Netrix GLOBAL

SMALL BUSINESS OPERATIONS GUIDE

AI-Ready in 90 Days

A practical operations checklist for small businesses that need to run IT, secure Microsoft 365, govern AI use, and give leadership a clear plan before next quarter.

BUILT FOR MICROSOFT 365 BUSINESSES WITH 50 TO 500 USERS

START — *Understand*

DAY 30 — *Strengthen*

DAY 60 — *Build*

DAY 90

CONTENTS

What's inside

EXECUTIVE SUMMARY

AI readiness is not only an AI project

For small and mid sized businesses, AI readiness is an operating condition. It depends on how well the business manages users, devices, identity, Microsoft 365 permissions, endpoint security, backup, data access, employee behavior, and leadership accountability.

That is why turning on AI tools before reviewing the environment can create real, business impacting, risk.

Employees may already be using ChatGPT, Copilot, AI meeting assistants, AI features inside SaaS tools, or no code workflows connected to business systems. Some use cases may be helpful. Some may be risky. Most are difficult to manage if the business doesn't know what is being used, which data it has access to, or who owns the decision.

The issue is not that AI is bad. The issue is that AI moves faster than most small business IT teams can govern.

AI can make work faster. It can also make old access problems easier to find. Microsoft 365 permissions, stale sharing links, ownerless sites, personal AI accounts, unmanaged endpoints, weak multi-factor authentication (MFA) coverage, and unclear policy decisions can all become larger risks when AI is added to daily work.

This checklist is designed to help small businesses create practical AI-Ready Operations in 90 days. It focuses on five outcomes:

FIVE OUTCOMES

- Know what is in the environment
- Secure the basic IT foundation
- Review Microsoft 365 access before AI expands visibility
- Bring shadow AI under governance
- Give leadership a clear report with next steps

The goal is not to create a long strategy document. The goal is to create something your CEO, CFO, insurer, customer, and IT team can understand by next quarter.

GETTING STARTED

How to use this guide, and who it is for

How to use this checklist

This checklist is built for IT leaders, operations leaders, security owners, and executives who need a practical first step.

Use it to:

- Review your current IT and security baseline
- Identify Microsoft 365 data access risks before broader AI adoption
- Discover where shadow AI may already exist
- Create a simple AI acceptable use policy
- Build a 90 day improvement plan
- Prepare leadership and customer facing evidence
- Decide what should be handled internally and where a managed partner should support you

You do not need to complete everything at once. Start with visibility. Then fix the highest risk gaps. Then document what changed.

Who this is for

This guide is designed for companies that match one or more of the following:

- Companies with 50 to 500 users
- Businesses running on Microsoft 365
- Lean IT teams that are already stretched
- Companies considering Microsoft Copilot
- Organizations where employees already use AI tools
- Companies facing cyber insurance renewal
- Businesses receiving customer security questionnaires
- Organizations with sensitive customer, employee, financial, legal, or operational data
- Companies using multiple IT, security, backup, and SaaS vendors
- Leadership teams asking whether AI can be used safely

DEFINITIONS

What AI-Ready Operations means

AI-Ready Operations means the business has the IT, security, data, and governance foundation to use AI without creating avoidable risk.

IT IS NOT:

- ✗ *The same as buying an AI license.*
- ✗ *The same as writing one policy.*
- ✗ *The same as blocking every tool.*

AI-READY OPERATIONS MEANS:

- ✓ Users are supported
- ✓ Devices are managed
- ✓ MFA is enforced
- ✓ Endpoints are protected
- ✓ Microsoft 365 is backed up
- ✓ Permissions are reviewed
- ✓ Sensitive data is identified
- ✓ Shadow AI is discovered
- ✓ AI use is governed
- ✓ Employees are trained
- ✓ Leadership has clear answers
- ✓ Customers and insurers can be shown proof

For a small business, this matters because AI does not stay inside one department. It touches email, documents, meetings, files, customer records, contracts, finance, HR, operations, and daily workflows.

The right question is not only: *Can we use AI?*

The better question is: ***Are we ready for what AI can access?***

OUR APPROACH

The Netrix point of view

AI readiness should be operational, not theoretical.

