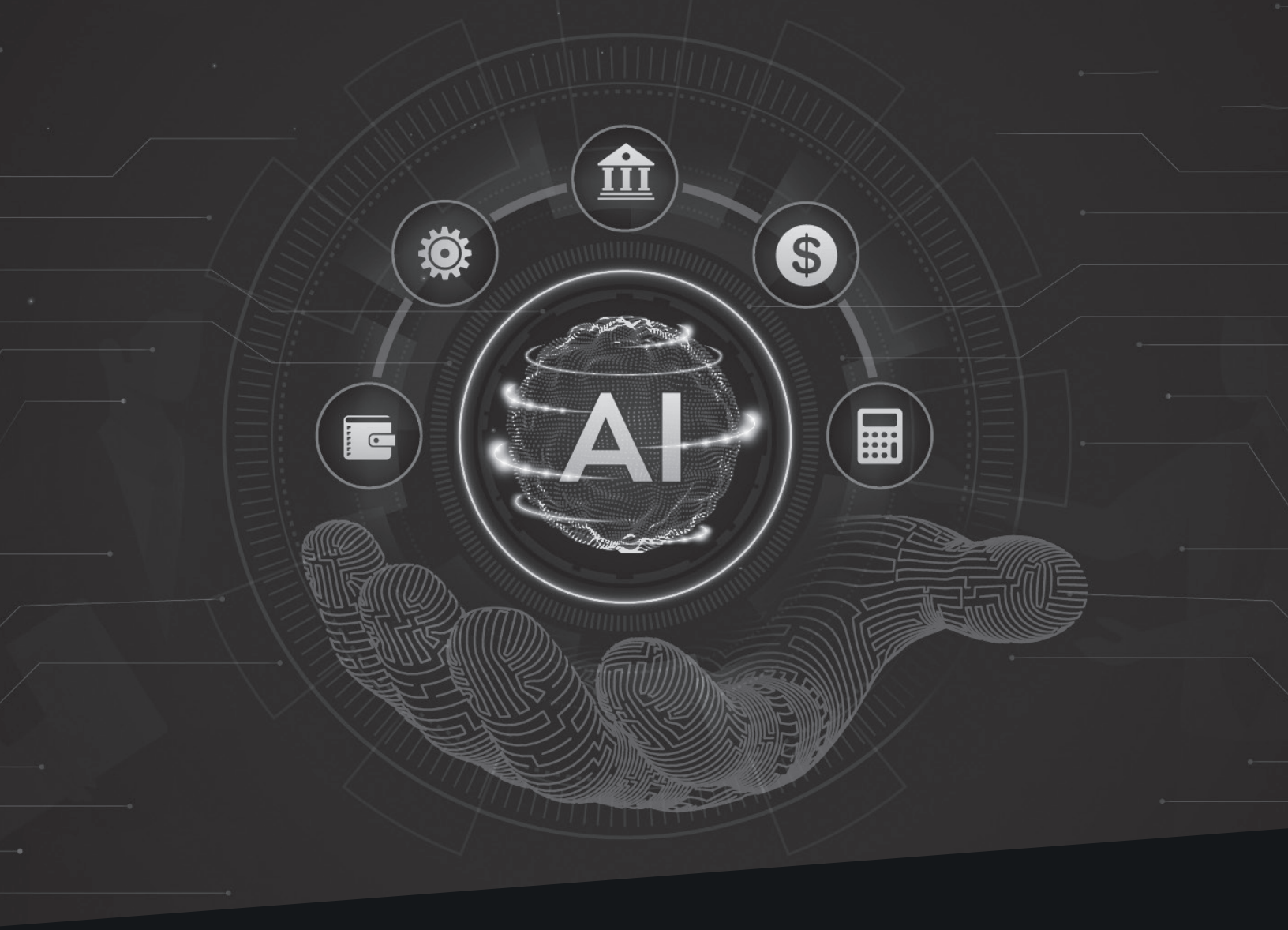


coretelligent

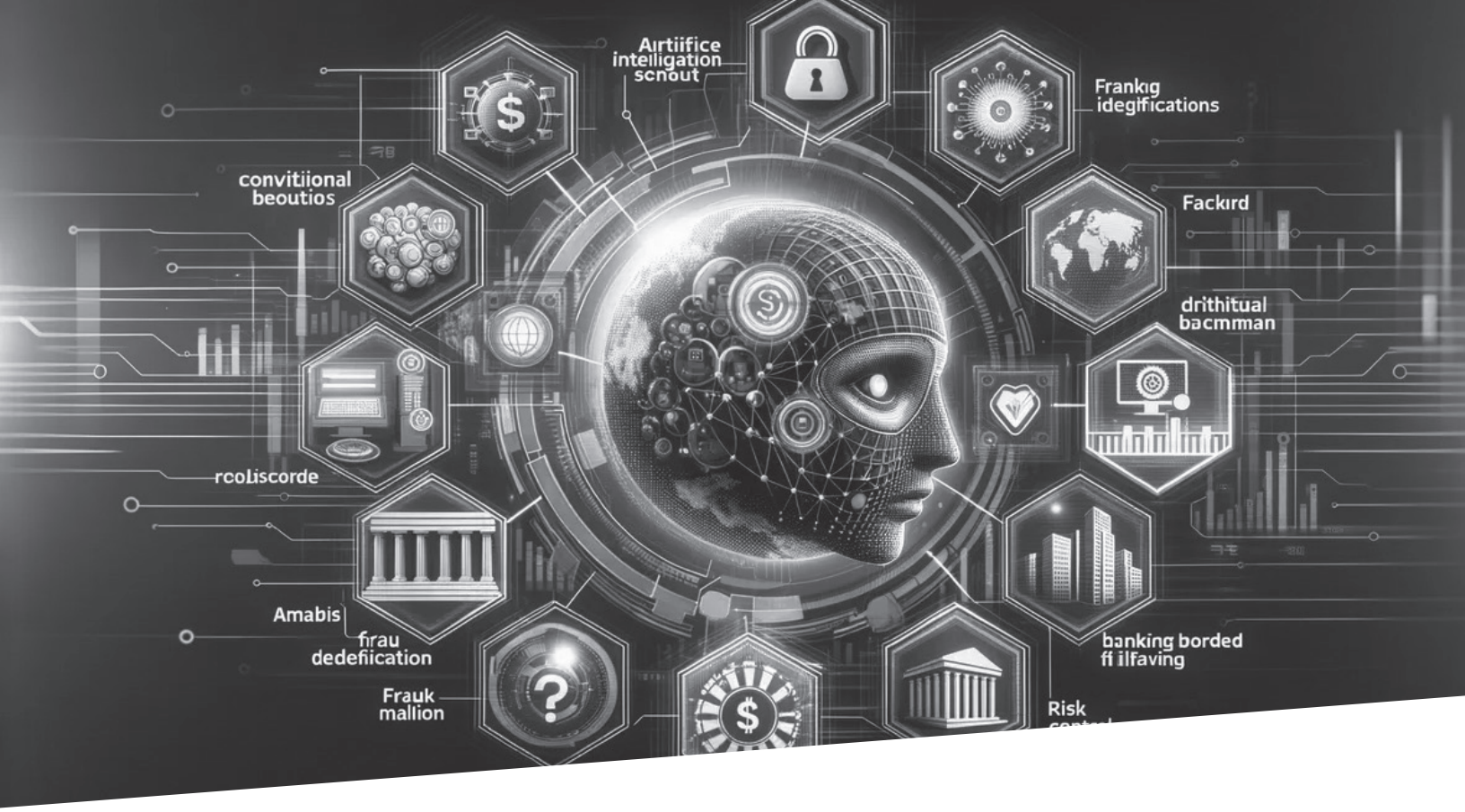
→ Coretelligent Whitepaper

Managing AI Financial and Cyber Risk: A CFO's Guide

Balancing Innovation with Governance in the Era of AI Automation

CFOs in mid-market, regulated industries face a dual imperative with generative AI: harness productivity gains while rigorously managing financial and cyber risks. This guide provides strategic insights for **AI risk management,** focusing on the adoption of Microsoft 365 Copilot for CFOs. It covers budgeting and ROI considerations, operational and data security risks, information protection with Microsoft Purview, compliance with regulations (SOX, SEC disclosure, GLBA, GDPR), incident response preparedness, and oversight of third-party risks. With an analytical and actionable tone, the guide provides **strategic recommendations** and highlights stats, expert quotes, and best practices to help CFOs govern AI initiatives responsibly and confidently.

