Is Your Business AI-Ready?

A 10-Point Checklist for Secure and Smart Adoption

2025

NETREADY

YOUR TECHNOLOGY & SECURITY EXPERTS

Introduction: Why You Need This Checklist

AI is no longer on the horizon — it's here, reshaping industries at lightning speed. From AI-driven assistants to automated analytics, organizations of every size are testing how these tools can boost productivity, cut costs, and drive innovation.

But here's the reality: AI adoption without guardrails can be more dangerous than doing nothing at all.

- Employees may already be using AI informally, feeding sensitive data into unsecured tools.
- Regulators are writing laws faster than most businesses can keep up.
- Missteps can lead to compliance fines, reputational damage, or loss of competitive trust.

This 10-point checklist is designed to help you evaluate your readiness for AI adoption. Answer honestly, and you'll quickly see whether your business is prepared or if there are hidden risks you need to address.

01 Do you know where AI is already being used in your business?

Most organizations underestimate how quickly AI sneaks in. An employee experimenting with ChatGPT to draft emails or a department testing AI analytics without approval creates “Shadow AI.”

→ Why it matters:

You can’t govern what you don’t know. Blind spots often become breach points.

→ Executive Tip:

Start with a discovery exercise. Survey teams, review SaaS usage logs, and build a baseline inventory of AI tools currently in use.

02 Do you have an AI usage policy in place?

Policies are your first line of defense. Without them, employees will create their own rules, often putting data at risk.

→ Why it matters:

A clear policy establishes what's approved, what's prohibited, and how AI should be used responsibly.

→ Executive Tip:

Keep it simple and actionable. Cover approved tools, data handling, employee responsibilities, and escalation processes.

03 Have you classified which business data is safe to use with AI?

Not all data is created equal. Feeding confidential contracts, customer records, or financial data into consumer AI tools is like leaving the company safe unlocked.

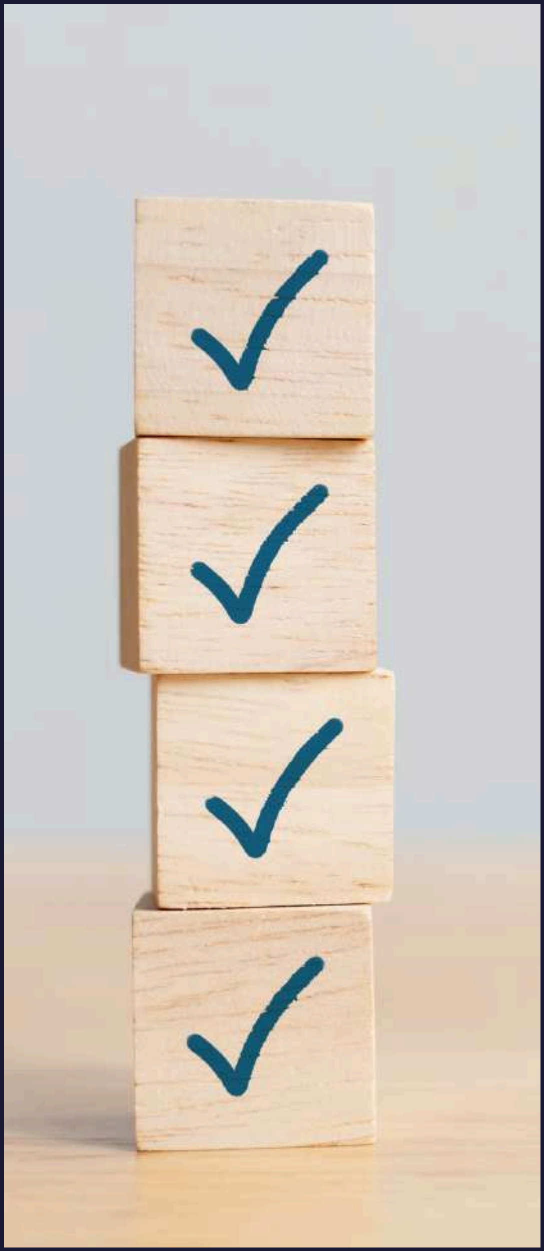
→ Why it matters:

Once data enters a public AI model, it may be retained, leaked, or even used to train future outputs.

→ Executive Tip:

Define clear “red lines” — e.g., no personally identifiable information (PII), financials, or proprietary IP should be input into AI without explicit approval.

04 Are you confident your AI vendors meet compliance standards?



Relying on AI vendors doesn't remove your accountability. These vendors include any third-party AI platform or service your business uses for example, Microsoft Copilot, Salesforce Einstein, or a recruiting system that uses AI to screen resumes. If those tools mishandle data, regulators won't just blame them — they'll blame you.

→ Why it matters:

Vendor compliance is an extension of your compliance. If your vendor falls short, you could face fines or legal issues.

→ Executive Tip:

Ask vendors about certifications (ISO 27001, SOC 2), data storage practices, and regulatory alignment (GDPR, HIPAA, etc.).

05 Do you have controls in place to prevent "Shadow AI"?

Employees are resourceful. If your business doesn't provide AI tools, they may find their own. This creates invisible risks.

→ Why it matters:

Shadow AI bypasses governance, monitoring, and compliance, exposing your organization to unvetted platforms.

→ Executive Tip:

Don't just ban tools — provide secure, approved alternatives. Adoption sticks when the safe option is also the easiest option.

