AI RISK MANAGEMENT PLAYBOOK

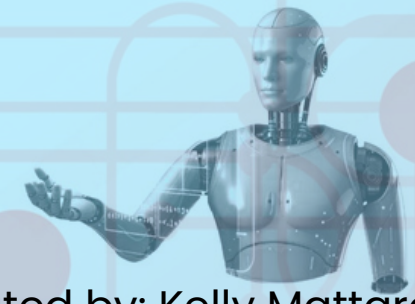
NIST AI RMF for Mid-Market Companies

Mitigate Risk. Control Costs. Govern AI with Confidence.

Prepared for forward-thinking organizations seeking structured, secure, and cost-efficient AI adoption.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

Table of Conents



Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

Executive Summary

Artificial Intelligence is transforming mid-market operations, accelerating productivity, insights, and efficiency. But it also introduces new categories of risk — operational, security, financial, and compliance — that many mid-market organizations are not yet prepared to manage.

This playbook delivers a professional, NIST-aligned AI governance framework designed specifically for lean teams and high-growth environments. It outlines how to govern AI safely while reducing cost waste, improving utilization, and eliminating hidden risks like dangling agents.

IN THIS PLAYBOOK YOU WILL LEARN:

- How to apply the NIST AI RMF: Govern → Map → Measure → Manage
- How to track AI utilization, cost efficiency, and ROI
- How to detect and eliminate dangling agents
- How to build a quarterly AI governance cadence
- How to measure bias, drift, and security exposure
- How to evaluate AI vendors and minimize spend
- How to present AI readiness to executives and boards

This is a complete and actionable framework for AI risk mitigation and operational excellence.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

THE NIST AI RMF FRAMEWORK (SIMPLIFIED)

The NIST AI Risk Management Framework provides a structured method for ensuring safe, reliable, and responsible AI use. This playbook adapts NIST for mid-market companies that need simplicity, clarity, and business alignment.

GOVERN

Establish leadership, policies, accountability, and culture.

MAP

Identify AI tools, use cases, data flows, costs, risks, and owners.

MEASURE

Evaluate performance, bias, security, utilization, spend, and agent behavior.

MANAGE

Mitigate risks, improve controls, retire unused tools, and optimize costs.

This model forms the foundation of responsible AI deployment and oversight.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

AI GOVERNANCE MATURITY MODEL

Use this 4-level model to evaluate your organization's current AI governance readiness.

LEVEL 1 — AD-HOC (High Risk)
- Shadow AI usage
- No governance or policies
- Unknown AI spending
- Dangling agents operating without owners

LEVEL 2 — EMERGING
- Early AI inventory
- Basic policies drafted
- Initial cost and utilization tracking
- Beginning to assign owners to AI tools and agents

LEVEL 3 — MANAGED
- Quarterly governance reviews in place
- Measurable utilization and cost KPIs
- Defined agent lifecycle governance
- Risk and compliance checkpoints established

LEVEL 4 — OPTIMIZED
- Centralized dashboards
- Automated license governance
- Predictive risk monitoring
- Full AI lifecycle and agent management

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

GOVERN

Governance sets the foundation for all safe AI activity.

STRUCTURE YOUR GOVERNANCE TEAM

- Executive Sponsor (CFO, COO, CRO)
- IT / Technical Lead
- Departmental AI Owners
- Finance or Risk Oversight

CREATE MINIMUM VIABLE AI POLICIES

- Responsible AI use
- Data classification and privacy
- Vendor approval standards
- Utilization requirements
- AI spend governance
- Agent lifecycle management (creation → review → retirement)

TRAIN EMPLOYEES ON RESPONSIBLE AI USE

Training should address:

- Data handling safety
- Bias awareness
- Limitations of generative AI
- Avoiding unauthorized automations
- The danger of dangling agents

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

MAP

BUILD YOUR AI INVENTORY

Track for every AI tool:

- Name & vendor
- Purpose
- Cost (monthly/annual)
- Assigned vs. active users
- Data processed
- Department owner
- Agents/workflows tied to the tool
- Agent owner
- Renewal date & contract tier

IDENTIFY RISK EXPOSURE AREAS

- Customer-facing impacts
- HR/hiring compliance exposure
- Pricing & financial automation risk
- Data leakage vulnerabilities
- Shadow AI tools purchased outside IT
- Dangling agents left from prior employees or old processes

