

SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

WP10 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0

Cloud Security Architecture Under SABSA

Navigating Multi-Cloud Complexity with NIS2 Alignment — Enterprise Cloud Security Doctrine for Regulated Environments



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. Cloud Security Architecture — Shared Responsibility Model
3. GDPR and Data Sovereignty in Cloud Architecture
4. Cloud Security Posture Management (CSPM)
5. Cloud-Native Security Architecture
6. Cloud Incident Response Architecture
7. Cloud Regulatory Compliance Architecture
8. Cloud Operating Models: Regulated vs. Hyperscale
9. Serverless & Container Security for Kubernetes-Native Flows
10. Monetized Cloud Risk Dashboard
11. Conclusions and Strategic Recommendations

Executive Summary

94% Enterprises using multi-cloud	80% Cloud breaches due to misconfiguration	GDPR Data Sovereignty Obligation	NIS2 Cloud ICT Risk Applies
---	--	--	---------------------------------------

Cloud adoption has become the default enterprise IT strategy. Yet the security implications of multi-cloud deployment — data sovereignty risks, shared responsibility model misunderstandings, misconfiguration-driven breaches, and regulatory compliance across heterogeneous cloud platforms — remain inadequately addressed by most enterprise security architectures. SABSA provides the governance and architecture framework that makes multi-cloud security coherent, regulatorily evidenceable, and operationally sustainable.

This white paper delivers the cloud security architecture doctrine for enterprises operating in AWS, Azure, Google Cloud, and SaaS environments under NIS2, GDPR, and ISO 27001:2022 obligations. It provides SABSA-based architecture patterns, shared responsibility clarity, multi-cloud governance models, and the compliance evidence architecture that makes cloud security auditable.

Cloud Security Architecture Imperatives

- NIS2 Art.21 applies to cloud-hosted systems — cloud is not outside regulatory scope
- GDPR Art.25: Privacy by Design applies to cloud architecture — data residency must be designed, not assumed
- ISO 27001 A.5.23 (new 2022): ICT supply chain security — cloud providers ARE supply chain risk
- Shared Responsibility: Cloud providers secure the platform; customers secure everything they deploy ON the platform
- SABSA Role: Governance framework and architecture model that spans on-premises and all cloud platforms uniformly

Cloud Security Architecture — Shared Responsibility Model

The cloud shared responsibility model defines which security controls are the cloud provider's responsibility and which are the customer's. The most common source of cloud security failures is customer assumption that the cloud provider has covered more than it actually has. SABSA L0 governance must make the shared responsibility boundary explicit for every cloud platform and service type in use — so that architecture gaps at the customer boundary are designed away, not discovered during a breach.

Shared Responsibility Matrix — Enterprise Cloud

Security Domain	IaaS (AWS/Azure/GCP)	PaaS (RDS/App Service/BigQuery)	SaaS (M365/Salesforce/Workday)
Physical Security	Provider	Provider	Provider
Network Infrastructure	Provider	Provider	Provider
Hypervisor/Platform	Provider	Provider	Provider
Operating System	Customer	Provider	Provider

Network Controls (Security Groups)	Customer	Customer	Provider (limited)
Application Security	Customer	Customer	Customer/Provider
Data Classification & Encryption	Customer	Customer	Customer
Identity & Access Management	Customer	Customer	Customer
Monitoring & Logging	Customer (CloudTrail etc.)	Customer	Customer (API access)
Compliance & Regulatory	Customer	Customer	Customer

SABSA Cloud Security Architecture Model

Multi-Cloud Security Architecture — SABSA Governance	
L0: Cloud Governance	Cloud Security Architecture Standard (platform-agnostic policy); Cloud ARB; CSPM programme; Board-approved cloud risk appetite.
L1: Cloud Risk Model	Cloud-specific threat model (CSA STRIDE); GDPR data sovereignty risk; NIS2 cloud asset scoping; concentration risk assessment.
L2: Logical Cloud Architecture	Cloud security zones (Landing Zone); data classification; cloud IAM governance; third-party SaaS governance.
L3: Physical Cloud Architecture	Per-platform security design: AWS SCPs; Azure Policy; GCP Org Policy; VPC/VNET architecture; network security groups.
L4: Cloud Component Architecture	Encryption standards (KMS/BYOK/HYOK); container security; serverless security; API security; cloud-native WAF configuration.
L5: Cloud Operations	CSPM continuous monitoring; SIEM cloud log integration; cloud incident response; compliance evidence generation.

