PREVENANCE

CASE STUDY • M&A DUE DILIGENCE

$4.2M in Hidden Risk Identified in 72 Hours

Pre-LOI technical due diligence on a renewable energy critical infrastructure target, conducted inside an active exclusivity window.

$4.2M

IN HIDDEN RISK IDENTIFIED, 72-HOUR DELIVERY

Prévenance
The AI-native operating partner for PE-backed SaaS

ENGAGEMENT SUMMARY

At a glance

Client	Mid-market PE fund (Australia/UK), AUM circa $1.2B
Target	PE-backed renewable energy critical infrastructure operator
Target headline metrics	$42M ARR • Series C • Distributed renewable generation & grid services
Deal context	Competitive auction, 14-day exclusivity window, indicative $310M enterprise value
Prévenance engagement	Pre-LOI Technology Due Diligence Sprint
Delivery window	72 hours from data room access to written report
Headline outcome	$4.2M in quantified hidden technology risk; $2.1M purchase price reduction; signed at revised valuation

SITUATION

A competitive auction with no time to do due diligence properly

The client was a mid-market PE fund with an active investment thesis in distributed renewable energy and grid services. The target was a Series C operator of distributed renewable generation assets and grid-edge services, with operations across three jurisdictions and a hybrid OT/IT technology stack that combined SCADA-equivalent generation control, customer-facing energy management software, and a centralised data platform that fed into regulatory reporting and commercial settlement.

The deal was a competitive auction with seven shortlisted bidders. Exclusivity was granted with a 14-day window to confirm and close. Within that window, the fund needed to complete commercial, financial, technical, and ESG diligence simultaneously. The fund's in-house operating team had pre-engaged a tier-one financial diligence firm and a commercial DD firm; technology diligence was the gap. The standard quote from established tech DD boutiques for a target of this complexity was four to six weeks. The fund had three days.

> *Critical infrastructure technology debt is the kind that results in a $310M deal with a 12-month integration cost the buyer didn't price in. We don't fix that in three days. But we surface it.*

DIAGNOSIS

What 72 hours bought

Prévenance was engaged on a Friday afternoon. Read-only access to the target's data room and a 90-minute scoping call with the target CTO were available by Friday evening. Our AI-native diligence stack was operating against the data room by Saturday morning. The written report was delivered the following Monday at 5 pm — 72 hours and 47 minutes from first data room access. The diligence covered four workstreams in parallel.

Workstream 1. Operational technology and SCADA exposure

The target's OT environment combined three generations of generation control hardware, the oldest of which had been running on an unsupported firmware revision for two years. Our agents cross-referenced the vendor's published end-of-support dates with the target's asset register, flagged the gap, and ran the affected devices against a published vulnerability database. Four CVEs of high or critical severity were identified, none of which were remediated. None had been disclosed in the target's vendor questionnaire. Estimated remediation cost: $1.8M, with a 4–6-month exposure window.

Workstream 2. Data architecture and regulatory reporting integrity

The target's commercial settlement and regulatory reporting depended on a centralised data warehouse that ingested generation telemetry, grid interconnection events, and customer consumption data. Our agents traced the data lineage from sensor to settlement and identified a class of edge-case events — specifically, generation-curtailment events triggered by grid operators — that were being recorded inconsistently between two of the three jurisdictions. The effect was a small but systematic understatement of curtailment revenue, with a knock-on effect on settlement reconciliation. Quantified exposure across the prior 18 months: $1.4M in potentially recoverable revenue, but also a $900K regulatory disclosure risk if not properly remediated and reported.

Workstream 3. Cybersecurity posture against critical infrastructure mandates

The target operated assets that fell within the scope of the relevant jurisdictional Security of Critical Infrastructure legislation, which mandates specific requirements for incident response, asset registers, and risk management programmes. Our agents mapped the target's documented controls against the mandate, identifying three areas of material non-compliance — most significantly, the absence of a tested incident response plan covering OT/IT convergence scenarios. Estimated remediation cost: $600K within the first 12 months of ownership. Regulatory penalty exposure under existing instruments: up to $11M, although prosecution likelihood was assessed as low.

Workstream 4. Technical debt and product roadmap exposure

The target's customer-facing energy management platform was running on a framework that the original vendor had announced as end-of-life eighteen months prior. The internal engineering plan for re-platforming had been deferred twice in favour of new feature development. The fund's investment thesis explicitly required the platform to scale into two new jurisdictions within 24 months. The re-platforming cost, in our quantification: $1.4M, plus an estimated 9-month delay to the geographic expansion timeline.