Small businesses don't need a large AI committee before taking action. They need a practical operating model that connects IT support, security controls, Microsoft 365 governance, AI policy, monitoring, and leadership reporting.

Netrix organizes this work into three jobs.

1

Run

Keep the business operating.

This includes service desk, endpoint management, patching, Microsoft 365 administration, user provisioning, mailbox health, backup, and recovery support.

2

Secure

Protect users, devices, data, and AI usage.

This includes MFA, endpoint detection and response (EDR), threat monitoring, endpoint protection, Microsoft 365 permissions cleanup, stale access review, shadow AI inventory, AI monitoring, acceptable use policy, and staff training.

3

Guide

Give leadership practical answers.

This includes a named advisor, quarterly review, cyber insurance support, customer security questionnaire support, AI policy guidance, Copilot readiness guidance, and recommendations for what to fix next.

The goal is one accountable operating model. Not five vendors. Not five renewals. Not one internal IT leader trying to stitch everything together alone.

Netrix GLOBAL

PART 1

The AI-Ready Operations risk model

Before you build a plan, understand where the risk comes from.

PART 1 RISK MODEL

Identity, device, and data risk

01 Identity risk

Identity is the front door.

If MFA is not enforced, if stale accounts remain active, if admin access is not protected, or if guest users are not reviewed, the business has a security problem before AI enters the picture.

AI does not remove the need for identity control. It makes identity control more important.

02 Device risk

AI tools are often accessed from browsers, desktop apps, mobile devices, meeting tools, and SaaS platforms.

If devices are unmanaged, unpatched, or missing endpoint protection, it becomes harder to know where data is being accessed, copied, uploaded, or shared.

03 Microsoft 365 data risk

Many businesses have years of Microsoft 365 content spread across SharePoint, OneDrive, Teams, Outlook, and shared sites.

Over time, permissions drift. People change roles. Projects end. External sharing links remain active. Ownerless sites accumulate. Sensitive files may be stored in places that were convenient at the time but not properly governed.

When AI tools rely on existing access, these permission problems matter more.

PART 1 RISK MODEL

Shadow AI risk

04 *Shadow AI is employee use of AI tools that the business has not approved, monitored, or governed.*

It can include personal ChatGPT accounts, AI meeting assistants, browser-based AI tools, AI features inside CRM or finance platforms, no code AI automations, Copilot pilots without clear governance, and AI tools connected to company files or email.

Most shadow AI does not begin with bad intent. It usually begins with employees trying to work faster.

The risk starts when the business cannot answer:

- ☐ What tools are being used?
- ☐ What data is being entered?
- ☐ Which tools are approved?
- ☐ Who owns review?
- ☐ What should be blocked?
- ☐ What should be trained?

PART 1 RISK MODEL

Leadership proof risk

05 ***Executives, customers, insurers, auditors, and boards do not only want good intentions. They want proof.***

They may ask:

- ☐ Is MFA enforced?
- ☐ Are endpoints protected?
- ☐ Is Microsoft 365 backed up?
- ☐ Are permissions reviewed?
- ☐ Is AI use governed?
- ☐ Can employees use public AI tools?
- ☐ Is there an AI policy?
- ☐ Are users trained?
- ☐ Can you show evidence?

AI-Ready Operations should help answer these questions with confidence.

Netrix GLOBAL

PART 2

The 90-day AI-Ready Operations Checklist

Use this section as your working checklist.
Score each item as:

NOT STARTED | IN PROGRESS | COMPLETED | NEEDS PARTNER SUPPORT

Netrix GLOBAL

DAYS 1 TO 30 PHASE 1

Establish visibility

The first 30 days are about knowing what is true today.
Do not start by buying more tools.
Start by building a clear current state view.

DAYS 1 TO 30 PHASE 1

Confirm ownership

CHECKLIST

- ☐ Identify the executive sponsor
- ☐ Identify the internal IT owner
- ☐ Identify the security or compliance owner
- ☐ Identify the Microsoft 365 admin
- ☐ Identify department leaders who own sensitive data
- ☐ Identify who will approve AI tools
- ☐ Identify who will own AI policy updates
- ☐ Identify who will report progress to leadership

WHY THIS MATTERS

AI risk crosses departments. If no one owns the operating model, the work will remain scattered.

