Microsoft 365

The Executive Playbook for Building AI Readiness

A shared operating model for CIOs and CISOs to help move from AI ambition to organisational readiness.





03
How to use this playbook

04
Executive summary: Ambition is outpacing AI readiness

05
The readiness gap: Assess what may be slowing AI adoption

06
The AI ready secure foundation framework

09
Three shifts that help build AI readiness

10
Role-based next steps

11
Start building your AI readiness

How to use this playbook

This playbook gives CIOs and CISOs a shared framework for building a foundation that may help their organisations unlock AI readiness and empower business transformation. The framework is to help you identify areas at your organisation where gaps may exist and then determine how you want to address those gaps. It is organised around one idea: frontier transformation starts with a secure foundation that helps bring together productivity, security, data and management. Use the information in this playbook as a guide to:

1. **Align.** Discuss and agree on where readiness gaps are slowing AI value.
2. **Assess.** Use the five steps in the AI-ready secure foundation framework to determine the highest impact and highest risk areas at your organisation as a starting point.
3. **Act.** Build a plan together for where to start and how to scale over time.

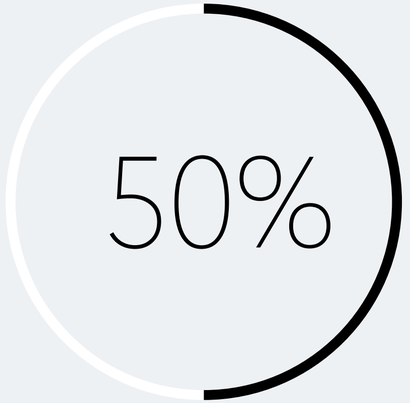


Ambition for AI may be outpacing organisational readiness.

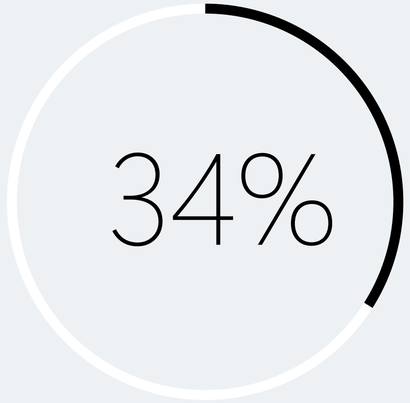
AI is widespread. According to Deloitte's 2026 State of AI in the Enterprise report, those surveyed said that their organisations have roadened worker access to AI by **50%** in just one year and **34%** reported that their companies are starting to use AI to deeply transform their products, processes and business models.[1] Ambition is high as employees are already re-imagining how work gets done with AI. They are experimenting, creating new workflows and may be moving faster than their organisations anticipated. At the same time, the systems, policies and operating models around them often continue to reinforce previous ways of working.

Microsoft's 2026 Work Trend Index calls this the Transformation Paradox[2] where employees are ready and starting to reinvent how they work, but the organisational system around them – metrics, incentives and norms – continue to reinforce the previous way of working. The same forces accelerating AI adoption might be holding it back. This gap isn't just about technology adoption. It may also be amplified by whether your organisation is ready for AI at scale in very specific places: across your tools, data, identities, endpoints and controls – essentially your foundation.

When your organisation operates from a connected and secure foundation, you unlock confidence to scale AI. This strong AI foundation is more than infrastructure – it's an operating model. By connecting people, content, communications, workflows, identities and devices on a unified platform, organisations can also embed security, compliance and management into the flow of work. This helps create the trust and control to transform workflows and build business impact. The opportunity becomes not just keeping pace with AI, but re-imagining how work gets done. It is about not how fast your organisation adopts and scales AI experiences, but how you can help enable transformation securely.



broader worker access to AI in one year reported by business leaders surveyed.[1]



of leaders surveyed reported using AI to transform products, processes and business models.[1]

The readiness gap: Assess what may be slowing AI adoption.

Employees are adopting AI to work in new ways, teams are uncovering new use cases and early pilots are demonstrating possible productivity gains. Across the business, leaders are seeing the potential for broader, larger-scale transformation. The challenge is not a lack of AI enthusiasm. The challenge is that the operational foundation has not always evolved at the same pace as employees have changed how they work.

In the 2026 Work Trend Index report, **more than 60%** of AI users surveyed[2] say AI has allowed them to spend more time on high-value work and **more than 50%** say they're producing work they couldn't have a year ago.[2] Yet at the same time, **one in four** of these same AI users[2] said that they feel their leadership is consistently aligned on their approach to AI.

