

2026 Application Access Governance Report

Secure Now or Pay Later

What confidence in access controls can conceal and
how leaders should prepare for the AI era

Foreword

by Michael Rasmussen, GRC Pundit & Analyst at GRC 20/20 Research

Application access governance is fundamental to an organization's ability to reliably achieve objectives, address uncertainty and act with integrity. Business applications support financial reporting, operational decisions and the transactions through which the organization delivers value. The permissions assigned within and across these applications determine who can act, what they can change and which controls constrain those actions. Governing that access requires a clear understanding of business processes and accountability for the risks those permissions create.

This research provides a useful perspective from 1,000 senior finance and finance technology decision-makers in the United States and United Kingdom. Two findings warrant particular attention. First, 95% of respondents express confidence that their access controls would withstand external audit scrutiny, while 51% report the same or similar access findings recurring in consecutive years or the same findings open for three or more years. These aggregate responses invite leaders to examine the evidence supporting their own confidence. A completed review has limited value if the underlying access remains inappropriate or the conditions that produced a finding persist.

Second, only 46% report continuously monitoring and managing cumulative access risk across applications. Business processes routinely cross application boundaries, and permissions that appear reasonable within one system can create a segregation of duties conflict when combined with access elsewhere. An effective governance approach follows the business process across those boundaries. It connects access decisions to the objectives, responsibilities and obligations of the organization, with enough context for business owners to judge whether access remains appropriate.

AI extends this responsibility to identities that can act on behalf of people. Where an agent can initiate a transaction, modify a record or change permissions, its authority needs an explicit business purpose, appropriate limits and an accountable owner. Human oversight should reflect the consequences of the action. Organizations also need evidence that allows them to reconstruct what happened and respond when access or behavior exceeds approved boundaries. These principles apply throughout the life of an identity, including when responsibilities change or the person who deployed an agent leaves.

Readers should use the findings to examine how governance operates in practice.

- Are access decisions informed by business risk?
- Does remediation result in verified change?
- Can management see cumulative exposure across critical applications and obtain timely evidence that controls remain effective?

Progress depends on clear ownership, coordinated processes and technology that supports those responsibilities. The objective is continuous assurance that access remains aligned with business needs as the organization changes. That is the contribution application access governance must make to reliable performance and accountable decision-making.

Application access governance is advancing, but AI is raising the bar

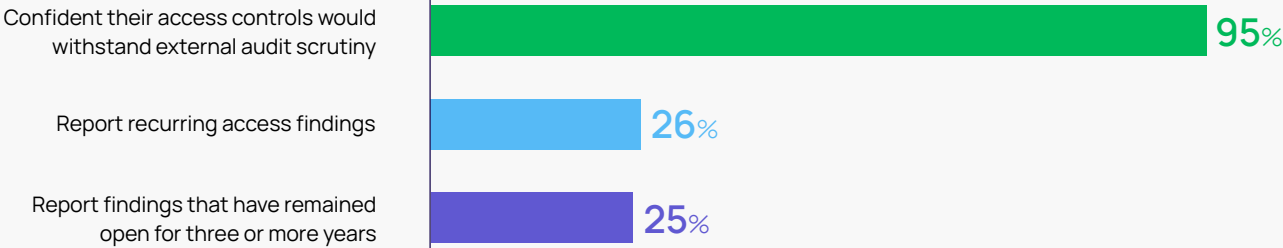
As business application environments expand, access governance must keep pace with more users, permissions and connections between systems. Finance and finance technology leaders need to identify access risk, enforce segregation of duties (SoD) and demonstrate that controls remain effective as people change roles and AI tools and agents become part of critical business processes.

Delinea commissioned an independent research agency to survey 1,000 senior finance and finance technology decision-makers in the US and UK on how they govern application access in the AI era.

The findings reveal a gap between confidence and control outcomes: 95% are confident their access controls would withstand external audit scrutiny, yet 51% report recurring access findings or findings that have remained open for three or more years.

Figure 1 | High confidence in controls, yet audit findings persist

Confidence in external audit readiness compared with reported access finding outcomes. Base: 1,000 respondents. Percentages rounded.



AI raises the stakes. Among organizations using AI tools or agents in critical business applications, 84% report at least one AI-related issue in the past year, including incorrect financial transactions and actions that could not be traced or explained. These findings make agent permissions, accountability and oversight important priorities for business leaders.

