



Executive **EDGE**™

WHAT TO DO NEXT: AN EXECUTIVE PLAYBOOK FOR AI-READY DATA ARCHITECTURE

By Jess Mand



AI READINESS IS NOT A TOOLING DECISION – IT’S AN INFRASTRUCTURE, GOVERNANCE, AND RISK DECISION. BEFORE SCALING AI INITIATIVES, LEADERSHIP TEAMS SHOULD BE ABLE TO ANSWER THE FOLLOWING:

1. FIRST, CLARIFY THE “WHY” BEHIND AI

- Have we clearly defined the business purpose for AI adoption?
- What specific outcomes are we expecting (efficiency, revenue, risk reduction)?
- Where should AI not be used in our organization?

2. ESTABLISH A BASELINE: KNOW YOUR DATA

- Do we know where our data lives —across IT, cloud, and operational systems?
- Have we classified data by type (sensitive, proprietary, operational, public)?
- Can we map how data flows across systems and teams?

3. CONDUCT DATA DISCOVERY BEFORE DEPLOYMENT

- Have we completed a formal data discovery and inventory process?
- Do we understand which data sources AI tools will access or train on?
- Are there “unknown” or unmanaged data sources in the environment?

AI READINESS IS NOT A TOOLING DECISION – IT’S AN INFRASTRUCTURE, GOVERNANCE, AND RISK DECISION. BEFORE SCALING AI INITIATIVES, LEADERSHIP TEAMS SHOULD BE ABLE TO ANSWER THE FOLLOWING:

4. ASSESS ARCHITECTURE FOR AI READINESS

- Is our current infrastructure designed to support AI workloads securely?
- Are IT and Operational Technology (OT) environments segmented—or fully exposed?
- Do we have visibility into systems connected outside traditional IT (e.g., building systems, IoT, industrial controls)?

5. VALIDATE DATA INTEGRITY, NOT JUST SECURITY

- How do we ensure the data feeding AI systems is accurate—not just protected?
- Do we have processes to detect corrupted, manipulated, or low-quality data?
- Are backups validated for correctness—not just availability?

6. DEFINE IDENTITY, ACCESS, AND PERMISSIONS

- Who has access to what data—and is it consistently enforced?
- Are permissions aligned to roles, or is data broadly accessible?
- How do we prevent AI from unintentionally exposing restricted data across systems?

AI READINESS IS NOT A TOOLING DECISION – IT’S AN INFRASTRUCTURE, GOVERNANCE, AND RISK DECISION. BEFORE SCALING AI INITIATIVES, LEADERSHIP TEAMS SHOULD BE ABLE TO ANSWER THE FOLLOWING:

7. INTRODUCE GOVERNANCE BEFORE SCALE

- Do we have clear policies for how AI tools can be used across the organization?
- Are there defined guardrails, approvals, and oversight mechanisms?
- Are we balancing accessibility with control—or defaulting to convenience?

8. EVALUATE RISK TOLERANCE—EXPLICITLY

- What level of AI-related risk is acceptable to the organization?
- What scenarios would be considered intolerable (data breach, misinformation, operational disruption)?
- Is leadership aligned on those thresholds?

9. PRESSURE-TEST AGAINST ADVERSARIAL RISK

- How could AI be used against our organization?
- Are we prepared for AI-driven fraud, ransomware, or data manipulation?
- Have we assessed exposure across both IT and OT environments?

AI READINESS IS NOT A TOOLING DECISION – IT’S AN INFRASTRUCTURE, GOVERNANCE, AND RISK DECISION. BEFORE SCALING AI INITIATIVES, LEADERSHIP TEAMS SHOULD BE ABLE TO ANSWER THE FOLLOWING:

10. DECIDE: RETROFIT OR REBUILD

- Can our current systems realistically support AI securely?
- Should we build a parallel, AI-ready environment instead of retrofitting legacy systems?
- Do we have the investment roadmap to support that decision?

THE BOTTOM LINE:

If leadership cannot confidently answer these questions, AI is being deployed on an unstable foundation. The organizations that get this right will not be the ones that adopt AI fastest—but the ones that build the infrastructure to support it safely, securely, and at scale.