally to SABSA architecture layers: Organisational controls map to SABSA L0–L1 (Contextual/Conceptual); People controls to L1–L2 (Conceptual/Logical — identity and access management); Physical controls to L3 (Physical Architecture); Technological controls to L4–L5 (Component/Operational). This alignment enables systematic architecture-to-control traceability.

ISO 27001 Theme	SABSA Layer(s)	Control Count
Organisational (A.5)	L0–L1	14 controls
People (A.6, A.7)	L1–L2	7 controls

Physical (A.7)	L3	6 controls
Technological (A.8)	L4–L5	87 controls

The ISMS as Architecture

An architecture-centric ISMS treats the organisation's information security posture as a designed system with explicit layers of abstraction, defined security zones, trust boundaries, and operational procedures. This contrasts with documentation-centric ISMS, which produces control registers and procedures but does not ensure architectural coherence or operational effectiveness. The SABSA architecture model provides the framework that makes ISMS implementation architectural rather than administrative.

Architecture Evidence Ladder — Six-Rung Framework for Audit-Ready Compliance

The Architecture Evidence Ladder is a proprietary six-rung model that maps evidence types to SABSA architecture layers, auditor expectations, and continuous compliance monitoring. Each rung represents a level of architectural maturity and evidence sophistication, from policy documentation at the bottom to automated continuous compliance evidence at the top. The ladder provides a structured pathway for organisations to progress from documentation-centric compliance to architecture-driven assurance.

Architecture Evidence Ladder — Six Rungs of Compliance Maturity	
Rung 6: Continuous Evidence	Automated, real-time evidence collection (L4–L5). Monitoring produces control evidence as operational byproduct. Audit accesses evidence through dashboard. Example: EDR tool automatically collects endpoint security evidence; audit accesses via SIEM dashboard.
Rung 5: Architecture Artefacts	Design documents produce evidence (L2–L4). Control architecture blueprints, configuration baselines, security zone diagrams ARE the evidence. Auditors review architecture to verify design intent.
Rung 4: Operational Procedures	Documented runbooks and procedures (L5). Control execution is procedurally formalised; audit verifies procedure compliance through operational logs.
Rung 3: Policy & Standards	Organisational policies define controls (L0–L1). Audit verifies policy existence and Board approval; evidence is documentary only.
Rung 2: Control Register	ISMS produces control register (meta-level). Controls listed, ownership assigned, status tracked. Evidence is meta — about controls, not from controls.
Rung 1: Compliance Obligation	Regulatory or standard requirement identified (meta-level). Compliance obligation documented; no implementation evidence yet.

Mapping Evidence Types to SABSA Layers

Evidence Rung	SABSA Layer	Evidence Type
Rung 6	L4–L5	Automated monitoring output

Rung 5	L2–L4	Architecture artefacts (diagrams, baselines, designs)
Rung 4	L5	Operational procedures and logs
Rung 3	L0–L1	Policies, standards, procedures
Rung 2	Meta	Control register/tracking sheet
Rung 1	Meta	Regulatory requirement mapping

Climbing the Evidence Ladder — Maturity Progression

Organisations typically begin at Rung 1 (compliance obligation identified) or Rung 2 (control register created) during ISMS design. Phase 1 implementation produces Rungs 3–4 (policies and procedures). Phase 2 (architecture implementation) produces Rung 5 artefacts. Phase 3 (operational maturity) automates evidence collection at Rung 6. This progression is not instantaneous — it typically takes 12–18 months to reach Rung 5 maturity across the full control set, and 24+ months to achieve Rung 6 across all 114 ISO 27001:2022 controls. However, organisations that commit to architecture-centric ISMS reach these higher rungs substantially faster than documentation-centric programmes.

Evidence Ladder Maturity Indicators

Rung 3–4 Organisations: ISMS audit involves document review; auditors spend 40–60% of time examining policies and procedures.

Rung 5 Organisations: ISMS audit involves architecture review; auditors spend 40–60% of time examining blueprints and baselines; less policy review.

Rung 6 Organisations: ISMS audit involves dashboard queries and automated evidence export; auditor review time cut by 50%; zero-finding audits possible.

