

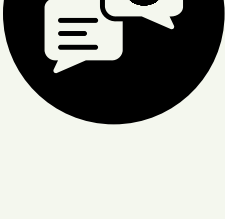


The AI Readiness Alignment Worksheet

This worksheet is designed to help technology and security leaders identify potential readiness gaps for scaling AI adoption. Across five foundational areas; connect work, ready data, secure access, manage at scale, and protect and respond, leaders can work together to uncover where potential gaps may exist and prioritize where focused action is needed. Use this guide to facilitate productive conversations, establish shared priorities, align stakeholders, and determine where to invest time and resources first to help scale AI adoption.

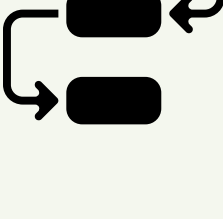
Assess

Use the questions in each of the five areas to determine where you may have potential gaps.



Align

Discuss which of the gaps could be slowing AI adoption and agree on what areas to prioritize.



Act

Build out a plan for where your organization should start and how you can scale over time.



Five foundation areas for AI readiness

Each area in this AI readiness alignment worksheet is designed to help you identify ways to strengthen specific parts of your operating environment. Together, these areas help empower enterprise momentum by helping to build readiness. The result will be the start of a plan across stakeholders for what areas to action first, building readiness over time to help evolve organizational practices with context, control, and confidence.

Connect work

Create a connected work graph across people, content, conversations, and business processes so AI has the organizational context to support workflows across the tools where work happens.

Assess.	Align.	Act.
Answer the following with yes or no.	Define and prioritize potential gaps.	Establish a plan for where to start.
Can AI access organizational context across people, content, conversations, and workflows employees need to work more effectively?		
Can AI access organizational context without creating new visibility, governance, or security gaps?		

Ready data

Prepare and govern high-value data so AI can securely ground outputs in trusted organizational knowledge while sensitivity carries into what it generates, respecting security, compliance, and business policies.

Assess.	Align.	Act.
Answer the following with yes or no.	Define and prioritize potential gaps.	Establish a plan for where to start.
Is our most valuable data discoverable, governed, and usable by AI?		
Can AI distinguish sensitive information from other information and apply the appropriate protections?		

Secure access

Establish a trust layer that helps you verify users, devices, and access requests so people and AI can securely retrieve and act on organizational information without expanding risk.

Assess.	Align.	Act.
Answer the following with yes or no.	Define and prioritize potential gaps.	Establish a plan for where to start.
Can employees securely access the information and AI experiences they need without unnecessary friction?		
Can we verify that each user, device, and AI agent is trusted before granting access to business data?		

Manage at scale

Help keep users, devices, apps, and Cloud PCs healthy and governed — extended to frontline, BYOD, contractors, and agents.

Assess.	Align.	Act.
Answer the following with yes or no.	Define and prioritize potential gaps.	Establish a plan for where to start.
Can we consistently manage and govern users, devices, apps, and AI-enabled endpoints across the organization?		

Protect and respond

Correlate signals across your organization to detect, investigate, and respond to threats across identities, devices, data, and AI-enabled workflows to help keep the organization resilient as AI adoption grows.

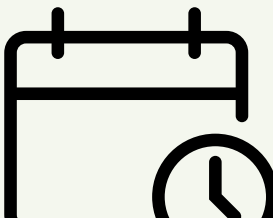
Assess.	Align.	Act.
Answer the following with yes or no.	Define and prioritize potential gaps.	Establish a plan for where to start.
Can our security operations keep pace with the speed and scale that AI introduces to the business?		
Can we rapidly detect, investigate, and contain threats before they impact data, operations, or AI-powered workflows?		

Note: Each of the five steps are interconnected capabilities which allows you to decide the best way to sequence implementation for your organization.

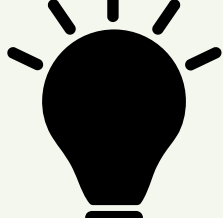
Explore more resources to support your first action steps:



Complete the [Shadow AI Risk Sprint Kit](#), a general informational framework designed to support structured conversations about potential unsanctioned AI use, data handling considerations, and governance approaches.



Find a [Microsoft Discovery session](#) and learn what's possible with Microsoft technologies—an always-on series of digital events featuring live demos, expert perspectives, and practical insights to help you achieve more with Microsoft.



Learn more about [Microsoft 365](#) to transform with AI built for work, empower productivity on any device with, [Windows 365](#), and safeguard your AI, clouds, apps, data, devices, and identities with [Microsoft Security solutions](#).

This document is provided for informational purposes only and does not constitute legal, regulatory, compliance, security, or investment advice. Microsoft makes no warranties, express or implied, in this document. References to potential benefits describe intended or possible outcomes and are not guarantees. Customers are responsible for evaluating their own legal, regulatory, security, compliance, technical, and business requirements.

