THE LININGER GROUP

PORTCO AI PLAYBOOK SERIES · NO. 2

Cost & Risk Avoidance

How to find what's about to break before your sponsor does.

> For sponsors who need early warning across the portfolio, and for the leaders who need to see risk while it's still cheap to fix.

$52M
Projected cost avoided before a 1M-unit IoT rollout

6 months
Lead time on a sub-prime wind-down before the 2008 crash

$18M
Cost out in Year 2 of a $1.1B integration

© 2026 The Lininger Group. May be shared with attribution to Rebecca S. Lininger and LiningerGroup.com.

OperationalAlpha@LiningerGroup.com

EXECUTIVE SUMMARY

The risk that kills deal theses

If you're a sponsor: customer concentration, supply chain fragility, financial controls gaps, and inventory problems are invisible in a pitch deck and fatal after close.

If you're running the business: you have blind spots. Not because you aren't paying attention, but because your current systems weren't built to surface them. AI doesn't eliminate risk. It makes risk visible early enough to act on.

WHAT YOU WILL LEAVE WITH

1. **A diagnostic framework**
   For the blind spots most likely to hurt your business right now.

2. **A case-validated method**
   From two real risk-avoidance cases: $52M of projected cost avoided and $50M+ of losses averted.

3. **A 90-day framework**
   That ends with a one-page risk dashboard your board can use.

> *The signal that saves $52M is never in the deck. It's in the engineering specs, the vendor contract, and the data pipeline your investment committee never asked to see.*

CONTENTS

01	**The four blind spots**	Where the risk hides, and what it costs per year
02	**Case studies**	The method behind $52M and $50M+ of avoided cost and losses
03	**The 90-day playbook**	Three phases, each with an output you can check
04	**The numbers**	What each phase takes and Year 1 risk scenarios
05	**Week 1 without a vendor**	Seven actions you can take this week, with no budget
06	**Three AI exercises**	Prompts for customer, supply chain, and controls scans
07	**Appendix**	Diagnostic scorecard and glossary

SECTION 1 OF 7

The four blind spots every sponsor should audit

1 **Customer concentration risk**

Your top three customers are 30% or more of revenue. Renewals depend on relationships, not data. No early warning exists for a slipping relationship, and one lost contract is a board-level event.

2 **Supply chain and inventory opacity**

You know what you ordered. You don't know what you'll receive, when, or at what cost. Demand forecasting is manual, safety stock is a guess, and stockouts and overstock are happening at the same time across different SKUs.

3 **Financial controls gaps**

AP/AR discrepancies surface only at audit. Expense patterns that don't match business activity go unnoticed for months, and vendor concentration creates leverage risk. These visibility gaps become fraud risk.

4 **Operational anomaly blindness**

Equipment runs outside normal parameters before it fails. Process steps vary by shift or operator with no documented reason, and quality problems are caught downstream instead of at the source.

Standard frameworks assume a stable environment, clean data, and a compliance mindset. Risk monitoring for a PE-backed business has to run on incomplete data, produce signals people act on rather than reports, and fit how the business already operates.

Blind spot	Typical exposure
Customer concentration	A 10–20% revenue cliff from a single non-renewal
Supply chain opacity	3–8% margin compression from reactive purchasing
Financial controls gaps	1–3% revenue leakage; audit findings that delay exits
Operational anomaly blindness	15–40% higher maintenance costs; unplanned downtime

SECTION 2 OF 7

Case studies from the operating record

Both cases come from Rebecca S. Lininger's corporate leadership roles at Ecolab and at GE Capital / CareCredit.

CASE A · ECOLAB: $52M OF PROJECTED COST AVOIDED

$52M	1M units	4 of 5	20+
Projected cost avoided	Planned IoT rollout	Global business units	AI and IoT products

The context. A one-million-unit IoT rollout across global operations, with about 5,000 units already deployed. The commercial and operating strategy, from pricing to service dispatch to account retention, assumed the IoT signals were accurate.