GDPR and Data Sovereignty in Cloud Architecture

GDPR data sovereignty requirements are among the most architecturally complex cloud security obligations. Chapter V restrictions on cross-border data transfers, Article 25 Privacy by Design, and the data residency requirements for personal data of EU data subjects create specific architecture constraints that must be designed into cloud deployments — they cannot be addressed through cloud provider terms of service alone.

Data Sovereignty Architecture Decisions

Data Category	Sovereignty Requirement	Architecture Solution
EU Personal Data (GDPR)	EU-only processing; no transfer to non-adequate third countries	Cloud region selection: EU-only regions; GDPR data residency constraints in IaC templates
Health Data (GDPR Special Category)	Highest GDPR protection; explicit consent; DPIA mandatory	Dedicated cloud environment; enhanced encryption (HYOK); strict

Financial Data (DORA)	EU regulatory access requirements; audit trail; supervisory examination rights	access control; DPIA for every processing change EU cloud regions; no data residency restriction in provider contract; data portability guaranteed
Critical Infrastructure Data (NIS2)	NIS2 Art.21 measures apply; potential data localisation requirements	National security classification assessment; government cloud consideration; hybrid cloud for highest criticality
Employee Data (GDPR Art.88)	Employment law data minimisation; purpose limitation; retention limits	HR SaaS with EU data centre; data retention policy enforcement; access limitation to HR function

Standard Contractual Clauses and Cloud Providers

Following the Schrems II ECJ ruling and the replacement EU-US Data Privacy Framework, data transfers to cloud providers with US-based processing require either the EU-US Data Privacy Framework adequacy decision or Standard Contractual Clauses (SCCs) supplemented by a Transfer Impact Assessment (TIA). The SABSA L1 trust model must document the legal basis for every cross-border data transfer — this documentation is both a GDPR obligation and a supervisory examination expectation under NIS2.

Cloud Security Posture Management (CSPM)

Cloud Security Posture Management is the continuous monitoring of cloud infrastructure configurations against security and compliance standards. CSPM tools — Wiz, Prisma Cloud, Microsoft Defender for Cloud, AWS Security Hub — continuously scan cloud environments for misconfigurations, exposed credentials, overly permissive IAM policies, and unencrypted data stores. For SABSA-based enterprises, CSPM is the L5 Operational monitoring capability for the cloud security domains defined at L2–L4.

CSPM Architecture — Multi-Cloud Coverage

CSPM Capability	AWS	Azure	GCP
Native CSPM	AWS Security Hub + Macie + Inspector	Microsoft Defender for Cloud	Security Command Center
Unified Multi-Cloud CSPM	Wiz / Prisma Cloud / Orca Security (spans all three)	Same	Same
IaC Security Scanning	Checkov + AWS CFN Guard	Checkov + tfsec	Checkov + Terrascan
Runtime Protection	GuardDuty + Inspector	Defender for Servers	Security Command Center Threat Detection
Data Security Posture	Macie (S3 data classification)	Purview (storage data classification)	DLP API + Data Catalog
NIS2/ISO 27001 Compliance	Security Hub — CIS AWS Foundations	Defender — Azure Security Benchmark	SCC — CIS GCP Benchmark

CSPM Compliance Evidence Architecture

Continuous compliance: CSPM generates real-time compliance score against CIS benchmarks, NIS2 measures, ISO 27001 controls

Evidence export: Monthly compliance report exported from CSPM → uploaded to compliance evidence repository

Audit trail: All configuration changes tracked — who changed what, when, from what state to what state

Remediation tracking: CSPM findings linked to JIRA/ServiceNow tickets — architecture remediation tracked to closure

Board reporting: Monthly CSPM compliance score included in Board cyber risk dashboard — trend charted quarterly

Cloud-Native Security Architecture

Cloud-native applications — built on containers, serverless functions, microservices, and API-first architectures — introduce security requirements that traditional enterprise security architectures were not designed to address. SABSA L4 Component Architecture specifications for cloud-native environments must cover container security, Kubernetes (K8s) security, API security, and the supply chain security of the software components that compose cloud-native applications.

