GENETRIX TECHNOLOGY · REFERENCE DOCUMENT

Offshore IT Vendor Due Diligence Guide

A working reference for evaluating offshore IT partners — before you sign, during the vendor call, when reviewing the SOW, and in the first month after kick-off.

- 20 vendor call questions
- 8 reference check questions
- 10 contract clauses
- SLA benchmarks to negotiate
- 10 walk-away signals
- First-30-days checklist

Use this document in sequence: complete pre-call vetting before the first meeting, run the vendor call questions during your evaluation, send reference check questions to their named clients, assess technical deliverables, review the SOW against the contract clauses, benchmark their SLAs, and run the first-30-days checklist within a month of kick-off. Treat walk-away signals as dealbreakers — contract language does not fix structural problems.

CONTENTS

1 Pre-Call Vetting

Signals to screen for before spending time on an evaluation call. Many disqualifiers are visible in public information or in how vendors respond to initial outreach.

Verify certifications independently — do not take the deck at face value

For Salesforce-focused vendors, check claimed certifications on Trailhead Trailblazer profiles. A vendor with 12 "Salesforce experts" should have verifiable cert counts publicly listed. If they push back on this request, treat it as a signal.

Check LinkedIn profiles of the named team members they pitch

Do the people in the slide deck actually work there? How long have they been there? Mid-career contractors are common — the person pitched to you is often not the person who works on your project.

Ask for three reachable references before the first scoping call

Not logos. Not case study links. Actual names and contact details of clients at comparable scale who will take your call. A vendor who cannot provide this before the call is signalling something about their track record.

Evaluate how they respond to your RFP or initial brief

Do they ask clarifying questions about your use case, data model, and integrations — or do they send a template SOW with your company name inserted? Vendors who understand scope ask questions first. Vendors who want to sign fast send templates.

Check for sub-contracting disclosures upfront

Ask directly: "Do you sub-contract any work?" before the first formal call. This surfaces both the practice and the vendor's transparency about it. Many body-shop models rely on sub-contracting layers that are never disclosed unless asked.

Review publicly available work product

GitHub repos, Trailhead community posts, and open-source contributions give independent verification of claimed expertise. A vendor whose team participates in the Salesforce community or maintains documented public repos is verifiable before you engage.

Ask about team stability before discussing scope

Attrition in Indian IT is structurally high. Ask: "What is your annual team attrition rate?" and "What is your policy when a named resource leaves mid-engagement?" Vendors who have not thought about this will answer in a way that tells you so.

2 Vendor Call Questions

20 questions organised by theme. The "weak signal" callouts describe what a non-answer looks like — be as attentive to evasion as to the content of the answer.

A — ACCOUNTABILITY & TEAM STRUCTURE

Q1 **Who is the named architect or tech lead for this engagement? What is their current availability, and what is your contractual process if they leave mid-project?**

■ Weak signal: "The team" — no individual owns architecture decisions. Bait-and-switch on named resources is one of the most common offshore engagement failures.

Q2 **Who — by name or title — has contractual accountability for deliverable quality? Who do I escalate to if a milestone is missed?**

■ Weak signal: A named contact is listed in the slide deck but not in the SOW. Accountability that is not in the contract does not exist.

Q3 **What is your onsite/offshore ratio for this engagement? How many hours of real-time daily overlap can you guarantee?**

■ Weak signal: Under 2 hours of real-time overlap means async delivery. Decision cycles slow to 24+ hours, defect resolution drags, and QA rounds compound. For IST-to-EST engagements this requires deliberate scheduling — it does not happen by default.

Q4 **What is your team's attrition rate? What happens if the lead developer or architect is unavailable for two or more weeks mid-engagement?**

■ Weak signal: No named backup or replacement SLA in the SOW. Your project timeline absorbs the gap at your cost.

Q5 **Do you sub-contract any portion of the work? If yes, to whom, and what is your disclosure policy? Are sub-contractors bound by the same confidentiality and IP terms?**

■ Weak signal: Denial followed by a sub-contractor appearing during the project, or a blanket "we handle it internally" without specifics. Ask for the sub-contracting clause — if it is absent from the MSA, assume sub-contracting is happening undisclosed.

B — DELIVERY PROCESS & PROJECT MANAGEMENT

Q6 **Walk me through your SOW-to-kickoff process. What do you need from us to start, and how long does kickoff typically take?**

■ Weak signal: No defined onboarding checklist. Access requests, environment setup, and tool provisioning handled ad hoc — which delays every subsequent milestone.