VALUE & COST MAPPING

- Underutilized licenses
- Duplicate vendors
- Tools on high-risk billing models
- Low-ROI features
- Growing spend without proportional business value

Mapping creates clarity, which is the first step toward risk control.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

TOP 10 AI RISKS FOR MID-MARKET COMPANIES

1. Cost creep
2. Hallucinations and inaccurate outputs
3. Data leakage
4. Unauthorized agents
5. Overuse of generative models
6. Model drift
7. Vendor instability
8. Compliance exposure
9. Shadow AI spend
10. Weak identity and access controls

Develop a risk heatmap that scores each item by its likelihood and impact, allowing you to visually identify and prioritize high-risk areas for mitigation.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

MEASURE

Measurement ensures visibility — and visibility enables control.

UTILIZATION METRICS

- Active 30/60/90-day users
- Percentage of features used
- Department-level adoption
- Unapproved or shadow tools

COST METRICS

- Cost per active user
- License underutilization
- Vendor overlap index
- Usage-based billing risk
- AI premium feature fees

AGENT METRICS

- Last run date
- Owner verification
- Data accessed
- Status (active, deprecated, obsolete)

QUARTERLY AI RISK & PERFORMANCE REVIEW

Evaluate:

- Accuracy and reliability
- Bias and drift
- Data exposure
- Access control & MFA
- Compliance alignment
- Utilization metrics
- Cost vs. ROI
- Agent performance & necessity

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

MANAGE

Managing AI means controlling both the technology and the lifecycle of its automations.

IMPLEMENT RISK MITIGATION

- Add human review checkpoints
- Retire unused licenses
- Consolidate redundant vendors
- Strengthen identity & access controls
- Improve data quality
- Apply updated models or rulesets

DANGLING AGENT RISKS (WITH REAL EXAMPLES)

- A former employee's bot continued sending automated emails
- A deprecated pricing model kept adjusting discounts incorrectly
- An abandoned CRM workflow used outdated segmentation logic

These create financial exposure, customer experience issues, and compliance risk.

AGENT LIFECYCLE GOVERNANCE

- Quarterly agent audits
- Mandatory owner assignment
- Documentation of purpose and logic
- Auto-retirement after inactivity (90–180 days)

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

AI COST GOVERNANCE MODEL

CORE FINANCIAL METRICS

- Cost per active user
- License utilization rate (%)
- Vendor overlap index
- Usage-based billing exposure
- Contract renewal timeline
- AI feature consumption cost
- Agent runtime cost

RED FLAGS

- >50% inactive licenses
- >3 tools with overlapping capabilities
- Agents running without owners
- Monthly cost spikes
- Tools with unclear billing structures

A structured cost model protects margins and prevents AI spend from spiraling.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

GLOSSARY

Agent — Autonomous or semi-autonomous AI process executing tasks or decisions.

Workflow — Rule-based automation triggered by predefined logic.

Bot — Scripted interaction tool or automation assistant.

Model — Predictive or generative AI engine producing outputs.

Clear definitions reduce confusion and improve cross-department alignment.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

GOVERNANCE CADENCE

MONTHLY
- AI Owners Sync
- License Reconciliation

BI-MONTHLY
- Risk & Compliance Checkpoint

QUARTERLY
- AI Governance Review
- Cost & Utilization Audit
- Agent Audit

REQUIRED ARTIFACTS
- AI Inventory
- Agent Registry
- Risk Register
- Cost Dashboard
- Policy Library

Consistent cadence ensures momentum, compliance, and visibility.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

VENDOR RISK CONSIDERATIONS

1. Security Controls
2. Compliance Standards (SOC 2, ISO 27001, etc.)
3. Data Handling & Retention
4. Vendor Stability (roadmap, financial health)
5. Cost Transparency & Billing Predictability

Use these risk considerations for a vendor scorecard to streamline vendor evaluation and renewal decisions.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

EXECUTIVE DASHBOARD

At-A-Glance-Metrics

- Total AI Tools
- Active Users
- Utilization Rate (%)
- Cost per Active User
- Total Agents
- Dangling Agents Identified
- Top 3 Current Risks
- Top 3 Priorities This Quarter
- Overall Compliance Status

This becomes the executive team's single-page AI health snapshot.

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869

Ready to Strengthen Your AI Governance?

Contact Us to Schedule an Appointment

Kelly Mattarocci ,CPA, MBA

Created by: Kelly Mattarocci and AI
kelly@theexecutiveagents.com
(512) 436-3869