As employees adopt AI-driven ways of working, legacy processes, fragmented tools, inconsistent controls and unmanaged data can slow progress. The very momentum driving AI adoption can expose the systems that were built for a different era. This is the readiness gap – and is often a foundation challenge. There are wo main areas that could contribute to this foundation challenge: disconnected experiences and security concerns.

- **2/3 of senior executives surveyed** say their organisations are overly complex and inefficient.[3]
- **More than 90% of CIOs and CTOs surveyed** said generative AI has already driven or will drive greater cybersecurity investment.[4]

Let's explore some illustrative scenarios to consider where readiness gaps could emerge across employee experiences and security. The first scenario is on the employee experience side. CIOs may start to notice more frequent employee frustrations being reported related to the time it takes them to find information or access all the apps or tools they need to get work done. These issues could indicate a readiness gap from disconnected experiences across apps, workflows, devices and data that may become larger issues as AI is scaled.

The second scenario is on the security side. As more people start to experiment and use AI in their daily workflows, CISOs may notice potential growing incidents around oversharing or an increase in the use of unsanctioned AI tools. These issues could highlight a readiness gap related to data governance and access management.

Together, these gaps may create friction that can make enterprise-wide scale for AI adoption harder to achieve. What starts as separate productivity, security and IT challenges can evolve into a shared foundation challenge. As AI adoption grows, these gaps in readiness can become more visible and more consequential.

While these are hypothetical examples of how readiness gaps may emerge, they illustrate how the opportunity cost is not simply falling behind in AI adoption. It's creating a widening gap between what your employees can achieve with AI and what your organisation is prepared to scale. Employees may be ready to reinvent work; the question is whether your foundation is ready to empower that change.

That's why scaling AI is also about aligning business, IT and secured around a shared operating model. The organisations capturing the potential from AI are not simply deploying more AI. They are strengthening their foundation to enable productivity, security and management to work together, at scale.

Readiness Check-In

Before scaling AI further, start with two questions:

- Where in your organisation do you think that AI adoption may be moving faster than your policies related to AI use and access?
- Can AI securely access enough organisational context to meaningfully improve how work gets done?

For CIOs, consider the following:

- Do we have the operational foundation to scale AI across the business?

For CISOs, consider the following:

- Do we have the control foundation to scale AI with confidence?

The AI-ready secure foundation framework

What does it take to build a secure foundation that is AI ready? One framework can help you organise your approach to start building a foundation with five steps that are designed to work together.

In each area: connect work, ready data, secure access, manage at scale and protect and respond – can help to identify potential areas for the most critical place for your organisation to start and then build, consolidate, transform and scale over time.



1.

Connect Work

Create a connected work graph across people, content, conversations and business processes so AI can have organisational context based on how work happens at your organisation. When tools are connected, employees can move from isolated AI use cases to AI-assisted workflows that span meetings, documents, business apps and collaboration tools.

Where to start
Determine your highest-value productivity tools, collaboration systems and data to prioritise connecting what employees use most frequently first.

Potential impact
Employees may spend less time searching[1] for information, switching between applications and recreating context, while AI delivers insights, recommendations and actions grounded in the way the organisation actually works.

Readiness Check-In

For CIOs consider the following:
- Can AI access the people, content, conversations and workflows employees need to work more effectively?

For CISOs consider the following:
- Can AI access organisational context without creating new visibility, governance or security gaps?

2.

Ready Data

Discover, classify, label, protect and govern high-value data so AI operates with awareness – and sensitivity carries into what it generates respecting security, compliance and business policies. When data is governed, searchable and connected, AI can ground responses in organisational knowledge rather than incomplete or outdated information.

Where to start
Don't wait for a complete labelling strategy. Focus on helping to prevent the exposure of your most sensitive information like financial, customer and intellectual property data first with Data Loss Prevention (DLP) policies. At the same time, identify and automatically label your most sensitive data that create the greatest business value – and risk. From there expand to build a broader data classification and governance programme across your organisation.

Potential impact
Employees and agents can work with trusted, sensitive information while leaders maintain visibility, control and confidence that data is used and protected in AI-powered workflows. These persistent policies remain attached to sensitive data as it moves across your organisation and is stored, shared or accessed.

Readiness Check-In

For CIOs consider the following:
- Is our most valuable data discoverable, governed and usable by AI tools and agents?

For CISOs consider the following:
- Can AI distinguish sensitive information from other information and apply the appropriate protections?

3.

Secure Access

Establish a trust layer that helps you verify users, devices and access requests so people and AI can securely retrieve in addition to acting on organisational information without expanding risk. When identity, access and permissions are aligned, employees and AI agents can securely access the information needed to get work done so organisations can expand AI adoption across teams, roles and business processes.

