

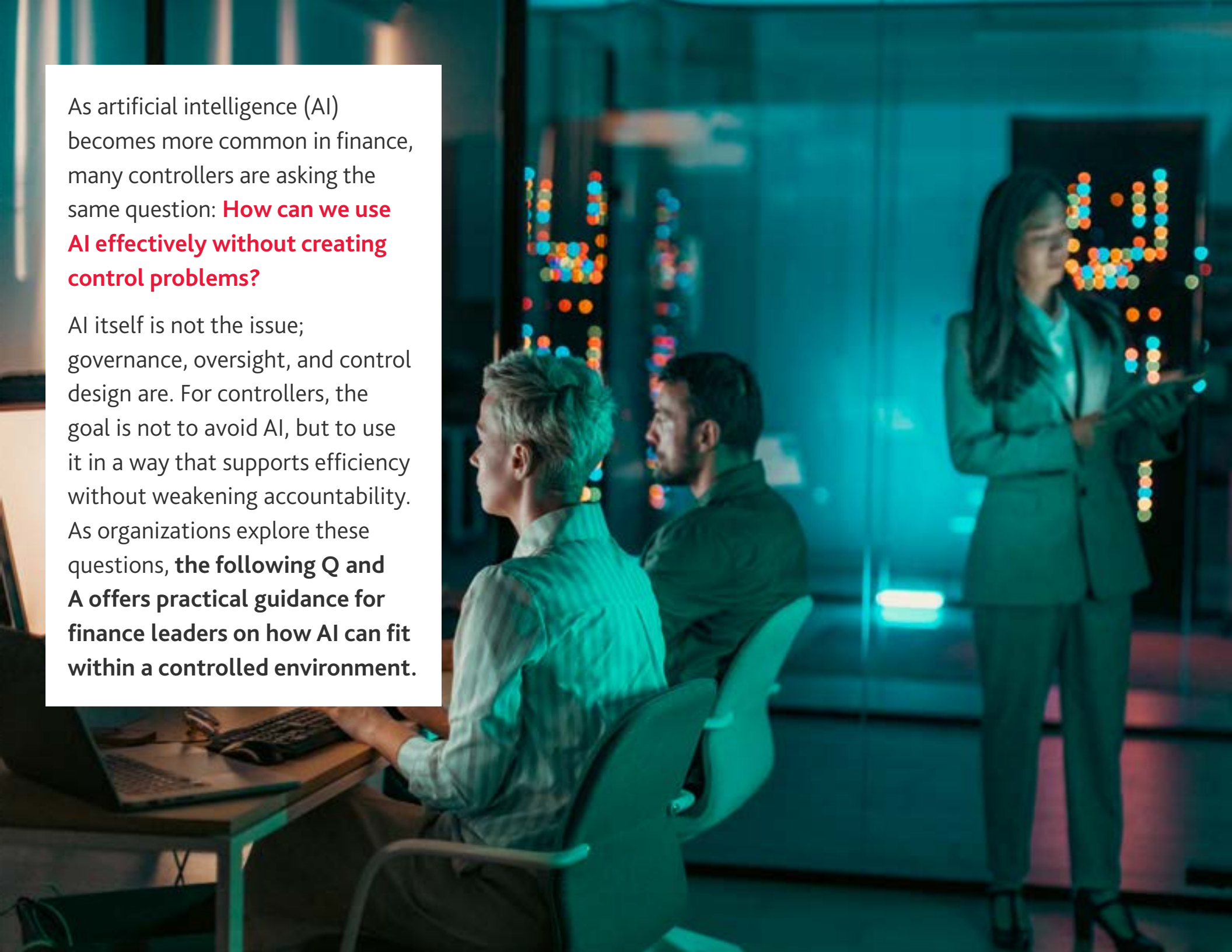
A woman with dark hair, wearing a grey blazer over a white shirt, is seated at a desk in a dimly lit office. She is looking down at a laptop. In the background, other people are working at computers, and the office is illuminated by blue and green ambient lighting. The overall atmosphere is professional and focused.

Reviewing AI in Finance Processes

Practical Audit Considerations for Controllers

As artificial intelligence (AI) becomes more common in finance, many controllers are asking the same question: **How can we use AI effectively without creating control problems?**

AI itself is not the issue; governance, oversight, and control design are. For controllers, the goal is not to avoid AI, but to use it in a way that supports efficiency without weakening accountability. As organizations explore these questions, **the following Q and A offers practical guidance for finance leaders on how AI can fit within a controlled environment.**





**We're starting to use AI in finance.
What should we focus on first?**

We recommend starting with governance before scale. Your organization should have an AI usage policy, a clear approval process for use cases, defined ownership, and coordination between AI governance and data governance. A steering committee or similar review group is a strong sign that the organization is approaching AI thoughtfully. Organizations can also identify department champions who can evaluate opportunities, monitor adoption, and escalate risks as AI use expands.

