coretelligent

→ Coretelligent Whitepaper

Top 5 Questions Every C-Suite Should Ask About Microsoft Copilot

Exploring the strategic value, risks, and governance of Microsoft 365 Copilot for mid-market leaders in finance, life sciences, AEC, and professional services

Executive Summary

Microsoft 365 Copilot – an AI assistant embedded in Office apps – promises to revolutionize work, but C-suite leaders must approach it with the right questions. This brief addresses the top executive questions about Microsoft Copilot in regulated industries, covering its business value, potential risks, compliance considerations, governance needs, and return on investment (ROI). Mid-market firms in finance, healthcare, engineering, and other sectors can gain productivity and insights from Copilot, **provided they implement it securely and strategically.** We outline five critical questions every executive should ask – from *"What value can Copilot deliver for us?"* to *"How do we ensure compliance and measure ROI?"* – and provide guidance grounded in best practices and industry standards. Each section includes key insights (like Microsoft's security commitments and NIST's AI Risk Management Framework) and practical tips to help leadership evaluate Copilot's fit into their organization.

1. What Value Can Microsoft 365 Copilot Deliver for Our Organization?

Microsoft 365 Copilot's value lies in its ability to **augment knowledge workers** and automate routine tasks, driving efficiency and innovation. It integrates large language models (LLMs) with your business data through Microsoft Graph, meaning it can generate context-rich responses based on your documents, emails, calendars, and chats. For executives, this translates to faster research synthesis, automated report drafting, intelligent email summaries, and insights distilled from data – all within the familiar Microsoft 365 environment. By offloading repetitive work to Copilot, teams can refocus on strategic activities and creative problem-solving. Early studies show substantial productivity gains; for example, one analysis found that workers were **33% more productive per hour when using generative AI assistance.** This boost can level the playing field for mid-market firms, allowing them to compete with larger enterprises by d**oing more with the same resources.**

Copilot's AI capabilities also help democratize expertise. Employees can ask natural-language questions and get instant answers or drafts, which is like having a business analyst or creative assistant on call for everyone. Over time, this can improve decision-making quality and speed. However, to realize these benefits, organizations should identify high-impact use cases (e.g. drafting client proposals, analyzing financial trends, generating project plans) where Copilot saves significant time or improves outcomes. The value is maximized when Copilot is introduced with training and clear objectives, so employees know how to use it effectively rather than as a novelty. **In essence, Copilot's promise is a smarter, more responsive workplace – delivering insights and content in seconds instead of hours.** Leaders should align Copilot with their strategic goals (like accelerating client deliverables or reducing administrative overhead) to ensure its adoption drives tangible business value.

Stat:

Generative AI tools can boost user performance on complex tasks by an average of 66%, with less-skilled workers seeing the greatest improvement. This suggests Copilot can significantly elevate productivity across skill levels.

2. What Risks Should We Consider with Microsoft Copilot (Security, Privacy, Accuracy)?

Any AI that has access to corporate data warrants a thorough examination of its risks. **Data security and privacy** are top of mind – in fact, 75% of customers worry about data security when using generative AI. The good news is that Microsoft designed 365 Copilot with a robust security and compliance architecture. Copilot **does not use your prompts or business data to train the underlying AI model,** and all interactions stay within your Microsoft 365 tenant boundaries. In other words, your proprietary information isn't leaked to OpenAI's public models or the internet. Copilot abides by your existing **identity and access permissions** – it will only surface content a given user already has permission to access. This helps prevent unauthorized data exposure across users. Additionally, Copilot inherits Microsoft 365's enterprise security controls, including data encryption at rest and in transit, as well as tenant isolation to ensure your data remains segregated. Microsoft also deploys content filtering and monitoring to block sensitive or harmful outputs (for example, preventing the AI from revealing confidential info or generating harassment). These built-in safeguards mitigate many traditional AI risks.

However, **executives must still proactively manage the risks associated with Copilot.** One concern is **output accuracy and compliance:** Copilot may sometimes produce incorrect or fabricated information ("AI hallucinations") or content that could be biased. Users should be trained to treat Copilot's output as a draft and verify critical facts, especially in regulated contexts where an error could have legal implications. Another risk is **intellectual property:** if Copilot generates content based on training data, could it inadvertently resemble copyrighted material? Microsoft has addressed this issue with a Copilot Copyright Commitment, pledging to defend customers against IP infringement claims on Copilot outputs, provided that recommended safeguards are in place. To further reduce risk, organizations can configure **Microsoft Purview** data loss prevention (DLP) policies to prevent users from entering ultra-sensitive data into prompts or to monitor Copilot's usage for compliance. It's also wise to disable the optional **Bing web search plugin** in Copilot for sensitive environments, since the same contractual protections don't cover web queries (they are handled under Microsoft's consumer services terms). In summary, while Microsoft 365 Copilot has robust security by design, C-suites should institute **internal usage policies and training** to ensure employees use it responsibly, verify its outputs, and avoid inputting data that shouldn't be in an AI prompt. By pairing Copilot with robust cybersecurity practices (such as those provided by partners in cybersecurity and compliance solutions like Coretelligent) and oversight, organizations can confidently mitigate risk while reaping the benefits of Copilot.