Case Study: ISO 27001 Stage 2 Audit — Architecture as Evidence

A mid-market financial software company (350 employees, €45M revenue) operating SaaS platforms for payment processing and banking integration sought ISO 27001:2022 certification within 12 months to meet customer procurement requirements. The organisation had conducted a Stage 1 (documentation review) audit that identified 8 non-conformities, primarily related to missing policies and incomplete control documentation. The company engaged an architecture-centric approach to transform these documentary gaps into architectural controls that would be both compliant and operationally effective. The result was a Stage 2 audit with zero non-conformities — achieved through SABSA architecture implementation, not policy writing.

Situation: Stage 1 Non-Conformity Profile

Non-Conformity	Audit Finding
A.5.12 Access Control	Policy absent; no documented access control strategy
A.5.33 Information Handling	Data classification absent; no handling procedures

A.7.2 Physical Entry	Facility access procedures not documented; tailgating observed
A.8.3 Cryptography	Cryptographic standard not specified; inconsistent algorithms in use
A.8.9 Configuration Management	Configuration baseline missing; no drift detection
A.8.16 Monitoring Activities	SIEM deployed but not integrated; monitoring logs not retained
A.8.27 Secure Development	Code review process informal; no secure coding standards
A.8.28 Secure Coding	SAST tools not integrated; vulnerability management reactive

Architecture Response: Four-Month Remediation Programme

Rather than writing policies and procedures (documentary fix), the remediation programme applied SABSA architecture discipline: L0–L1 governance structures, L2 logical security domains, L3 physical security architecture, L4 component standards, and L5 operational procedures integrated with monitoring. Each non-conformity was resolved through architectural implementation, producing artefacts that served both as ISMS controls and as working operational documents.

Non-Conformity	Architectural Response	Evidence Artefact Produced
A.5.12 Access Control	L2 Identity Architecture: Logical access control domains; RBAC model	Access control architecture blueprint; Role definition matrix; Approval workflow
A.5.33 Information Handling	L1–L2 Data Classification: Business Attribute Profile assigned data sensitivity; handling rules	Data classification scheme; BAP mapping; Handling procedure matrix
A.7.2 Physical Entry	L3 Physical Architecture: Security zone design; access control by zone; badging system	Physical architecture diagram; Zone access matrix; Badge issuance SOP
A.8.3 Cryptography	L4 Component: Cryptographic standards library; approved algorithms; implementation guide	Standards document; Algorithm whitelist; Implementation decision log
A.8.9 Configuration Management	L4 Baseline: Configuration baseline published; ARB change control process; drift detection rules	Configuration baseline document; ARB charter; Drift detection dashboard
A.8.16 Monitoring	L5 Operational: Logging architecture; SIEM integration; evidence retention SLAs	SIEM architecture diagram; Log retention policy; Evidence chain SOP
A.8.27/28 Secure Development	L4 Secure SDLC: Development architecture; code review gates; SAST integration; feedback loop	SDLC architecture diagram; Tool integration specification; Code review SOP

Stage 2 Audit Outcome

The Stage 2 audit was conducted 4 months after the architecture remediation programme began. Every non-conformity from Stage 1 was resolved through architectural implementation. The audit approach differed markedly from typical compliance audits: instead of reviewing 200+ pages of policy and procedure documentation, auditors reviewed SABSA architecture artefacts (6 core architecture diagrams), visited configuration baselines and monitoring dashboards, and traced 5 sampled controls from SABSA layer down to operational evidence. The audit concluded with zero non-conformities and issued the ISO 27001:2022 certificate.

