ONE EVIDENCE BASE. FOUR FRAMEWORKS

WHERE THE FRAMEWORKS GCC ORGANISATIONS REPORT AGAINST CONVERGE — AND THE FIVE AREAS WHERE THEY GENUINELY DIVERGE.

Four core frameworks, plus SAMA CSF and NCA OTCC-1:2022.

Most GCC organisations of scale report against three or more cybersecurity frameworks. In practice these run as separate exercises — different teams, different cycles — each gathering substantially the same evidence.

The overlap is significant and exploitable. The differences are real and must be handled explicitly. This **crosswalk** sets out both.

	NCSC CAF v4.0	NCA ECC-2:2024	UAE IA Standard v2	NIST CSF 2.0
Issuing body	NCSC (UK)	National Cybersecurity Authority (KSA)	UAE Cyber Security Council	NIST (US)
Current version	v4.0 — released 4 Aug 2025	ECC-2:2024	v2 / v2.1	2.0 (2024)
Supersedes	v3.2	ECC-1:2018	**UAE IA Regulation v1.1 (TDRA)**	CSF 1.1
Top level	4 objectives	4 main domains	15 families	6 functions
Second Level	14 principles	28 subdomains	47 sub-families	22 categories
Assessable Units	41 contributing outcomes	108 main controls · 92 sub-controls	**134 controls** **449 Sub-controls**	106 subcategories
Structure	Outcome-based	Control-based	Control-based	Outcome-based
Assessment model	Outcomes vs Indicators of Good Practice	Control implementation	Effectiveness measurement, continuous improvement	Organisational Profiles
Applicability	Scoped to essential functions	Entity-based	**Always Applicable (70) / Based on Risk (64)**	Voluntary
Regulatory force	Determined by the relevant UK regulator	NCA mandate	UAE mandate, CSC supervision	Voluntary framework

CAF v4.0 objectives: A Managing security risk · B Protecting against cyber-attack · C Detecting cyber security events · D Minimising the impact of incidents

ECC-2:2024 domains: Cybersecurity Governance · Cybersecurity Defence · Cybersecurity Resilience · Third-Party and Cloud Computing Cybersecurity

NIST CSF 2.0 functions: Govern · Identify · Protect · Detect · Respond · Recover

ALSO MAPPED IN THE FULL CROSSWALK

SAMA Cyber Security Framework — 4 domains; maturity model 0–5, with Level 3 the general regulatory expectation. As currently in force, including applicable circulars.

c2 — Operational Technology Cybersecurity Controls. 4 main domains, 23 subdomains, 47 main controls, 122 sub-controls. Applies to industrial control systems in critical facilities owned or operated by government organisations, and to private-sector organisations that own, operate or host Critical National Infrastructure in the Kingdom.

Note: The Industrial Control Systems domain present in ECC-1:2018 does not appear in ECC-2:2024; OT and ICS requirements are addressed by OTCC-1:2022. A structural decision, not an omission.

WHERE ALL FOUR CONVERGE

Different structures, different vocabularies, substantially the same underlying expectations. Every one of these frameworks requires:

1. Asset inventory — the precondition to everything else
2. Access control on least privilege, with periodic entitlement review
3. Logging and monitoring, with defined detection capability
4. Incident response that is defined, owned and exercised
5. Third-party risk assessment before onboarding and on an ongoing basis
6. Business continuity that has been tested, not merely documented
7. A cybersecurity function with defined authority and board-level visibility

The convergence is not coincidental. All four draw on the same body of established practice.

Structural figures verified against NCSC, NCA, UAE Cyber Security Council, SAMA and NIST publications as of September 2026. Verify the current issue of any framework against its issuing body before relying on this summary.

OVERLEAF: the method, the five divergences, and the full download.

GATHER ONCE. REPORT NATIVELY.

1 Build one evidence register, structured by control question — not by framework chapter. Assessments duplicate because each follows its own framework's running order. Restructure around the underlying question and the duplication disappears.
2 Gather each evidence item once. One asset inventory exercise. One access review. One logging assessment. Each with a named owner and a refresh cycle.
3 Map outward. Every evidence item carries its mapping to each framework it satisfies, and how completely it satisfies it.
4 Report natively. Each framework in its own structure, language and assessment model. Each output must stand alone and be defensible to its own regulator. Never present a merged score.
5 Handle divergences explicitly. Document every point where the frameworks genuinely differ, and address each in the relevant report.