Q7 **How are scope changes handled? What specifically triggers a change order, and what is the approval process?**

■ Weak signal: Verbal agreements on scope changes. "We handle it flexibly" means the vendor decides unilaterally what is in scope and bills accordingly.

Q8 **Give me a specific example from a prior project where scope changed materially. Who initiated it, and how was the cost and timeline impact negotiated?**

■ Weak signal: Full blame assigned to the client. Most scope creep has shared origins. A vendor who cannot describe their own role in scope evolution is either not self-aware or is misleading you.

Q9 **Walk me through your QA process. Who signs off on deliverable quality internally before it comes to us for review?**

■ Weak signal: No internal QA stage — client UAT is the first real test. This means defect discovery happens at your cost and on your time.

Q10 **Walk me through your knowledge transfer process at project end. What exactly does my team receive, and over what timeline?**

■ Weak signal: KT described as "training sessions" with no specified deliverables. Post-launch dependency on the vendor is the intended business model for many offshore firms — KT that does not produce documentation keeps them engaged.

C — TECHNICAL CAPABILITY

Q11 **Show me a sample deliverable — architecture document, technical design, or QA report — from a comparable engagement. Not anonymised to the point of meaninglessness.**

■ Weak signal: Cannot provide samples, or provides a blank template. A confident vendor has sample work product ready. References without work evidence are unverifiable.

Q12 **What version control, branching strategy, and code review process do your developers follow? Who owns the repository?**

■ Weak signal: Work done in environments you do not own or repositories the vendor controls. Direct production deployments without a review process. You want to own the repo from day one.

Q13 **How do you handle production monitoring and alerting post-launch? Who owns the runbook, and how is it transitioned to our team?**

■ Weak signal: Monitoring is an add-on, or "the team is available" is offered as a substitute for documented runbooks and alerting configuration.

Q14 **Walk me through a specific technical challenge you encountered on a past project in our stack. What was the root cause, and how did you resolve it?**

■ Weak signal: Vague or generic answer with no technical specifics. Inability to answer a domain-specific question in a domain they claim to specialise in is a direct signal about depth.

D — COMMERCIAL & LEGAL

Q15 **Are payment milestones tied to calendar dates or to written deliverable acceptance? Walk me through how the milestone structure would work.**

■ Weak signal: Front-loaded milestones — more than 40% of contract value due before the first formal deliverable acceptance. This eliminates the financial incentive to deliver on scope.

Q16 **What is your contractual SLA for P1 production incident response? Give me a specific example of when you missed an SLA commitment and how you handled it.**

■ Weak signal: "Commercially reasonable efforts" as the stated SLA. This is legally meaningless. A vendor who has never missed an SLA has either never had a real production engagement or is not being honest.

Q17 **What does your post-launch support window include, and is it time-boxed (calendar days) or effort-boxed (hours of support)?**

■ Weak signal: 30-day bug-fix window defined in calendar days with no effort commitment. A vendor can satisfy this by being technically available without resolving issues.

Q18 **What is the largest engagement you have delivered end-to-end independently — without a larger SI managing you?**

■ Weak signal: All large references involved a Tier-1 SI as the prime contractor and this vendor as a sub. A vendor who has only operated as a sub has not owned full project accountability.

E — TRACK RECORD & FAILURE HISTORY

Q19 **What have you had to remediate on a prior engagement — a failed deployment, a missed go-live, a data issue — and how specifically did you handle it?**

■ Weak signal: Claiming zero failures. No credible vendor operating at any meaningful scale has a perfect delivery record. Deflection signals that problems are not acknowledged internally and therefore not learned from.

Q20 **Provide two references at comparable scope and size who I can reach directly this week. Not testimonials — reachable humans who will take a 15-minute call.**

■ Weak signal: References provided are from the same parent company, are former colleagues, or take weeks to arrange. A vendor confident in their track record produces references without friction.

3 Reference Check Questions

Questions to ask the client references directly — not the vendor. Keep calls to 15 minutes. Ask these in order. The point is to hear what the vendor does not control.

REF Q1

Did the project deliver on time and within the original SOW cost?

If not, by how much did it slip and who absorbed the cost? Push for the actual number, not a diplomatic answer.

