

Point of View

The Five Shifts Redefining Cybersecurity for Saudi Arabia's Private Sector

Turning regulatory compliance into operational resilience.



EXECUTIVE SUMMARY

NCNICC-1:2025 will be won or lost in execution, not in documentation. Organizations that treat it as a bolt-on absorb the same control costs as those that integrate it — for a fraction of the resilience.

The National Cybersecurity Authority’s (NCA) **Non-CNI Private Sector Entities Cybersecurity Controls (NCNICC-1:2025)** establishes 65 main controls across 22 sub-components and 3 main components: Cybersecurity Governance, Cybersecurity Defense, and Third-Party and Cloud Computing Cybersecurity. These are underpinned by 47 sub-controls that specify minimum implementation expectations and apply selectively by entity category.

For **Class A (large entities)**, all 65 main controls are mandatory. For **Class B (small and medium entities)**, 26 main controls, all concentrated in the Cybersecurity Defense component, across 13 of its 15 sub-components, are mandatory; the remaining 39 are recommended.

Most programs do not fail on the technical control list. They fail on the operating discipline that surrounds it — periodic review, independent assurance, demonstrable cloud-tenancy separation, and the obligations the NCA has set specifically for the Kingdom: Saudization of cyber leadership, adoption of an NCA-licensed managed SOC (mandatory for Class A; recommended for Class B), and prompt incident reporting to the NCA.

Three actions for leadership in the next 90 days

- **Confirm Class A / Class B applicability** and formally scope in-scope entities (most groups will be both, depending on the subsidiary).
- **Run a control-level NCNICC gap assessment** by component and sub-component, prioritized on risk and regulatory exposure rather than on tooling coverage.
- **Publish a board-level NCNICC dashboard** that tracks evidence readiness, not policy coverage, by sub-domain.

Our view in one line: NCNICC-1:2025 is the regulator’s quiet shift from “do you have a policy?” to “can you prove it runs?”, and the boards that answer “yes” first will gain a durable commercial and reputational advantage.



Bharat Chadha
Partner, Tech Consulting



Tarandeep Bindra
Partner, Tech Consulting

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model

What Is NCNICC-1:2025?

NCNICC-1:2025 is a minimum, not an aspirational, control framework issued by the NCA for non-CNI private-sector entities operating in the Kingdom. It is anchored in the classical information security triad of confidentiality, integrity, and availability and is built as a lifecycle framework: every domain defines not only what to implement but also how to document, adopt, implement, and periodically review each control.

The framework should be read simultaneously as:

- A **regulatory baseline** that the NCA, and, where relevant, sectoral regulators, will evidence against during reviews.
- A **practical operating model** for cyber discipline that stands on its own and, where a program such as an ISMS already exists, can reuse existing evidence rather than duplicate it.

Applicability — who must act

NCNICC-1:2025 applies to private sector entities in Saudi Arabia that are not classified as Critical National Infrastructure (CNI). Obligations differ by entity size:

Entity class	Threshold	Mandatory main controls	Recommended
Class A — Large	>250 employees or >SAR 200M revenue	65 of 65 (100%)	0
Class B — Small & Medium	6–249 employees or SAR 3M–200M revenue	26 of 65 (40%)	39 of 65 (60%)

What this means in practice: Class B classification is not an exemption; it is a sequencing concession. Every “recommended” control still carries regulator expectation as maturity grows, and recommended controls routinely surface as findings when an incident occurs. Group structures with mixed subsidiary profiles should expect Class A obligations at the parent level. A complete evidence program must address both the 65 main controls and the 47 sub-controls, which follow the same category logic.

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model

Why This Matters Now

The NCA, established by **Royal Order No. 6801 dated 11/2/1439H**, is the national reference authority for cybersecurity in the Kingdom. NCNICC-1:2025 is the NCA's first cybersecurity control framework purpose-built specifically for non-CNI private-sector entities, the very segment Vision 2030 is counting on to raise the private sector's contribution to GDP to 65%, and the SME contribution to 35%, by 2030. The regulator's message is clear: growth and cyber resilience must go hand in hand.