This report provides benchmarks to assess application access governance (AAG), explains what the findings mean for the business and identifies the controls leaders should prioritize to address access risk across applications and AI agents.

Key takeaways

1

Excess access lacks continuous oversight.

Fifty-two percent of respondents do not continuously monitor and remediate excess access. Only 46% continuously monitor and manage cumulative access risk across applications.

2

Automation is common but accountability remains fragmented.

Roughly two-thirds of respondents report that each access governance activity covered in the survey is mostly or fully automated. Only 22% have a single named owner for each application tracked in one centralized system of record.

3

Governance coverage is struggling to keep pace with application growth.

Sixty-eight percent report an increase in critical applications within access governance or Sarbanes-Oxley Act (SOX) scope, while 60% report an increase in critical applications operating outside that scope. Leaders need visibility into permissions within each application and across connected systems.

4

AI-related issues are widespread.

Among organizations using AI tools or agents in critical business applications, 84% report at least one AI-related issue in the past year. Incorrect financial transactions and actions that could not be traced or explained make oversight a practical business concern.

5

Confidence needs to be tested against unresolved findings.

Ninety-five percent express confidence in their access controls, yet 26% report recurring access findings and 25% report findings open for three or more years.

Key finding 1

Least privilege isn't achieved and excess access persists

As business application ecosystems expand, keeping access aligned with users' responsibilities becomes more challenging. Users can retain privileges they no longer need after changing roles. Accounts and permissions can remain active after an employee leaves the organization or a contractor completes an assignment.

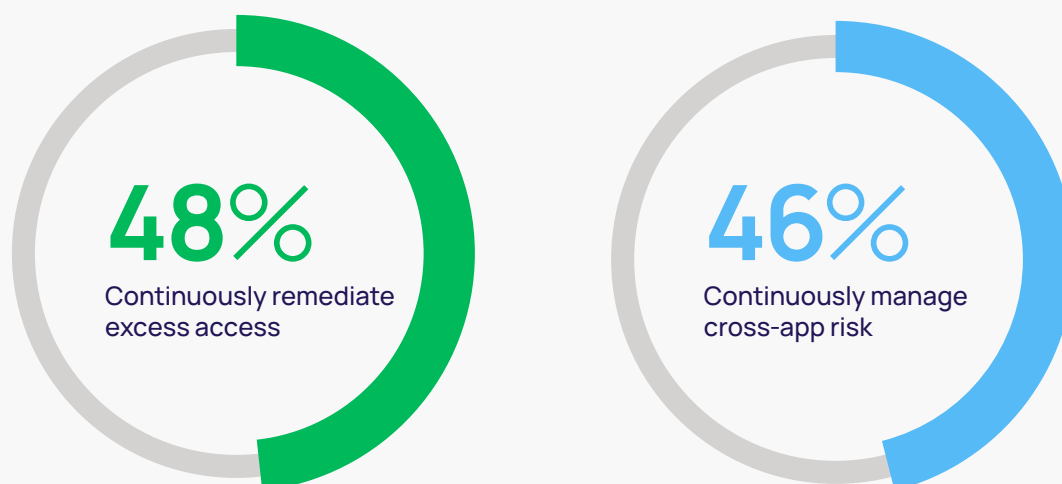
The growing adoption of AI is complicating oversight even further. Respondents list AI agents and copilots as one of their top three identity governance challenges.

Only 48% of respondents say their organizations continuously monitor and remediate excess access. The rest either have no visibility into excess access, suspect it exists but have not measured it or have identified excess access without remediating it.

Access across multiple applications creates an additional challenge. Only 46% continuously monitor and manage cumulative access risk across applications. More than half do not continuously monitor and manage cumulative user access across enterprise resource planning (ERP), customer relationship management (CRM), human capital management (HCM) and other critical business applications. Without a consolidated view, organizations may miss SoD conflicts and other risks.

Figure 2 | Continuous control is not yet the norm

Current state of least-privilege and cross-application risk management. Base: 1,000 respondents.