A CFO interacts with an AI chatbot interface, symbolizing the integration of Microsoft 365 Copilot into financial workflows.



The CFO's AI Risk Landscape

Artificial intelligence (AI) is rapidly becoming a cornerstone of business strategy, and finance leaders are taking notice. In a 2024 Gartner survey, 58% of finance teams reported using AI, representing a 21% point increase from the previous year. Moreover, 66% of CFOs are more optimistic about the value of AI than they were a year ago. This optimism stems from AI's potential to automate processes and uncover insights, with nearly half of companies viewing AI as a top growth enabler. At the same time, CFOs recognize that **AI adoption must be paired with robust risk management.** KPMG notes that while private companies are "laser-focused" on AI, they "must be mindful of risks, governance, and talent". CFOs, as stewards of financial integrity and enterprise risk, are uniquely positioned to ensure that AI initiatives, such as Microsoft 365 Copilot, drive value **without** exposing the firm to undue cyber or financial risk. This requires an executive-level focus on governance, aligning AI projects with compliance requirements and organizational risk appetite. **In short, CFOs must champion AI innovation with a strong framework for risk oversight,** setting the tone that productivity gains will not come at the expense of security, compliance, or financial control.

From establishing AI-use policies to participating in cross-functional AI governance committees, CFOs are evolving into key influencers of digital risk. The sections that follow provide a comprehensive look at how CFOs can evaluate Microsoft 365 Copilot through a risk-aware lens, covering budget strategy, data protection via Microsoft Purview, regulatory compliance, incident readiness, vendor management, and more, to **maximize AI-driven returns while minimizing exposure.**

72%

of business leaders see significant opportunities in AI, yet 58% also foresee notable challenges, underscoring the need for balanced governance.

Budgeting for AI: Balancing Investment and ROI

While generative AI promises efficiency and competitive advantage, CFOs are approaching spending with caution. Close to two-thirds (62%) of CFOs plan to allocate **less than 1%** of their organization's budget to generative AI in the following year. Another 37% expect only a **1–10%** share, reflecting a "modest" investment approach. This caution is driven by uncertainty in measuring AI's tangible business value and the desire to see proven results before scaling up. **As both strategist and steward, the CFO must ensure AI investments are prudent** and tied to clear outcomes. For Microsoft 365 Copilot, this means piloting use cases with a measurable return on investment (ROI), such as time saved in financial reporting or improvements in forecasting accuracy. Notably, 70% of finance chiefs anticipate a productivity boost of at least 1–10% from GenAI, yet many are still determining the right metrics to gauge success. Standard measures include workforce productivity gains (cited by 40% of CFOs), cost savings (29%), and ROI/growth indicators.

A finance executive reviews budget allocations for AI initiatives, with a focus on cost management and return on investment (ROI).

62%
of CFOs anticipate investing under 1% of budgets in GenAI, preferring a cautious "test-and-learn" approach.

Budgeting recommendations:

Treat AI expenditures as strategic investments with defined key performance indicators (KPIs). Develop a financial model to compare Copilot's expected benefits (e.g., reduced manual effort in creating reports or analyzing data) with its costs (licenses, training, and governance overhead). Consider establishing an "AI innovation fund" that allocates a small percentage of the IT or R&D budget to pilot projects, with further funding contingent upon meeting milestones. Also account for hidden costs, such as integration, change management, and risk mitigation tools (like additional security or compliance controls). **Microsoft 365 E5 Compliance licensing (part of Microsoft Purview)** may be an accompanying investment to ensure Copilot's deployment remains within compliance boundaries. By budgeting for AI holistically – including both the **enablement costs and the risk management costs** – CFOs can ensure they aren't blindsided by compliance expenses or security remediations later. This proactive financial planning ultimately helps validate AI's ROI, giving the board and stakeholders confidence that AI-driven productivity gains justify the investment and are achieved within a controlled risk profile.

