AN EXECUTIVE BRIEFING

The AI Business Enablement Audit™

The operating system for running AI as a permanent business function.

Stephen R. Jordan

Founder, SRJ Consulting & Services LLC

> You're not behind on AI.
> You're running it without a system.

Stephen R. Jordan · The AI Business Enablement Audit™

WHERE MOST COMPANIES ARE

AI is already inside the business.

Most mid-market and enterprise organizations have multiple AI tools in active use across at least three departments.

Some are licensed and tracked. Many are not. Embedded AI features inside existing tools (Microsoft, Google, Salesforce, accounting platforms, CRM) get switched on quietly.

The question is no longer whether to adopt AI. It is whether anyone in leadership can answer four questions about what is already running.

Four questions executives cannot answer today:

01 What AI tools is the business using right now?

02 What is the fully loaded cost?

03 What outcomes is AI producing against baseline?

04 Who is accountable when something goes wrong?

THE HIDDEN NUMBER

Most organizations underestimate their fully loaded AI cost by:

2 to 4×

Direct subscriptions show up on the P&L. The other three cost layers usually do not: variable usage, integration, and labor.

PILLAR 1

The Governance Gap

Most companies have adopted AI tools without adopting AI governance.

The gap is where risk and waste accumulate:

- Fragmented use across departments
- Hidden cost that does not appear in any report
- Unclear ownership and accountability
- Data exposure leadership has not been briefed on
- Vendor dependency that is harder to unwind every quarter

THE EXPOSURE INSIDE THE GAP

Shadow AI

AI being used by employees, contractors, and embedded vendor features, without leadership approval, security review, or governance oversight.

WHAT LEADERSHIP SEES

- Approved AI tools on the inventory
- Tracked subscriptions on the P&L
- Reviewed vendor contracts

WHAT IS ACTUALLY RUNNING

- Shadow tools downloaded by individual employees
- AI features quietly switched on inside Microsoft, Google, Salesforce
- Vendor APIs running on data without contractual review

PILLAR 2

Function, Not Project

"

AI is not a project. It is a function. Treat it like one.

Projects end. Functions persist. The AI Operating System™ treats AI as a permanent business function with the same operating discipline you already apply to finance, HR, IT, and vendor risk.

WHAT EVERY BUSINESS FUNCTION NEEDS

Apply the same discipline to AI

that you already apply to every other business function.

01	**Named owner**	A specific human accountable for outcomes.
02	**Defined budget**	Visible spend, not hidden across departments.
03	**Documented controls**	Written, enforceable, and reviewable.
04	**Recurring review**	On the operating calendar, not an afterthought.
05	**Clear exit criteria**	When you stop, when you pivot, when you retire.

PILLAR 3

Performative vs Operational

Activity is not the same as productivity.

PERFORMATIVE

- Slide-deck strategy with no named owner
- Tool count substituting for tool value
- Demos and pilots, no production deployments
- Activity metrics: logins, approvals, attendance

OPERATIONAL

- Named owner with written policy
- P&L impact measured against baseline
- Production deployments with monitoring
- Outcome metrics: margin, cycle time, error rate

SELF-DIAGNOSTIC

Three signs your AI is performative

01 No one can name the owner.

Ask the leadership team who is accountable for AI outcomes. If you get three different answers, AI is unowned.

02 The metrics are activity, not outcome.

Logins, approvals, hours saved, and meetings held are not business metrics. Margin, cycle time, error rate, and revenue per employee are.

03 It lives only in a slide deck.

If your AI strategy is a quarterly slide refresh that never converts into operating discipline, you have strategy theater, not an operating function.

PILLAR 4

Owner Operator Reality

AI advice written for Silicon Valley does not work in a 200-person accounting firm or a 600-person manufacturer.

Different operating realities. Different playbooks.

THREE REASONS

Why Silicon Valley AI advice fails mid-market

DIFFERENT SCALE

Silicon Valley playbooks assume large engineering teams, generous risk tolerance, and venture capital runway. Mid-market and operating businesses run on margin, not optionality.

DIFFERENT RISK PROFILE

A regulated CPA firm or healthcare provider cannot "move fast and break things." Compliance, accreditation, and audit trails are not optional.

DIFFERENT TALENT POOL

Most organizations do not have AI engineers on staff and will not hire a Chief AI Officer. Governance must run on the leadership team already in place.

PILLAR 5

The Audit Framework

The AI Business Enablement Audit™ examines five dimensions.

01	02	03	04	05
Tools	Costs	Performance	Risk	Governance

Each dimension is examined with structured questions and produces a written outcome.

DIMENSION 01

Tools

A complete inventory of every AI tool and embedded feature in active use across the business.

THE AUDIT IDENTIFIES THREE CATEGORIES

Approved tools

Licensed, tracked, and on the official inventory.

Shadow tools

Individual employees and contractors using AI without authorization.

Embedded features

AI quietly switched on inside Microsoft, Google, Salesforce, accounting platforms, CRM.

DIMENSION 02

Costs

The four cost layers most organizations underestimate by two to four times.