Insight:

"After last year's hype, executives are impatient to see returns on generative AI investments, yet organizations are struggling to prove and realize value," notes Gartner's distinguished VP analyst. This underscores the importance of managing expectations and risks so Copilot deployments deliver sustainable value, not just hype.

3. How Will Copilot Affect Our Compliance Obligations (HIPAA, GDPR, SOX, etc.)?

For regulated industries, any new technology must be vetted against a web of data regulations and standards. **The reassuring news is that Microsoft 365 Copilot is built on Microsoft's existing compliance framework and inherits its commitments.** Microsoft acts as a data processor for Copilot under your organization's existing Microsoft 365 Data Protection Addendum and Product Terms. In practice, this means Copilot comes under the same compliance umbrella as the rest of M365. For example, Copilot (including its chat interactions) is covered by Microsoft's HIPAA Business Associate Agreement (BAA) when properly configured. Because Microsoft 365 is already certified for standards like ISO 27001, SOC 2, and offers **GDPR compliance,** Copilot does not introduce a new compliance gap – it adheres to the same controls. Microsoft explicitly supports GDPR and regional data boundaries with Copilot, and as of 2024 has included Copilot in its EU Data Boundary commitments for European customers. Likewise, for FINRA or SOX in finance, or 21 CFR Part 11 in life sciences, the key is that Copilot data (prompts and outputs) can be retained and audited just like emails or documents. Copilot usage logs (the prompts users enter and content it generates) are available for eDiscovery and audit via Microsoft Purview's Content Search and retention policies. This auditability is crucial for demonstrating compliance and investigating any incidents of improper use.

That said, **executives must ensure Copilot is used in a compliant manner.** "Covered" by a BAA does not mean one can ignore privacy rules – you must still configure and use Copilot in line with regulations. For healthcare (HIPAA), for instance, you should train users not to include Protected Health Information in prompts unless your instance is configured correctly and access-controlled. Microsoft notes that if users employ the web search feature, those queries fall outside the BAA scope; therefore, healthcare organizations may disable web search to maintain all data under HIPAA protections. Financial firms should consider how Copilot might generate content related to financial reports or client data – outputs may need review to ensure they don't unintentionally violate disclosure rules or record-keeping requirements. Sensitivity labels in Microsoft Purview play a big role here: Copilot respects **sensitivity labels** on data and will **not return content the user isn't allowed to access or that's labeled highly confidential.** If a document is encrypted and labeled (e.g. "Secret – Finance Department Only"), Copilot will not surface it to an unauthorized user or to any user without the decryption right. By leveraging tools like Purview's Information Protection, DLP, and retention, companies can ensure that Copilot operates within the bounds of their compliance policies.

It's also wise to update your **governance documents** (such as privacy policies and employee IT use policies) to cover generative AI usage explicitly. Regulators and auditors will expect that you've assessed Copilot's impact on things like data privacy, accuracy of records, and intellectual property. Documenting that Copilot is part of your secure, compliant IT ecosystem – and that you have controls (such as monitoring, training, and human oversight) in place – will be crucial for passing audits in highly regulated sectors. Partnering with a compliance-focused IT provider (like Coretelligent's compliance solutions) can help in mapping Copilot's capabilities to specific regulatory requirements and implementing any needed compensating controls. Overall, with due diligence, companies can deploy Copilot **while fulfilling requirements of HIPAA, GDPR, SOX, and other laws,** since Microsoft 365 Copilot "adheres to all existing privacy, security, and compliance commitments to Microsoft 365 customers". Compliance isn't a blocker to Copilot – it's an operating condition that must be managed.

Stat:

Non-compliance comes at a cost – data breaches where regulatory compliance failures are a factor incur an average of **$220,000 in additional costs.** This underscores why implementing Copilot with proper compliance controls (to avoid regulatory violations) is financially prudent in addition to being a legal requirement.

