FluidOne

Copilot for Microsoft 365

Mitigating the Risks of AI Adoption

Copilot

Contents

1 Introduction

The adoption of artificial intelligence (AI) technologies into businesses is a transformative trend that holds immense potential for driving innovation, enhancing efficiency, and gaining a competitive edge. And as Microsoft continues to push the boundaries of this innovation, the introduction of Copilot for Microsoft 365 has sparked excitement and anticipation within the business community.

This AI-powered assistant promises to revolutionise productivity and collaboration by seamlessly integrating with various Microsoft 365 applications. However, as with any cutting-edge technology, the integration of AI into business operations also raises legitimate concerns that must be carefully addressed to ensure a smooth and responsible adoption process.

One of the primary concerns surrounding AI adoption is data privacy and security. AI systems – including Copilot – often rely on large volumes of data, including potentially sensitive personal information, for training and operation. To mitigate this and other risks, businesses must adopt a proactive and holistic approach in order to maximise the benefits of AI and create long-term value for all stakeholders.

Wherever you are in your AI journey, this guide is designed to help you understand your role in securing your IT environment, adopting best practice and supporting your organisation in its adoption of this incredible technology.

2

Pre-deployment: Security and Data Privacy

As AI systems become increasingly integrated into our business operations, the potential risks associated with data breaches, unauthorised access, and unintended consequences grow more pronounced. Failure to mitigate these risks could lead to devastating consequences, including financial losses, reputational damage, and erosion of public trust. So, when it comes to securing Copilot, where do you start?

Data Protection and Access Controls
Copilot's seamless integration with everyday Microsoft 365 applications undoubtedly raises concerns about vulnerabilities when it comes to sensitive information. But tools like Microsoft Purview allow you to implement robust access controls, encryption mechanisms, and data governance policies, so you can effectively safeguard sensitive information from unauthorised access or data leakage. Moreover, by enforcing strict permissions and access controls, you can clearly define what types of data Copilot can and cannot access. We'll dive deeper into what Purview can do later in this guide.

Insider Threat Prevention
While Copilot aims to enhance productivity, it could inadvertently facilitate insider threats if misused. As a result, businesses must establish clear policies and monitoring mechanisms to detect and prevent insider threats, such as the misuse of Copilot's capabilities for unauthorised access or data exfiltration. Regular auditing and user activity monitoring will also help identify and mitigate potential risks.

Compliance and Regulatory Adherence
Depending on the industry and geographic location of a business, there may be specific regulations governing data privacy, security, and the use of AI technologies such as Copilot. It's therefore essential

that you ensure deployment and usage complies with relevant data privacy regulations, industry standards, and organisational policies. Conduct regular compliance assessments and seek guidance from legal and regulatory experts if necessary.

Secure Integration and Testing
As with any new addition to your IT environment, the testing phase is crucial. Thoroughly test and validate the integration of Copilot with existing Microsoft 365 applications and workflows to identify and address any potential security vulnerabilities or compatibility issues before deploying in live production environments.

Incident Response
Despite the best laid plans, things may very well still go wrong at some point – and that's okay (as long as you plan for it). Make sure to set up incident response mechanisms to detect and respond to potential security incidents or data breaches involving Copilot, and regularly review and update security measures based on emerging threats and evolving best practices.

3 Pre-deployment: Reliability and Accuracy

As we all know, even AI technology is not infallible. Mitigating the reliability and accuracy risks associated with Copilot for Microsoft 365 is crucial to ensuring the tool enhances productivity while maintaining the integrity and quality of outputs.

Output Validation and Quality Assurance
Despite Copilot's advanced capabilities, its suggestions and outputs may contain errors or inconsistencies. To combat this, you must implement rigorous validation processes and quality checks to ensure accuracy and reliability. This may involve manual reviews, peer-checking, or automated validation mechanisms tailored to specific use cases.

Algorithmic Bias and Fairness Monitoring
Like many AI models, Copilot may exhibit biases based on its training data. As such, robust bias testing and monitoring mechanisms should be implemented to ensure fairness and non-discrimination in Copilot's outputs and decision-making processes. Furthermore, regular audits and assessments will be required to clock potential biases and take corrective actions to mitigate any identified issues.

