ALQABBAT ADVISORY
Riyadh, Kingdom of Saudi Arabia

VENDOR COMPLIANCE READINESS SCORECARD

SEVEN CATEGORIES · TWENTY-ONE QUESTIONS · ONE NUMBER THAT TELLS YOU WHERE YOU STAND

CAT 1	Information Security Governance
CAT 2	Access Management
CAT 3	Incident Response
CAT 4	Security Awareness Training
CAT 5	Change Management
CAT 6	Asset and Device Management
CAT 7	Business Continuity

A structured self-assessment for Saudi industrial contractors and suppliers facing vendor qualification requirements they have never been asked for before.

Ahmad Alqabbat · Founder & Principal Advisor · Alqabbat Advisory · 2026

HOW THIS SCORECARD WORKS

Who This Is For

Saudi industrial contractors, service providers, integrators, and equipment suppliers who serve operators in the Kingdom's industrial sector — and who are seeing compliance requirements in vendor qualification forms and RFQs that they have never been asked for before.

This scorecard assesses your company's readiness across the seven compliance evidence categories that operator vendor qualification processes now evaluate. It does not test your knowledge. It tests whether you can produce the evidence an operator's evaluator will ask for.

Scoring

Score each question on a scale of 0 to 4:

SCORE	WHAT IT MEANS	WHAT THE OPERATOR SEES
0	**Nothing exists**	A blank cell in the evaluation form. Automatic disqualification in scored assessments.
1	**Informal practice**	People follow a habit or verbal instruction, but nothing is documented. Evaluator cannot verify. Scores poorly.
2	**Partial documentation**	Some documents exist but do not cover the full scope, are outdated, or were written for a different purpose. Evaluator asks follow-up questions. Scores average.
3	**Documented, not tested**	A complete, current policy or procedure exists. Evaluator accepts it. Scores well — but does not demonstrate live capability.
4	**Documented, tested, evidenced**	Policy exists, has been applied or tested, and evidence of outcomes can be produced. Full score. Competitive advantage in any scored evaluation.

Each category has 3 questions. Maximum score per category: 12. Maximum total score: 84.

CATEGORY 1 OF 7

Information Security Governance

Does your company have the policies and ownership structures that an operator's evaluator will look for first?

Q1	Does your company have a written Information Security Policy that covers your industrial operations — including work performed inside client (operator) environments?	____ / 4
Q2	Is the policy signed by a named individual with authority (GM, CEO, or designated compliance owner), and has it been reviewed or updated within the last 12 months?	____ / 4
Q3	Does the policy specifically address the types of systems, data, or environments your teams access at operator sites — not just your own internal IT?	____ / 4
	Category 1 Subtotal	**____ / 12**

CATEGORY 2 OF 7

Access Management

Can you show an operator exactly who has access to their environment, how it was granted, and how it gets revoked?

Q4	Does your company have a documented procedure for requesting, approving, and revoking access to client site environments — covering both physical gate passes and any system or network access?	____ / 4
Q5	Is there a process for managing devices (laptops, diagnostic tools, USB media) that enter client environments — including pre-deployment checks and return verification?	____ / 4
Q6	When an employee leaves your company or transfers off a client project, is there a documented process for revoking all their access (physical and digital) within a defined timeframe?	____ / 4
	Category 2 Subtotal	**____ / 12**

CATEGORY 3 OF 7

Incident Response

If something goes wrong inside an operator's environment, do you have a documented plan — and can you prove it has been tested?

Q7	Does your company have a written Incident Response Plan that covers security events — not only HSE incidents — including detection, reporting, investigation, and client notification?	____ / 4
Q8	Does the plan include defined response timelines (e.g., notify client within X hours) and assigned roles for who manages a security incident?	____ / 4
Q9	Has the plan been tested, exercised, or applied to a real event within the last 12 months? Can you show evidence of the test or response?	____ / 4
	Category 3 Subtotal	**____ / 12**

CATEGORY 4 OF 7

Security Awareness Training

Are your people trained on security before they step inside a client site — and do you have records to prove it?