Saudi Arabia's cybersecurity agenda has shifted from broad awareness to structured accountability. Three forces converge in 2026:

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model

Regulatory density

NCNICC-1:2025 sits alongside the NCA's ECC-2:2024, CCC-1:2020, OTCC-1:2022, and DCC-1:2022, the SAMA Cyber Security Framework, and the Personal Data Protection Law (PDPL). Cybersecurity can no longer be treated as a single-regulator conversation.



Attack-surface expansion

Cloud adoption, outsourcing, and digitization under Vision 2030 have widened private-sector exposure faster than governance has caught up. Mid-market entities now operate with an attack surface comparable to what only large enterprises and CNI operators managed five years ago: cloud environments, SaaS ecosystems, outsourced development, API-driven integrations, and extensive partner connectivity, without the corresponding governance maturity.



Board accountability

NCNICC formally moves cyber out of the IT function and onto the senior-executive and board agenda. Control 1-1-1 requires a dedicated cybersecurity unit, organizationally separate from IT and reporting to the head of the entity or an authorized delegate — a structural change, not a policy change.



Framework Structure and Strategic Implications

	Main component	Scope	Strategic implication	Evidence that a reviewer will expect
Executive Summary	Cybersecurity Governance	14 main controls across 5 sub-components: management, policies, risk, audit & review, and awareness.	All 14 mandatory for Class A; 0 mandatory for Class B, yet B entities adopt it anyway to pass third-party due diligence. Governance is the gateway.	Approved policies, RACI matrix, risk register, cyber-function charter, audit and review minutes, and awareness records.
What Is NCNICC-1:2025?				
Why This Matters Now				
Framework Structure and Strategic Implications	Cybersecurity Defense	45 main controls across 15 sub-components: IAM, endpoint, email, network, mobile/ BYOD, data, cryptography, backup, vulnerability, pen-test, logging/SOC, incident, physical, web.	Where NCNICC is most prescriptive. Class A: all 45 mandatory; Class B: 26 across 13 of 15 sub-components. Failure is rarely about tool acquisition; it is about proving the tool operates.	Hardening baselines, MFA/PAM matrix, DMARC enforcement, backup-restore logs, VA/PT reports, NCA-licensed SOC contract, incident playbooks.
The Five Shifts NCNICC Forces on the Saudi Private Sector				
What Most Entities Get Wrong				
The NCNICC Maturity Grid	Third-Party & Cloud	6 main controls across 2 sub-components: vendor cyber risk and cloud/ hosting security.	0 of 6 mandatory for Class B, yet this is where most SMEs are already materially exposed (tenancy misconfiguration, weak vendor contracts). Treating it as “not mandatory yet” is a common strategic error.	Vendor due diligence files, signed cyber addenda (SLAs, audit rights, data return), cloud tenancy evidence, sub-processor inventory, and exit records.
Key Implications for Leadership Teams				
How We Can Help				
Staged Engagement Model				

Avoid duplicate effort. Most Saudi entities already operate one or more control sets, the ECC, the SAMA Cyber Security Framework, the PDPL, sector rules, or an ISMS. The strategic play is to express NCNICC as a single integrated control library across all of these, reuse existing evidence, and close only the true gaps. Rebuilding from zero is the most expensive path.

The Five Shifts NCNICC Forces on the Saudi Private Sector

Beneath the control list, NCNICC-1:2025 encodes five structural shifts that most private-sector boards have not yet priced in.

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model

Shift 1 — From documentation to demonstrable operation

The phrase “define, document, approve, implement, and periodically review” recurs in virtually every sub-domain. The regulator is signaling that policy on paper will no longer suffice for a review. Evidence of periodic operation is now the differentiator.

Shift 2 — From IT function to independent cyber function

Control 1-1-1 requires a dedicated cybersecurity unit, separate from IT, that reports to the entity’s head. For mid-market firms where the IT Manager is effectively the security function today, this is a structural re-organization, with implications for hiring plans, HR bands, and board reporting lines.