4. What Governance and Oversight Do We Need for Copilot (Policies, NIST AI RMF, etc.)?

Adopting generative AI at an enterprise level calls for strong **governance.** Executives should treat Microsoft Copilot not as a simple software install, but as a new capability that needs policies, oversight, and cross-functional management. A starting point is to establish an internal **AI governance committee or working group,** involving stakeholders from IT, security, compliance, legal, and business units, to define how Copilot will be used and monitored. This group can develop an **acceptable use policy for AI:** for example, outlining what types of content are approved for Copilot-generated output and what data should never be input into Copilot. Clear guidelines help employees use Copilot responsibly (e.g., "Do not paste client-identifiable data into Copilot prompts unless the dataset is approved" or "A human must review Copilot suggestions before external release"). Many organizations are extending their existing data governance and IT policies to cover AI systems in this way. Training and communication from leadership are key so that end-users understand Copilot is a tool to assist, not replace, their judgment. Leaders might also designate "Copilot champions" or power users in each department to gather feedback and ensure they're delivering value in an ethical and effective manner.

In terms of frameworks, aligning with established **AI risk management guidelines** will strengthen governance. The NIST AI Risk Management Framework (AI RMF 1.0), released in 2023, provides a solid foundation. It encourages organizations to govern AI across four functions: Govern, Map, Measure, and Manage. In practice, this means: **Govern** – have structures and policies in place (e.g., an AI policy and accountability for Copilot oversight); **Map** – identify the context and potential harms of Copilot (what decisions or processes is it involved in, and what could go wrong?); **Measure** – analyze and monitor Copilot's performance and risk (track error rates, user feedback, any incidents of misuse or policy violation); **Manage** – take action to mitigate risks (for instance, refining policies, adjusting Copilot's access, or providing additional training where issues are found). Executives should ask for regular reports on Copilot usage and outcomes. Microsoft Purview's new AI monitoring capabilities (Data Security Posture Management for AI) can provide dashboards on how Copilot and other AI apps are being used in the tenant. These insights aid in governance decisions, such as identifying when someone attempts to feed unusually large amounts of sensitive data or when Copilot is underutilized in a department.

Crucially, governance isn't just internal; **external accountability** is emerging. Regulators are increasingly interested in AI oversight. Gartner predicts that by 2026, 40% of boards will require organizations to have formal AI risk management processes in place. Already, generative AI failures are common: Gartner research has found that **at least 30% of generative AI projects will be abandoned by the end of 2025** due to issues such as poor data quality or a lack of risk controls. Good governance can prevent your Copilot initiative from becoming part of that statistic. Consider conducting an **AI risk assessment** before full deployment – evaluating Copilot's potential impact on privacy, cybersecurity, and ethical considerations (e.g., avoiding biased outputs) – and document the results. This is where engaging outside expertise can help. An **outsourced Chief Information Security Officer (CISO)** or AI risk consultant (such as Coretelligent's Outsourced CISO services) can provide guidance aligned with industry best practices and frameworks like NIST, ensuring no blind spots in your Copilot governance. They can assist in creating governance playbooks and incident response plans specific to AI (e.g., what if Copilot inadvertently generates sensitive info or inappropriate content – how will it be handled?).

In summary, executives should ensure **Copilot governance is an ongoing, dynamic process,** not a one-time checklist. Set the tone at the top that Copilot will be rolled out responsibly, with adequate oversight and adjustments as needed. With strong governance, you can confidently scale Copilot's use cases, knowing that risks are managed and the technology's usage stays aligned to your business values and regulatory obligations.

> NIST's guidance for generative AI (July 2024) identifies *12 specific risk areas and over 200 recommended actions* for managing AI risks. This highlights that a comprehensive approach – covering everything from data quality to transparency – is needed when governing tools like Copilot. Executives should familiarize themselves with such guidelines as part of their AI strategy.

5. What Is the Expected ROI and How Do We Measure Success with Copilot?

When considering an investment in Microsoft 365 Copilot, C-suite leaders will ask: Does it justify the cost? To answer that, it's critical to define **return on investment (ROI)** in both quantitative and qualitative terms. Microsoft 365 Copilot is a premium add-on; while exact pricing depends on licensing agreements, organizations must budget for per-user Copilot fees and potentially additional compute resources. However, early indicators suggest the ROI can be compelling. A recent IDC study (sponsored by Microsoft) found that companies are realizing an **average of $3.7 in returns for every $1 invested in generative AI** initiatives. In specific industries, such as financial services, the returns can be even higher (over four times, according to the study). These returns stem from multiple sources, including increased employee productivity, faster project delivery, automation of tasks that reduce labor costs, and even enhanced revenue due to improved client service or increased innovation speed. For instance, if Copilot enables your analysts to complete reporting in half the time, they can spend the freed hours on value-added analysis or serving more clients, directly impacting the bottom line.