OVERLAP IS NOT EQUIVALENCE

Treating these frameworks as interchangeable will fail an audit. They diverge genuinely — and predictably — in five areas.

1 **Data residency and cross-border transfer. The most consequential divergence. A control adequate in one jurisdiction may be non-compliant in another.**
2 **Third-party and cloud provisions. ECC-2:2024 gives this an entire domain. Others distribute it across control families with differing depth.**
3 **Incident reporting thresholds and timelines. What must be reported, to whom, within what period. These do not align. The strictest applicable requirement governs.**
4 **Maturity, prioritisation and applicability models. SAMA operates maturity 0–5 with Level 3 the general expectation. The UAE IA Standard v2 classifies controls as Always Applicable or Based on Risk and requires effectiveness measurement. CAF assesses contributing outcomes against Indicators of Good Practice. NIST CSF 2.0 uses Organisational Profiles. No defensible arithmetic combines these.**
5 **Operational technology scope. Largely outside the core four. The Industrial Control Systems domain present in ECC-1:2018 does not appear in ECC-2:2024; OT and ICS requirements are addressed by OTCC-1:2022. A structural decision, not an omission.**

The correct model is shared evidence with framework-native reporting, and every divergence documented rather than smoothed over.

Version 0.9.1 Structural Edition. This edition maps framework structures, convergence themes and divergences.

WHY DIRECTION OF FIT MATTERS

Framework mapping is not symmetric. A control that fully satisfies one framework's requirement may satisfy its counterpart only partially — or may contribute without satisfying it at all. Most published framework mappings omit this. Without it, a mapping is a similarity claim, not an assurance statement — and it will not survive an assessor's first question. Every mapping in this crosswalk is marked:

●	Full	Satisfies the corresponding requirement completely
◐	Partial	Satisfies part; additional framework-specific evidence needed
○	Supports	Contributes to the requirement but does not satisfy it
—	None	No equivalent requirement exists in that framework

This is the difference between a mapping you can use in an assessment and one you can only use in a presentation.

ILLUSTRATIVE — HOW A MAPPING READS

Control question: Does the organisation maintain a complete, current and authoritative inventory of information assets and systems, including ownership and criticality classification?

Framework	Maps to	Fit
NCSC CAF v4.0	Objective A — Managing security risk	●
NCA ECC-2:2024	Cybersecurity Governance / Cybersecurity Defence	●
UAE IA Standard v2	Asset management family	●
NIST CSF 2.0	Identify (ID)	●

Illustrative only, shown at domain and objective level. The full crosswalk maps to individual controls, sub-controls and contributing outcomes.

The full crosswalk. Free, no form.

· Framework structures and convergence mapping across eight control domains and twenty-four themes
· Direction-of-fit notation on every mapping
· Divergence register — the five areas of genuine difference
· Evidence Register template
· Source register with retrieval dates and stated mapping basis

praecepta.co/crosswalk

The PDF is ungated — one click, no email required. The editable working version, evidence register template and divergence register are available on request.

PRAECEPTA CYBERSECURITY

A specialist security architecture practice based in Dubai. We design Zero Trust, data security and regulatory assurance programmes for organisations across the Middle East and Africa.
Security Architecture · Zero Trust Advisory · Data Security & DSPM · Regulatory Assurance & Cyber Risk
Jawaid Ali — 28 years in IT and cybersecurity CISSP · CISM · CCZT · Associate C|CISO · CEH · Open FAIR and CAISP in progress
Our advisory work carries no product economics. Our fee is unaffected by what you subsequently buy — including if you buy nothing.
[Jawaid.ali@praecepta.ae] · [+971 (0) 56 9195050] · praecepta.co

v0.9.1 · September 2026 · Reviewed quarterly · Declared interests: praecepta.co/declaration. Corrections welcome at [ops@praecepta.ae] — incorporated at the next quarterly review with acknowledgement. This document constitutes security architecture guidance, not legal advice. Framework applicability is jurisdiction- and entity-specific; engage qualified legal counsel for binding interpretation.