InfoSecAI

A BRIEF FOR SECURITY LEADERS

REFERENCE CARD · 2026

The UK Security Leader's Multi-Framework Crosswalk

One matrix. Seven frameworks. Mapped to the evidence artefacts your auditors and regulators actually ask for.

AUTHORED BY

Paul Jolliffe

Founder & Director, InfoSecAI · Senior CISO / vCISO · ISO 27001 Lead Auditor · CISSP · MBA

01 · WHY THIS EXISTS

One business. Seven frameworks. The same controls.

Most UK security leaders are operating against several frameworks in parallel. ISO 27001 for certification, NIST CSF for the board narrative, CIS v8 for the technical baseline, DORA for financial-sector resilience, NIS2 for in-scope sectors, UK GDPR for privacy, and increasingly the EU AI Act and ISO 42001 for AI governance. **The control work is largely the same.** The work that drains time is translating between frameworks, and proving the same thing to different audiences.

This crosswalk is the working reference I keep close to hand on every engagement. It maps thirty control domains across the seven frameworks UK boards, regulators, auditors, customers and insurers care about. It is not a substitute for reading the standards; it is a navigation aid for practitioners who already know them, and a sanity check for security leaders who have to brief a board next Tuesday.

Who this is for

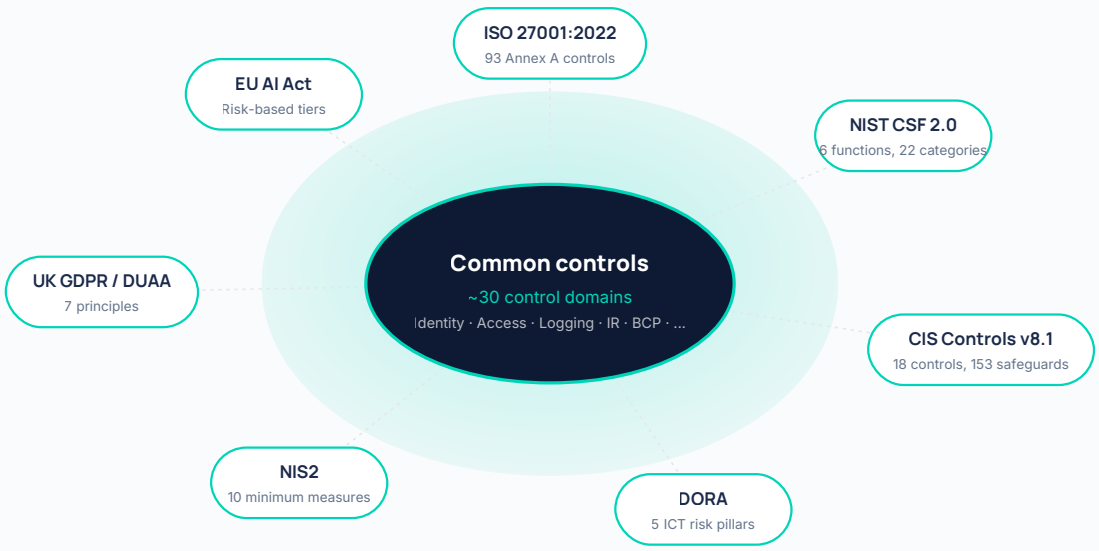
- CISOs and vCISOs running multi-framework programmes.
- Heads of GRC preparing for certification or attestation.
- DPOs and privacy leads working alongside security teams.
- Internal audit and risk functions building integrated assurance.
- Security architects deciding what to design once and reuse.

> **Heuristic:** if a control appears in five or more frameworks, it is not optional and should sit on Page 1 of your roadmap. The crosswalk on the next pages flags those.

02 · HOW TO USE IT

Read across, not down.

The most useful pattern is to pick a control domain (left column) and read across to see how each framework expresses the same underlying expectation. The differences in language are real but rarely material — what auditors ask for at the evidence layer is largely shared.



The frameworks circle the same operational core. Most controls are reused.

Three modes of use

- **Programme design.** Pick the dominant framework for your sector; map your investment plan to the rest in advance.
- **Audit prep.** Pull the references for the framework being audited; the evidence artefacts (next page) give you the things to gather.
- **Board narrative.** Translate from technical-control language to business-impact language without losing fidelity.

Where to be careful

- **Sectoral nuance.** DORA's RTS layer adds expectations on top of generic resilience controls; NIS2 transposition varies by member state.
- **UK vs EU divergence.** The Data (Use and Access) Act 2025 amends UK GDPR around automated decision-making — re-read Articles 22 and 35.
- **AI overlay.** ISO 42001 and the EU AI Act sit on top of, not instead of, your existing security and privacy stack.