Testing and Pilot Projects
Copilot's integration into existing development workflows, tools, and processes may require adjustment and optimisation, so it's important to assess the impact and develop strategies to seamlessly integrate the tool into established practices. A great way to do this is to conduct pilot projects with select user groups to gather valuable feedback, identify potential challenges and even spot opportunities for process optimisation before a broader rollout. Users should also be encouraged to identify and document best practices, known issues, and workarounds related to Copilot's reliability and accuracy.

Ensuring Copilot for Microsoft 365 enhances productivity while maintaining the integrity and quality of outputs is more than achievable, but keep in mind that regular reviews, updates, and adaptations will be necessary as the tool evolves and new use cases emerge.

4 Pre-deployment: Ethical and Legal

The era of AI has brought with it a new type of regulatory risk that many organisations have never faced before. And while ethics may seem outside the remit of most IT teams, it's a very real concern when ensuring responsible and compliant adoption of this AI-powered tool.

Ethical Governance Framework
When it comes to AI, clear governance is key. Establish an ethical governance framework that involves diverse stakeholders, including business ethics leaders, legal experts, and user representatives. This group of individuals should guide the responsible development, deployment, and monitoring of Copilot within the organisation, addressing potential ethical concerns and ensuring alignment with organisational values and principles.

Intellectual Property and Attribution
Copilot's generated content may inadvertently incorporate third-party content, raising concerns about intellectual property rights and licensing violations. To combat this, it's crucial to establish clear policies and guidelines for content review, attribution, and intellectual property rights to avoid potential legal issues or licensing violations.

Collaboration and Knowledge Sharing
While Copilot can enhance productivity, it's important to acknowledge the risk of overreliance on the tool, which may lead to complacency or a lack of understanding of the underlying subject matter. As such, training programs are important to foster collaboration and knowledge sharing among teams and users beyond AI outputs.

Clear Communication and Change Management Plan
The way you communicate Copilot's adoption to the workforce is key. Develop a clear communication plan to inform stakeholders about the benefits, impacts, and expectations surrounding the adoption of Copilot, and maintain transparency regarding the tool's capabilities, limitations, and decision-making processes, fostering trust and accountability. Most importantly, you need to establish a structured change management plan that outlines roles, responsibilities, timelines, and milestones for a phased rollout.

5 Post-deployment: Change Management and Adoption

Effective change management and user adoption are critical for successful AI implementation within organisations. Failure to manage this change effectively can lead to underutilisation of AI investments, decreased productivity, and missed opportunities for innovation. But thankfully, this facet of the challenge is relatively straightforward to overcome.

Cultural Shift and Resistance
The introduction of Copilot may face resistance from users who are accustomed to more traditional practices. Clear communication, change management strategies, and fostering a culture of continuous learning can help mitigate this risk. Pilot programs can also help by giving hesitant users earlier access to the tool or pre-establishing best practices these users can adopt.

Controlled Rollout and Phased Deployment Consider a phased deployment, initially introducing Copilot in low-risk scenarios or specific use cases. This controlled rollout will allow for iterative improvements and refinements based on real-world feedback and performance data, gradually expanding its usage as reliability and accuracy are validated.

Comprehensive, Ongoing User Training and Support
Copilot may well be many individuals' first experience of interactive AI. As such, it's imperative that you provide comprehensive training programs and resources to equip users with the necessary knowledge and skills to effectively use the tool. Ensure training covers not only the technical aspects but also best practices, limitations, appropriate use cases, and the importance of critical thinking and validation. Education should also emphasise the importance of data privacy and the potential risks associated with misuse or negligence. Above all, ongoing support is necessary to address user questions and concerns and foster a culture of responsible and ethical AI adoption within an organisation.