What she found. The devices were sending false alerts. She traced them through the time-series telemetry pipeline to the wrong sensor, using Gage R&R and designed experiments. At one million units, those false alerts would have generated a projected $52M in service and replacement cost.

What she did. Fixed 98% of the false positives and gave leadership a quantified findings brief with a defined remediation plan, not just a stop order.

- Worked with the engineering team directly, not the vendor's sales organization.
- Tested against real operating data, not vendor demo scenarios.
- Translated every technical finding into a financial exposure leadership could act on.
- Delivered a path forward, not just a diagnosis.

CASE B · GE CAPITAL / CARECREDIT: $50M+ OF LOSSES AVERTED BEFORE THE 2008 CRASH

6X	54%	6 months	$50M+
Receivables growth, $940M to $6B	Net income CAGR	Lead time before the crash	Projected losses averted

The context. A consumer credit portfolio growing fast during the mid-2000s credit expansion. Risk models were running, and the dashboards were green.

What she found. Behavioral signals in the sub-prime segment that diverged from headline portfolio metrics. The gap wasn't large enough to trip standard risk thresholds, but its direction and speed were anomalous.

What she did. Built an independent risk model that isolated the sub-prime signal and made the case that won CEO and CFO support for an early wind-down of the highest-exposure product in Q1 2008, six months before the crash.

- Independent modeling, not the same data feeds producing the green dashboards.
- Behavioral signals, not just balance-sheet metrics.
- Acting on an early signal before it was obvious, the only time acting is cheap.

What this means for your business

The same principles (independent signals, behavioral anomaly detection, early action) apply at $30M of revenue as readily as at $6B. The tools are cheaper now; the method is the same.

SECTION 3 OF 7

The 90-day risk visibility playbook

Three phases, each with an output you can check on its own.

PHASE 1 · WEEKS 1–4 Map the blind spots

Blind spot audit	A facilitated two-day session using the diagnostic scorecard in the Appendix. Identify your two highest-priority risk areas.
Data inventory	Map the signals you have against the ones you'd need: CRM, ERP, financial system outputs, and operating data.
Risk quantification	Put a dollar number on each blind spot. Unquantified risk doesn't get managed.
Stakeholder mapping	Decide who needs to know when a risk signal fires. Build the escalation chain before the alert, not after.

PHASE OUTPUT

A risk exposure brief: two priority areas, a dollar figure for each, a data inventory, and the escalation chain.

WHAT IT TAKES

A two-day working session with finance and operations leaders, plus risk quantification.

PHASE 2 · WEEKS 5–8 Build the signal layer

Data connectivity	Connect the minimum data sources for your two priority areas. This is where most of the complexity lives: data quality, system interoperability, and interpretation gaps are common, so let budget and timeline flex with what Phase 1 found.
Anomaly detection	Customer concentration: relationship health scoring. Supply chain: a demand/supply variance model. Financial controls: AP/AR pattern monitoring. Operations: a process baseline with deviation alerts.
Alert design	Define what triggers an alert, what it says, who receives it, and what action it requires.
Baseline validation	Run the models against historical data. If they don't surface risks you already know about, fix the model before deploying it.

PHASE OUTPUT

Two validated signal models with alert design and historical validation.

WHAT IT TAKES

Data connectivity and model build. Effort depends most on your data environment, which Phase 1 sizes.

PHASE 3 · WEEKS 9–12 Operationalize and report

Escalation testing	Run live for 30 days. Fire at least one test alert through the escalation chain and confirm it reaches the right person and triggers the right action.
Board-ready dashboard	One page: current risk status for each monitored area, trend versus the prior period, and open alerts with their status.
Documentation	Operating manual, model ownership, refresh cadence, and escalation protocol.
Exit criteria	Define what "stable" looks like, and when monitoring moves from active to maintenance mode.

PHASE OUTPUT

A live risk dashboard, an operating manual, and a board-ready risk brief.

WHAT IT TAKES

Dashboard build and documentation, with an owner named for ongoing monitoring.