03 · THE CROSSWALK — PART 1 OF 2

Control domains × ISO, NIST, CIS, DORA.

Cells reference the canonical clause / control identifier. "—" indicates the framework does not address the domain explicitly (the obligation may still be implied by overlapping legislation).

CONTROL DOMAIN	ISO 27001:2022 (ANNEX A)	NIST CSF 2.0	CIS V8.1	DORA
Information security policy	A.5.1	GV.PO-01	CIS 14.1	Art. 9 (1)
Roles, accountability & RACI	A.5.2, A.5.3	GV.RR-01..05	CIS 14.9	Art. 5–6
Risk management	A.5.7, A.5.9, Cl.6.1.2	ID.RA-01..06, GV.RM	CIS 14, 17	Art. 6–8
Asset management	A.5.9–A.5.11	ID.AM-01..05	CIS 1, 2	Art. 8(1)–(3)
Identity & access mgmt	A.5.15–A.5.18	PR.AA-01..05	CIS 5, 6	Art. 9(2), 9(4)(c)
Authentication / MFA	A.5.17, A.8.5	PR.AA-03	CIS 6.3, 6.5	Art. 9(4)(c)
Privileged access	A.8.2, A.5.16	PR.AA-05	CIS 5.4, 6.7	Art. 9(4)(c)
Cryptography & key mgmt	A.8.24	PR.DS-02	CIS 3.10, 3.11	Art. 9(4)(d)
Data classification & handling	A.5.12–A.5.14	PR.DS-03	CIS 3.1–3.7	Art. 9(4)(d)
Data loss prevention	A.8.10–A.8.12	PR.DS-05	CIS 3.13	Art. 9(4)(d)
Vulnerability management	A.8.8	ID.RA-01, PR.IR-04	CIS 7.1–7.7	Art. 10
Patch management	A.8.32, A.8.8	PR.PS-02	CIS 7.3–7.7	Art. 10
Secure configuration	A.8.9	PR.PS-01	CIS 4.1–4.12	Art. 9(4)(c)
Endpoint protection / EDR	A.8.7	PR.PS-05, DE.CM-01	CIS 10.1–10.7	Art. 9(4)(d)
Network security	A.8.20–A.8.23	PR.IR-01	CIS 12.1–12.8, 13.1–13.10	Art. 9(4)(b)
Email & web filtering	A.8.7, A.8.23	DE.CM-01	CIS 9.1–9.7	Art. 9(4)(b)
Logging & monitoring (SIEM)	A.8.15–A.8.17	DE.CM-01..09, DE.AE-01..06	CIS 8.1–8.12	Art. 10–12, Art. 17
Incident response & reporting	A.5.24–A.5.27	RS.MA, RS.AN, RS.CO, RC	CIS 17.1–17.9	Art. 17–23
Threat intelligence	A.5.7	ID.RA-02..03	CIS 13.4	Art. 13
Backup & recovery	A.8.13	PR.IR-04, RC.RP-01..06	CIS 11.1–11.5	Art. 12(1)–(3)
Business continuity	A.5.29–A.5.30, ISO 22301	RC.RP, GV.RM	CIS 11.5	Art. 11–14
Physical security	A.7.1–A.7.14	PR.AA-06, PR.IR-02	CIS —	Art. 9(4)(a)
Personnel security & awareness	A.6.1–A.6.8	PR.AT-01..02, GV.RR-04	CIS 14.1–14.9	Art. 13(6), Art. 16(2)
Third-party / supplier risk	A.5.19–A.5.23	GV.SC-01..10	CIS 15.1–15.7	Art. 28–30
Secure SDLC / change	A.8.25–A.8.34	PR.PS-06	CIS 16.1–16.14	Art. 9(4)(e)
Cloud security	A.5.23, A.8.20	PR.IR-01, GV.SC-04	CIS 12.6, 15.4	Art. 28(2), 30
Data subject rights (GDPR)	—	GV.OC-03	CIS —	—
Records of processing (RoPA)	—	ID.AM-04	CIS 1.1–1.5	—
AI inventory & governance	—	—	—	—
Operational resilience (OR)	A.5.29–A.5.30	RC, GV.RM	CIS 11	Art. 11–14, 17–23

03 · THE CROSSWALK — PART 2 OF 2

Control domains × NIS2, UK GDPR, EU AI Act.

Continuation. Domain column repeats so each page reads independently.