OUTPUT

AI readiness ownership map

DAYS 1 TO 30 PHASE 1

Review users and identity

CHECKLIST

- ☐ Confirm all active users
- ☐ Identify stale or inactive accounts
- ☐ Review admin accounts
- ☐ Review guest accounts
- ☐ Review external users
- ☐ Confirm MFA coverage
- ☐ Document MFA exceptions
- ☐ Review conditional access policies where available
- ☐ Review sign in activity for unusual patterns

WHY THIS MATTERS

Identity control is the foundation for secure AI adoption. If accounts are weak, stale, or over privileged, AI governance cannot compensate for that weakness.

OUTPUT

Identity and MFA baseline

DAYS 1 TO 30 PHASE 1

Review endpoints

CHECKLIST

- ☐ Confirm all laptops and desktops are inventoried
- ☐ Confirm devices are managed
- ☐ Confirm patch status
- ☐ Confirm endpoint protection coverage
- ☐ Identify unmanaged or unknown devices
- ☐ Review remote access methods
- ☐ Review device encryption status
- ☐ Document unsupported or outdated operating systems

WHY THIS MATTERS

Employees use AI from endpoints. If endpoints are unmanaged, the business has limited visibility into data movement, browser use, downloads, and risky behavior.

OUTPUT

Endpoint readiness baseline

DAYS 1 TO 30 PHASE 1

Review Microsoft 365 backup

CHECKLIST

- ☐ Confirm whether Microsoft 365 backup is in place
- ☐ Confirm what is backed up
- ☐ Confirm backup retention
- ☐ Confirm restore process
- ☐ Confirm last successful restore test
- ☐ Identify gaps across Exchange, OneDrive, SharePoint, and Teams
- ☐ Document recovery owner and escalation path

WHY THIS MATTERS

Microsoft 365 data is business critical. AI readiness should not move forward if recovery posture is unclear.

OUTPUT

Microsoft 365 backup status summary

DAYS 1 TO 30 PHASE 1

Map sensitive business data

CHECKLIST

- ☐ Identify high risk departments
- ☐ Identify sensitive SharePoint sites
- ☐ Identify sensitive Teams
- ☐ Identify sensitive OneDrive locations
- ☐ Identify HR, payroll, finance, legal, customer, executive, and regulated data
- ☐ Identify external sharing concerns
- ☐ Identify data owners for each sensitive area

WHY THIS MATTERS

You cannot protect what you have not named.

OUTPUT

Sensitive data location map

DAYS 1 TO 30 PHASE 1

Review Microsoft 365 sharing posture

CHECKLIST

- ☐ Review tenant level sharing settings
- ☐ Review site level sharing settings for sensitive sites
- ☐ Identify broad sharing links
- ☐ Identify external sharing links
- ☐ Identify anonymous or anyone links where applicable
- ☐ Identify organization wide links
- ☐ Identify ownerless or inactive sites
- ☐ Identify sites with broken or unusual permissions
- ☐ Identify broad groups with access to sensitive data

WHY THIS MATTERS

AI can make existing access easier to use. Permission cleanup should happen before broader AI adoption.

OUTPUT

Microsoft 365 access risk register

DAYS 1 TO 30 PHASE 1

Begin shadow AI discovery

CHECKLIST

- ☐ Survey department leaders
- ☐ Ask which AI tools employees are using
- ☐ Identify personal AI accounts used for work
- ☐ Identify AI meeting tools
- ☐ Identify AI tools connected to Microsoft 365, CRM, finance, HR, or support platforms
- ☐ Identify AI features inside existing SaaS platforms
- ☐ Identify teams using Copilot or planning to use Copilot
- ☐ Identify use cases involving customer or sensitive data

WHY THIS MATTERS

The official AI roadmap may not match actual employee behavior.