AI Operational Risks and Data Security

Adopting Microsoft 365 Copilot introduces **operational risks** that CFOs must consider when developing their risk management strategy. One key concern is the **oversharing or leakage of sensitive information**. Copilot works by accessing organizational data (emails, documents, chats) to generate responses, which can inadvertently expose data if permissions are misconfigured. For example, if a SharePoint site's permissions are too open, Copilot could surface confidential documents to a broader audience. As Microsoft warns, the power and speed of AI can *"amplify the problem and risk of oversharing or leaking data".* CFOs should ensure that **strict access controls and data classification** are in place. Microsoft 365 Copilot honors existing Microsoft 365 permissions and will only surface data that users have at least view access to. Implementing **Microsoft Purview Information Protection sensitivity labels** is a best practice to add an extra layer of control: labeled (and encrypted) documents won't be revealed by Copilot to unauthorized users. Purview's Data Loss Prevention (DLP) policies can also prevent users from inadvertently sharing Copilot-generated content containing sensitive data outside approved channels.

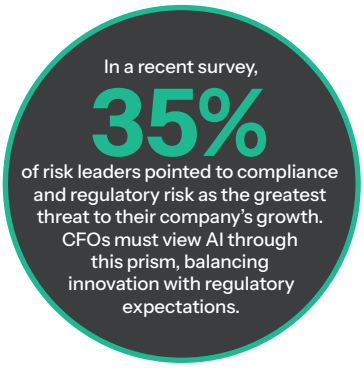
Another operational risk is the **accuracy and misuse of AI output.** Copilot can draft emails, analyses, or code, but it doesn't guarantee factual correctness. There is a risk of "automation complacency," where staff might over-rely on Copilot's output. CFOs should enforce a policy that all AI-generated content (such as financial summaries, forecasts, and client communications) is reviewed by a human for accuracy and compliance **before** external use. Training finance teams on AI literacy—understanding Copilot's strengths and limitations—is crucial to prevent errors from propagating into financial decisions or disclosures.

> If a user account is compromised, an attacker could exploit Copilot's broad access to search and extract confidential data. This underscores the need for multi-factor authentication and monitoring Copilot usage for anomalies.

Microsoft Purview also provides capabilities to mitigate operational AI risks. Its **Insider Risk Management** can detect and alert on risky user activities, such as unusual data access patterns with Copilot (potentially flagging a malicious insider or compromised account). Additionally, Purview's oversight tools for AI can *"identify oversharing risks, protect against data leaks, and help ensure AI usage complies with regulations".* CFOs should collaborate with their CIO/CISO to implement these controls, such as utilizing Purview's dashboards to identify AI usage trends and potential policy violations. By proactively addressing Copilot's operational and data security risks—tightening access permissions, leveraging Purview's protection features, and fostering a culture of human oversight—CFOs can support innovation with confidence that company data and finances remain secure.

Regulatory Compliance: SOX, SEC, GLBA, GDPR, and Beyond

In regulated industries, any deployment of AI like Microsoft 365 Copilot must be navigated through a compliance lens. **Sarbanes-Oxley (SOX)** mandates strict internal controls over financial reporting, which means if Copilot is used to assist in financial statement preparation or analysis, the CFO must ensure those AI-generated contributions are accurate and auditable. Controls should be updated to include verification of Copilot outputs and restriction of its use in final-stage financial reporting without review. CFOs may document how Copilot is utilized in financial processes to demonstrate to auditors that **SOX 404** controls are not compromised by AI assistance.



The **U.S. Securities and Exchange Commission (SEC)** has sharpened its focus on AI-related disclosures and governance. In 2024, the SEC brought its first enforcement actions for *"AI washing"* – penalizing companies for misrepresenting their AI capabilities in investor materials. This serves as a warning: CFOs must ensure any claims made about AI are truthful and substantiated. Existing SEC disclosure rules on risk factors and Management Discussion & Analysis (MD&A) already require that material risks – including those stemming from AI use – be transparently disclosed. **Qualitative factors**, such as algorithmic bias or model errors, can be material to a business and may need to be disclosed in filings. For instance, if Copilot materially aids decision-making, the company may disclose its reliance on AI and associated risks (including data privacy, accuracy, and security) in its 10-K risk factors. Finance chiefs should also brief audit committees and boards on AI deployments, since only ~15% of S&P 500 firms currently disclose board-level AI oversight (a figure expected to rise). The SEC's emphasis on governance means that CFOs should establish internal AI oversight committees and be prepared to demonstrate to regulators that robust governance is in place for AI projects.

