

FRAMEWORK QUICK-REFERENCE TABLE

ALQABBAT ADVISORY · SAUDI INDUSTRIAL EDGE COMPLIANCE SERIES · TOOLKIT
RESOURCE

PURPOSE

What does this reference cover?

Every Saudi and international compliance framework relevant to industrial edge environments — what each one governs, who enforces it, and what it means for your bid. Keep this on your desk when writing compliance documentation.

SAUDI NATIONAL FRAMEWORKS

Mandatory compliance requirements issued by Saudi regulatory authorities

EXHIBIT 1 — NCA CYBERSECURITY FRAMEWORK FAMILY

FRAMEWORK	VERSION	SCOPE & PURPOSE	APPLICABILITY	STATUS
ECC Essential Cybersecurity Controls	ECC- 2:2024	Saudi baseline cybersecurity standard. Establishes minimum cybersecurity controls for all organisations operating in Saudi Arabia. Foundation beneath all sector- specific NCA requirements.	All organisations in Saudi Arabia	MANDATORY
OTCC Operational Technology Cybersecurity Controls	OTCC- 1:2022	Saudi-specific cybersecurity controls for OT environments. Evaluated across five control domains: asset management, network security, identity & access management, security monitoring, and incident response.	Any vendor operating or supplying to OT environments in Saudi industrial sectors	MANDATORY

FRAMEWORK	VERSION	SCOPE & PURPOSE	APPLICABILITY	STATUS
CCC Cloud Cybersecurity Controls	CCC- 2:2024	Cybersecurity requirements for cloud service providers and cloud consumers operating in Saudi Arabia.	Cloud deployments within Saudi jurisdiction	MANDATORY
DCC Data Cybersecurity Controls	DCC- 1:2022	Controls specific to data protection, classification, and lifecycle management within Saudi cybersecurity framework.	Organisations handling classified or sensitive data	MANDATORY
CSCC Critical Systems Cybersecurity Controls	Current	Enhanced cybersecurity requirements for systems classified as nationally critical infrastructure.	Critical national infrastructure operators	MANDATORY

Key Distinction

ISO 27001 is not equivalent to NCA compliance. IEC 62443 is not equivalent to OTCC compliance. Saudi procurement committees treat framework substitution as a compliance gap, not an alternative. Reference both Saudi and international standards — but lead with the Saudi framework.

EXHIBIT 2 – DATA PROTECTION & AI GOVERNANCE

FRAMEWORK	VERSION	SCOPE & PURPOSE	ISSUER	STATUS
PDPL Personal Data Protection Law	Royal Decree M/19 (2021)	Saudi data protection regulation governing collection, processing, storage, and cross- border transfer of personal data. Enforced September 2023.	SDAIA	DATA LAW
Cross-Border Transfer Risk Assessment	February 2025	Guideline for assessing risk of transferring personal data outside the Kingdom of Saudi Arabia.	SDAIA	DATA LAW
National Data Governance Interim Regulations	Current	Interim governance regulations for national data management, classification, and sharing.	NDMO / SDAIA	DATA LAW
AI Governance Framework	Current	Governance requirements for AI systems operating in Saudi Arabia, including industrial AI and digital twin deployments.	SDAIA	DATA LAW

SAUDI MARKET & LOCALISATION FRAMEWORKS

Vision 2030 compliance and local content requirements

EXHIBIT 3 – LOCALISATION & MARKET ACCESS REQUIREMENTS

FRAMEWORK	DESCRIPTION	BID RELEVANCE
IKTVA In-Kingdom Total Value Add	Saudi Aramco's local content programme measuring supplier contribution to the Saudi economy. Scored via Saudi Content Value (SCV) verified by LCGPA.	Active enrollment and current SCV score required for energy sector bids. Low SCV signals weak local commitment.
Nitaqat Saudisation Programme	Ministry of Human Resources programme classifying companies by Saudi national employment ratio. Bands: Platinum, Green (High/Mid/Low), Yellow, Red.	Red or Low Green restricts visa issuance and signals operational risk. Band classification visible to procurement committees.
Etimad Government Procurement Platform	Saudi government procurement and tendering platform. Pre-qualification gateway for government and semi-government contracts.	Active registration required. Entity must match bidding entity exactly.
NIDL National Industrial Development & Logistics Program	Vision 2030 programme setting sector-specific industrial development targets, including local content thresholds.	SCV scores mapped to applicable NIDL sector targets demonstrate Vision 2030 alignment.
LCGPA Local Content & Government Procurement Authority	Authority responsible for verifying and certifying Saudi Content Value (SCV) scores for all government and semi-government procurement.	LCGPA-verified SCV score required. Self-reported SCV scores are not accepted.