Q10	Do your personnel who access operator environments receive security awareness training — separate from or integrated into existing HSE inductions — that covers device handling, access control, and incident reporting?	____ / 4
Q11	Are training attendance records maintained with dates, topics covered, and participant signatures or acknowledgments?	____ / 4
Q12	Is the training delivered at a defined frequency (e.g., annually, at onboarding, before new project deployment) and updated when requirements change?	____ / 4
	Category 4 Subtotal	**____ / 12**

CATEGORY 5 OF 7

Change Management

When your teams make changes inside a client's environment, is every step documented, approved, and recoverable?

Q13	Does your company have a documented process for managing changes to systems, configurations, or equipment in client environments — including pre-change approval, client notification, and rollback procedures?	____ / 4
Q14	Are change records maintained (what was changed, who approved it, when it was executed, what the outcome was)?	____ / 4
Q15	Do your existing method statements, job safety analyses, or permit-to-work processes cover the security implications of the changes your teams perform?	____ / 4
	Category 5 Subtotal	**____ / 12**

CATEGORY 6 OF 7

Asset and Device Management

Do you know exactly which devices your teams take into client sites — and can you prove each one has been checked before entry?

Q16	Does your company maintain a register of all devices (laptops, tablets, diagnostic tools, USB media, network equipment) that are used in or taken into client environments?	____ / 4
Q17	Does the register include security status for each device — software version, patch status, encryption status, and authorisation for client use?	____ / 4
Q18	Is there a pre-deployment verification process that checks device security status before equipment enters a client site?	____ / 4
	Category 6 Subtotal	**____ / 12**

CATEGORY 7 OF 7

Business Continuity

If your operations are disrupted, can you show an operator that service delivery to them has a plan — and that the plan has been tested?

Q19	Does your company have a written business continuity plan that covers how you maintain service delivery to operator clients during disruptions — including staffing contingency, data backup, and client communication?	____ / 4
Q20	Have backup and recovery procedures been tested within the last 12 months?	____ / 4
Q21	Is there a defined process for notifying clients if a disruption will affect your ability to deliver contracted services?	____ / 4
	Category 7 Subtotal	**____ / 12**

YOUR SCORE SUMMARY

CATEGORY	YOUR SCORE
Cat 1 Information Security Governance	____ / 12
Cat 2 Access Management	____ / 12
Cat 3 Incident Response	____ / 12
Cat 4 Security Awareness Training	____ / 12
Cat 5 Change Management	____ / 12
Cat 6 Asset and Device Management	____ / 12
Cat 7 Business Continuity	____ / 12
Total Score	____ / 84

READINESS BANDS

SCORE	BAND	WHAT IT MEANS	PRIORITY ACTION
0 – 21	Critical Gap	Your company cannot answer a vendor qualification form today. A scored RFQ evaluation would produce a failing result. Contract renewals are at risk.	Start with Category 1 (Information Security Policy) and Category 2 (Access Management). These are the first two items every operator evaluator checks. See the 90-day build plan in *Already Here*, Chapter 9.
22 – 49	Partial Readiness	You have raw material — practices, habits, partial documentation. But the evidence is not formatted, not complete, and not current enough to survive an operator evaluation.	Identify which categories scored 0–1 (critical gaps) versus 2–3 (formalisation opportunities). Prioritise the gaps that appear in your top clients' vendor qualification forms.
50 – 84	Competitive Position	Your compliance evidence is substantially in place. You are ahead of most contractors in your category. The focus shifts from building to maintaining currency and demonstrating the advantage proactively.	Review any category scoring below 3. Ensure all documentation has been reviewed within 12 months. Begin using your compliance posture proactively in proposals and contract renewals.

THE FULL FRAMEWORK

Your score tells you where the gaps are.
Already Here tells you how to close them.

The book provides the complete seven-category evidence framework, a scored RFQ evaluation walkthrough, a full document inventory method, and a 90-day build plan. Every contractor who has worked through it left with something an evaluator can actually verify.

Get the complete framework at
alqabbatadvisory.com/already-here

CONTACT
ahmad@alqabbatadvisory.com

ALQABBAT ADVISORY
Saudi Industrial Edge Compliance Series · Riyadh, Kingdom of Saudi Arabia