For **industry-specific regulations** like the **Gramm-Leach-Bliley Act (GLBA)** in financial services or HIPAA in healthcare, the introduction of Copilot must not violate customer privacy rules. GLBA requires safeguarding customer financial information; thus, CFOs should confirm that Copilot's use of data stays within the firm's secure boundary and that no personally identifiable financial data is exposed in AI outputs. Microsoft affirms that Copilot complies with **GDPR** and won't use customer prompts or content to train its models. Prompts and responses stay within the Microsoft 365 service boundary and aren't sent to public OpenAI services. These are reassuring compliance commitments, but the CFO should still consult legal/compliance officers to update data privacy impact assessments for Copilot's usage, especially if operating in the EU under GDPR. They should leverage tools like **Microsoft Purview Compliance Manager**, which can map Copilot's use to regulatory requirements and track controls to meet GDPR, SEC, SOX, and other frameworks.

Maintaining **audit trails** is another compliance aspect. CFOs should ensure that Copilot's activity (prompts, outputs) is logged for auditability. Microsoft 365's audit logs and eDiscovery tools in Purview can capture AI-generated content and user interactions, which is helpful for both internal review and responding to regulators or legal matters. The **bottom line:** In many cases, regulators haven't issued AI-specific laws, but they expect companies to apply existing laws to AI. CFOs must thus proactively integrate AI into their compliance programs – from updating policies and training (e.g., a code of conduct that includes AI use guidelines) to reporting to the board on AI risk management. By doing so, they turn regulatory compliance into a competitive advantage, using compliance as a driver to build customer and investor trust in their responsible AI adoption.

Incident Readiness and AI Risk Response

No system is foolproof, and CFOs must assume that even well-governed AI deployments can encounter incidents. Microsoft 365 Copilot could be involved in various incident scenarios, including a data breach where sensitive data is leaked via Copilot, a scenario where AI produces defamatory or biased content, or an outage of the Copilot service that disrupts business processes. **Incident readiness** means having a plan that explicitly addresses these AI-driven contingencies as part of the company's broader disaster recovery and business continuity plans. The **cost of not preparing is high**: companies suffer an average of $220,000 in additional breach costs when non-compliance is a factor, for example, if an AI inadvertently causes a privacy breach that violates regulations. CFOs should quantify potential financial impacts of AI-related incidents (fines, legal fees, loss of business) as part of enterprise risk assessments.

A robust **incident response (IR) plan** for AI should include detection capabilities for AI misuse or anomalies, a straightforward process for containing and remediating any data leaks, and communication protocols to inform stakeholders and regulators as needed. Microsoft Purview can assist in detection – for instance, **Defender for Cloud Apps** (part of Purview's suite) can monitor unusual data access patterns, and DLP policies can trigger alerts if Copilot-generated content with sensitive info is shared outside allowed channels. CFOs should ensure that such alerts feed into the security operations center (SOC) for immediate investigation. Additionally**, tabletop exercises** that simulate AI-related incidents (such as a Copilot data leakage scenario or erroneous financial analysis leading to a poor decision) are valuable. These drills, ideally involving finance, IT, legal, and PR teams, help the organization practice its response, from technical containment to public communication.

Preparedness Tip:
Coretelligent's compliance advisory recommends having detailed incident response plans and regular training. Engaging employees with scenario-based exercises (e.g., a ransomware attack or a misuse of Copilot) builds readiness.

CFOs should also clarify **insurance coverage** for cyber incidents – does the cyber insurance policy cover losses from AI-induced incidents or only traditional breaches? This can influence financial contingency planning. Following an incident, the CFO's role is crucial in conducting an economic impact analysis and reassuring investors and customers. By demonstrating that the company had strong controls and responded swiftly (e.g., by showing logs from Purview that pinpoint what data was accessed by Copilot, or by showing how Microsoft's safeguards blocked prompt injection attacks), a CFO can maintain stakeholder trust even in the face of an incident. In summary, being **forewarned and forearmed** for AI-related incidents will reduce their financial impact and downtime. CFOs should champion an incident-ready culture, where deploying Copilot goes hand in hand with "copilot-proofing" the enterprise's response plans for worst-case scenarios.