06 Have you assessed the cybersecurity risks of AI tools?

Even a compliant AI vendor can still introduce vulnerabilities. AI systems expand your attack surface, with exposed APIs, third-party integrations, and potential data leakage points.

→ Why it matters:

Cybercriminals are already exploiting poorly secured AI integrations. One weak link can expose your entire environment.

→ Executive Tip:

Run security reviews before adopting any AI platform. Assess encryption, authentication, vendor security track records, and incident response capabilities.

07 Do you regularly audit AI outputs for accuracy and bias?

AI is confident — but not always correct. A flawed or biased output can mislead decision-makers or alienate customers.

→ Why it matters:

Trusting AI blindly can result in costly mistakes. Auditing ensures outputs are accurate, fair, and aligned with business standards.

→ Executive Tip:

Implement "human in the loop" reviews for all critical decisions influenced by AI. Automation should support judgment, not replace it.

08 Are your employees trained on responsible AI use?

Your people are the biggest success factor and the biggest risk factor in AI adoption.

→ Why it matters:

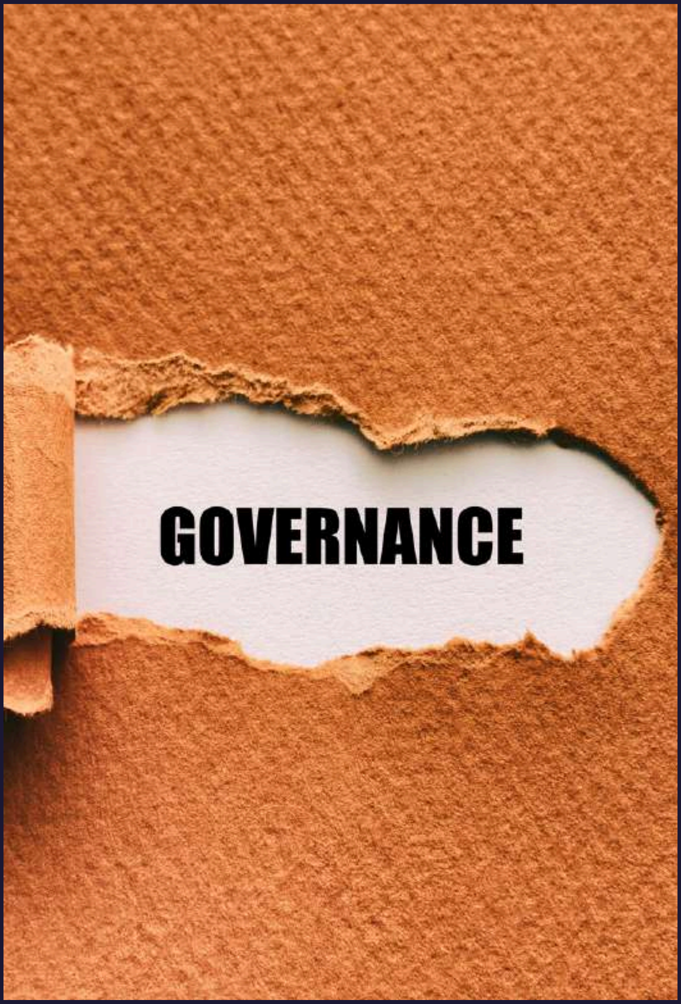
Without training, employees may overshare sensitive data, over-trust outputs, or misuse AI in ways that put the business at risk.

→ Executive Tip:

Training should include both the benefits of AI and the boundaries: what to share, what not to share, and how to question AI results.

09 Do you have an AI oversight process or governance framework?

Governance isn't about slowing down — it's about scaling safely.



→ Why it matters:

Without oversight, AI adoption becomes fragmented, inconsistent, and risky. Governance aligns AI with business goals, ethics, and compliance obligations.

→ Executive Tip:

Establish a cross-functional AI committee (IT, Legal, HR, Operations). Review AI usage quarterly to ensure it remains secure, compliant, and valuable.

10 Do you have a plan for scaling AI securely?

AI adoption is rarely "one and done." Early wins often lead to rapid expansion across the business.

→ Why it matters:

Scaling without planning multiplies risks — more tools, more data flows, more compliance requirements.

→ Executive Tip:

Build a roadmap. Start with controlled pilots, measure impact, and scale responsibly with clear governance checkpoints.

Scoring Your Readiness

- → 8–10 “Yes” answers: You’re AI-ready. Your focus should be on refining governance and expanding safely.
- → 5–7 “Yes” answers: You’re making progress but gaps remain. Prioritize policy, oversight, and training.
- → 0–4 “Yes” answers: Pump the brakes. You’re exposed to serious risks. Secure foundations are needed before scaling.

Next Steps: Secure Your AI Advantage

AI should accelerate your business, not compromise it. By working through this checklist, you've already taken the first step toward responsible adoption.

At Netready, we help businesses:

- Build custom AI usage policies.
- Train employees for safe adoption.
- Assess vendor and compliance risks.
- Establish governance frameworks for scaling securely.

Is your business truly AI-ready?
Schedule your complimentary AI Readiness Consultation with Netready. Together, we'll walk through this checklist, identify your risk areas, and design a roadmap for safe and competitive AI adoption.

NETREADY
YOUR TECHNOLOGY & SECURITY EXPERTS

Contact Information

Office :

251 S. Lake Avenue
Suite 800
Pasadena, CA 91101

Phone Number :

213-463-2100

Email :

sales@netreadyit.com

Website:

www.netreadyit.com

2025