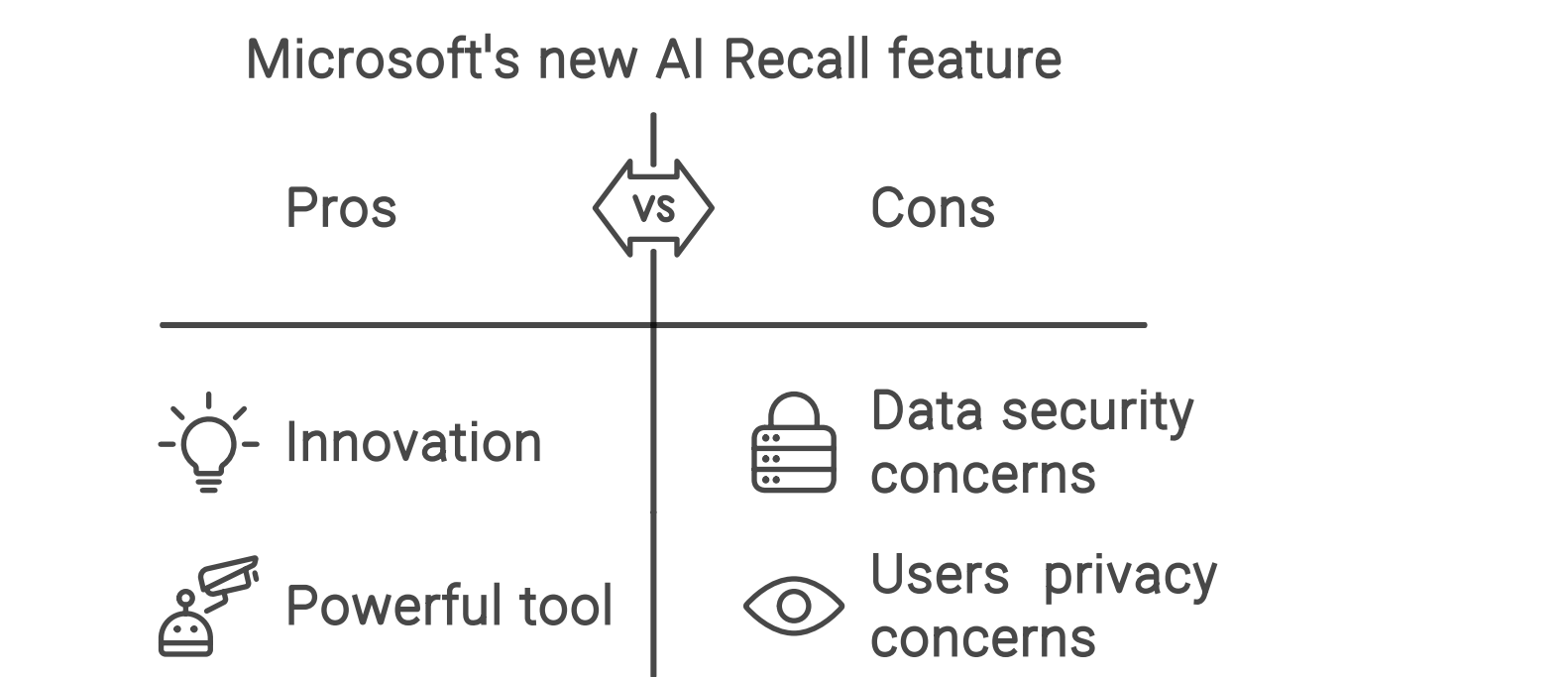# Unpacking Microsoft's New AI Recall Feature: A Must-Know for Internal Audit!

By Sanjay Vadlamani (CISA & CISM) and Scott Madenburg (CIA, CISA, CRMA)

Microsoft has once again pushed the boundaries of innovation with its new AI Recall feature. But with great power comes great responsibility—something that raises its head when it comes to data security and users' privacy. This new tool, set to be included on Copilot+ PCs, has sparked quite a stir in the tech world. But what does it mean for internal audit? Let's unpack it together.