Cloud-Native Security Architecture Specifications

Cloud-Native Layer	Security Architecture Requirement	Technology Controls
Container Images	Signed images only; vulnerability scanning; minimal base images	Trivy/Grype scanning in CI/CD; Docker Content Trust; distroless base images
Kubernetes Clusters	RBAC; network policies; Pod Security Standards; secrets management	K8s RBAC; Calico/Cilium network policies; OPA/Gatekeeper; Vault for secrets
Microservices	mTLS between services; API authentication; service mesh	Istio/Linkerd service mesh; SPIFFE/SPIRE identity; API gateway authentication
Serverless Functions	Least privilege execution role; VPC deployment; no hardcoded credentials	Lambda/Cloud Functions IAM; VPC endpoint; Secrets Manager integration
CI/CD Pipeline	SAST; DAST; SCA; secrets scanning; SBOM generation	Snyk/Checkmarx SAST; OWASP ZAP DAST; Dependabot; Gitleaks; CycloneDX SBOM
API Security	API gateway; OAuth 2.0; rate limiting; API inventory	AWS API GW/Azure APIM; OAuth/OIDC; WAF rate limiting; API Security Posture Management

Cloud Incident Response Architecture

Cloud incident response requires architecture-specific playbooks that account for the ephemeral nature of cloud resources, the shared responsibility model, and the API-driven forensics capabilities of cloud platforms. A cloud incident where evidence is lost because the ephemeral container was terminated before forensic capture is both a security failure and a regulatory compliance failure — destroying evidence required for NIS2 incident reporting and GDPR breach notification.

Cloud IR Architecture

IR Phase	Cloud Architecture Requirement
Detection	CloudTrail/Activity Log alerts; CSPM runtime alerts; SIEM cloud log correlation; GuardDuty/Defender threat detection
Containment	Automated quarantine via Lambda/Logic App/Cloud Function; Security Group modification to isolate compromised instance; snapshot before termination
Evidence Preservation	Automated memory dump; EBS/Managed Disk snapshot; VPC Flow Log export; CloudTrail log export to immutable S3
Investigation	Cloud forensics tooling; CloudTrail event reconstruction; SIEM timeline; CSPM configuration diff
Notification	Automated NIS2 Art.23 severity assessment; DORA Art.19 classification; DPA notification workflow if personal data involved
Recovery	IaC re-deployment from known-good state; no manual rebuild from compromised instance; post-incident architecture review

Cloud Regulatory Compliance Architecture

Cloud environments must satisfy the same regulatory obligations as on-premises environments — NIS2, ISO 27001, GDPR, and DORA do not have cloud exemptions. The SABSA compliance evidence architecture for cloud must generate regulatory compliance evidence from cloud-native tooling and integrate it into the unified compliance evidence repository that serves all three regulatory frameworks.

Regulation	Cloud Compliance Obligation	Architecture Evidence Source	SABSA Layer
NIS2 Art.21	Technical measures for cloud-hosted systems	CSPM compliance report; CloudTrail audit log; SIEM alert evidence	L5: Cloud monitoring architecture
ISO 27001 A.5.23	ICT supply chain security — cloud provider assessment	Cloud provider SOC 2 Type II; ISO 27001 certificate; CSA STAR	L1: Supply chain trust model
ISO 27001 A.8.9	Configuration management — cloud configurations	IaC templates in VCS; CSPM configuration baseline; drift alerts	L4–L5: IaC architecture
GDPR Art.25	Privacy by Design — cloud architecture	Data residency architecture documentation; DPIA for cloud processing	L2–L3: Cloud data architecture

GDPR Art.32	Technical measures — encryption, access control	CSPM encryption report; IAM access review; KMS key rotation log	L4: Cloud component security
DORA Art.28	ICT third-party risk — cloud providers	Cloud provider risk assessment; SLA monitoring; exit plan	L1: TPRM trust model

Cloud Operating Models: Regulated vs. Hyperscale

Cloud operating models in regulated enterprises diverge into two distinct paths: "Regulated Model" (EU data, GDPR/NIS2 first, compliance-driven design, sovereignty priority) and "Hyperscale Model" (global optimization, cost reduction, scale efficiency, regulatory compliance secondary). Attempting to apply one model to both fails catastrophically. Architecture decisions, governance, and control selection must align to the chosen operating model.