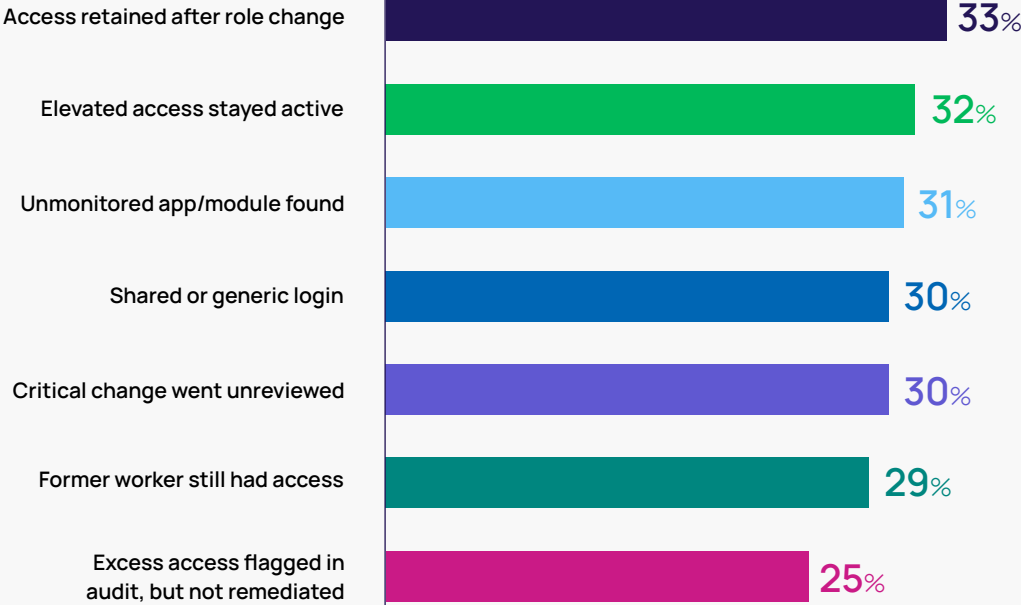


| Access risk is showing up in everyday operations

Ninety-one percent of respondents report at least one of the access-related conditions measured in the survey. One-third report users retaining access from a previous role after changing roles or departments. Thirty-two percent report emergency or elevated access remaining active after it was no longer needed, and 29% report former employees or contractors retaining access after departure. One-quarter say excess access was flagged in an audit but not remediated. These findings make both access removal and follow-through important areas for review.

Figure 3 | Access-related conditions experienced by respondents

Access-related conditions experienced by respondents. Multiple responses permitted. Base: 1,000 respondents.