Shift 3 — From global talent market to sovereign talent market

Control 1-1-2 requires the head of the cybersecurity function and its supervisory and sensitive roles to be filled by full-time, highly competent Saudi nationals. This is the framework’s most distinctive provision. It reshapes the local talent market, creates salary pressure, and makes structured academies, rotation programs, and fractional-CISO models a strategic necessity rather than a recruitment tactic.

Shift 4 — From vendor trust to vendor evidence

The third component, confidentiality clauses, incident-response procedures, cloud-tenancy separation, data return at the end of service, and data classification before cloud migration, requires vendor relationships to be backed by written evidence: executed contract clauses, measurable SLAs, incident-response commitments, and periodic test results, rather than trust alone.

Shift 5 — From compliance sprint to assurance as an operating rhythm

The framework is built around periodic-review controls, the third control in each sub-component (for example, 2-1-3, 2-9-3, 3-2-3). Assurance is not a project; it is a recurring cadence that integrates second-line risk and compliance with third-line internal audit. Entities running cyber as an annual event will generate findings by design.

What Most Entities Get Wrong

Across financial services, retail, healthcare, energy services, and logistics in the Kingdom, five recurring failure modes account for the majority of NCNICC gaps:

1

Mistaking control existence for control operation

MFA is logged as “done” when only email is covered, while remote access, SaaS, and privileged accounts still rely on passwords. Control 2-2-1-2 requires MFA for remote access, including external applications; 2-2-1-4 adds privileged access management.

2

Running backups without restoration tests

Control 2-9-1-2 explicitly requires periodic restoration testing. Untested backups are not, for NCNICC purposes, backups.

3

Cloud-tenancy assumptions

Teams assume that hyperscaler-default separation satisfies Control 3-2-1-2; reviewers expect explicit evidence of logical segregation from co-tenants, not the provider’s marketing page.

4

Email-domain protection left partial

DMARC tells a receiving server how to treat messages that claim the organization’s domain but fail SPF or DKIM. Many entities are set to p=none (monitoring only), which does not block impersonation. Control 2-4-1-2 requires the email domain to be documented through the NCA’s Haseen platform using SPF, DKIM, and DMARC. Leading practice is to move DMARC past p=none to p=quarantine or p=reject, reached via a 90–120-day enforcement path: inventory legitimate senders, align SPF/DKIM, monitor aggregate reports, then ratchet the policy.

5

Incident-response plans without NCA reporting protocols

Control 2-13-1-2 mandates reporting cybersecurity incidents to the NCA, and 2-13-1-3 mandates sharing cybersecurity information with the NCA. Many existing plans stop at internal stakeholders and never trigger the formal NCA notification that Control 2-13-1-2 requires upon a cybersecurity incident.

The underlying pattern: these are not funding failures; they are failures of ownership and evidence. Organizations fail NCNICC reviews not because controls are unknown, but because responsibility for proving they run is fragmented.

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model

The NCNICC Maturity Grid

A two-axis view helps boards diagnose where they actually sit. The vertical axis is Evidence Strength (proof of periodic, auditable operation); the horizontal axis is Control Coverage (breadth of NCNICC controls deployed). Evidence Strength asks one question: Can you prove, with logs, tickets, minutes, and attestations, that each control actually ran last quarter?