0	4	€180K	12
Stage 2 Non-Conformities	Months Remediation	Cost vs. €450K Documentary Fix	Months ISMS Operational

Key Evidence Architecture Mappings

Control (Clause)	SABSA Architecture Layer
A.5.12 (Access Control)	L2 Logical Architecture
A.5.33 (Information Handling)	L1 Conceptual (BAP)
A.7.2 (Physical Entry)	L3 Physical Architecture
A.8.3 (Cryptography)	L4 Component
A.8.9 (Configuration Management)	L4 Component + ARB
A.8.16 (Monitoring)	L5 Operational
A.8.27 & A.8.28 (Secure Development)	L3–L4 SDLC Architecture

Certification Timeline Artefact & Audit Pack

ISO 27001:2022 certification requires a structured sequence of assessment and implementation phases, each with documented artefacts, evidence requirements, and regulatory touchpoints. The Certification Timeline Artefact maps each phase to its evidence requirements and SABSA architectural layer, enabling organisations to plan certification programmes with precision and predictability.

ISO 27001 Certification Stages — Timeline and Deliverables

Stage	Name	Duration	Key Deliverables & Evidence
Phase 0	Gap Analysis & Scoping	4 weeks	Current ISMS assessment; scope definition; compliance maturity baseline; risk landscape characterisation
Phase 1	Risk Assessment & Design	6 weeks	ISMS design document; L0–L2 SABSA architecture; risk treatment plan; BAP design; control selection rationale

Phase 2	Control Implementation	12 weeks	Control implementation across L2–L4 SABSA layers; operational procedures (L5); training delivery; configuration baselines; architecture evidence repository
Phase 3	Internal Audit	3 weeks	Internal audit plan; audit findings report; evidence compilation; remediation tracking; audit closing meeting
Stage 1 Audit	Documentation Review	2 weeks	Auditor review of ISMS design documents, policies, architecture artefacts; gap identification; readiness assessment
Stage 2 Audit	Operational Verification	3 weeks	Auditor on-site verification; process observation; evidence validation; control effectiveness testing; certification decision
Post-Cert	Surveillance & Improvement	Ongoing	Annual surveillance audits; internal audit programme; control effectiveness reviews; CAPA management; certification renewal (3-year cycle)

Audit Evidence Pack — Mapped to SABSA Layers

The audit evidence pack organises all required evidence into 6 categories aligned to SABSA architecture layers. Each category contains architecture artefacts, operational logs, and documentation that collectively demonstrate compliance design and operational effectiveness.

SABSA Layer	Evidence Category	Audit Pack Contents	Sufficiency Criterion
L0–L1 (Contextual/Conceptual)	Governance & Strategy	Board ISMS approval; Risk appetite statement; BAP document; Regulatory obligation register; Annual management review records	Complete coverage of governance chain from Board to operations; audit scope definition clear
L2 (Logical)	Architecture & Policy	Security domain diagrams; Trust boundary specifications; Policy framework; Access control matrices; Data classification scheme	Every control linked to architecture artefact; policies derive from architecture, not standalone
L3–L4 (Physical/Component)	Infrastructure & Configuration	Physical security diagrams; Configuration baselines; cryptographic standards; Tool specifications; Secure SDLC architecture	Configuration baselines version-controlled; deviations tracked; component certifications provided
L5 (Operational)	Procedures & Evidence	Runbooks; Training records; Incident logs; Audit trails; Monitoring	Evidence is continuous and automated where possible; manual procedures have

		evidence; Change management records	execution logs; evidence retention meets regulatory timelines
Cross-Layer	Controls Mapping	Control-to-SABSA-Layer matrix; Evidence trail for sampled controls (end-to-end from requirement to evidence)	Auditors validate 15–20 sampled controls; 100% traceability from control clause to operational evidence required
Assessment	Audit-Ready Indicators	Internal audit checklist completion; Maturity assessment (Rung 4–5 evidence target); Evidence repository access for auditor queries	Minimum Rung 4 (Operational Procedures) for Stage 2 readiness; Rung 5 (Architecture Artefacts) target for efficient audit

Certification Timeline Critical Path

Week 0–4: Establish scope and baseline maturity — determines overall timeline
Week 4–10: Risk assessment + SABSA architecture design — longest lead-time activity
Week 10–22: Control implementation + internal audit prep — heaviest resource load
Week 22–25: Internal audit + remediation — typically 1–2 findings for architecture-led programmes
Week 26–28: Stage 1 audit — usually closes with minimal gaps when architecture-centric
Week 29–31: Stage 2 audit — 3-week operational verification; zero findings achievable with Rung 5 maturity
Week 32+: Post-certification; annual surveillance audits every 12 months

AI-Driven Automated Audit Verification (Rung 6)

The Architecture Evidence Ladder reaches maturity at Rung 6 when evidence collection is fully automated through SABSA L5 operational architecture. AI-driven audit verification uses machine learning to continuously assess control compliance, aggregate evidence, and flag anomalies requiring human investigation. This approach transforms auditing from a time-intensive excavation activity into a continuous dashboard-based assurance model.