OUTPUT

Initial shadow AI inventory

DAYS 1 TO 30 PHASE 1

Review current AI guidance

CHECKLIST

- ☐ Confirm whether an AI policy exists
- ☐ Check if employees know about it
- ☐ Check whether approved tools are listed
- ☐ Check whether restricted data is defined
- ☐ Check whether use cases are explained
- ☐ Check whether approvals are documented
- ☐ Check whether monitoring is disclosed
- ☐ Check whether training has happened

WHY THIS MATTERS

A policy that employees do not know about will not reduce risk.

OUTPUT

AI policy maturity snapshot

DAYS 1 TO 30 CHECKPOINT

PHASE 1

Leadership checkpoint

By the end of Day 30, leadership should be able to see:

- ☐ What systems and users are in scope
- ☐ Where identity and device gaps exist
- ☐ Whether Microsoft 365 backup is ready
- ☐ Which sensitive data locations need attention
- ☐ Where Microsoft 365 sharing may be too broad
- ☐ Which AI tools are already being used
- ☐ Whether policy and training are missing

Netrix GLOBAL

DAYS 31 TO 60 PHASE 2

Secure and govern the foundation

The second phase is about reducing the highest risk gaps.

DAYS 31 TO 60 PHASE 2

Enforce MFA and reduce identity gaps

CHECKLIST

- ☐ Enforce MFA for in scope users
- ☐ Prioritize admin accounts
- ☐ Remove or document exceptions
- ☐ Disable stale accounts
- ☐ Review guest access
- ☐ Review privileged roles
- ☐ Review conditional access policy where available
- ☐ Document identity changes

WHY THIS MATTERS

MFA is one of the most visible controls for insurers, customers, and leadership.

OUTPUT

MFA enforcement and identity cleanup report

DAYS 31 TO 60 PHASE 2

Bring endpoints under management

CHECKLIST

- ☐ Enroll unmanaged devices where possible
- ☐ Apply patching standards
- ☐ Confirm endpoint protection coverage
- ☐ Identify unsupported systems
- ☐ Review remote access risk
- ☐ Create an endpoint exception list
- ☐ Document device ownership

WHY THIS MATTERS

AI governance needs managed endpoints because browsers, files, prompts, downloads, and SaaS access often happen from employee devices.

OUTPUT

Endpoint control report

DAYS 31 TO 60 PHASE 2

Clean up Microsoft 365 permissions

CHECKLIST

- [ ] Prioritize sensitive sites
- [ ] Assign site owners
- [ ] Review external sharing links
- [ ] Review organization wide links
- [ ] Remove access that is no longer needed
- [ ] Tighten HR, finance, legal, executive, customer, and regulated data locations
- [ ] Review guest access
- [ ] Review broken permission inheritance
- [ ] Document what was changed

WHY THIS MATTERS

Copilot and other AI tools work better and safer when Microsoft 365 permissions are intentional.

OUTPUT

Permissions cleanup tracker

DAYS 31 TO 60 PHASE 2

Apply interim controls where cleanup needs more time

CHECKLIST

- ☐ Identify high risk sites that need immediate containment
- ☐ Limit discovery or access where appropriate
- ☐ Restrict risky sharing patterns
- ☐ Review data loss prevention (DLP) needs
- ☐ Apply sensitivity labeling where available
- ☐ Document temporary controls
- ☐ Assign follow up owners

WHY THIS MATTERS

Some sites cannot be cleaned in one day. Interim controls help reduce risk while deeper remediation continues.

OUTPUT

Interim control register

DAYS 31 TO 60 PHASE 2

Build an approved AI tools list

CHECKLIST

- ☐ List approved AI tools
- ☐ List approved pilot tools
- ☐ List unsanctioned tools
- ☐ List blocked tools
- ☐ Assign owners to approved tools
- ☐ Define allowed users
- ☐ Define allowed data types
- ☐ Define review dates

WHY THIS MATTERS

Employees need a clear answer to the question: Can I use this tool?