**Our organization rolled out an AI tool
to employees. Are there any audit
considerations around this?**

Not necessarily; the key questions to ask are what can the tool access, how permissions are configured, and whether employees understand acceptable use. AI can make it easier to find, summarize, and connect information, which means weak access controls may become more visible in an AI-enabled environment. In many cases, the issue is not the tool itself, but whether the underlying data environment is properly secured. For example, if sensitive data such as salary information or Social Security numbers are buried somewhere in a folder structure, an AI tool may surface it far more quickly than a human would. That creates risk. More directly related to the audit, consider whether an employee could ask the tool to find and summarize draft financial information prior to issuance, potentially resulting in an inappropriate disclosure.

**What kinds of AI use cases in
finance are generally considered
lower-risk use cases?**

Lower-risk use cases typically involve AI supporting a person rather than making decisions for them. That may include drafting narratives, summarizing reports, organizing data, highlighting contract terms for review, or assisting with trend analysis. In these situations, the preparer remains responsible for the output, and the reviewer still performs a meaningful review. Used this way, AI can help improve efficiency without fundamentally changing the control structure.

**When does AI become a bigger
concern from an audit perspective?**

The risk increases when AI begins to affect financial reporting or financial transactions with limited human oversight. Examples include automated journal entries, invoice processing, payment decisions, or support for accounting estimates where management relies heavily on the output. If AI is effectively deciding, posting, approving, or driving the result, the focus shifts quickly to whether controls are designed to prevent errors, detect anomalies, and help support management accountability.

Is it acceptable if AI helps prepare invoices or journal entries?

It can be, but the quality of the review control matters. If AI ingests invoices, suggests coding, or prepares support for a journal entry, someone with the appropriate knowledge should review the output before it is finalized. An understanding of the full workflow is critical: what the AI is doing, what the reviewer can see, whether data can be changed, and whether the review is substantive or just a sign-off. The more automation is involved, the more important it is that human review is real and well understood.

CONSIDER THE FOLLOWING EXAMPLES:

Scenario 1

An invoice comes in, a preparer creates and submits a journal entry based on the invoice, and a reviewer posts it. This is a traditional manual process that auditors have evaluated for years.

Scenario 2

An invoice comes in, AI generates a journal entry based on the invoice, the preparer reviews and submits the AI-generated entry, and a reviewer posts it. Here, AI is supporting the process, but there are still effectively four eyes on the journal entry. In many cases, a traditional audit approach may still be appropriate.

Scenario 3

An invoice comes in, AI generates and submits a journal entry based on the invoice, and then a reviewer posts it. This is a different workflow, with AI taking on the role of the preparer. In this case, the technology may become more critical to the process and may require additional audit attention, including understanding third-party assurance reporting and evaluating whether the automated control is operating effectively.

Does using AI mean our audit will require more work?

It depends. It changes the focus of the work. Auditors may spend less time on traditional manual evidence and more time understanding governance, data access, workflow design, change management, and management review controls. If a third-party platform is involved, you may also consider whether relevant controls are addressed in a SOC 1 report. As noted in the examples above, the audit approach may shift more significantly when AI becomes a critical part of the process.

We already use scripts, queries, and spreadsheets. Is AI really that different?

The core principle is similar; the important question is whether the tool is assisting the preparer or functioning as part of the control itself. If a staff accountant uses queries, scripts, or AI to support a reconciliation and then performs a meaningful review, the focus remains on the individual's control activity. But if the organization is relying on the tool to produce a complete and accurate result without that first layer of review, then the tool may become part of the key control environment, requiring more attention to access, change control, and governance over the underlying logic. From an audit perspective, the thought process remains consistent: what is the risk, and what is the control that addresses it? AI may present different risks, but the response still centers on identifying and testing the controls that matter.

What should controllers be most careful about right now?

First, low-oversight use cases tied to financial transactions or reporting deserve caution, particularly automated journal entries, invoice approvals, and accounting estimates. Second, do not overlook access risk. AI can make it easier for users to retrieve, infer, or alter information they should not access if permissions are too broad. For many organizations, the biggest immediate AI risk is not that the model is wrong; it is that the surrounding control environment is not ready for the speed and reach of AI-enabled tools.

What is the bottom line for controllers who want to stay audit-ready while adopting AI?

Be intentional. Approve use cases before deployment, define ownership, document workflows, restrict access to sensitive data, and keep a human at the helm—especially in processes affecting financial reporting. If AI is used in areas such as journal entries, transaction processing, estimates, or reconciliations, make sure preparer and reviewer responsibilities are clear and that review is more than a formality. AI can help improve efficiency, but it does not replace management's responsibility for the result.

For controllers, that is the practical takeaway: AI can be a valuable tool in finance, but only if it operates inside a disciplined control framework. The companies making the best progress are not the ones moving fastest; they are the ones adopting AI thoughtfully with governance, clear accountability, and meaningful human oversight at every critical point.



For organizations evaluating the audit and control implications of AI-enabled finance processes consider:

BDO'S TECHNOLOGY RISK ASSURANCE SERVICES

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.

