Company Implementation Checklist

Practical actions for founders, CEOs, HR leaders, product teams, and boards.

By David H. Wever

Use this checklist as an operating tool for responsible AI adoption.

Governance

- Assign an executive or board-level AI owner
- Establish an internal AI governance group
- Adopt a written AI governance policy
- Define approval thresholds for higher-risk systems
- Set a review cadence for AI governance

AI Inventory

- List all material AI systems in use
- Record each system’s purpose
- Identify internal owner or team
- Document vendor involvement
- Record main data sources
- Note affected users, workers, or customers
- Assign a risk category to each system

Risk Classification

- Mark low-risk systems
- Mark moderate-risk systems
- Mark high-risk systems
- Mark sensitive relational systems
- Mark systemic-impact systems
- Route high-risk and sensitive systems to enhanced review

Pre-Deployment Review

- Confirm intended use is clearly defined
- Document benefits and possible harms
- Identify affected populations
- Review privacy implications
- Review fairness concerns
- Review security risks
- Identify failure modes
- Define fallback procedures
- Build in human oversight
- Provide a complaint path
- Review legal and reputational risk

Human Oversight

- Confirm no fully automated final decisions in high-stakes domains
- Ensure meaningful human review is possible
- Ensure decision-makers understand the system’s role and limits
- Create a process for appeal or reconsideration
- Provide plain-language explanation where relevant

Workforce Impact

- Identify affected roles or departments
- Estimate likely job redesign or displacement
- Estimate timeline of change
- Identify retraining opportunities
- Identify redeployment options
- Prepare communication plan
- Define severance or transition support if needed

- Assess morale and trust implications

Privacy and Data Governance

- Limit data collection to necessary use
- Identify sensitive data categories involved
- Confirm lawful basis for data use
- Prevent quiet repurposing of employee or customer data
- Review vendor data terms
- Establish retention and deletion practices
- Document whether model training uses internal data

Security

- Test for data leakage
- Test for prompt injection or misuse
- Control access to sensitive systems
- Monitor for unsafe outputs
- Create escalation path for security incidents
- Review third-party vendor protections

Children and Vulnerable Users

- Assess dependency risk
- Restrict manipulative engagement features
- Limit sensitive data use
- Prohibit deceptive human-like claims
- Define escalation rules for crisis or harm
- Ensure heightened review before launch

Transparency

- Disclose material AI use to workers where relevant

- Disclose material AI use to users or customers where relevant
- Label synthetic public-facing content where needed
- Prepare internal FAQ for AI use
- Publish annual AI transparency summary if appropriate

Incident Response

- Define what counts as an AI incident
- Create reporting mechanism
- Assign escalation owners
- Document remediation process
- Notify affected persons when appropriate
- Record lessons learned and system changes

Ongoing Review

- Reassess systems after major model changes
- Reassess systems after complaints or incidents
- Reassess systems when new regulations emerge
- Sunset or suspend systems that cannot be adequately governed
- Review governance program at least annually