Third-Party and Vendor Risk Management

Microsoft 365 Copilot, although a Microsoft product, represents a **third-party service** deeply integrated into your enterprise's ecosystem. CFOs need to extend their vendor risk management practices to AI tools, such as Copilot, and any associated plugins or services. A key step is performing due diligence on Microsoft's security and compliance standards for Copilot. Microsoft has made firm commitments – Copilot is compliant with GDPR, HIPAA, and ISO/IEC 27001, and undergoes regular audits. It also runs on **Azure OpenAI within the Microsoft 365 security boundary**, meaning data isn't shared with OpenAI's public services. CFOs should obtain and review documentation, such as Microsoft's **Service Trust reports, SOC 2/Type 2 reports**, or any other relevant certifications related to Copilot. This not only checks the box for vendor compliance but also provides insight into residual risks.

Beyond Microsoft, third-party risk extends to **plugins and other AI vendors**. Copilot can be extended with third-party plugins, which, if enabled, could send organizational data to external providers. Finance leaders should enforce strict policies on which (if any) plugins are allowed, working closely with IT to whitelist only those that have been vetted for security and compliance. As noted by Financial Executives International, investing heavily in third-party AI solutions can "introduce data privacy or IP risks" that must be evaluated. CFOs should mandate that any AI vendor or plugin undergo a comprehensive **risk assessment,** covering how they handle data, their breach history, data residency (necessary for GDPR compliance), and contractual liability in the event of an incident. For instance, what if a plugin misuses data or has a vulnerability? Ensure contracts have provisions for data protection and clarity on liability.

Vendor Insight:
Many companies are forming cross-functional AI governance teams to **track third-party AI risks,** often anchored by legal, finance, and IT departments. This ensures a 360-degree view of vendor impacts on security and compliance.

Integrating **third-party risk management tools** can also aid CFOs. Platforms like Coalition Control (as used in Coretelligent's services) continuously monitor the external cyber hygiene of third parties and can alert if a key vendor shows security weaknesses. CFOs in financial services or life sciences, for example, may require that Microsoft (and any AI vendors) meet specific standards, such as FEDRAMP or HITRUST certification, as applicable. They should also be aware of concentration risk – if your workflows become too dependent on Copilot, any outage or change in terms could pose operational risk. Mitigation can include having alternative processes or ensuring you retain key data and prompts internally as backup.

Treat Copilot as you would a critical outsourcing partner: **trust but verify**. Leverage internal or outsourced compliance experts to review Microsoft's AI compliance documentation. Stay informed on any new Copilot features or incidents (via Microsoft's security advisories). Integrate AI services into the enterprise vendor risk register, assigning risk owners and conducting periodic reviews. By actively managing third-party risk, CFOs ensure that the convenience of AI doesn't create an **Achilles' heel** in the organization's risk posture.

Strategic Recommendations for CFOs

AI adoption, especially via tools like Microsoft 365 Copilot, is as much a **strategy exercise** as it is a technology deployment. CFOs should approach it with a comprehensive plan that aligns with enterprise risk management and business objectives. Here are key strategic recommendations for CFOs to consider:

Governance and Oversight:

Establish an AI governance committee (if one doesn't exist) that includes finance, IT, compliance, and legal. As highlighted in FEI's guidance, many firms are instituting cross-functional teams to oversee AI use cases, policies, and third-party risks. If your board has not yet defined AI oversight, take initiative to brief the audit or risk committee on Copilot plans and how you are managing risks. Aim to be part of the 11–15% of companies with board-level AI oversight, a figure expected to grow as AI becomes ubiquitous. Governance also means defining clear **ownership** of AI risks – e.g., the CIO might own technical risk, but the CFO should own financial and compliance risk aspects, ensuring they're addressed in enterprise risk registers.

Inventory and Assess AI Use:

Conduct an organization-wide inventory of current and proposed AI uses. CFOs should have visibility into where Copilot and other AI tools are used – from finance and accounting (FP&A analysis, report generation) to other departments (marketing content creation, HR analytics). For each use case, perform a **risk materiality assessment:** what could go wrong (e.g., error in output, data leak, non-compliance) and how material would the impact be? This exercise aligns with FEI's advice to evaluate which AI-related risks or dependencies are material to your financials or controls. Focus on high-impact areas first, such as any AI involvement in financial reporting, customer data handling, or decision-making that could affect financial results.