SECTION 4 OF 7

The numbers: what to expect and when

These ranges reflect lean, focused implementations. Adjust for your revenue base and starting data quality.

WHAT EACH PHASE TAKES

Phase	Timing	Primary work
1 · Map	Weeks 1–4	Working session, risk quantification, escalation chain
2 · Build	Weeks 5–8	Data connectivity and signal models
3 · Operationalize	Weeks 9–12	Live testing, dashboard, documentation

Phase 2 effort varies most. Companies with integrated ERP and CRM and clean history move faster; fragmented data needs connection and interpretation work before models run reliably. The method requires no new platform license.

RISK AVOIDANCE SCENARIOS, YEAR 1

Illustrative, modeled on a $75M revenue business; scale proportionally.

Scenario	What happens	Risk averted	Margin protected
Conservative	One blind spot addressed, partial signal coverage	$1–3M	30–50 bps
Base	Two blind spots, full signal layer	$3–7M	75–100 bps
Upside	Three blind spots, board dashboard, exit-ready reporting	$8–15M+	120 bps or more

WHERE THE RETURN COMES FROM

Lever	Typical effect
Early churn detection	4–8 more months of relationship, or $500K–$2M per at-risk account
Supply chain anomaly detection	3–5% lower premium on reactive purchasing
Financial controls monitoring	1–2% of revenue leakage plugged; a clean audit record speeds the exit
Operational anomaly detection	20–30% lower unplanned downtime cost

The 150 bps threshold

Any AI risk investment that can't defend 150 basis points of margin protection in Year 1 doesn't meet the bar. The upside scenario clears it.

SECTION 5 OF 7

Getting started: Week 1 without a vendor

Seven actions. No vendor and no budget required. Finish them before any outside conversation.

1 **Name your top three customers**
Calculate their combined share of revenue. If it's above 30%, write down who holds each relationship and when each renews.

2 **Compare purchase orders with receipts**
Use the last 12 months to calculate your on-time, in-full delivery rate. If you don't know this number, that's the answer.

3 **Ask your CFO one question**
What was our largest AP/AR discrepancy in the last six months? If the answer takes more than 10 minutes, you have a controls visibility problem.

4 **List your three most critical processes**
For each, is performance measured in real time or reported after the fact? After the fact is a blind spot.

5 **Pull inventory turnover by SKU**
Find the 10 SKUs with the most overstock and the 10 with the most stockouts. If they overlap with your highest-margin products, you have a supply chain problem.

6 **Score your risk data**
Rate completeness, timeliness, and independence 1–5 each. Independence means the data doesn't come from the same system that would hide the problem.

7 **Define your one risk**
Which blind spot, if it hit in the next 90 days, would be a board-level event? That's your Phase 1 target.

COMMON PITFALLS

Pitfall	How to avoid it
Treating risk AI as compliance	It's an operations project. Run it like one.
Building alerts nobody acts on	Define the escalation chain before the model runs.
Letting a system monitor itself	Independent signal is the whole point. Don't use the feed that reports performance to check it.
Waiting for clean data	Build the signal on what you have, and improve the data as you go.

SECTION 6 OF 7

Three AI exercises you can run this week

Each exercise uses tools you can access today, runs on your own data in an afternoon, and maps to one blind spot.

Before you start: never put company data into a free AI tool.

Free versions of AI tools may use your inputs to train their models. A paid Claude subscription starts at about $20 a month; Google Workspace with Gemini starts at about $14 a month. Either gives you business-grade data protection. Confirm with IT or legal before running any exercise below.

1 Customer concentration scan

Addresses: Customer concentration

Map relationship health across your top accounts with data you already have.

Set up: Claude (paid) or Gemini (Google Workspace). Paste your customer revenue table and CRM activity log.