Continuous Improvement and Adaptation
One of the most valuable things you can do when adopting AI is to encourage open communication channels for users to provide feedback and address any concerns or resistance early on. Alongside this, you should continuously monitor user adoption rates and performance metrics to identify areas for improvement. Adapt and refine this change management strategy as needed, addressing emerging challenges and leveraging best practices from successful adoption experiences.

6 Protection with Purview

Given what you've read about AI (including the information in this document), it may surprise you to learn that Copilot does not in fact hold any inherent security functionality. Instead, Microsoft has taken the approach of leveraging existing Microsoft 365 security features and harnessing the capabilities of Microsoft Purview, their unified data governance solution. Here's what you need to know.

Access Controls and Permissions Management
Copilot for Microsoft 365 incorporates granular access controls and permissions management to ensure that users can only access and interact with data and resources they are authorised to access. Administrators can define and enforce role-based access controls, limiting Copilot's capabilities based on user roles and responsibilities.

Data Encryption
Copilot leverages end-to-end encryption to protect data in transit and at rest. This ensures that any sensitive information processed or generated by Copilot remains secure and inaccessible to unauthorised parties, mitigating the risk of data breaches or interception.

Secure Collaboration and Sharing
Copilot seamlessly integrates with Microsoft's secure collaboration and sharing features, such as Microsoft Teams and SharePoint. This allows users to collaborate and share information securely, with built-in controls for data protection, access management, and compliance.

Threat Protection and Malware Scanning
Microsoft's advanced threat protection and malware scanning capabilities are integrated into Copilot, providing an additional layer of security against potential threats, such as malicious code or attachments.

Audit Logging and Monitoring
Copilot for Microsoft 365 includes comprehensive audit logging and monitoring features, allowing administrators to track user activities, detect potential security incidents, and investigate any anomalies or suspicious behaviour.

Purview

Microsoft Purview is ultimately what provides Copilot's enhanced data protection and governance capabilities. It's a comprehensive data governance solution that helps organisations discover, protect, and govern their data across Microsoft 365 and beyond.

Data Discovery and Classification
Purview enables organisations to discover and classify sensitive data across various data sources, including Microsoft 365 applications, on-premises systems, and cloud platforms. This capability is crucial for ensuring that Copilot only interacts with data that adheres to organisational policies and compliance requirements.

Data Protection and Compliance
Purview provides advanced data protection capabilities, such as automatic labelling, encryption, and access restrictions, based on data classification and organisational policies. This ensures that Copilot's interactions with sensitive data are governed by strict security and compliance measures.

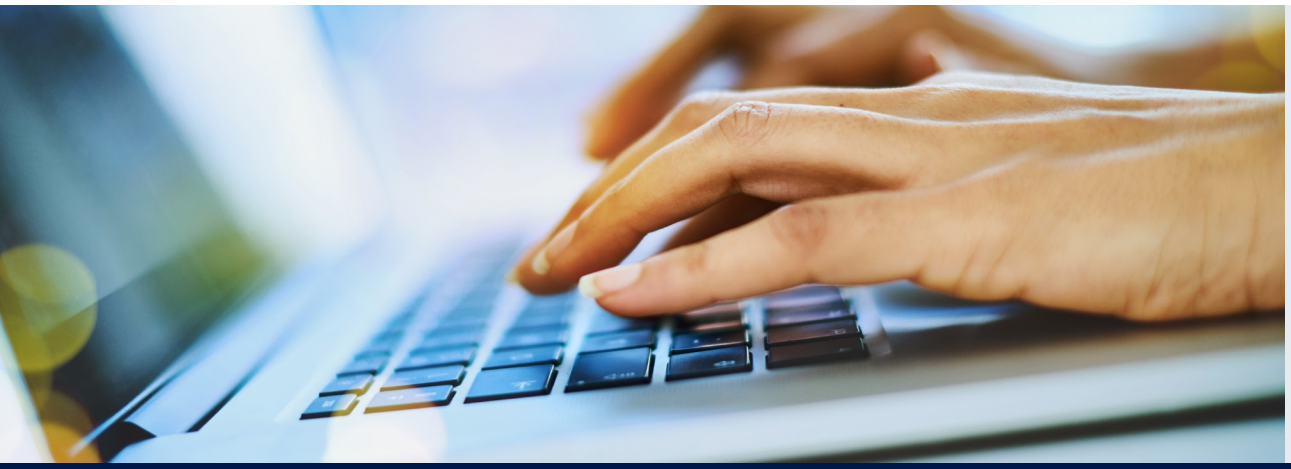
Monitoring and Reporting
Purview offers comprehensive monitoring and reporting features, allowing organisations to track data usage, identify potential risks, and generate compliance reports. This visibility ensures that Copilot's usage aligns with organisational security and compliance standards.