Policy and Controls Framework:

Update or develop policies to guide the use of AI. This includes an **AI Acceptable Use Policy** for employees using Copilot, clarifying what types of data can be input into prompts (e.g., no sensitive personal data) and how outputs should be vetted. Embed AI considerations into existing IT and security policies (data classification, data retention, acceptable software, etc.). Utilize frameworks like the **NIST AI Risk Management Framework,** which emphasizes core functions – govern, map, measure, manage – to ensure AI systems are trustworthy and risks are mitigated. For example, set metrics ("measure") to regularly evaluate Copilot's performance and error rate in finance tasks, and implement controls ("manage") like DLP rules or requiring human sign-off on AI-generated financial content. Map these controls to compliance requirements as needed. Essentially, treat Copilot as a process that requires internal controls, just like any other finance process.

Leverage Technology for Risk Mitigation:

Utilize Microsoft 365's comprehensive security and compliance features to support your risk strategy. **Microsoft Purview** should be configured to its potential – enable sensitivity labels (with encryption) across SharePoint/OneDrive so Copilot can respect them, turn on DLP policies for data categories relevant to GLBA or GDPR, and use Insider Risk Management to catch any anomalous use of AI outputs (like large downloads of AI-generated content or attempts to paste sensitive outputs externally). Additionally, consider third-party solutions or expert services where gaps in your current approach exist. For instance, if you lack in-house expertise to tune these controls continuously, an **outsourced vCISO service** could provide ongoing cybersecurity and compliance leadership. Coretelligent's *CISO as a Service* offering, for example, can help navigate complex regulatory landscapes and facilitate proactive threat mitigation without the need for a full-time hire – an approach that protects both your data and your budget.

Training and Culture:

Invest in training programs to raise AI awareness. Ensure finance teams (and all Copilot end-users) understand how to use Copilot securely – e.g., not to input confidential deal data or unpublished financial results into prompts, and to be alert for unexpected outputs. Training should also cover basic AI literacy, recognizing that Copilot might "sound confident but be wrong," thereby encouraging a verification mindset. Building a culture of **responsible AI use** is perhaps the best defense against both cyber and financial risks. Encourage employees to report any unusual behavior or potential security concerns related to AI (using the same channels as other IT incidents). Recognize that **human factors** often determine security outcomes; well-informed employees are a strong line of defense. According to Coretelligent's compliance services, regular risk assessments and ongoing education are key to reducing vulnerabilities and ensuring that everyone understands their role in protecting data.

Align AI with Business Continuity and Strategy:

Lastly, incorporate AI considerations into strategic planning and budgeting cycles. For continuity, ask "How do we operate if Copilot is unavailable?" – ensure critical functions have a fallback. For strategy, continue to evaluate new AI advancements (e.g., Microsoft's following Copilot features or Security Copilot for cyber defense) in terms of potential ROI and risk trade-offs. By framing AI adoption within the company's broader strategic objectives (growth, efficiency, innovation) and risk tolerance, CFOs can help the organization pursue AI initiatives that genuinely add value. As Deloitte's CFO program leader noted, *"CFOs have a critical role to play to help determine how best to use AI… and with the appropriate guardrails in place."*. In practice, this means the CFO should be the voice ensuring those guardrails (financial controls, compliance checks, security measures) keep pace with the enthusiasm for AI-driven growth.

By following these strategic steps, CFOs will not only mitigate the financial and cybersecurity risks associated with Microsoft 365 Copilot but also set the stage for sustainable innovation. With prudent oversight, budgeting, and alignment to compliance, **AI can become a driver of competitive advantage rather than a source of uncertainty.** Remember that managing "AI financial and cyber risk" is an ongoing journey – as AI evolves, so must the CFO's playbook for governance. This guide provides the foundation for that journey, empowering CFOs to lead with confidence in the age of intelligent automation.

CFO Quote :

"As both stewards and strategists, CFOs have a critical role to play to help their companies determine how best to use AI... and with the appropriate guardrails in place."

Next Steps

For further guidance, explore Coretelligent's resources on cybersecurity and compliance (e.g., our **Cybersecurity & Compliance Solutions and IT Compliance Management** offerings) to see how expert partners can augment your AI risk management efforts. With the right strategy and support, CFOs can safely navigate the AI revolution, unlock value while protecting the enterprise's financial integrity and trust.

Secure Your Integration Today

Email:
info@coretelligent.com

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

Call:
855.841.5888