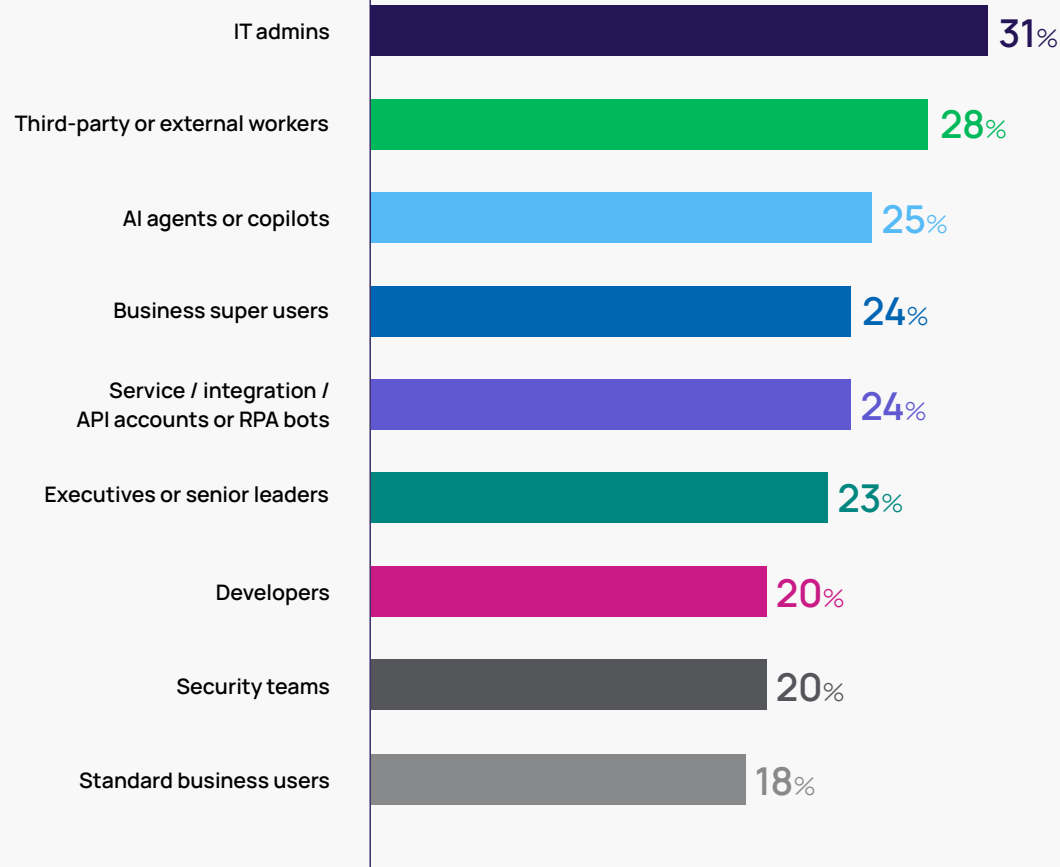


91%
of organizations experienced
at least one access-related
condition

Privileged access challenges extend beyond traditional IT administrators. While IT admins are the user type most often identified as difficult to govern (31%), respondents point to third-party or external workers (28%), AI agents or copilots (25%) and business super users (24%) as well. These findings highlight the need to govern elevated access across a broader range of human and non-human identities (NHIs).

Figure 4 | User types most difficult to govern for privileged or elevated access

User types organizations find most difficult to govern for privileged or elevated access. Base: 1,000 respondents. Respondents could select up to three answers.



Excess and elevated access create broader business risks. They can weaken SoD enforcement, expose sensitive data and undermine confidence that financial controls are operating as intended.



What to examine

- Do role changes, departures and emergency-access expiry reliably trigger access removal?
- Can you demonstrate that rejected or unnecessary access was removed, including when an audit has already identified it?