Rung 6 — Continuous Evidence Architecture

Evidence Ladder Rung 6 — Continuous Compliance Monitoring	
Rung 6: Continuous Evidence	Automated, real-time evidence collection (L4–L5). Monitoring produces control evidence as operational byproduct. Audit accesses evidence through dashboard.
Rung 5: Architecture Artefacts	Design documents produce evidence (L2–L4). Control architecture blueprints, configuration baselines, security zone diagrams ARE the evidence.
Rung 4: Operational Procedures	Documented runbooks and procedures (L5). Control execution is procedurally formalised; audit verifies procedure compliance.

Rung 3: Policy & Standards	Organisational policies define controls (L0–L1). Audit verifies policy existence and Board approval; evidence is documentary.
Rung 2: Control Register	ISMS produces control register (meta-level). Controls listed, ownership assigned, status tracked.

Autonomous Evidence Collection at L5

Evidence collection at Rung 6 operates across three parallel streams: (1) System-generated evidence (logs, metrics, alerts) — captured automatically by monitoring infrastructure without human intervention. (2) Process-generated evidence (change approvals, approvals, incident closure records) — extracted from workflow systems. (3) Assessment evidence (control testing results, vulnerability scans, compliance assessments) — triggered on schedule and integrated into evidence repository.

Evidence Stream	Example Evidence Type	Collection Method
System-Generated	EDR logs; SIEM alerts; firewall blocks	Continuous log shipping (agent-based)
Process-Generated	Change approval records; incident closure notes; training completion dates	Workflow system API; database replication
Assessment-Generated	Vulnerability scan reports; penetration test results; control test results	Scheduled assessments (quarterly); ad-hoc testing

AI Compliance Assessment Models

Machine learning models assess control compliance by comparing current evidence against baseline patterns trained on historical data. Isolation Forest models identify anomalies indicating control failure (e.g., access controls disabled, logging stopped, approved changes not deployed). Time-series analysis detects drift in control effectiveness (e.g., incident resolution SLA degradation, audit finding frequency increase). Decision tree models filter false positives — distinguishing between benign anomalies (temporary disruption) and genuine compliance failures.

Rung 6 Audit Efficiency Gains

✓ Auditor document review time: 40–60% reduction (architecture artefacts are pre-validated by AI)

✓ Evidence compilation time: 80%+ reduction (evidence exported on-demand vs. manual gathering)

✓ Audit cycle time: 50%+ reduction (evidence ready before auditor arrival)

✓ Non-conformity discovery time: Near-zero (anomalies detected within 24 hours vs. findings discovered during audit)

✓ Zero-finding audits: Achievable with Rung 6 maturity + continuous remediation

Monetized Audit ROI & Compliance Value

ISO 27001 certification requires ongoing investment: initial certification (€180K–€450K), annual internal audits (€30K–€80K), external surveillance audits (€25K–€65K/year). Yet many organisations do not calculate the value realisation from certification. Architecture-centric ISMS produces quantifiable audit cost savings that exceed certification costs within 2–3 years, whilst simultaneously reducing compliance risk.