HOW

How AI-native diligence compresses 4 weeks into 72 hours

The diligence was not the reason we worked faster. It was faster because the architecture is different. Four specific capabilities accounted for the time compression:

Document corpus ingestion at scale. The data room contained 2,847 documents across 41 folders. A traditional diligence team would assign analysts to specific folders and produce summaries over 7–10 days. Our AI infrastructure ingested the full corpus within two hours, generated structured metadata against a critical-infrastructure DD taxonomy, and surfaced 312 documents flagged for analyst review based on risk-relevance scoring.

Automated cross-reference against external data. Vendor support dates, CVE databases, regulatory mandates, and industry incident reports were programmatically cross-referenced against the target's asset register and vendor questionnaire responses. The CVE finding in Workstream 1 took our agents 11 minutes; a traditional review of the same scope would have taken several days of senior analyst time.

Source-traced findings throughout. Every finding in the report was linked to its source evidence — a specific log file, contract clause, configuration export, or vendor disclosure. The fund's deal team could audit any claim's underlying source in seconds, materially shortening the IC discussion.

Human-in-the-Lead verification at every stage. Every finding above a defined materiality threshold was reviewed by a senior operator before inclusion in the report. AI scaled the analysis; humans owned the conclusions. No finding was published without senior sign-off.

> *AI surfaced everything. We chose what mattered. The 72-hour delivery is not a technology story. It is an architectural story.*

OUTCOMES

What changed in the deal

Item	Original deal position	Revised post-diligence
Enterprise value	$310M (LOI indicative)	$307.9M (signed)
Purchase price reduction	—	$2.1M
Quantified technology risk	Not in deal model	$4.2M, 100-day remediation roadmap
Reps & warranties	Generic	Specific carve-outs for OT vulnerability and curtailment reporting
Geographic expansion timeline	24 months in IC thesis	33 months in revised thesis (re-platforming gated)
100-day plan	Generic operating plan	OT remediation, IR plan build, re-platforming gate decision

Net value created for the client

The headline number is $4.2M of risk surfaced before the term sheet was signed. The real value was structural. The fund did not simply negotiate a $2.1M price reduction — that figure is small relative to the deal size. What the diligence produced was certainty: a quantified risk register, a costed remediation plan, and a revised investment thesis with a credible timeline. The fund's Investment Committee approved the deal with materially higher conviction than they would have under a no-tech-DD scenario, and the operating team had a 100-day plan they could execute from day one of ownership.

Across the engagement, four findings stand out as the kind of issues a traditional 4-week diligence would have surfaced; one of them — the curtailment reporting issue — is the kind of nuance that often gets missed even in extended diligence because the lineage was buried inside the data warehouse and only visible by tracing specific event types end-to-end. AI surfaced it within hours; a senior operator confirmed it during a working session with the target CTO; the fund's commercial team priced it in the deal model.

REFLECTION

Why this kind of engagement matters now

Three structural changes in the 2026 PE-backed renewable energy environment make this kind of compressed, AI-native diligence increasingly necessary.

First, deal velocity has accelerated. Exclusivity windows that used to run 30–45 days now routinely close in 14–21 days. A four-week tech DD process simply does not fit inside the calendar.

Second, critical infrastructure regulation has tightened. The relevant Security of Critical Infrastructure mandates across Australia, the UK, the EU, and, increasingly, the US impose specific risk management and reporting obligations that materially alter the cost basis for operating these assets. A diligence process that does not specifically map the target against jurisdictional mandates is leaving exposure unpriced.

Third, the integration of operational technology and customer-facing software is creating new risk surface areas that traditional diligence frameworks were not designed to evaluate. The curtailment-reporting issue surfaced in this engagement was a classic OT/IT convergence finding: the technical lineage spanned a SCADA-equivalent control system, a data warehouse, and a regulatory reporting layer. Each part was individually documented. The seam between them was not.

> *Critical infrastructure deals are no longer commercial-and-financial DD with technology as a sidecar. Technology is the deal.*

About this case study

This case study is illustrative and is based on a real Prévenance engagement. The client is not named in accordance with the confidentiality terms of the engagement. Identifying details — including sector specifics, identifying personnel, and certain financial markers — have been altered to protect client confidentiality. The engagement structure, methodology, timeline, and reported order-of-magnitude outcomes reflect the actual engagement. Named references can be arranged under NDA for qualified prospects during the engagement scoping process.

If this is relevant to a PortCo in your portfolio

Prévenance offers M&A Technology Due Diligence Sprints inside the exclusivity windows of competitive auctions. Fixed-fee, AI-native delivery, source-traced findings, and a 72-hour standard turnaround on data rooms under 5,000 documents.

To discuss: contact@prevenance.ai

To learn more: prevenance.ai

PREVENANCE