PASTE THIS PROMPT

I'm sharing two tables: (1) our top 20 customers by annual revenue, with contract renewal dates and three-year revenue trend; (2) our CRM log of the last six months of activity with each customer: meetings, calls, emails, escalations, and support tickets. Tell me: (1) which customers show declining revenue together with declining engagement, (2) which renewals in the next 12 months are at highest risk based on engagement, and (3) the top three early warning signals I should track in our CRM. Format the output as a one-page brief I can share with my sponsor.

What you'll get	A relationship health map and renewal risk ranking: the manual prototype of the customer concentration signal model.
Time required	45–60 minutes, including data prep

2 Supply chain anomaly scan

Addresses: Supply chain and inventory

Surface demand and supply mismatches hiding in your purchasing and inventory data.

Set up: Same tool. Paste or upload your inventory and purchase order data.

> **PASTE THIS PROMPT**
>
> I'm sharing 12 months of purchase order data and current inventory by SKU. Each row includes SKU, category, units ordered, units received, on-time delivery rate, current inventory, and average monthly sales. Tell me: (1) which SKUs have the largest gap between ordered and received quantities, (2) which SKUs are overstocked and undersold at the same time, (3) which supplier is responsible for the most delivery shortfalls, and (4) which three SKUs and which supplier to address first to cut reactive purchasing by 20%.

What you'll get	A supplier performance ranking and inventory mismatch map, enough to start a procurement conversation this week.
Time required	30–45 minutes, including data prep

3 Financial controls scan

Addresses: Financial controls

Surface AP/AR patterns that don't match expected business activity.

Set up: Same tool. Export a summary AP/AR aging report; no individual employee or vendor names needed.

> **PASTE THIS PROMPT**
>
> I'm sharing our AP/AR aging summary for the past six months, by vendor category and payment terms. Tell me: (1) which vendor categories show the most variance between invoice date and payment date relative to stated terms, (2) whether any months show AP volume well above the six-month average, and which categories drove it, (3) our average days to collect by customer segment, and (4) whether late payment patterns correlate with specific segments or deal sizes. Flag anything anomalous compared with the overall trend.

What you'll get	A controls pattern brief with anomaly flags: the starting point for a controls monitoring model.
Time required	30–45 minutes, including data prep

> *These exercises are the manual version of what Phase 2 automates. If any output surprises you, or you can't run one because the data doesn't exist, that's your Phase 1 target.*

SECTION 7 OF 7

Appendix: diagnostic scorecard and glossary

Score each statement from 1 (strongly disagree) to 5 (strongly agree). Your highest-scoring cluster is your Phase 1 target.

Score (1–5)	Statement
CUSTOMER CONCENTRATION	
___	Our top three customers are more than 30% of revenue.
___	We have no systematic early warning for a slipping relationship before renewal.
___	We track account activity in a CRM but don't analyze it for risk signals.
SUPPLY CHAIN AND INVENTORY	
___	We have no real-time view of supplier on-time, in-full delivery.
___	We have overstock and stockouts at the same time right now.
___	Our demand forecast relies mainly on manual input from sales.
FINANCIAL CONTROLS	
___	We find AP/AR discrepancies at audit, not in real time.
___	We can't tell within 48 hours whether an expense pattern is anomalous.
___	Our largest vendor is more than 20% of total procurement spend.
OPERATIONAL ANOMALIES	
___	Operating performance is reported after the fact, not monitored in real time.
___	We have no baseline parameters for our most critical processes.
___	Quality problems are caught downstream, at inspection or by the customer.

GLOSSARY

Independent signal

A risk data source that is separate from the system being monitored. Missing independent signal is the most common reason risk goes undetected until it becomes a crisis.

Anomaly detection

Spotting data, patterns, or behavior that deviate from the norm: the system that tells you something is wrong before it becomes a board-level event.

150 bps

150 basis points, or 1.5 percentage points of margin protection. The bar for a defensible AI risk investment.

Want help putting this to work?

The Lininger Group leads the blind spot audit and the work that follows it alongside your team on a monthly retainer. The first 30 days set the plan and the baselines.

OperationalAlpha@LiningerGroup.com · LiningerGroup.com