Unified Data Governance
Purview provides a unified data governance platform, enabling organisations to centrally manage and enforce data policies across Microsoft 365 and other connected data sources. This ensures consistent and effective data governance, regardless of where data resides or how Copilot interacts with it.

The essential add-on
The integration of Copilot for Microsoft 365 with Microsoft Purview creates a powerful combination of AI-driven productivity and robust data governance capabilities. By leveraging Purview's data discovery, classification, protection, and compliance features, organizations can confidently embrace Copilot's AI-powered assistance while maintaining stringent data security and compliance standards.

However, it is important to note that security and data governance are ongoing processes that require continuous monitoring, updates, and adaptation to emerging threats and evolving regulatory landscapes.

By embracing the security features of Copilot for Microsoft 365 and the data governance capabilities of Microsoft Purview, organisations can quickly unlock the full potential of AI-driven productivity while maintaining a secure and compliant environment for their sensitive data and operations.



7 A Copilot for Microsoft 365 Risk Management Strategy

Now you're in the know when it comes to AI risks and concerns, here's how your comprehensive risk management strategy should start to shape up:

Conduct a thorough risk assessment
Identify and prioritise potential risks associated with Copilot's deployment, considering your organisation's specific context, industry, and regulatory environment.

Implement robust security measures
Establish strict access controls, data governance policies, and secure coding practices to protect sensitive information and ensure the integrity of the generated code.

Develop clear policies and guidelines
Establish comprehensive policies and guidelines for the responsible and ethical use of Copilot, addressing issues such as intellectual property, accountability, and compliance.

Foster a culture of continuous learning and improvement
Encourage users to continuously improve their skills and knowledge, while also providing ongoing training and support for Copilot's effective utilisation.

Embrace a phased approach
Consider a gradual and phased deployment of Copilot, starting with low-risk scenarios and incrementally expanding its usage based on feedback and performance monitoring.

Collaborate and engage stakeholders
Involve stakeholders from various teams, including development, security, legal, and compliance, to ensure a holistic and well-rounded risk mitigation strategy.

Continuously monitor and adapt
Regularly monitor Copilot's performance, outputs, and potential risks, and be prepared to adapt and refine risk mitigation strategies as needed.

By proactively addressing these risks and implementing appropriate mitigation strategies, you can unlock the full potential of Microsoft Copilot while maintaining a secure, reliable, and ethical development environment.

Embracing a culture of continuous learning, collaboration, and responsible innovation will be key to successfully navigating the challenges and opportunities presented by this groundbreaking technology.

Secure Copilot Success with FluidOne

There's no doubt Copilot is a truly remarkable tool that can transform and enhance the working practices of businesses of all sizes. However, despite media and marketing narratives, it's no out-of-the-box magic wand.

As we've addressed, adoption will require a significant amount of time and planning – not to mention the involvement of a wide range of stakeholders. The all-important data governance piece is also a sizeable task, and the rollout itself will simply not garner user buy-in without specialised training.

At FluidOne, we have extensive experience in helping organisations plan and implement AI projects. As well as conducting a comprehensive Copilot Readiness Assessment that will highlight where your business needs to focus its efforts pre-deployment, we'll also help you with everything from integration to user training, so you can rest assured you're getting the most out of your AI investment.

Book a readiness assessment today, or, for more information, **reach out to our experts**.

FluidOne

5 Hatfields
London SE1 9PG

T 0345 868 7848
contact@fluidone.com

www.fluidone.com