REF Q2

Who was your main technical point of contact? Are they still at the vendor?

If the person they worked with has left, the reference tells you less about the team you are evaluating than it appears to.

REF Q3

How did they handle scope disputes? Did you ever have to invoke contract clauses?

Positive-only references are coached. A reference who describes a real dispute and how it was resolved tells you far more than one who says everything went smoothly.

REF Q4

Would you re-engage them without any conditions or caveats?

Not "would you recommend them" — that gets a social reflex. "Without conditions" forces a more honest response.

REF Q5

How was the documentation quality? Could your internal team maintain what was delivered?

Poor documentation is the most common structural dependency trap. If the reference's team cannot maintain the work, the vendor has built in a retainer.

REF Q6

Did any sub-contractors appear during the project that were not part of the original team?

Undisclosed sub-contracting is common. References often do not realise it happened — which is itself informative.

REF Q7

Did they escalate problems to you early, or did you typically find out about issues late?

Proactive escalation is a cultural indicator. Vendors who hide problems until they become crises have the same pattern across all their engagements.

REF Q8

What is the single thing you would tell a company evaluating this vendor that their sales team won't?

Open-ended and direct. Most references will answer honestly if asked this way. It often surfaces the one structural issue the vendor has not addressed.

4 Technical Signals — What to Evaluate

When reviewing sample deliverables or conducting a technical screen. Salesforce-specific signals are particularly diagnostic for SFMC, Sales Cloud, and Service Cloud work.

Architecture Documents

Ask for a sample architecture doc or technical design from a comparable engagement. Evaluate: does it reflect actual decisions made for that client, or is it a reused template with company names swapped? Meaningful arch docs contain tradeoff rationale — why X was chosen over Y.

✔ Look for: Includes decision rationale, data model diagrams, integration architecture, and security considerations specific to the client.

✘ Red flag: Boilerplate with client name inserted. No specifics about data volumes, API limits, or environment constraints.

Salesforce-Specific Best Practices

For SFMC / Sales Cloud / Service Cloud work: ask how they handle governor limits, bulkification in Apex, named credentials for external callouts, and metadata deployment strategy. These are non-negotiable fundamentals — incorrect answers are instant disqualifiers.

✔ Look for: Clear answers on bulkification, governor limit handling, proper use of named credentials, and deployment via change sets or SFDX pipelines.

✘ Red flag: Developing directly in production. Storing credentials in custom settings rather than named credentials. "We haven't hit limits on past projects" — this means they haven't worked at scale.

Version Control & Code Review

Ask specifically: Do you use Git? What is your branching strategy? Who does code reviews and at what stage? You should own the repository from day one — if the vendor controls it, you have no visibility into what is being built and no leverage if the relationship ends.

✔ Look for: Git with feature/dev/main branching, pull request reviews before merge, client owns the repository, deployment pipelines are documented.

✘ Red flag: Work done in a repo the vendor owns. Direct pushes to main or production. Code reviews described as "we review before delivery" — meaning after the fact.

Testing & QA Process

Is UAT scripted or ad hoc? Do they produce test plans, test cases, and defect logs, or is testing described as "we test it before it goes to you"? Scripted UAT with documented test cases is a maturity signal — it also means you can compare defect rates across milestones.

✔ Look for: Written test plans, scripted test cases linked to requirements, defect tracking in a shared tool (Jira, Azure DevOps), Apex test coverage metrics provided.

✘ Red flag: UAT is "click through it and tell us what's broken." No test coverage metrics. Client discovery of defects is the primary QA mechanism.

Documentation Standards

Request their documentation template from a comparable engagement: runbook, data dictionary, API integration spec. The test is whether your team could maintain the system six months post-handover without calling the vendor.

✔ Look for: Runbooks with step-by-step ops procedures, data dictionaries with field-level documentation, integration specs with error handling, README files in all repos.

✘ Red flag: Documentation promised as a final deliverable that never materialises. "We'll walk your team through it" substituted for written handover material.

Monitoring & Production Observability

Who sets up monitoring? What does the alert stack look like post-launch? Who is paged for a P1 at 2am EST? For SFMC engagements: what monitoring covers Data Extension errors, Journey failures, and send-time anomalies?

✔ Look for: Monitoring is scoped in the SOW, not an afterthought. Named escalation contacts, defined paging process, alerting thresholds documented before go-live.