Microsoft's new AI Recall feature

| Pros | vs | Cons |
|------|-----|------|
| Innovation | | Data security concerns |
| Powerful tool | | Users privacy concerns |

What is Recall? It's not that movie starring Arnold Schwarzenegger, where he travels to Mars to recover memories from his past, but it's not too far off. Microsoft's Recall will capture screenshots of its consumers' machines every few seconds to enable users to locate information they viewed on their device. While Microsoft assures users strong protection against accidental leakage of sensitive information or unauthorized access to it, some complain that this may result in a "privacy disaster".

For organizations considering using Recall, it's crucial to implement robust access controls and advanced encryption protocols. Regular privacy impact assessments are also a must to ensure compliance with data protection regulations.

Data Protection
- Access Controls
- Encryption Protocols
- Privacy Impact Assessments
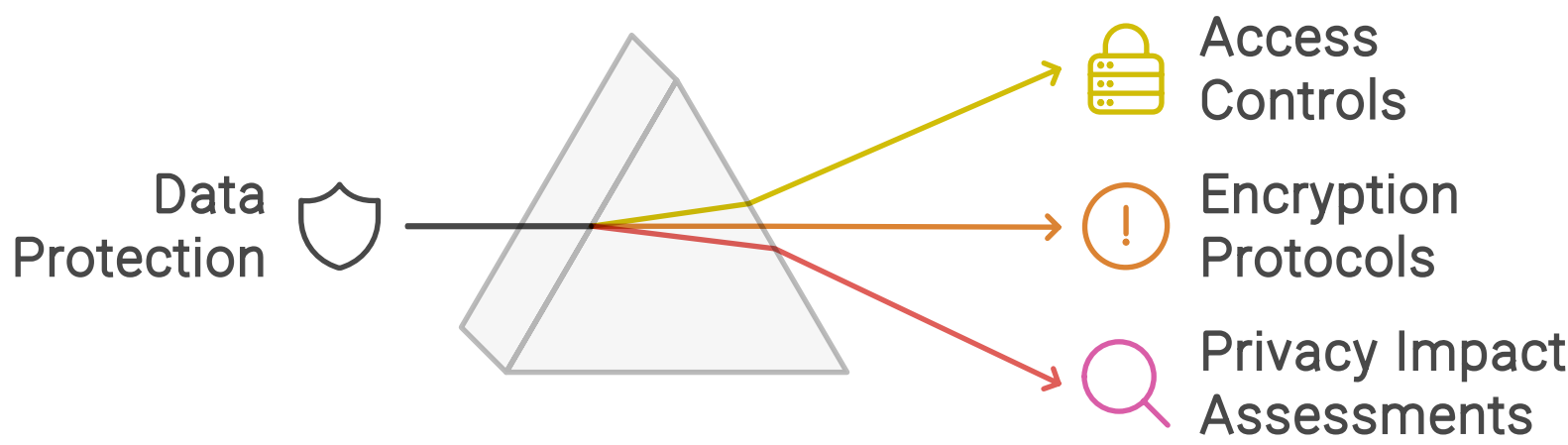
But who will be responsible for ensuring that these measures are effectively implemented and adhered to? Enter the unsung heroes of the corporate world—Internal Audit. These individuals play a crucial role in evaluating the effectiveness of data protection controls within an organization.

As an internal audit professional, your role is more critical than ever. Internal audit must not only assess the technological safeguards put in place but also ensure that legal and regulatory requirements are being met. With Microsoft's Recall feature serving as a wake-up call for the importance of data security, internal audit professionals must step up to the plate and ensure that their organizations are adequately protected.

But how?
- Stay informed about the latest AI developments and adapt audit methodologies to address emerging risks effectively.
- Collaborate across IT, legal, and compliance teams to navigate the complex landscape, especially in areas that are highly regulated.
- Implement proactive risk management strategies to ensure AI tools do not compromise user privacy or lead to data compliance issues.

