

SABSA ENTERPRISE SECURITY ARCHITECTURE — ULTIMATE FLAGSHIP SERIES

WP15 · ULTIMATE FLAGSHIP EDITION · VERSION 3.0

DORA-Aligned Architecture

Using SABSA to Meet Digital Operational Resilience Requirements



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. DORA and the Architecture Imperative
2. SABSA Architecture Mapping to DORA Five Pillars
3. ICT Risk Management Framework Architecture
4. Major Incident Classification and Notification Architecture
5. TLPT Programme Architecture
6. ICT Business Continuity Under DORA
7. ICT Third-Party Risk Under DORA
8. TIBER-EU Red Team Scoping Template
9. DORA Incident Classification and Automated Workflow
10. ICT Third-Party Risk Register Architecture
11. Conclusion and Recommendations

DORA and the Architecture Imperative

Jan 2025 DORA effective date — EU 2022/2554	5 Pillars ICT Risk, Incidents, Resilience Testing, Third- Party, Information Sharing	4h/72h major incident initial notification / detailed report deadlines	20,000+ EU financial entities in DORA scope
--	--	--	--

The Digital Operational Resilience Act (DORA, Regulation EU 2022/2554) entered into force across the European Union on 17 January 2025, establishing binding requirements for digital operational resilience across the entire EU financial sector — from systemic banks and insurance companies to crypto-asset service providers and crowdfunding platforms.

DORA is not a compliance framework in the traditional sense. It is an architecture mandate — requiring financial entities to demonstrate, through structured testing and documented governance, that their ICT systems can withstand, adapt to, and recover from ICT-related disruptions. The SABSA framework is uniquely positioned to meet this mandate through its business-aligned, layered architecture approach.

DORA Architecture Mandate

DORA Article 6(1) requires financial entities to establish and maintain a robust and comprehensive ICT risk management framework as an integral part of their overall risk management system. This is an architectural requirement — ICT risk management must be embedded in governance and architecture, not managed as a standalone IT function.

SABSA Architecture Mapping to DORA Five Pillars



D	O	R
R	e	q
S	A	B

ICT Risk Management Framework Architecture

DORA Article 6 requires a "robust and comprehensive ICT risk management framework" that identifies and classifies ICT assets, assesses ICT risks, implements risk response measures, and maintains the framework through continuous review. This is precisely the SABSA architecture lifecycle.

The SABSA ICT Risk Management Framework under DORA encompasses:

ICT Asset Register: A complete and current inventory of all ICT assets — hardware, software, data, and external services — classified by criticality and supporting business function. Asset register completeness is a prerequisite for credible risk assessment.

Dependency Mapping: Comprehensive mapping of dependencies between ICT assets, business processes, and external providers. DORA requires entities to identify single points of failure in ICT infrastructure.

Risk Scenario Library: A documented library of ICT risk scenarios — hardware failure, ransomware attack, cloud provider outage, critical supplier compromise — with assessed impact and likelihood, aligned to the entity's risk appetite.

Risk Response Architecture: For each risk scenario above appetite, documented architectural controls, with residual risk assessment and board/management acceptance where residual risk remains above tolerance.

SABSA Business Risk Model

The SABSA Business Risk Model (BRM) is the natural instrument for DORA ICT risk framework documentation. The BRM maps business attributes (availability, integrity, confidentiality, reliability) to risk scenarios, enabling risk quantification in business terms that satisfy DORA governance obligations and provide meaningful board-level reporting.

Major Incident Classification and Notification Architecture

DORA Article 18 establishes criteria for classifying ICT-related incidents as "major," triggering mandatory notification obligations. The classification criteria include: number of clients affected, data losses, criticality of affected services, geographic spread, duration, and economic impact.

The DORA notification timeline creates hard architectural requirements:

N	o	t
T	i	m
A	r	c

The 4-hour initial notification deadline is particularly demanding. It requires that: the incident is detected promptly (MTTD < 1 hour for major incidents), classification is automated or requires minimal human judgement, notification templates are pre-approved and only require incident-specific data population, and escalation to authorised signatory is immediate.

DORA Notification Architecture Gap

Analysis of financial sector organisations reveals that most lack the architectural infrastructure to meet the 4-hour initial notification deadline. Common gaps include: slow incident classification (manual triage with no automated severity scoring), unsigned

notification templates requiring legal review, and unclear escalation paths causing delays in obtaining management authorisation.

DORA 4-Hour Notification Architecture



TLPT Programme Architecture

DORA Article 24 mandates Threat-Led Penetration Testing (TLPT) for significant financial entities. TLPT under DORA follows the TIBER-EU framework developed by the European Central Bank.

TIBER-EU TLPT is not a standard penetration test. It is a structured, intelligence-led assessment conducted by specialist providers under regulatory supervision, simulating realistic advanced persistent threat actor TTPs against live production environments.

T	L	P	T
A	c	t	i
D	u	r	a
O	u	t	p

TLPT Mutual Recognition

DORA Article 26 establishes a mutual recognition framework — a TLPT certificate issued by one national competent authority is recognised by other EU competent authorities. This allows financial groups operating across multiple EU jurisdictions to conduct a single TLPT exercise.

The SABSA architecture supports TLPT preparation by ensuring that the organisation's threat model (Contextual Layer) and control architecture (Logical and Physical Layers) are documented and current.

ICT Business Continuity Under DORA

DORA Article 11 requires financial entities to implement ICT business continuity policies and plans that address recovery from major ICT incidents.

Recovery Time Objectives (RTO): Define and test recovery timelines for all critical ICT systems, with evidence that RTO targets are achievable.