01	**Direct subscriptions**	Named tools on a P&L line. The visible tip.
02	**Variable usage**	Per-token, per-call, per-seat. Often consumption-based.
03	**Integration**	Engineering hours, middleware, connectors, configuration.
04	**Labor**	Employee time learning, prompting, reviewing, correcting. The largest hidden layer.

DIMENSION 03

Performance

Business metric impact, measured against a documented baseline.

METRICS THE AUDIT EVALUATES

Cycle time

How long it takes to complete the work AI is touching, before and after.

Error rate

Mistakes per unit of output, including AI-introduced errors that did not exist before.

Margin contribution

Direct P&L impact, fully loaded across all four cost layers.

Revenue per employee

Productivity baseline, measured per headcount, before and after.

DIMENSION 04

Risk

Exposure identified at the tool, workflow, and policy level.

Data exposure

Where customer, employee, financial, or proprietary data is being processed by AI tools.

Vendor dependency

Which workflows would break if a vendor changed terms, raised prices, or shut down.

Regulatory posture

Whether current AI use creates exposure under industry regulators or accreditation bodies.

Operational continuity

What stops working if AI tooling fails, gets blocked, or behaves unexpectedly.

DIMENSION 05

Governance

The infrastructure that distinguishes a managed function from a tolerated one.

- **Named owner** — A specific human accountable for AI outcomes.
- **Written controls** — Policy that can be enforced and reviewed.
- **Recurring review** — On the operating calendar at a defined cadence.
- **Exit criteria** — When to stop, when to pivot, when to retire a tool.
- **Audit trail** — Documentation that holds up to financial, IT, internal, and accreditation auditors.

THE ENGAGEMENT

How the audit is performed

01	Discovery	Sessions with leadership and named function owners. We start by listening, not by handing you a worksheet.
02	Inventory	Review of formal and informal AI usage. Approved tools, shadow tools, and embedded features.
03	Evaluation	AI outputs and the business decisions that depend on them. Examined against documented baseline.
04	Cost mapping	Across direct, variable, integration, and labor layers. The full picture, not the visible tip.
05	Scoring	Against the five-dimension framework. Standardized so results can be benchmarked over time.

DELIVERABLES

What you receive

A written set of deliverables structured for immediate action.

01 Executive AI Scorecard

One page. Five dimensions. Strengths, gaps, and priority interventions flagged at a glance.

02 Tool Inventory and Cost Map

Every AI tool and embedded feature in use, paired with the full cost picture across all four cost layers.

03 Risk and Governance Summary

Identified risks paired with practical remediation. Documented governance baseline that meets auditor rigor.

04 90-Day Operating Plan

Prioritized action plan covering the first ninety days. Steps are specific, owned by name, executable without additional headcount.

THE PLAN YOU LEAVE WITH

The 90-day operating plan

Specific. Owned by name. Executable without additional headcount.

DAY 1–30

Stabilize

- Document the AI inventory in one place
- Assign a named owner
- Close the highest-priority governance gaps
- Stop the most exposed shadow AI use

DAY 31–60

Standardize

- Roll out written AI policy
- Establish recurring review cadence
- Begin baseline performance tracking
- Document vendor and data dependencies

DAY 61–90

Operationalize

- Integrate AI review into operating rhythm
- Complete cost mapping across all four layers
- Define exit criteria for each major tool
- Brief board, audit committee, or leadership team

TO SET EXPECTATIONS CLEARLY

What this audit is not

This is a business performance review, not a technology assessment.

✕ Not a software implementation	We do not install platforms, configure tools, or deploy systems.
✕ Not a vendor recommendation	We do not sell AI tools. We do not refer to vendors for commission.
✕ Not a technical systems audit	Not an IT or cybersecurity review. The AI IT Security Audit™ is a separate engagement.
✕ Not a generic strategy framework	Not a slide deck of trends. Specific to your organization, scored against the five dimensions.

BUILT FOR

Who this audit is for

Designed for executives, not engineers. No technical background required.

ROLES

- Owners and presidents
- CFOs and COOs
- Boards and audit committees
- Leadership teams overseeing AI risk

SECTORS

- Professional services and consulting
- Financial services and accounting
- Legal and healthcare
- Manufacturing and distribution

Built for organizations from mid-market to large multinational conglomerates.

ABOUT THE AUTHOR

Stephen R. Jordan

Founder, SRJ Consulting & Services LLC

Author of The AI Business Enablement Audit™, the first in a series on running AI as a permanent business function. Stephen draws on three decades of senior security and operations leadership at Citi, Intel, McAfee, and Optiv.

BACKGROUND

Citi
Intel
McAfee
Optiv

Based in Dallas–Fort Worth, working with executives nationwide. SRJ Consulting & Services LLC delivers AI Business Services™ and AI Risk Governance & Security™ to organizations from mid-market to large multinational conglomerates.

Ready for a defensible read on your AI exposure?

Book a consultation with Stephen R. Jordan.

srjconsultingservices.com

SRJ Consulting & Services LLC

Dallas–Fort Worth · Nationwide