✘ Red flag: "We're available for support" with no defined monitoring setup. Your team finds out about production failures before the vendor does.

5 Contract Language to Demand

Standard MSA and SOW language that protects your interests. Insert verbatim or adapt to your legal counsel's style. Do not waive any of these for a "faster close."

DELIVERABLE ACCEPTANCE CRITERIA

"Deliverable acceptance requires written sign-off by [Client Role]. The vendor may not proceed to subsequent milestones, and no payment for the current milestone is due, until written acceptance is received. Acceptance shall not be unreasonably withheld if the deliverable meets the specifications in Schedule [X]."

Why this matters: Prevents payment for incomplete work and removes the milestone-creep pattern where vendors proceed to the next phase before the current one is closed.

CHANGE ORDER PROCESS

"No out-of-scope work commences without a written Change Order specifying: (i) description of the change, (ii) revised timeline impact, and (iii) revised cost. No Change Order is effective until approved in writing by both parties. Verbal approvals are not binding."

Why this matters: Verbal scope changes are the primary mechanism for billing disputes in offshore engagements. This clause makes the process explicit and removes ambiguity about what was agreed.

IP OWNERSHIP & WORK-FOR-HIRE

"All work product, code, configurations, documentation, and other deliverables created under this Agreement are works-for-hire and are assigned to [Client] upon creation. Vendor hereby assigns all right, title, and interest to [Client] upon payment, with no residual rights, licence, or claim retained by Vendor or any sub-contractor."

Why this matters: Without this, the vendor may argue joint ownership over reusable components or configurations built on your engagement. "Upon payment" preserves your leverage during milestone disputes.

NAMED ACCOUNTABILITY & ESCALATION

"[Vendor Role / Name] is designated as the primary accountable party for deliverable quality and is the named escalation contact. Escalations carry a maximum response SLA of [X] business hours. Vendor shall notify Client within [48] hours of any change to this named contact, and the replacement must be approved by Client."

Why this matters: Accountability diffused across "the team" is accountability that does not exist. This clause gives you approval rights over key personnel changes — critical when the architect is the primary value being delivered.

SUB-CONTRACTOR DISCLOSURE & CONTROL

"Vendor shall not sub-contract any portion of the Services to any third party without prior written Client approval. Approved sub-contractors are bound by the same confidentiality, IP ownership, and data security obligations as Vendor. Vendor remains fully liable for sub-contractor performance. Client may request the removal of any sub-contractor at any time."

Why this matters: Without this, you may not know who has access to your systems, data, or codebase. The removal right is critical — it gives you recourse without terminating the primary contract.

SLA WITH DEFINED REMEDIES

"P1 incident response SLA: [2] hours from client notification. P1 resolution SLA: [8] hours. For each hour of breach beyond the response SLA, Vendor shall credit Client [X]% of the monthly support fee, up to a maximum of [25]% per month. 'Commercially reasonable efforts' is not an accepted substitute for defined response times."

Why this matters: An SLA without a remedy is a target, not a commitment. The credit mechanism creates a financial consequence for missed SLAs and aligns the vendor's incentives with your uptime.

DATA SECURITY & ACCESS CONTROLS

"Vendor shall: (i) access Client systems only through named user credentials — shared or generic credentials are prohibited; (ii) limit access to personnel directly performing work; (iii) revoke all access within [24] hours of project completion or personnel change; (iv) not store Client data on personal or non-approved devices. Vendor shall notify Client within [24] hours of any actual or suspected security incident."

Why this matters: Shared credentials and lingering access are the two most common security failures in offshore engagements. The 24-hour incident notification creates a legal obligation to disclose — without it, vendors have no incentive to surface security issues promptly.

KNOWLEDGE TRANSFER & HANDOVER

"KT deliverables shall include: (i) system architecture documentation; (ii) runbooks for all operational procedures; (iii) API and integration specifications; (iv) user administration guides; (v) [X] hours of documented walkthrough sessions. KT is not complete until Client confirms in writing that their team can operate the system independently."

Why this matters: KT defined only as "training sessions" creates a structural post-launch dependency. This clause makes KT a contractual deliverable with defined components and client sign-off required.

TERMINATION FOR CONVENIENCE

"Client may terminate this Agreement for convenience upon [30] days' written notice. Upon termination, Vendor shall: (i) deliver all completed and in-progress work product; (ii) provide a transition plan within [10] business days; (iii) cooperate with any incoming replacement vendor for up to [60] days. Client shall pay for work completed and accepted prior to the termination notice date only."