OUTPUT

Approved AI tools register

DAYS 31 TO 60 PHASE 2

Create the AI acceptable use policy

CHECKLIST

- ☐ Define approved tools
- ☐ Define restricted data
- ☐ Define acceptable use cases
- ☐ Define use cases that need approval
- ☐ Define how to request a new tool
- ☐ Define employee responsibilities
- ☐ Define manager responsibilities
- ☐ Define monitoring notice
- ☐ Define policy owner
- ☐ Define review cadence

WHY THIS MATTERS

A one page policy employees understand is better than a long document that never reaches the workforce.

OUTPUT

AI acceptable use policy

DAYS 31 TO 60 PHASE 2

Train employees and managers

CHECKLIST

- ☐ Train employees on approved AI tools
- ☐ Explain restricted data
- ☐ Explain examples of allowed use
- ☐ Explain examples of risky use
- ☐ Train managers to identify new AI tools
- ☐ Explain reporting process
- ☐ Explain consequences of policy violations
- ☐ Keep attendance or acknowledgement records

WHY THIS MATTERS

AI governance fails when employees do not know what the policy means in daily work.

OUTPUT

AI awareness training record

DAYS 31 TO 60 PHASE 2

Start customer and insurer evidence collection

CHECKLIST

- [ ] Collect MFA evidence
- [ ] Collect endpoint protection evidence
- [ ] Collect Microsoft 365 backup evidence
- [ ] Collect permissions review evidence
- [ ] Collect AI policy evidence
- [ ] Collect training evidence
- [ ] Collect security monitoring evidence
- [ ] Collect incident response contact information
- [ ] Collect executive review notes

WHY THIS MATTERS

Security questionnaires and cyber insurance reviews become easier when evidence is prepared before the request arrives.

OUTPUT

Security and AI readiness evidence pack

DAYS 31 TO 60 CHECKPOINT

PHASE 2

Leadership checkpoint

By the end of Day 60, leadership should be able to see:

- ☐ MFA progress
- ☐ Endpoint management progress
- ☐ Sensitive Microsoft 365 sites reviewed
- ☐ Shadow AI inventory started
- ☐ Approved AI tools list drafted
- ☐ AI use policy created
- ☐ Training started
- ☐ Evidence collection underway

Netrix GLOBAL

DAYS 61 TO 90 PHASE 3

Validate, report, and operationalize

The final phase is about proving progress and making the process repeatable.

DAYS 61 TO 90 PHASE 3

Validate Microsoft 365 access cleanup

CHECKLIST

- ☐ Review priority sites again
- ☐ Confirm access changes were completed
- ☐ Confirm site owners are assigned
- ☐ Confirm sharing settings are documented
- ☐ Confirm external links were reviewed
- ☐ Confirm exceptions have owners and dates
- ☐ Confirm sensitive areas are better controlled

WHY THIS MATTERS

Cleanup must be validated. Otherwise, leadership cannot trust the report.

OUTPUT

Microsoft 365 permissions validation summary

DAYS 61 TO 90 PHASE 3

Validate AI monitoring and review process

CHECKLIST

- ☐ Confirm approved AI tools list is live
- ☐ Confirm unsanctioned tools are reviewed
- ☐ Confirm blocked tools are documented
- ☐ Confirm risky use cases are escalated
- ☐ Confirm employees know how to request approval
- ☐ Confirm monitoring owner is assigned
- ☐ Confirm monthly review cadence is set

WHY THIS MATTERS

AI governance is not a one time project. It needs an ongoing operating rhythm.

OUTPUT

AI monitoring and governance cadence

DAYS 61 TO 90 PHASE 3

Complete training and acknowledgement

CHECKLIST

- ☐ Confirm employees received guidance
- ☐ Confirm managers understand escalation
- ☐ Confirm training attendance
- ☐ Confirm policy acknowledgement where required
- ☐ Confirm new hire training plan
- ☐ Confirm refresher plan

WHY THIS MATTERS

Customers, insurers, and leaders increasingly expect proof that employees were trained, not just told once.

OUTPUT

Training completion summary

DAYS 61 TO 90 PHASE 3

Build the executive scorecard

CHECKLIST

- ☐ Use a simple scorecard
- ☐ Do not overload leadership with technical detail

WHY THIS MATTERS

Leadership needs a clear read on progress, not a technical debrief.