Recovery Point Objectives (RPO): Establish and test data recovery capabilities, demonstrating backup and replication architectures can restore critical systems within defined data loss tolerance.

Crisis Communication Architecture: Maintain documented crisis communication procedures for major ICT incidents.

Playbook Library: Develop and maintain response playbooks for key ICT risk scenarios — ransomware, DDoS, cloud provider outage, critical SaaS failure, data centre loss — tested annually through tabletop exercises.

DORA vs. Traditional BCM

Traditional BCM focuses on business process continuity with ICT as a supporting element. DORA inverts this, making ICT resilience the primary focus. SABSA architects must reframe BCM architecture to satisfy this ICT-centric regulatory lens.

ICT Third-Party Risk Under DORA

DORA establishes the most comprehensive ICT third-party risk management requirements in EU financial regulation. Article 28 requires a complete strategy; Article 30 specifies mandatory contract provisions; Articles 31–44 establish an EU-level oversight framework for Critical ICT Third-Party Service Providers (CTPPs).

D	O
S	A

TIBER-EU Red Team Scoping Template

TIBER-EU is the ECB/EBA framework for threat intelligence-led penetration testing within EU financial sector. Unlike standard penetration tests, TIBER-EU focuses on testing defences against threats relevant to the tested entity.

T	I	B	E
D	u	r	a
S	c	o	p
D	e	l	i

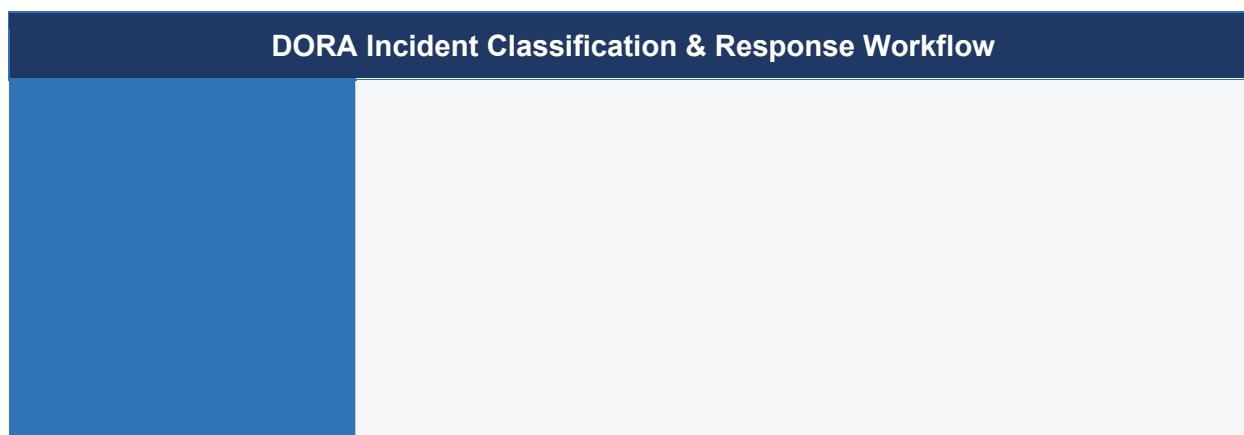
TIBER-EU scoping requires organisations to collaborate with threat intelligence teams to define threat actors most likely to target them.

Threat Intelligence-Led Scenarios: TIBER-EU scenarios mirror real threat actors. Example: Carbanak-like attacker targeting FX trading infrastructure drives specific TTP sequencing.

DORA Incident Classification and Automated Workflow

DORA mandates incident classification, notification workflows, and regulatory reporting with strict timelines. DORA distinguishes Major Incidents from Critical Incidents, triggering different reporting obligations.

D	O	R
T	r	i
N	o	t



Automated Classification Engine: Incident ticket creation automatically evaluates DORA classification criteria. ML models assess impact magnitude.

4-Hour Notification Workflow: Critical/Major detection triggers automated notifications to NCA. Failure to meet timelines results in regulatory fines.

DORA Incident Reporting Portal

EU regulators operate centralised DORA incident reporting platforms. Regulatory communication is non-negotiable; late reporting results in automatic supervisory findings.

ICT Third-Party Risk Register Architecture

DORA Article 28 mandates a Critical ICT Provider Register: financial institutions must identify all third-party ICT service providers whose failure would jeopardise operational resilience.

R	i	s	k
A	s	s	e
D	a	t	a

D	O	R	A
---	---	---	---

€1M–10M DORA fines for Art.28 breaches	20% Concentration threshold	12 mo Max exit strategy window	2x/year Mandatory continuity testing
--	---------------------------------------	--	--

DORA Article 28 Deadlines
Phase 1 (Jan 2025): Identify critical ICT providers. Phase 2 (Jan 2026): Implement Article 28 governance. Phase 3 (Jan 2027): Supervisory examination of Article 28 compliance.

Conclusion and Recommendations

DORA is the most comprehensive operational resilience mandate ever applied to the EU financial sector. Its five-pillar framework maps directly to the SABSA architecture lifecycle, making SABSA the natural framework for DORA compliance architecture design.

- Conduct a DORA gap assessment mapping current ICT risk management practices against all five DORA pillars within 60 days.. 1.
- Design and implement the 4-hour major incident notification workflow, testing end-to-end through a live drill within 90 days.. 2.
- Commission TIBER-EU TLPT programme if in scope.. 3.
- Audit ICT third-party contracts against DORA Article 30 mandatory provisions.. 4.
- Embed DORA requirements into the SABSA Architecture Review Board terms of reference.. 5.

SABSA Enterprise Security Architecture — Ultimate Flagship Series

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.