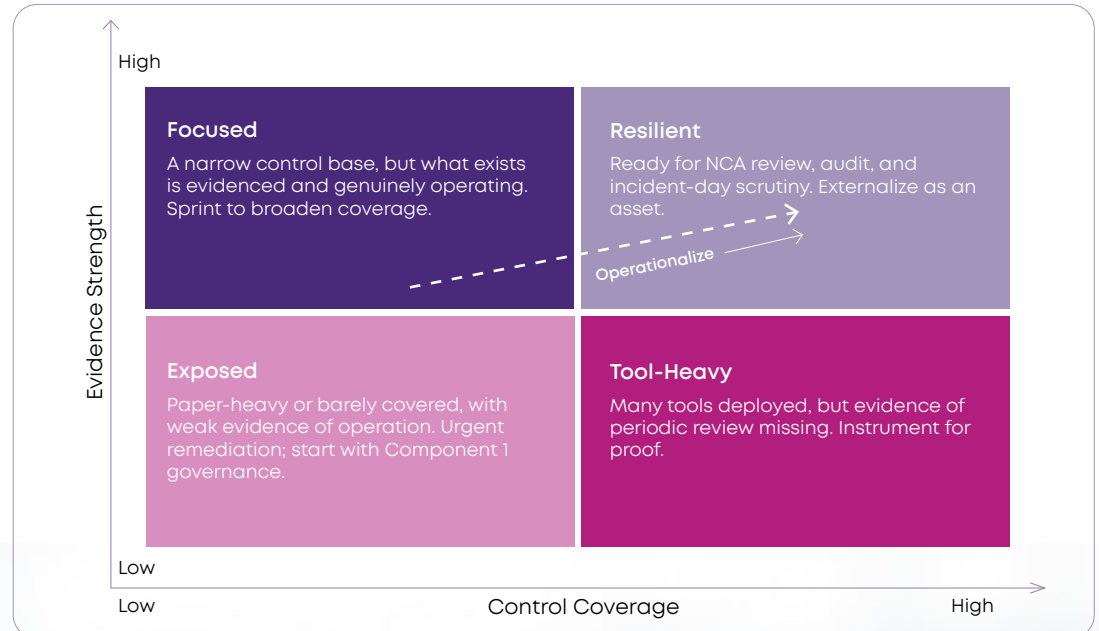


Figure. NCNICC Maturity Grid — a 2x2 of Control Coverage and Evidence Strength.

Most Saudi mid-market entities cluster in Tool-Heavy or Exposed, not Resilient — which is precisely why operationalization, not procurement, is the frontier.

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model

Key Implications for Leadership Teams

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Staged Engagement Model



Board & Audit Committee

Require a quarterly NCNICC dashboard reporting mandatory-control coverage, evidence readiness, and periodic-review cadence by sub-domain. Ask for three specifics: MFA coverage across privileged accounts, restoration-test frequency, and NCA incident-reporting readiness.



CEO

Resolve ownership between CIO, CISO, and COO. NCNICC moves the cyber unit out of IT; settle reporting lines before remediation begins.



CIO & CISO

Converge NCNICC with existing ISO/IEC 27001:2022, ECC, and SAMA CSF programs under one control library. Duplicate controls generate duplicate findings.



CFO

Budget for three-year sustained assurance, not a one-off implementation. Evidence generation is a headcount question as much as a tooling question.



CHRO

Build a Saudization plan for cyber leadership, structured academies, university pipelines, rotations from adjacent domains, and fractional-CISO arrangements for mid-market entities.



Risk, Compliance & Internal Audit

Sequence NCNICC into the three-lines model now. Validate implementation, evidence, and sustainability, not just existence.

Conclusion

NCNICC-1:2025 is more than a compliance exercise. It is a strategic prompt for the Saudi private sector to move from fragmented cybersecurity activity to a structured, defensible, and resilient operating model, the first private-sector regulatory framework in the Kingdom built entirely around demonstrable, periodically reviewed operation.

The organizations that will lead are not those that document the fastest. They are those who operationalize the earliest, build assurance as a rhythm rather than a project, and treat cybersecurity talent and evidence as strategic assets.

How we can help

Uniqus Consultech's Risk, Regulation & Cyber Advisory practice supports entities across the Kingdom in operationalizing NCNICC-1:2025, an AI-enabled, expert-led practice anchored in a single, integrated view of risk, regulation, and resilience.

A phased, risk-based approach

Assess applicability and scope

classify Class A / Class B by legal entity, map in-scope subsidiaries, and build a single integrated control library from NCNICC and applicable overlays (ECC, SAMA CSF, PDPL, sector rules).

Readiness and gap assessment

review governance, policies, control evidence, and technical coverage against all 65 main controls and the 47 applicable sub-controls; position on the NCNICC Maturity Grid.