OUTPUT

AI-Ready Operations scorecard

AI-READY OPERATIONS SCORECARD

Control area	Day 0 status	Day 90 status	Next action
MFA			
Endpoint management			
Microsoft 365 backup			
Sensitive data map			
Permissions cleanup			
Shadow AI inventory			
Approved AI tools			
AI acceptable use policy			
Staff training			
Evidence pack			

DAYS 61 TO 90 PHASE 3

Prepare the customer and insurer response pack

CHECKLIST

- ☐ Create standard answers for AI use
- ☐ Create standard answers for MFA
- ☐ Create standard answers for endpoint protection
- ☐ Create standard answers for backup
- ☐ Create standard answers for access review
- ☐ Create standard answers for security monitoring
- ☐ Create standard answers for employee training
- ☐ Create standard answers for incident response
- ☐ Create standard answers for third party AI tools
- ☐ Link answers to evidence

WHY THIS MATTERS

The goal is not to rebuild answers every time a customer or insurer asks.

OUTPUT

Reusable response library

DAYS 61 TO 90 PHASE 3

Create the next quarter roadmap

CHECKLIST

- [ ] Identify remaining high risk permissions
- [ ] Identify unmanaged devices
- [ ] Identify MFA exceptions
- [ ] Identify backup improvements
- [ ] Identify AI tools needing review
- [ ] Identify departments needing deeper training
- [ ] Identify policy updates
- [ ] Identify reporting improvements
- [ ] Assign owners and dates

WHY THIS MATTERS

The first 90 days should create progress, not finish every possible task.

OUTPUT

Quarter two roadmap

DAYS 61 TO 90 CHECKPOINT

PHASE 3

Leadership checkpoint

By the end of Day 90, leadership should be able to answer:

- ☐ What changed?
- ☐ What risk was reduced?
- ☐ What still needs attention?
- ☐ Which AI tools are approved?
- ☐ Which data is restricted?
- ☐ Who owns AI governance?
- ☐ Can we show evidence to customers and insurers?
- ☐ What will we do next quarter?

Netrix GLOBAL

PART 5

The AI-Ready Operations worksheet

Use this section as a working template.

DOWNLOAD THE EDITABLE FILE

PART 5 WORKSHEET

Company profile

Company name	Number of users
Primary Microsoft 365 owner	Internal IT owner
Executive sponsor	Security or compliance owner
AI policy owner	Cyber insurance renewal date
Customer security questionnaire frequency	Current MSP or IT partner

PART 5 WORKSHEET

Quick self-assessment

Question	Yes	No	Not sure
Do we know which AI tools employees are using?			
Do we have an AI acceptable use policy?			
Do employees know what data should not go into AI?			
Are we planning to use Microsoft Copilot?			
Have Microsoft 365 permissions been reviewed recently?			
Is MFA enforced for all users?			
Are endpoints managed and protected?			
Is Microsoft 365 backup in place?			
Can we answer cyber insurance questions with proof?			
Can we answer customer security questionnaires with proof?			

PART 5 WORKSHEET

Sensitive data review

Data type	Location	Owner	Access reviewed	Risk level
HR records				
Payroll data				
Customer contracts				
Legal documents				
Financial reports				
Board materials				
Regulated data				
Source code or technical IP				

PART 5 WORKSHEET

Shadow AI inventory

Tool	Department	Use case	Data involved	Approved status	Owner
ChatGPT					
Microsoft Copilot					
AI meeting assistant					
CRM AI feature					
Finance AI tool					
No code AI workflow					
Other					

PART 5 WORKSHEET

Risk classification

Use this model to classify each AI tool or use case.

Approved	The tool is sanctioned, monitored, and supported by policy.
Approved with conditions	The tool is allowed for certain teams, data types, or use cases.
Pilot	The tool is temporarily allowed with a named owner and review date.
Needs review	The tool is in use but has not been fully assessed.
Unsanctioned	The tool is not approved for company data.
Blocked	The tool is prohibited due to security, privacy, compliance, or business risk.