INTERNATIONAL STANDARDS

Referenced but not equivalent to Saudi national frameworks

EXHIBIT 4 – INTERNATIONAL INDUSTRIAL & INFORMATION SECURITY STANDARDS

STANDARD	VERSION	SCOPE & PURPOSE	SAUDI RELATIONSHIP
IEC 62443-2-1	2010	Establishing an Industrial Automation and Control System Security Management System.	Related frameworks addressing overlapping technical content in different evaluation contexts. Not equivalent to OTCC. Reference alongside Saudi frameworks, not as substitutes.
IEC 62443-3-2	2020	Security risk assessment for system design.	
IEC 62443-3-3	2013	System security requirements and security levels.	
IEC 62443-4-1	2018	Product security development life-cycle requirements.	
IEC 62443-4-2	2019	Technical security requirements for IACS components.	
NIST SP 800-82	Rev. 3 (2023)	Guide to Operational Technology (OT) Security. US federal guidance for OT environments.	REFERENCE ONLY
ISO/IEC 27001	2022	Information Security Management Systems — Requirements. Demonstrates an ISMS is in place.	Not equivalent to NCA compliance. Does not demonstrate Saudi-specific control domain implementation.
ISO/IEC 27002	2022	Information Security Controls — guidance on implementing controls referenced by ISO 27001.	REFERENCE ONLY

OTCC CONTROL DOMAINS

The five domains your OTCC evidence package must cover

EXHIBIT 5 — OTCC-1:2022 CONTROL DOMAIN STRUCTURE

DOMAIN	NAME	WHAT THE AUDITOR EVALUATES	EVIDENCE REQUIRED
1	Asset Management	Complete inventory of OT/edge assets, classification, ownership, and lifecycle tracking.	Signed asset register, classification schema, update logs
2	Network Security	Network segmentation, zone/conduit architecture, traffic monitoring, boundary controls.	Network architecture diagrams, firewall rules, segmentation evidence
3	Identity & Access Management	Authentication controls, privilege management, access review cycles, credential governance.	Access control policies, privilege reviews, authentication logs
4	Security Monitoring	Event logging, anomaly detection, alerting, log retention, and correlation capabilities.	SIEM configuration, alert procedures, log retention evidence
5	Incident Response	Incident detection, containment, recovery procedures, and post-incident review.	IR plan, exercise records, post-incident reports

FIVE-STAGE TENDER COMPLIANCE MAP

Which frameworks apply at each procurement evaluation stage

EXHIBIT 6 – FRAMEWORK REQUIREMENTS BY PROCUREMENT STAGE

PROCUREMENT STAGE	FRAMEWORKS EVALUATED	KEY DOCUMENTS
Stage 1 Pre-qualification	Etimad, Nitaqat, IKTVA/LCGPA, Saudi Commercial Registration	Registration certificates, Nitaqat classification, SCV score
Stage 2 Compliance Qualification	ECC-2:2024, OTCC-1:2022, PDPL, Supply Chain Security	NCA Compliance Declaration, OTCC Evidence Package, Supply Chain Posture
Stage 3 Technical Evaluation	IEC 62443 (supporting), ISO 27001 (supporting), NIST 800-82 (supporting)	Technical specifications, architecture documentation
Stage 4 Commercial Evaluation	IKTVA/SCV targets, NIDLP sector alignment, Vision 2030 commitments	Saudi Localisation Plan, SCV improvement roadmap
Stage 5 SAO Sign-Off	Full NCA/OTCC compliance review, Governance Accountability Framework	Governance Accountability Framework, final compliance package

Framework Substitution Rule

ISO 27001 certification submitted in place of NCA compliance documentation is treated as a gap, not an alternative. IEC 62443 certification submitted in place of OTCC evidence is treated as a gap, not an alternative. Saudi procurement committees require Saudi-specific framework compliance. International standards demonstrate complementary capability — they do not replace Saudi requirements.

The framework exists. The audit is coming. The question is whether your evidence will hold. This reference table tells you which evidence, for which framework, at which stage.