Measuring Copilot's success requires setting clear KPIs (Key Performance Indicators) upfront. Executives should ask their teams to establish baseline metrics before Copilot deployment – for example, the average time to create a specific report or the number of support tickets resolved per agent per day – and then track those after Copilot is introduced. Possible success metrics include a reduction in time spent on content creation, improvement in response times to internal or customer inquiries, the number of tasks automated by Copilot, employee satisfaction or engagement scores (as mundane work is lifted from them), and error rates in outputs (hopefully decreasing as Copilot reduces manual mistakes). It can also be beneficial to run a **pilot program** with a small group of users and measure the results in a controlled manner. For example, one team uses Copilot for a month while a control group doesn't, and compares outcomes, like how one might A/B test a new process. Beyond efficiency metrics, don't overlook the **strategic ROI:** Copilot might enable capabilities that were previously infeasible. Perhaps your firm can take on more projects without increasing headcount or deliver analyses to clients that differentiate your services. These competitive advantages translate to ROI even if they're harder to measure in dollars immediately. Gartner's research noted that among early adopters of generative AI, around 22–23% saw noticeable productivity improvements or cost reductions so far, meaning a majority have yet to fully realize gains, often due to not integrating AI effectively. The lesson is that ROI won't magically materialize; it comes from thoughtful implementation targeting the correct problems.

To maximize ROI, treat Copilot deployment as a strategic initiative: invest in training employees to utilize it effectively (an underused Copilot yields no ROI), iterate on use cases that show promise, and collect feedback. Engage financial controllers to track realized savings or output gains attributable to Copilot. Also, consider the **opportunity cost** of not using AI – if competitors adopt Copilot and gain a speed advantage, the relative ROI of your own adoption might include *staying competitive*. Finally, include risk-adjusted factors in your ROI analysis: effective use of Copilot might reduce compliance costs or cyber risks (e.g. by avoiding shadow AI tools and keeping everything within a governed platform), which is an indirect financial benefit. Many mid-market firms partner with providers like Coretelligent to monitor these benefits; for example, leveraging Coretelligent's cybersecurity and IT **analytics solutions** to continuously measure performance improvements and ensure that the anticipated ROI is being captured. In summary, **ask not just "What's the ROI?" but "How will we know if Copilot is successful?"** Define success criteria (time savings, cost savings, new capabilities, risk mitigation) and regularly report on them. With a data-driven approach, the C-suite can demonstrate whether Copilot is delivering value and adjust strategy accordingly – scaling up usage where it works and refining or retraining where it doesn't.

Stat:

A Microsoft-sponsored IDC survey of over 4,500 business leaders reported that **72% of companies using generative AI are already experiencing significant productivity increases,** and business leaders plan to reinvest those efficiency gains into growth. The expectation of multi-fold ROI is driving rapid adoption, but measuring those gains concretely will validate the investment to stakeholders.

Conclusion & Next Steps

Microsoft 365 Copilot represents a breakthrough in how mid-market firms can leverage AI for productivity, but realizing its potential requires asking the right executive questions upfront. By examining Copilot's value proposition, assessing security and compliance risks, establishing strong governance, and defining ROI metrics, C-suite leaders can make an informed decision about adoption. The common theme across these five questions is **due diligence:** successful Copilot implementation isn't just an IT project; it's a strategic business initiative that touches culture, process, and policy. Leaders in finance, life sciences, AEC, professional services, and other regulated sectors must ensure Copilot is introduced in a way that **upholds trust with customers, regulators, and employees** while unlocking new efficiencies and insights. This means leveraging trusted frameworks (such as NIST's AI RMF for risk management) and tools (like Microsoft Purview for data protection), and potentially augmenting internal capabilities with external expertise.

As you transition from the awareness stage to piloting or deploying Copilot, consider engaging partners who have a deep understanding of both AI technology and industry regulations. **Coretelligent,** for example, offers **cybersecurity & compliance solutions** tailored to help organizations safely embrace innovations like Copilot. Our team can assist with readiness assessments, policy development, user training, and ongoing management to ensure your Copilot deployment aligns with best practices and your business goals. The opportunity is significant – from boosting productivity to enhancing decision-making – but it must be pursued with a clear strategy and oversight. By asking the executive questions outlined in this brief, you position your organization to adopt Microsoft 365 Copilot in a secure, compliant, and value-generating manner. The result can be a smarter workforce and a competitive edge in your market. In the era of AI-powered productivity, those who lead with both enthusiasm and prudence will achieve the best outcomes.

Secure Your Integration Today

Email:
info@coretelligent.com

Schedule a Discovery Call:
https://coretelligent.com/contact

Call:
855.841.5888