Regulated Cloud Operating Model

Dimension	Governance	Control Deployment	Compliance Evidence
Data Residency	EU-only; Sovereign Cloud (AWS GovCloud EU / Azure Sovereign / SecNumCloud)	Data encryption; geo-fence storage; DLP at egress; compliance validation	Quarterly data residency audit; physical audit of cloud data centres
Vendor Governance	Cloud provider NIS2 third-party assessment; ISO 27001 + SOC2 mandatory	Cloud provider audit trails; CloudTrail for compliance evidence; SLA-backed audit rights	Annual third-party audit; vendor risk register; SLA enforceability verified
Architecture Assurance	Compliance-first design; regulatory approval of architecture before implementation	Network isolation mandatory; encryption mandatory; policy-based access control	CISO architecture sign-off; compliance officer pre-implementation review; architecture audit trail
Incident Response	Forensic preservation mandatory; regulatory notification within 24–72h	Cloud forensic service contracts; log retention policy >90 days; evidence preservation	Incident playbook with regulatory notification; forensic review quarterly

Hyperscale Cloud Operating Model

Dimension	Governance	Control Deployment	Compliance Evidence
Cost Optimization	Cost efficiency primary; multi-region deployment; spot instances; reserved capacity	Shared responsibility model; controls deployed incrementally based on ROI	Cloud cost reporting integrated with control effectiveness; cost-benefit trade-offs documented
Velocity	Rapid deployment; CI/CD every commit; infrastructure-as-code standard	Automation-first; controls embedded in pipelines; control costs minimize deployment friction	Continuous compliance; audit trails automated; regulatory examination evidence generated in real-time
Workload Distribution	Workloads in regions closest to users (US, Asia, EU)	Regional redundancy; replication automatic; data sovereignty optional (SCCs sufficient)	Data processing agreements in place; transfer mechanisms documented; regulatory notification contingency

Team Autonomy	Teams own their infrastructure; guardrails (not gatekeeping); self-service cloud resources	Guardrails implemented as policy-as-code; teams deploy within approved patterns; policy violations auto-remediated	Policy violations logged; trend analysis; policy tuning quarterly based on violations
---------------	--	--	---

Decision Framework: Which Operating Model?

Cloud Operating Model Selection Decision Tree

Question 1: Is data residency regulatory requirement? YES → Regulated Model. NO → Continue to Q2.

Question 2: Is multi-region deployment required for availability/latency? YES → Evaluate Hybrid Model. NO → Continue to Q3.

Question 3: Is cost optimization core business driver? YES → Hyperscale Model. NO → Continue to Q4.

Question 4: Are customers primarily regulated entities requiring audit trails? YES → Regulated Model. NO → Hyperscale Model.

Serverless & Container Security for Kubernetes-Native Flows

Serverless functions (AWS Lambda, Azure Functions) and containers (Kubernetes) dominate cloud-native architecture. However, function isolation, container runtime security, and Kubernetes networking introduce new attack surfaces. This section formalises K8s security architecture, pod security policies, container image signing, runtime protection, and serverless function isolation patterns.

Kubernetes Security Architecture Layers

K8s Security Layer	Control Requirement	Implementation Pattern	Verification
API Server Access	Authentication + Authorization via RBAC	Service accounts + RBAC roles; cluster-admin role minimal	Audit logging; access review quarterly
Pod Network Isolation	NetworkPolicy for ingress/egress	Deny-all default; explicit allow-list per namespace	Policy testing; network segmentation validation
Pod Security	Pod Security Policy (deprecated) → Pod Security Standards	Restricted standards enforced; no privileged pods; read-only filesystem	Pod creation attempt logging; policy violation scan
Container Image Security	Signed images; vulnerability scanning; registry scanning	Image signing with Cosign; Trivy scanning in CI/CD; signed attestation	Image provenance audit; vulnerability trends quarterly
Runtime Protection	Runtime anomaly detection; syscall monitoring; kill-chain interruption	Falco rules for suspicious syscalls; automated pod isolation on detection	Runtime event audit; incident response runbooks tested

Container Image Signing & Provenance

Image Security Artifact	Requirement	Implementation
-------------------------	-------------	----------------

Image Signature	Cryptographically signed by build pipeline	Cosign signing with private key; signature stored in registry
SBOM (Software Bill of Materials)	Component inventory; vulnerability correlation	SPDX format; generated during build; stored as image attestation
Build Attestation	Proof of image creation; build environment integrity	Build system signs attestation (builder identity + build logs + git commit)