Why this matters: Without this clause, you are locked in for the SOW duration regardless of performance. This also prevents the "hold your data hostage" pattern when vendor relationships deteriorate.

NON-SOLICITATION

"During the term of this Agreement and for [12] months following termination, Vendor shall not, directly or indirectly, solicit, recruit, or hire any employee or contractor of Client who was involved in the performance of this Agreement."

Why this matters: Vendors with access to your team often view your talent as a recruiting pipeline. This is a standard commercial clause and any vendor who pushes back is signalling intent.

6 SLA Benchmarks — Negotiate to These

The "Minimum" column is what most offshore vendors offer by default. "Standard" is what a well-structured engagement looks like. Push for standard before signing.

Obligation	Minimum (Default)	Standard (Push For)	Notes
P1 incident response	2 hours	**< 1 hour**	*Must be calendar hours, not business hours.*
P1 resolution	8 hours	**< 4 hours**	*Distinguish "in progress" from "resolved."*
P2 incident response	1 business day	**< 4 business hours**	*P2s degrade performance — 1 day is too long.*
Change order turnaround	5 business days	**2–3 business days**	*Slow CO process stalls timelines. Define it.*
Status reporting	Weekly written report	**Weekly + async blocker updates**	*Define the format. "On track" without metrics is noise.*
Sprint / milestone velocity	Reported at month end	**Weekly burn-down in shared PM tool**	*You should not find out a milestone is at risk the day it is due.*
UAT defect resolution	Next sprint	**P1: 24 hrs · P2: 3 days**	*Define severity tiers in the SOW.*
Post-launch support window	30 calendar days, bug-fix only	**90 days + defined effort hours**	*Calendar days ≠ effort hours. Define the hours included.*
Knowledge transfer period	5 business days	**10+ days with written deliverables**	*KT complete only on your written sign-off, not the vendor's.*
Access revocation on exit	Not defined	**24 hours**	*Make it a contractual obligation with a defined window.*

7 Commercial Red Flags in the SOW

Billing structures and contract mechanics that favour the vendor at your expense. Review every SOW against this list before signing.

Front-loaded milestone schedule — more than 40% due before first acceptance

The financial incentive to deliver is concentrated in the early milestones. Once you have paid 50-60% of the contract, the vendor's leverage is gone and yours is too. Restructure so the majority of value is tied to accepted deliverables, not kick-off and design sign-off.

T&M; with no not-to-exceed cap

Uncapped T&M; transfers all project risk to you. Scope surprises, inefficiency, and underestimated complexity become your problem in real time. If a vendor will not offer fixed-price for well-defined work, they are either unable to estimate accurately or are deliberately leaving room to bill over.

Deliverables defined by time periods, not acceptance criteria

"Month 1: Discovery" is not a deliverable — it is a billing period. Every milestone should have a specific, testable output. Time-based milestones let vendors bill for presence, not delivery.

"Commercially reasonable efforts" as the SLA standard

This phrase is legally unenforceable as an SLA. It means whatever the vendor can argue was reasonable after the fact. Every SLA commitment needs a specific time value with a defined remedy for breach.

Daily or weekly rate cards without defined deliverable scope

Rate cards without a deliverable scope are open-ended billing authorisation. A vendor quoting you $X/day/developer needs to also define what that team produces — otherwise there is no basis for measuring progress or holding them to a timeline.

KT defined as "training sessions" rather than documented handover deliverables

Training sessions transfer verbal knowledge that decays. A KT defined as sessions only means your team's ability to maintain the system depends on what they remembered from a call. Push for written runbooks, data dictionaries, and documented procedures your team can use six months later.

Post-launch support defined in calendar days without effort hours

A "60-day support period" where the vendor is available but not obligated to spend any specific effort is a nominal commitment. Push for effort-hour commitments within the support window — e.g. up to 40 hours of remediation effort included.

No version-control or repository ownership clause

If the SOW does not specify that you own the repository from day one, you may find yourself negotiating access to your own codebase if the relationship deteriorates. Demand: "Client shall own and control the primary version control repository throughout the engagement."

8 Walk-Away Signals

Conditions that should end the evaluation. Not negotiating positions — dealbreakers. If you see more than two of these, contract terms will not fix the underlying problem.