Want to fill this out as a team?

Download the AI-Ready Operations Worksheet as an editable file.

DOWNLOAD THE EDITABLE FILE

Netrix GLOBAL

PART 6

AI acceptable use policy starter

Use this as a first draft. It should be reviewed by your legal, HR, IT, and security stakeholders before release.

DOWNLOAD THE EDITABLE FILE

PART 6 POLICY STARTER

Purpose, approved tools, and restricted data

Purpose

This policy explains how employees may use AI tools at work. The goal is to help employees benefit from AI while protecting company, customer, employee, and partner data.

Approved tools

Employees may use only company approved AI tools for work related activity. If a tool is not listed as approved, employees should assume it is not approved for company data.

Restricted data

Employees must not enter the following into unapproved AI tools:

- Customer confidential data
- Employee records
- Payroll information
- Financial close materials
- Legal documents
- Contracts under privilege
- Source code
- Security credentials
- API keys
- Network details
- Unreleased business plans
- Regulated personal data
- Any file labeled confidential or highly confidential

PART 6 POLICY STARTER

Acceptable use, and use that needs approval

Acceptable use cases

Employees may use approved AI tools for:

- Drafting internal content
- Summarizing approved documents
- Brainstorming ideas
- Preparing meeting notes
- Creating outlines
- Translating non sensitive content
- Improving readability
- Generating first drafts for human review

Use cases that need approval

Employees must request approval before using AI for:

- Customer facing responses
- Legal, HR, finance, or compliance decisions
- Automated workflows
- Tools connected to company systems
- Uploading large data sets
- Processing customer confidential files
- Generating regulated advice
- Security analysis involving sensitive systems
- External publication without human review

PART 6 POLICY STARTER

Roles, monitoring, and ownership

Employee responsibilities

Employees must:

- Use only approved tools
- Protect restricted data
- Review AI output before using it
- Verify facts and sources
- Avoid entering confidential information
- Report new AI tools or use cases
- Ask for help when unsure

Manager responsibilities

Managers must:

- Know which AI tools their teams are using
- Escalate new use cases
- Support employee training
- Review risky workflows
- Ensure team compliance with policy

Monitoring notice

The company may monitor AI usage on company systems, managed devices, browsers, Microsoft 365 services, and approved AI tools for security, compliance, and operational purposes.

Policy owner

The policy owner is:

Name

Role

Review cadence

Next review date

Need this in your own template?
Download the AI Acceptable Use Policy Starter as an editable Word file.

GET THE EDITABLE WORD DOCUMENT

Netrix GLOBAL

PART 7

Leadership scorecard

Use this section for your Day 90 leadership review.

DOWNLOAD THE EDITABLE FILE

PART 7 LEADERSHIP SCORECARD

Executive summary

In the first 90 days, we reviewed the IT, security, Microsoft 365, and AI governance foundation for the business. The review focused on identity, endpoints, backup, Microsoft 365 permissions, shadow AI, AI policy, training, and customer or insurer readiness.

WHAT CHANGED

REMAINING RISKS

Recommended next steps

- Complete remaining Microsoft 365 permission cleanup
- Expand endpoint management coverage
- Improve backup validation
- Finalize approved AI tools list
- Continue shadow AI monitoring
- Update AI acceptable use policy
- Train new users and managers
- Prepare customer and insurer response pack
- Schedule quarterly AI-Ready Operations review

PART 7 LEADERSHIP SCORECARD

Control area scorecard

Area	Status	Notes
MFA		
Endpoint management		
Microsoft 365 backup		
Microsoft 365 permissions		
Sensitive data locations		
Shadow AI inventory		
AI policy		
Training		
Evidence pack		
Leadership reporting		

Presenting this to leadership?
Download the Leadership Scorecard as an editable PowerPoint file.

GET THE EDITABLE POWERPOINT SCORECARD

Netrix GLOBAL

PART 8

Build it or manage it

Many small businesses ask whether they should hire internally, buy tools separately, or use a managed operating model.