**Collaboration Across Teams**
- IT Teams
- Legal Teams
- Compliance Teams

**Internal Audit Professional**

**Proactive Risk Management**
- Risk Strategies
- User Privacy
- Data Compliance

**Adapting Audit Methodologies**
- Latest AI Developments
- Emerging Risks
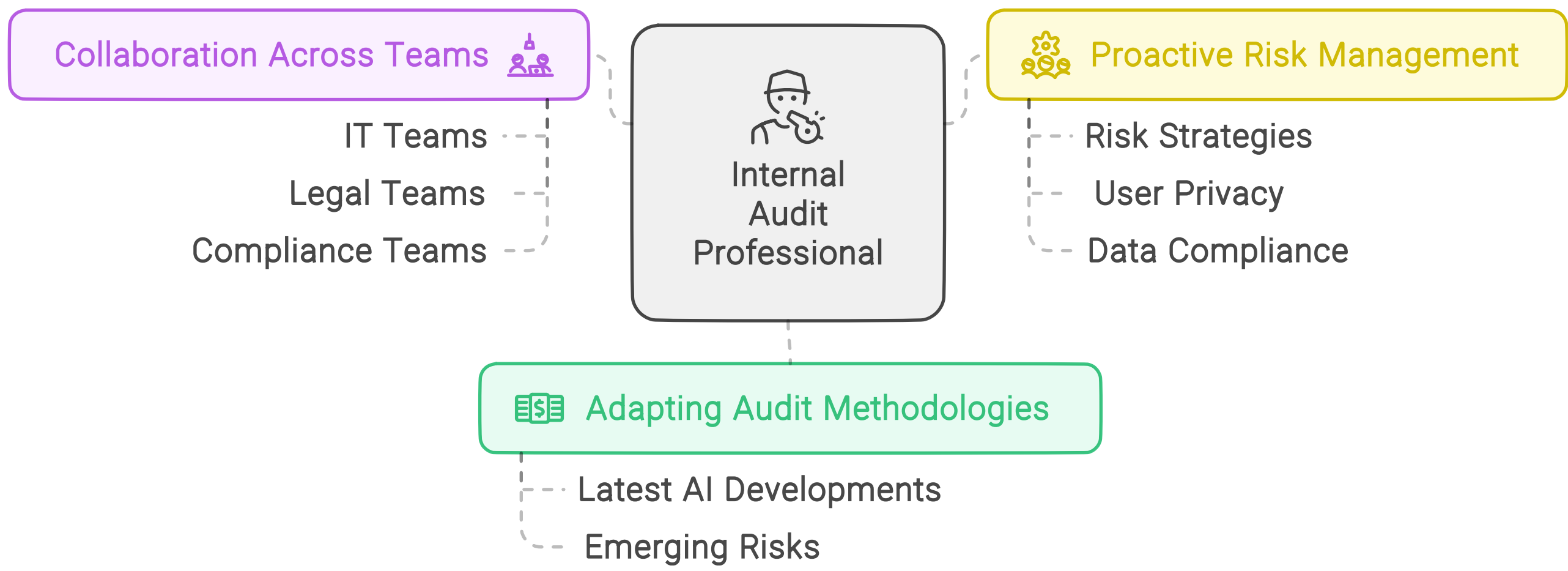
Microsoft's Recall feature may be a game-changer in terms of user convenience, but it also serves as a stark reminder of the need for robust data protection measures. Internal audit professionals have a key role to play in ensuring that organizations are equipped to handle the privacy and security challenges posed by this new technology. It's time to take action and make data security a top priority.

## Continuous Improvement in Data Security

- Make Data Security a Top Priority
- Implement Microsoft's Recall
- Highlight Data Protection Needs
- Involve Internal Audit Professionals
- Address Privacy and Security Challenges