Audit Cost Reduction Model

€320K	€95K	70%	€225K
Annual Audit Cost Baseline (Documentary ISMS)	Annual Audit Cost (Architecture-Centric ISMS)	Cost Reduction via Architecture	Annual Savings

Cost Category	Documentary ISMS (Year 1 Post-Cert)	Architecture-Centric ISMS
Internal Audit Preparation	€40K	€8K
External Stage 2 Audit	€65K	€18K
Annual Surveillance Audit	€55K	€18K
Non-Conformity Remediation	€80K avg	€12K avg
Management Review & CAPA	€25K	€8K
Compliance Reporting & Attestations	€55K	€25K
TOTAL ANNUAL COST	€320K	€95K

Compliance Value Realisation (3-Year View)

Value Dimension	Year 1	Year 2	Year 3
Audit Cost Savings	€90K (initial, partial realisation)	€225K (full year)	€225K (sustained)
Non-Conformity Avoidance	€0 (findings still occur)	€120K (fewer findings/remediation)	€150K (near-zero findings)
Insurance Premium Reduction	€0 (immediate, not captured)	€35K (renewal reflects maturity)	€50K (continued reduction)
Certification Integrity (Brand)	€0 (direct)	€200K (contract wins influenced)	€400K (reputation premium)
TOTAL VALUE REALISATION	€90K	€580K	€825K

Compliance Premium in Procurement

Procurement customers increasingly require ISO 27001:2022 certification as a minimum threshold. However, two equal certifications may have very different value signals: a documentary ISMS with non-conformity findings signals weak implementation; an architecture-centric ISMS with zero findings signals

institutional maturity. Procurement decisions are influenced by audit report quality: clean Stage 2 audits command procurement premium (3–8% of contract value in regulated sectors).

Procurement Value Drivers

Zero non-conformities in Stage 2 audit = procurement confidence premium (€1M–€4M per €100M contract in regulated sectors)

Published SABSA architecture maturity in proposal = competitive differentiation (15–25% higher win rate vs. certification-only positioning)

Continuous compliance evidence (Rung 5–6 maturity) = auditor attestation of institutional control (enhances Board confidence)

Real-time audit readiness (evidence dashboard access) = risk reduction perception (customer views you as low-risk vendor)

Conclusions and Strategic Recommendations

ISO 27001:2022 represents an opportunity for organisations to move beyond compliance-centric ISMS to architecture-centric information security. The new controls — particularly A.5.30 (ICT Continuity), A.8.9 (Configuration Management), and A.8.16 (Monitoring) — demand architectural thinking and continuous evidence. SABSA provides the framework that makes this transition systematic and sustainable.

The Architecture Evidence Ladder provides a maturity model for ISMS progression: organisations currently at Rungs 1–3 (compliance obligations, control registers, policies) can climb systematically to Rungs 5–6 (architecture artefacts, continuous evidence) through structured implementation. This progression increases both control effectiveness and audit efficiency — fewer audit findings, faster certification cycles, lower audit costs.

Strategic Recommendations

1. Map your current ISO 27001:2022 control set to SABSA layers — identify which controls are still at Rung 3–4 (policy/procedure) and which have progressed to Rung 5 (architecture).
2. Design your ISMS around SABSA architecture layers — treat information security as a designed system, not a documented checklist.
3. Develop architecture artefacts for every control — blueprints, baselines, zone diagrams, and procedures become the ISMS evidence.
4. Integrate ISMS controls into Configuration Management Baseline (L4) — architecture review board approval becomes control governance.
5. Automate evidence collection at the operational layer (L5) — SIEM, EDR, and monitoring systems produce control evidence as operational byproduct.
6. Plan for Rung 6 maturity (continuous evidence) — 18–24 months to achieve across full control set; prioritise high-risk controls for automation.

Summary: Architecture as ISMS Foundation

SABSA architecture transforms ISO 27001 from a documentation framework into an operational control system.

The Architecture Evidence Ladder provides a maturity pathway from documentation-centric ISMS (Rungs 1–4) to architecture-centric assurance (Rungs 5–6).

Organisations that implement architecture-centric ISMS achieve faster certification, fewer audit findings, and sustainable control effectiveness through change cycles.

About the Author

27	21	4	6
Years Cyber Security	Years Financial Services	Big 4 Firms	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

(ISC)² — London Chapter	Gold Member
PRMIA	Cyber Security Programme Lead
SABSA Institute	Accredited Practitioner & Author
ISF	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 | info@kieranupadrasta.com | 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, 2026.