SOW names "the team" as the accountable party

No individual is responsible means no one is responsible. A vendor who will not name a specific person as the contractual accountability point for deliverable quality is structurally incapable of owning the outcome.

P1 SLA uses "commercially reasonable efforts" or "best efforts"

Legally meaningless. If they will not commit to a time-bound SLA with a defined remedy, they have assessed that they cannot meet one. Particularly material for production engagements where downtime has revenue impact.

Cannot provide sample deliverables from a comparable engagement

A vendor who has delivered the work they claim to have delivered has documentation to show for it. Absence of samples is not a confidentiality issue — architecture docs and QA reports can be anonymised in 20 minutes.

Payment milestones are more than 40% front-loaded before first acceptance

You have no financial leverage after paying the front milestones. The vendor knows this. Refuse to restructure → walk away. This is the single most reliable predictor of delivery incentive problems.

Sub-contracting policy is absent from the MSA and they resist adding it

If a vendor will not agree to a sub-contracting disclosure clause, assume sub-contracting is happening at a scale they do not want you to know about. You will not know who has access to your systems, data, or codebase.

Cannot provide a reachable reference who will take a 15-minute call this week

Not a LinkedIn endorsement, not a case study, not a written testimonial. A reachable human who worked with them at comparable scale. A vendor who cannot produce this has a track record they are not willing to expose to scrutiny.

Named architect's certifications are not verifiable in the public registry

For Salesforce-specific engagements: Salesforce publishes all active certs on Trailhead. If the claimed certifications do not appear there, they are fabricated. This is more common than it should be.

They insist on T&M; for all work, including clearly-defined scope

Fixed-price resistance on clearly scoped work signals that the vendor does not believe they can deliver within the bounds they are about to agree to. This is valuable information about their internal estimation accuracy.

The person pitched to you does not appear in subsequent technical conversations

The bait-and-switch on technical staff is endemic in offshore sales cycles. If the architect who answered your technical questions in the sales call is no longer present once work begins, you were sold a person who is not on your project.

They resist repository ownership clauses or access revocation timelines

A vendor who will not agree to client repository ownership or defined access revocation windows is structurally planning to maintain control over your deliverables as a retention mechanism. Walk away before you are in that position.

9 First 30 Days Checklist — After Signing

What to verify in the first month of engagement. Problems that surface here almost always reflect structural issues that will compound over the project lifecycle. Address them immediately or formally document them.

ACCESS & SECURITY

- All team members have named individual credentials — no shared logins
- Access is limited to environments required for current work
- You have received a list of all personnel with system access
- MFA is enforced on all access points
- No sub-contractor has appeared without your prior written approval

PROJECT SETUP

- Shared PM tool (Jira, Azure DevOps) is live and you have admin access
- Client-owned repository is set up with the agreed branching structure
- Kickoff deliverables received: project plan, RACI matrix, architecture draft
- Weekly standup and status reporting cadence is actually happening — not just promised
- First milestone deliverable date is in the project plan with clear acceptance criteria

TEAM REALITY CHECK

- The named architect/lead who was pitched to you is doing the work
- Team members on your calls match the CVs you were shown
- You have been introduced to the escalation contact named in the SOW
- Real-time overlap hours are being honoured — not rescheduled to async

FIRST DELIVERABLE QUALITY

- First deliverable matches the SOW description — not a placeholder
- Architecture documents reflect your specific system, not a template
- Code commits are showing in the repository on a consistent cadence
- Defects and blockers were surfaced proactively, not discovered by you

PROCESS COMPLIANCE

- Change order process has been tested at least once — even on a small question
- No scope work has commenced outside a formal change order
- Status reports are specific — include burn-down, risks, blockers — not "on track"
- Defect tracking is in the shared tool, not in email threads

EARLY WARNING SIGNS

- Team has changed since kick-off → invoke the named accountability clause
- Milestone showing risk → get written acknowledgement and revised plan now
- Finding problems before vendor tells you → this is a pattern, not a one-off
- Sub-contractors appeared unannounced → invoke sub-contracting clause in writing

Running an active vendor evaluation?

If this framework surfaced gaps in an evaluation you are running, we are available for a direct conversation. We have been on both sides of this table — as the vendor being evaluated and as the team brought in to remediate what went wrong. No proposal. No pitch.

Talk to Genetrix

genetrix.tech/contact/

Genetrix Technology · genetrix.tech · team@genetrix.tech