Serverless Function Isolation & Cold Start Security

Serverless Threat	Isolation Risk	SABSA Control
Container Escape	Function environment isolation insufficient	AWS Lambda: managed; no escape possible. Custom runtimes: container scanning mandatory.
Secrets Exposure	Hardcoded credentials in function code; environment variable leakage	Secrets manager (AWS Secrets Manager / Azure Key Vault); no hardcoded secrets
Cold Start Timing Attack	Function initialization delay leaks information about internal state	Consistent latency design; time delays not dependent on data size
Supply Chain (Function Dependencies)	npm/pip packages in dependencies; vulnerable transitive dependencies	Dependency scanning (Snyk/Dependabot); pinned versions; periodic updates

Monetized Cloud Risk Dashboard

Cloud security costs money. Every security control — encryption key management, container scanning, network policies, logging, incident response — consumes cloud resources and budget. Conversely, every cloud misconfiguration costs money in breach risk. The Monetized Cloud Risk Dashboard correlates cloud spend with security risk, enabling CFO-understandable cost-of-breach analysis and ROI justification for security investments.

Cloud Spend vs. Security Risk Correlation

Cloud Service	Monthly Spend	Security Investment	Risk Cost (Annual)
Compute (EC2/VMs)	€50K	€2K (security tooling)	€500K (breach cost if compromised)
Storage (S3/Blob)	€30K	€1.5K (encryption + DLP)	€1.2M (if PII exposed)
Databases (RDS/SQL)	€40K	€3K (encryption + audit)	€800K (data breach)
Serverless (Lambda/Functions)	€15K	€1K (secrets + scanning)	€300K (data leak)
Total Monthly Cloud Cost	€135K	€7.5K (5.6% of spend)	€2.8M annual risk

FinOps + Security Integration Framework

Cloud Cost Category	Typical Spend	Security Control Requirement
Instance/Compute	40% of cloud bill	Runtime protection (Falco); patching compliance
Storage	25%	Encryption; DLP; versioning; immutable copies
Data Transfer	15%	Encryption in-transit; DLP at egress; VPC endpoints
Logging & Monitoring	10%	Compliance logging; long-term archive; SIEM ingestion
Other Services	10%	API security; container registry scanning; identity management

CFO Reporting: Cost-of-Breach Impact on Cloud ROI

Cloud Security Cost-Benefit Calculation for Finance Leadership

Annual Cloud Cost = €135K × 12 = €1.62M

Security Investment (FinOps alignment) = €7.5K × 12 = €90K (5.6% overhead)

Estimated Annual Breach Cost (unmitigated) = €2.8M

Residual Risk After Controls (40% effective) = €1.12M

Financial Impact of Breach (if it occurs) = €1.12M (vs. €2.8M without controls)

Security ROI = (€1.68M risk reduction) / (€90K investment) = 18.7:1 annually

CEO/CFO Decision: "We spend €90K to avoid €1.12M residual exposure (vs. €2.8M uncontrolled). The security investment is 1/12th of the residual risk and 1/30th of the uncontrolled risk." Clear financial justification for Board approval.

Conclusions and Strategic Recommendations

Multi-cloud security architecture under SABSA governance is both operationally achievable and commercially essential for regulated enterprises. The 94% of enterprises using multi-cloud cannot wait for simplified cloud environments — they must architect security across the complexity they actually operate in, not the simplicity they wish for. SABSA provides the framework; CSPM provides the continuous monitoring; cloud-native security tooling provides the controls; and the unified compliance evidence architecture satisfies regulators across all three EU regulatory frameworks.

1. Publish a Cloud Security Architecture Standard before any further cloud migration: a platform-agnostic policy document with AWS/Azure/GCP implementation annexes is the governance foundation.
2. Deploy CSPM across all cloud platforms immediately: 80% of cloud breaches involve misconfiguration — continuous posture management is the highest-value cloud security control available.
3. Design GDPR data residency into cloud architecture: EU data must stay in EU regions; document the legal basis for any cross-border transfer; include cloud provider SCCs in evidence repository.
4. Treat cloud providers as NIS2 supply chain risk: ISO 27001 A.5.23 (new control) requires supply chain security assessment — cloud providers require formal third-party risk assessment.

5. Build cloud incident response playbooks with forensic preservation: ephemeral cloud resources require automated evidence capture before quarantine or termination.
6. Integrate cloud compliance evidence into the unified SABSA compliance repository: cloud regulatory compliance evidence from CSPM, CloudTrail, and IAM reports serves NIS2, ISO 27001, and GDPR simultaneously.

About the Author

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