DOWNLOAD THE EDITABLE FILE

PART 8 BUILD IT OR MANAGE IT

What AI-Ready Operations actually includes

There is no one answer for every business. But the decision should not be based only on salary or software cost. AI-Ready Operations includes more than one role. It includes:

- Service desk coverage
- Endpoint management
- Microsoft 365 administration
- Backup and recovery
- MFA enforcement
- EDR and threat monitoring
- Microsoft 365 permissions cleanup
- Shadow AI inventory
- AI policy
- Training
- Cyber insurance support
- Customer security questionnaire support
- Leadership reporting
- Ongoing advisory

One internal hire may help. But one person may not provide full coverage, tool management, security expertise, Microsoft 365 governance, AI policy support, after hours response, and leadership reporting. The question to ask is:

What operating model gives us the right coverage, control, accountability, and speed?

PART 8 BUILD IT OR MANAGE IT

Comparison worksheet

Requirement	Internal only	Multiple vendors	Managed program
Service desk			
Endpoint management			
Microsoft 365 admin			
Microsoft 365 backup			
MFA enforcement			
EDR and threat monitoring			
Permissions cleanup			
Shadow AI discovery			
AI policy			
Staff training			
Customer security answers			
Cyber insurance support			
Quarterly leadership review			
One accountable owner			

Scoring this with your team?

Download the Build It or Manage It comparison worksheet as an editable Excel file.

GET THE EDITABLE EXCEL WORKSHEET

Netrix GLOBAL

PART 9

What to do next

AI readiness should not wait for a major incident, a failed customer questionnaire, a cyber insurance problem, or a rushed Copilot rollout.

PART 9 WHAT TO DO NEXT

Your next three actions

Start with the foundation.

- ✓ Know your users
- ✓ Know your devices
- ✓ Know your Microsoft 365 data
- ✓ Know your permissions
- ✓ Know your AI tools
- ✓ Know your policies
- ✓ Know your evidence

1 Complete the readiness worksheet

Use the checklist in this guide to identify your current gaps across identity, endpoints, backup, Microsoft 365 permissions, shadow AI, AI policy, training, and leadership proof.

2 Identify your first 90-day priorities

Choose the highest risk areas first. For most small businesses, that means MFA, endpoint management, Microsoft 365 backup, permission cleanup, shadow AI discovery, and AI acceptable use policy.

3 Book a working session

A Netrix engineer can help you review your current environment, identify quick wins, and map a practical 90-day AI-Ready Operations plan for your business.

Then decide what should be handled internally and where your team needs support.

PART 9 WHAT TO DO NEXT

Get every worksheet in an editable format

Every working document in this guide is also available as its own editable file:

AI-Ready Operations Worksheet	EXCEL
AI Acceptable Use Policy Starter	WORD
Leadership Scorecard	POWERPOINT
Build It or Manage It Comparison Worksheet	EXCEL

Get every worksheet in an editable format

Every working document in this guide is also available as its own editable file:

DOWNLOAD THE EDITABLE FILES

Netrix GLOBAL

WORK WITH HUMANS WHO KNOW AI

Get your AI-Ready Operations plan before next quarter

Netrix helps small businesses bring IT, security, data governance, and AI governance under one accountable managed program.

If your team is using Microsoft 365, considering Copilot, facing security questionnaires, preparing for cyber insurance renewal, or trying to understand shadow AI, start with a 45-minute working session.

BOOK A 45-MINUTE WORKING SESSION

netrixglobal.ai/learn/smb-ai-ready-operations

SOURCE NOTES FOR DESIGN AND LEGAL REVIEW

This guide is informed by Microsoft guidance on Microsoft 365 Copilot architecture, Microsoft 365 Copilot privacy and security, secure governed data foundations for Copilot, SharePoint governance, Purview AI protections, Purview DLP for Copilot, Purview audit, Defender for Cloud Apps discovery, NIST AI RMF, ENISA AI cybersecurity guidance, and current market guidance around AI related cybersecurity controls.

This material is for general informational purposes and does not constitute legal advice. Review the AI acceptable use policy starter in Part 6 with your legal, HR, IT, and security stakeholders before adoption.