Prioritize and roadmap

score each gap on risk, feasibility, and dependency; produce a phased 6/12/18-month roadmap with named owners, budget envelope, regulator-facing milestones, and target-operating-model choices (independent cyber unit, reporting lines, Saudization).

Execute remediation

roll out policies, harden technical controls (MFA/PAM, hardening baselines, DMARC enforcement, backup-restoration testing, logging/SOC), run role-based awareness and phishing simulations, close third-party and cloud gaps, and stand up the NCA-reporting runbook.

Sustain through assurance

instrument KPIs and KRIs, embed NCNICC into internal audit plans, and maintain a board-ready dashboard so the next review is a simple extraction, not a separate project.

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How we can help

Staged Engagement Model

Staged Engagement Model

Stage	Timing	Indicative deliverable
1. Applicability & Scoping Workshop	Weeks 1–2	Class A / B classification by legal entity, in-scope inventory, integrated control library.
2. Readiness & Gap Assessment	Weeks 3–6	Control-by-control gap heatmap, Maturity Grid position, prioritized findings, and duplicate-effort savings.
3. Prioritization & Roadmap	Weeks 7–8	Prioritized remediation plan, 12-month cost/effort roadmap, target-operating-model recommendations.
4. Remediation Program Support	Months 3–5	Policy, process, awareness, and technology remediation; NCA-reporting runbooks; periodic-review rhythms.
5. Sustained Assurance	Ongoing	Board-ready dashboard, internal audit alignment, refresher reviews.

Executive Summary

What Is NCNICC-1:2025?

Why This Matters Now

Framework Structure and Strategic Implications

The Five Shifts NCNICC Forces on the Saudi Private Sector

What Most Entities Get Wrong

The NCNICC Maturity Grid

Key Implications for Leadership Teams

How We Can Help

Where AI accelerates — and where judgment decides. AI is applied across four levers: document review (policy-to-control mapping), control mapping (NCNICC to ECC, DCC, PDPL), evidence clustering, and reporting, typically reducing readiness-assessment effort by 30–50%. Applicability interpretation, severity assessment, control-design judgment, and regulator-facing opinions remain expert-led and carry human accountability.

Complimentary 90-minute NCNICC Applicability Briefing for CISOs and Audit Committees — covering entity classification, your NCNICC control scope, the most common near-term remediation pitfalls, and next steps. Contact your Uniquis account lead.

Staged Engagement Model



About Uniquis Consultech:

Uniquis Consultech is an AI and global tech-enabled consulting company that specializes in Accounting & Reporting Consulting, Governance, Risk & Compliance, Sustainability & Climate Consulting, Tech Consulting, and Valuations. The Company is co-founded by consulting veterans Jamil Khatri and Sandip Khetan and backed by marquee investors such as Nexus Venture Partners, Sorin Investments, and UST.

Uniquis has a global team of 800+ professionals, led by 100+ Partners and Directors, across 13 offices in the USA, the Middle East, and India. The company serves more than 400+ clients, including marquee names in each of the markets it operates in.

Uniquis is committed to leveraging technology and an integrated global delivery model to provide best-in-class consulting services to its clients.

About Our Tech Consulting Services:

Technology is no longer just support—it is the engine of how you compete and create value. But as operations become digital end-to-end, complexity grows. Fragmented systems, ever changing regulations, and evolving risks can stall progress.

We cut through the complexity. Our practice pairs strong technical capabilities with deep functional expertise — specifically in finance, risk, and sustainability. We don't just modernize legacy landscapes; we build reliable data foundations that integrate seamlessly.

We embrace new technologies responsibly. We believe the most durable solutions blend human intelligence with AI. By embedding security and governance from day one, we help you innovate with confidence.

A Team That You Can Trust To Deliver



Bharat Chadha
Partner, Tech Consulting



Tarandeep Bindra
Partner, Tech Consulting



Scan this code to find
more content like this

Visit us at www.uniquis.com

or follow us on

