AI Integration Checklist

Category	Action Item	Owner
Governance & Strategy	Establish a lean AI governance framework (simplified roles, fewer committees)	CIO / IT Director
	Ensure compliance with essential regulations (GDPR, HIPAA if applicable)	Compliance Lead
	Define AI usage policy for employees (acceptable use, data handling)	HR / Legal
Zero Trust Architecture	Implement basic Zero Trust principles (MFA, conditional access)	IT Security Lead
	Use Microsoft Entra ID for identity and access management	IAM Lead
Microsoft Ecosystem Integration	Enable Microsoft 365 Copilot securely (limit access to sensitive data)	IT Ops Manager
	Configure Purview sensitivity labels for critical data	Compliance Lead
	Use Defender for Business (cost-effective security monitoring)	SOC Lead

Category	Action Item	Owner
Data Readiness & Security	Inventory core data sources (CRM, ERP, SharePoint)	Data Governance
	Apply DLP policies in Teams, SharePoint, and Exchange	IT Security Lead
	Encrypt data at rest and in transit using Azure defaults	Cloud Ops Lead
Risk & Vulnerability Management	Apply OWASP AI security basics (input validation, model integrity)	Security Team
	Implement NIST Cybersecurity Framework (simplified)	CISO / IT Lead
Operational Controls	Document AI changes in existing ITSM tool (no need for new system)	IT Ops Manager
	Update incident response playbook for AI-related risks	IR Lead
Training & Awareness	Provide executive briefing on AI risks and ROI	CIO / HR
	Offer basic AI training for employees (focus on Microsoft Copilot)	HR / L&D

Category	Action Item	Owner
Culture & Change Management	Communicate AI vision and benefits clearly to staff	Leadership Team
	Encourage safe experimentation (sandbox in Power Platform)	IT Ops Manager
Performance & ROI	Define KPIs (e.g., productivity gains, cost savings)	CFO/CIO
	Monitor Azure consumption and optimize workloads	Cloud Ops Lead