CONTROL DOMAIN	NIS2	UK GDPR / DUAA	EU AI ACT / ISO 42001
Information security policy	Art. 21(2)(a)	Art. 5(1)(f), Art. 24, Art. 32	AIA Art. 9 / 42001 6.2
Roles, accountability & RACI	Art. 21(2)(a)	Art. 24, Art. 39	AIA Art. 17 / 42001 5.3
Risk management	Art. 21(2)(a)	Art. 24, Art. 32(1), Art. 35 (DPIA)	AIA Art. 9 / 42001 6.1
Asset management	Art. 21(2)(a)	Art. 30 (RoPA)	AIA Art. 11 / 42001 7.5
Identity & access mgmt	Art. 21(2)(d)	Art. 32(1)(b)	AIA Annex IV §2
Authentication / MFA	Art. 21(2)(d)	Art. 32(1)(a)	—
Privileged access	Art. 21(2)(j)	Art. 32(1)(b)	—
Cryptography & key mgmt	Art. 21(2)(h)	Art. 32(1)(a)	—
Data classification & handling	Art. 21(2)(g)	Art. 5, Art. 32	AIA Art. 10 / 42001 7.5
Data loss prevention	Art. 21(2)(g)	Art. 32	—
Vulnerability management	Art. 21(2)(c)	Art. 32(1)(d)	AIA Art. 15
Patch management	Art. 21(2)(c)	Art. 32(1)(b)	—
Secure configuration	Art. 21(2)(d)	Art. 32	AIA Annex IV §3
Endpoint protection / EDR	Art. 21(2)(c)	Art. 32	—
Network security	Art. 21(2)(b)	Art. 32	—
Email & web filtering	Art. 21(2)(c)	Art. 32	—
Logging & monitoring (SIEM)	Art. 21(2)(c)	Art. 32, Art. 33	AIA Art. 12 / 42001 9.1
Incident response & reporting	Art. 23 (incident notif.)	Art. 33–34 (breach notif.)	AIA Art. 73
Threat intelligence	Art. 21(2)(c)	—	—
Backup & recovery	Art. 21(2)(c)	Art. 32(1)(c)	—
Business continuity	Art. 21(2)(c)	Art. 32(1)(c)	AIA Art. 15
Physical security	Art. 21(2)(j)	Art. 32	—
Personnel security & awareness	Art. 21(2)(g)	Art. 32, Art. 39(1)(b)	AIA Art. 4 (literacy)
Third-party / supplier risk	Art. 21(2)(d)	Art. 28 (DPA), Art. 32	AIA Art. 25
Secure SDLC / change	Art. 21(2)(e)	Art. 25 (data prot. by design)	AIA Art. 9, Art. 17
Cloud security	Art. 21(2)(d)	Art. 28, Art. 32, Art. 44–49	AIA Art. 25
Data subject rights (GDPR)	Art. 21(2)(g)	Art. 12–22	—
Records of processing (RoPA)	—	Art. 30	AIA Art. 11
AI inventory & governance	—	Art. 5, 22, 35	AIA Art. 11, Art. 9 / 42001 6.1.4, 8.2
Operational resilience (OR)	Art. 21(2)(c)	Art. 32(1)(c)	—

04 · WHAT AUDITORS ACTUALLY ASK FOR

The evidence artefacts that close the gap.

Knowing the control reference is half the work. The other half is producing the artefact an auditor can read, file, and use. These are the artefacts that close conversations across all seven frameworks.

DOMAIN	EVIDENCE ARTEFACTS (WORKING LIST)	WHY IT SATISFIES MULTIPLE FRAMEWORKS
Governance & accountability	Board-approved policy, signed RACI, quarterly Audit Committee minutes, terms of reference for security steering group.	ISO 27001 Cl.5; NIST GV; DORA Art. 5–6; NIS2 governance duty.
Risk management	Risk register with appetite statement, treatment plan, risk acceptance log, DPIA register, third-party risk register.	ISO 27001 Cl.6.1.2; UK GDPR Art. 35; DORA Art. 6–8; NIST ID.RA.
Asset & data inventory	Hardware/software inventory, RoPA, data flow maps, classification matrix, AI inventory.	ISO 27001 A.5.9–A.5.14; UK GDPR Art. 30; CIS 1–3; AIA Art. 11.
Access & identity	Joiner-mover-leaver records, access reviews (signed), MFA evidence by application, privileged access logs.	ISO 27001 A.5.15–A.8.5; NIST PR.AA; CIS 5–6; DORA Art. 9.
Vulnerability & patching	Scan output, SLA dashboards, patch compliance reports, exception register, KEV-driven prioritisation.	ISO 27001 A.8.8; CIS 7; DORA Art. 10; NIS2 Art. 21(2)(c).
Logging & monitoring	SIEM use-case catalogue, log retention policy, sample alerts triaged, SOC reports, MTTD/MTTR trend.	ISO 27001 A.8.15–A.8.17; CIS 8; DORA Art. 10–12; AIA Art. 12.
Incident response	IR plan, playbooks (P1/P2/P3), tabletop minutes, post-incident review, regulator notification log.	ISO 27001 A.5.24–A.5.27; UK GDPR Art. 33–34; DORA Art. 17–23; NIS2 Art. 23.
Backup & recovery	Backup test results, RTO/RPO statement per service, DR exercise minutes, immutability evidence.	ISO 27001 A.8.13; CIS 11; DORA Art. 12; UK GDPR Art. 32(1)(c).
Third-party & cloud	Supplier register with risk-tier, signed DPAs, sub-processor list, exit plans, attestations on file.	ISO 27001 A.5.19–A.5.23; UK GDPR Art. 28; DORA Art. 28–30; NIS2 supply-chain duty.
Personnel & awareness	Training completion (role-based), phishing simulation results, joiner attestations, leaver evidence.	ISO 27001 A.6; CIS 14; UK GDPR Art. 39; AIA Art. 4 (AI literacy).
AI governance	AI inventory with risk classification, model cards, FRIA / DPIA where high-risk, post-market monitoring plan.	EU AI Act Art. 9, 11, 26, 27; ISO 42001 Cl. 6.1.4, 8.2.

