WHITE PAPER

Rogue IT is a *measurement problem.*

Technology bought outside IT is not usually defiance. It is an expense line nobody categorized, in a system nobody joined to the asset register.

Riverton & Associates, Inc. · 28 April 2026

Executive summary

Most organisations discuss rogue IT — shadow IT, unsanctioned spend, whatever the local term is — as a behavioural problem. Somebody went around the process. The response is a policy memo, a stricter approval workflow, and a mild sense of grievance.

That framing is wrong, and it is why the problem never goes away.

Rogue IT is overwhelmingly a **measurement** failure. A manager needed a tool, the sanctioned route would have taken six weeks, and a corporate card took four minutes. The purchase was neither hidden nor defiant. It posted to a departmental expense code, under an approval threshold, against a merchant descriptor that matches nothing in the vendor master — and was never joined to the asset register, so no system anywhere knows the tool exists.

> You cannot govern what you cannot see. Attack rogue IT first as a data problem: find it in the spend, quantify it, and only then decide what to do about it. The enforcement conversation is unproductive until the number exists.

It is not a discipline problem

Start by discarding the moral frame. In our experience the overwhelming majority of unsanctioned technology purchases share one profile: a competent person, doing their job, choosing the fastest route to a tool they needed.

If the sanctioned path takes six weeks and a credit card takes four minutes, the organisation has expressed a preference, whatever the policy says. People followed the incentive that was actually in place.

This matters practically, not just rhetorically. If you treat it as defiance, your response is enforcement — blocking, memos, tighter thresholds — which pushes the same purchases further out of view. Personal cards. Expenses coded as "training". Purchases made by a team in another country. You have not reduced the spend; you have reduced the visibility of it, which is the opposite of the goal.

Why it is invisible

The invisibility is mechanical, and each mechanism is mundane.

- **It arrives as expense, not procurement.** No purchase order, so no procurement record, so none of the controls that hang off a PO.
- **It posts to the wrong place.** The GL code is departmental — marketing, operations, R&D — not technology. Any report built on spend under the IT cost centres excludes it by construction.
- **The supplier does not resolve.** A card line arrives as a merchant descriptor. It shares no field with a vendor master record, so it is not recognised as a technology supplier, or as the same supplier three other departments are also paying.
- **It sits under the threshold.** $400 a month is invisible in a way that $4,800 a year is not. Approval limits are per-transaction; the spend is per-month.
- **It renews silently.** Auto-renewal means the decision is made once and never revisited. No one re-approves it, so no one re-examines it.
- **Nothing joins it to the asset register.** The decisive one. Even where the spend is visible, the tool never enters the CMDB, the software asset register, the SSO directory or the offboarding checklist. The finance system knows you pay for it. No operational system knows it exists. Nothing connects the two.

What it costs

The direct overspend is real but it is rarely the largest number.

- **Duplicate tooling.** Four departments buy four different tools that do the same thing — and often several buy the *same* tool on separate contracts at separate prices.
- **Lost leverage.** Fragmented purchases of one vendor are invisible as a relationship, so you buy at list price repeatedly instead of negotiating once. This is the same fragmentation that breaks the supplier top-ten, arriving through a different door.
- **Retail renewal terms.** Nobody negotiates a renewal they do not know is coming.
- **Uncontracted data exposure.** Customer or employee data in a SaaS product with no contract, no data processing agreement, and no security review — an exposure that exists whether or not anyone has noticed it.
- **Access that outlives employment.** A tool outside SSO is a tool outside offboarding. The leaver keeps their login, and no process will ever catch it.
- **An asset register that is wrong.** Every downstream process that trusts it — audit, licence compliance, security posture, disaster recovery scope — inherits the error.

Only the first three are money. The rest are risk, and the risk is unquantified precisely because the spend was never measured.

Why the usual responses fail

Policy and blocking. Addresses the symptom, worsens the visibility, and does nothing about the six-week provisioning time that caused it.

Network discovery. Genuinely useful, and structurally incomplete. Traffic-based discovery misses anything used on a personal device, on a home network, or through a browser session it cannot inspect — which is most modern SaaS.

Asking people. Surveys of department heads return what they remember and are willing to declare. They often do not know either: the person who bought the tool left last year, and the card is now on someone else's expense report.

Each of these starts from the tool. The money is a better starting point, because a purchase always leaves a financial trace even when it leaves no technical one.

Measure it from the spend

The reliable path runs through accounts payable and the card programme, not the network.

- **Resolve the supplier.** Merchant descriptors, expense-line free text and vendor master records all have to resolve to one canonical supplier before anything can be counted. Unglamorous entity-resolution work, and nothing downstream works without it.
- **Classify at line-item level.** Not at supplier level — a supplier can sell you both technology and something else. Classification has to reach the individual line to separate a software subscription from a conference booking on the same card.
- **Enrich with what the supplier actually is.** A resolved supplier can be matched against reference data to establish that it is a software vendor at all, regardless of which GL code the line was posted to.
- **Join spend to the operational registers.** Take everything identified as technology spend and join it to the asset register, the CMDB and the SSO directory. **The gap between what is paid for and what is known about is the rogue IT number.** It is a join, not a discovery tool.
- **Flag it on the record, permanently.** The output should be an attribute on the transaction — *this line is technology, bought outside IT, on this cost centre* — so the measurement is continuous. A study is out of date the month it lands; a flag on every line is a live control.

What to do with the number

Lead with consolidation, not enforcement. The first pass usually reveals several departments paying separately for the same product. Consolidating those is a saving nobody has to be told off to achieve, and it buys the credibility for everything that follows.

Fix the risk before the commercials. Getting a discovered tool into SSO and the offboarding process is more urgent than renegotiating its price. Access outliving employment is the exposure that turns into an incident.

Fix the provisioning time. This is the actual root cause. If the sanctioned route stays six weeks, rogue IT regenerates continuously no matter how well you measure it. A fast-track path for low-value, low-risk tools removes most of the pressure.

Set thresholds that reflect annual value. Approve on the twelve-month cost, not the monthly charge, so a $400/month subscription meets the same scrutiny as a $4,800 purchase.

How to tell whether it is working

- **Rogue spend as a share of total technology spend**, trended. The absolute number matters less than the direction.
- **Time to provision a sanctioned tool.** The leading indicator. If this does not fall, nothing else will hold.
- **Duplicate tool count** — distinct products serving the same function.
- **Contract and DPA coverage** — the share of technology suppliers with both.
- **SSO and register coverage** — the share of paid-for tools that operational systems know about. The join above, reported as a percentage rather than a gap.

Conclusion

Rogue IT is not a story about people breaking rules. It is a story about an expense line that no system categorised as technology, attached to a supplier no system resolved, for a tool no system recorded.

Every part of that is a measurement failure, and every part is fixable with data work rather than policy. Resolve the supplier, classify the line, join it to the asset register, and the invisible spend becomes an ordinary number on an ordinary report.

Once it is a number, it can be managed. Until then, every conversation about it is a conversation about anecdotes.

Riverton & Associates implements the CXO Nexus enterprise spend analytics platform, which surfaces exactly this: technology spend resolved, classified at line-item level, and flagged against the cost centre that bought it.

Riverton & Associates, Inc. · Austin, Texas · riverton-assoc.com