Where to start
Start by enforcing Multi-Factor Authentication (MFA) and Conditional Access policies for all users. These controls help to provide protection while creating the foundation for secure access to approved AI tools.

Potential impact
Employees and agents gain secure, access to information and AI-powered experiences, while security teams maintain control over how sensitive data and systems are accessed across identities, devices and agents.

Readiness Check-In

For CIOs consider the following:
- Can employees securely access the information and AI tools they need without unnecessary friction?

For CISOs consider the following:
- Can we verify that each user, device and AI agent is trusted before granting access?

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

4.

Manage at Scale

Keep users, devices, apps and Cloud PCs healthy and governed – extended to your frontline, contractors, agents and personal devices. For example, organisations that have a seasonal workforce can deliver a secure Cloud PC with organisational policies, applications and protections already built in, to quickly onboard these teams into the same governed environment used by employees-rather than shipping, managing and recovering physical devices for each individual. When endpoints are managed and secured, AI can be deployed consistently and securely across the workforce regardless of device, location or work style.

Where to start
Focus first on bringing unmanaged and personal devices under policy control through device compliance and application protection policies before expanding broader management capabilities. Bringing endpoints under a common management framework can help enable immediate security and operational benefits while creating a foundation for broader AI adoption.

Potential impact
Employees get a streamlined experience across corporate, frontline, and personal devices, while IT gains the visibility, control and consistency needed to scale AI securely.

Readiness Check-In

For CIOs consider the following:
- Can we consistently manage and govern users, devices, apps and AI-enabled endpoints across the organisation?

For CISOs consider the following:
- Can our security and compliance controls scale consistently across employees, contractors, frontline workers and AI agents?

5.

Protect and Respond

Correlate signals across your organisation to detect, investigate and respond to threats across identities, devices, data and AI-enabled workflows to help keep the organisation resilient as AI adoption grows. When protection controls are built into the foundation, organisations can confidently expand AI to more users, more data and more business scenarios.

Where to start
Start by identifying your overall exposure risk across identities, endpoints, data, cloud-resources and applications. Rather than waiting for an incident to occur, understand where you are most at risk and what actions will have significant impact on reducing those risks. From there, bring AI into your defence strategy to help security teams correlate signals, prioritise response and investigate threats faster.

Potential impact
Employees can use AI securely to support their productivity with less interruptions, while security teams gain visibility to detect and respond to threats faster.

Readiness Check-In

For CIOs consider the following:
- Can our security operations keep pace with the speed and scale that AI introduces to the business?

For CISOs consider the following:
- Can we rapidly detect, investigate and contain threats before they impact data, operations or AI-powered workflows?

> By consolidating on Microsoft 365, we've created an environment where Copilot can do its best work. This is probably why we're seeing 90% to 95% daily active use for Copilot.

Elaine Smith
Program Lead for Copilot
PepsiCo

Read the full story: PepsiCo Customer Case Study

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

Three shifts that can help build AI readiness.

Each step in the secure foundation framework is designed to strengthen a specific part of the operating environment to connect work, ready data, secure access, manage at scale and protect and respond.

Together these steps help empower enterprise momentum for broader AI transformation by helping your organisation build readiness. The result is not just a strong foundation, but a set of practical shifts that can help evolve organisational practices with context, control and confidence.

Shift 1. From disconnected tools and information to connected work intelligence.

AI becomes more useful when it can draw from the way work actually happens across people, content, conversations, meetings, applications and workflows. When information remains trapped in disconnected tools, AI can only provide partial answers and employees still spend time searching, switching contexts and rebuilding background. A connected work foundation helps give AI the organisational context it needs to generate relevant insights, summarise work in motion, recommend next steps and support action across the flow of work. Just as importantly, the work experience itself should follow employees wherever work happens – across physical devices, cloud environments, locations and teams – without losing context, access or continuity. Whether someone is a full-time employee, contractor or project-based contributor, they can remain connected to the same applications, information, policies and AI experiences that support productive work. This shift can help move organisations from disconnected experiences to more AI-ready work environments, helping to enable AI to move beyond individual productivity gains to broader changes across teams and business processes.

Shift 2. From oversharing and access risks to protected data and control.

As AI use expands, organisations need confidence that sensitive data is discoverable, governed and available only to the right people, devices and agents. Without that foundation, AI can amplify existing oversharing, access and compliance gaps. This shift is about making protection part of the operating model: classifying and labelling high-value data, applying DLP and access policies, verifying identity and device posture and ensuring policies follow data as it is stored, shared, accessed and used in AI-powered workflows. The outcome is a more trusted environment where employees and agents can use relevant business context while leaders maintain visibility, governance and control.

Shift 3. From fragmented signals to unified defence that scales.