> **Practitioner note.** If the same artefact (e.g. a signed access review) is referenced in three audits, file it once with the canonical reference and let every audit point to it. The friction in most GRC programmes is duplication, not absence.

What twenty years of audits has taught me.

Auditors look for narrative, not just artefacts.

Most certifications and attestations are won or lost on whether you can tell a coherent story across policy → standard → procedure → evidence. A perfect SIEM with no incident-response narrative is a worse outcome than a modest SIEM with a clean tabletop record.

Treat ISO 27001 as the spine.

If you have to pick one programme to anchor multi-framework compliance, ISO 27001:2022 is the most generous spine. NIST CSF 2.0, CIS v8.1, DORA and NIS2 all map cleanly to it. UK GDPR and the EU AI Act add overlays; they don't replace the underlying control work.

Build for the noisier audit.

If you're DORA-regulated and ISO 27001 certified, design your evidence packs to satisfy the noisier of the two — typically the regulator-driven one. The certification body will read past the regulator's expectations; the regulator will not read up to the certification body's.

The five most over-claimed controls.

From client engagements, these are the ones organisations most often say they have but fail under examination:

- **Privileged access reviews.** Reviewed quarterly on paper, never re-signed for over 90 days.
- **Backup restoration.** Backups taken; restoration tested last in 2023.
- **Third-party security clauses.** In contract, never validated post-onboarding.
- **RoPA accuracy.** Last reviewed 18 months ago, several systems missing.
- **Phishing training.** Annual completion, no role-based escalation for high-risk teams.

What "good" looks like in 2026.

The leading UK security functions I see right now share four traits: a single integrated risk register feeding multiple audits; an evidence library indexed by control reference; a quarterly Audit Committee narrative tied to risk-appetite trends; and an AI inventory that pre-empts the EU AI Act's Article 26 deployer obligations.

If you would like senior support across any of this.

InfoSecAI is an independent UK consultancy providing fractional CISO, vCISO and security advisory services. We help boards, executives and security leaders deliver practical governance, controls and operating-model change across information security and AI.

20+
years senior security experience

£12m
largest cyber programme delivered

7
sectors regularly served

Where we typically help.

- **Fractional CISO & vCISO leadership** — strategy, board reporting, governance cadence, executive engagement.
- **Multi-framework GRC programmes** — ISO 27001, NIST CSF, CIS Controls, DORA, NIS2, UK GDPR, ISO 42001, EU AI Act.
- **Security programme & transformation** — Agile, Scrum and Waterfall, including the £12m T-Systems uplift.
- **MSSP solution architecture** — managed security services design, SOC, portfolio and product, commercial models.
- **AI governance** — AI inventories, secure adoption, AI risk assessment, EU AI Act readiness, ISO 42001 alignment.
- **Security architecture** — cloud and hybrid, SIEM, SOAR, IAM, DLP, CASB, incident response, operational resilience.

Engagement models.

Permanent, interim, fractional, contract (Inside or Outside IR35). Sectors served include financial services, telecommunications, energy, healthcare, technology, public sector and professional services.

To talk about your programme

Email **paul.jolliffe@infosecai.net** or book a 30-minute consultation directly: **infosecai.net**.

Founder credentials: MBA (Henley Business School) · CISSP · ISO 27001:2022 LA / LI / IA · PRINCE2 Practitioner. Past engagements: IBM, KPMG, PwC, T-Systems (Deutsche Telekom), Philip Morris International, Britannia Financial Group, MTN, Phoenix Software, Lloyds Banking Group, Petrofac.