Scaling AI increases the speed, volume and complexity of work, which can also increase the number of signals security teams need to understand and act on. A stronger foundation helps teams correlate identity, endpoint, data, app and threat signals into a more complete view of risk. It also helps bring AI into the defence strategy, supporting investigation, response and prioritisation while maintaining consistent controls across users, devices, Cloud PCs, agents and AI-enabled workflows. This shift can help organisations scale AI with resilience while empowering control in how AI is deployed, monitored and protected.

Role-based next steps.

Use the three shifts as an executive working session to turn AI readiness into a sequenced plan. The goal is not to solve every foundation gap at once, but to agree where CIO and CISO priorities must come together, what the CIO should modernise to unlock scale and what the CISO should strengthen to sustain trust as AI adoption grows.

Start together. Align on your AI-ready foundation.

Begin with a shared view of where AI ambition is moving faster than the operating model underneath it. CIO and CISO alignment should focus on the workflows, data, identities, devices and controls that matter most for the next wave of AI adoption.

1. Which AI-enabled workflows should we scale next, and what foundation needs to be in place before we expand?
2. Where do we need more connected context, stronger governance or clearer ownership to make AI useful and trusted?
3. What one readiness gap, if addressed first, would create the most confidence for the business?

CIO focus. Modernise the digital estate.

The CIO can help turn AI from isolated use cases into enterprise momentum by simplifying the digital estate, connecting the tools and workflows employees rely on and modernising endpoint and workspace experiences so AI can operate across the business with less friction.

1. How will our productivity, collaboration and endpoint strategy need to evolve as AI becomes embedded in everyday work?
2. Which employee groups, devices or work patterns need a more consistent experience before AI can scale broadly?
3. Where can consolidation and modernisation reduce complexity while increasing the value employees get from AI?

CISO focus. Extend trust and control.

The CISO can scale AI with confidence by helping to ensure sensitive data is discoverable and protected, access is governed across users, devices and agents, and security signals are unified enough to help detect and respond to threats as AI may increase speed and complexity of risks.

1. What controls need to follow data, identities, devices and agents as AI becomes part of more workflows?
2. Where do we need better visibility before expanding AI access to sensitive information or high-impact processes?
3. How should our detection, response and governance model evolve as AI and agents take on more work?

Start building your AI readiness.

AI transformation scales when work is connected, data is protected, access is governed, endpoints are managed and security signals work together. As work becomes more distributed and dynamic, organisations can benefit from a consistent, governed work environment where applications, data, policies and experiences remain connected across physical and cloud environments.

When the work experience follows employees without losing context, AI can help deliver more relevant insights, support action across workflows and scale more effectively across the organisation. That is the foundation Microsoft 365 is designed to help organisations build – bringing productivity, security, compliance, identity, endpoint management and AI into one integrated platform so CIOs, CISOs and business leaders can move forward together.

Call to action →

1. **Start together.** Align on the workflows, data, identities, devices and controls that matter most for the next phase of AI adoption.
2. **Build with Microsoft 365.** Use the integrated foundation across Microsoft 365 Suites and Microsoft 365 Copilot, and Windows 365 to connect work, protect data, govern access, manage at scale and respond with confidence.
3. **Scale with confidence.** Sequence the first moves that create momentum – starting with the highest-value use cases and the highest-risk data – then expand as the foundation strengthens.

Sources:
1 Deloitte's 2026 State of AI in Enterprise, PDF, A survey of more than 3,200 Business and IT leaders across 24 countries at organisations with 1 or more implementations of AI being used daily.
2 Work Trend Index 2026, Microsoft 365 Telemetry data is based on aggregated and anonymised Microsoft 365 productivity signals and a survey of 20,000 full-time employed or self-employed knowledge workers who use AI at work across 10 markets between February 18, 2026, and April 7, 2026. Global markets surveyed include: Australia, Brazil, France, Germany, India, Italy, Japan, Netherlands, United Kingdom and United States. 3 McKinsey's the-state-of-organisations 2026 A large-scale survey of leaders around the world from more than 10,000 senior executives across 15 countries and 16 industries.
4 NTT Data Research Reveals C-Suite Misalignment Over GenAI Adoption, June 20, 2025. A survey of more than 2,300 senior GenAI decision makers, comprising 1,500 C-Suite leaders across 34 countries.

© 2026 Microsoft Corporation. All rights reserved. This document is provided 'as-is'. Information and views expressed in this document, including URL and other Internet website references, may change without notice. You assume the risk of using said document. This document does not provide you with any legal intellectual property rights with respect to any Microsoft product. You may copy and use this document for your internal, reference purposes.