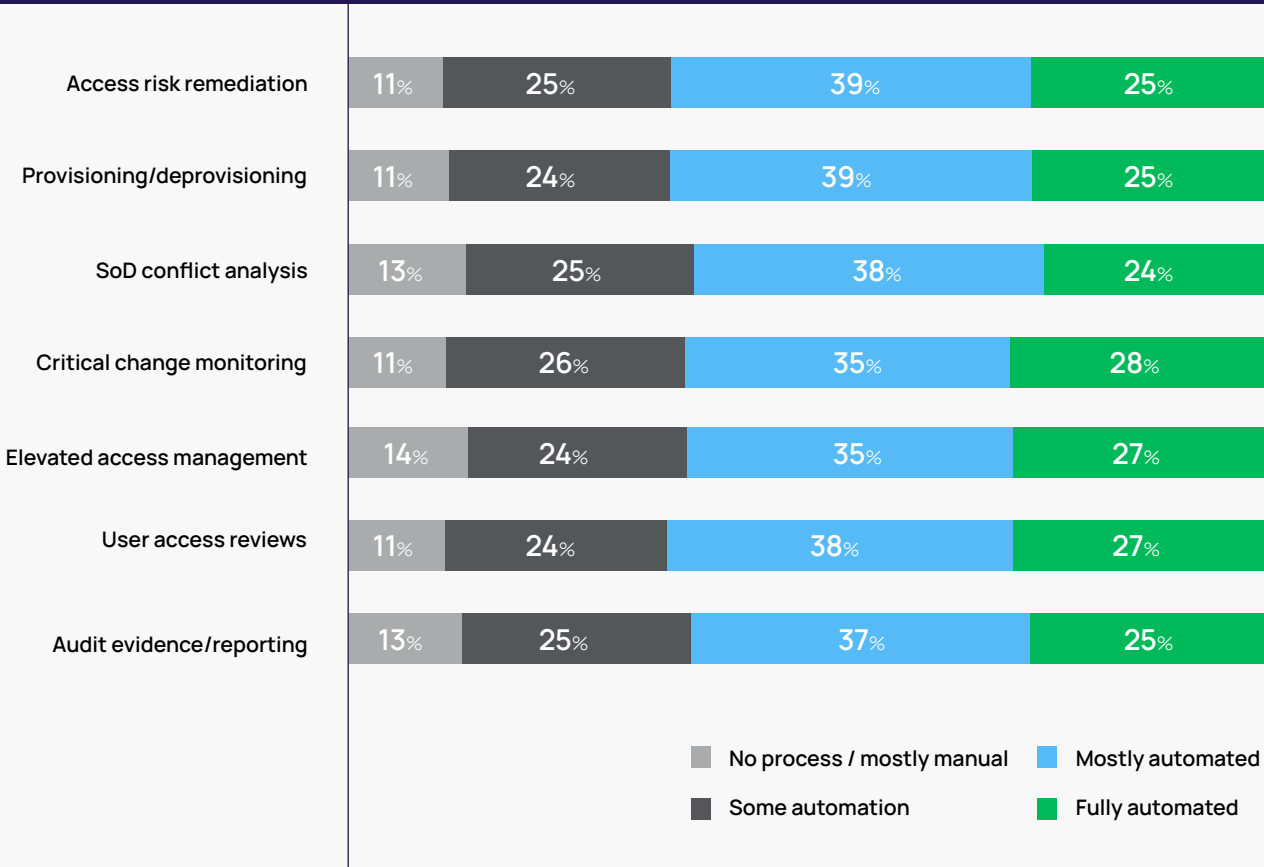
Key finding 2

Controls are becoming more automated, but manual work and fragmented ownership persist

Automation is now common across access governance activities, but manual work remains part of the equation. When asked to what extent common access governance activities were automated, nearly two-thirds of respondents said each activity was mostly or fully automated. Only about one-quarter reported full automation.

Figure 5 | Automation is widespread, but full automation remains limited

Maturity of seven AAG processes. Base: 1,000 respondents.



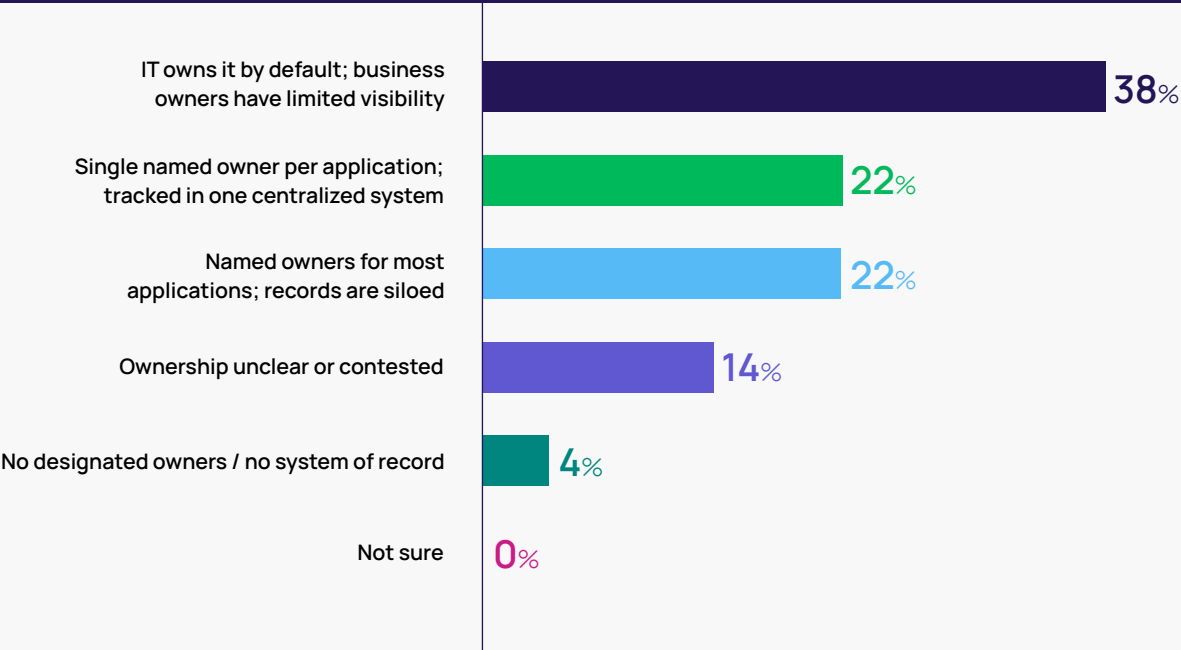
Automation isn't all-or-nothing. Organizations can automate significant portions of their access controls while still relying on people to complete other steps in the process.

Automation is only part of the challenge. Ownership of AAG is fragmented as well. Thirty-eight percent of respondents say IT owns access governance by default, with business application owners having limited visibility into who has access. Another 22% have named owners for most applications, but ownership records are siloed across teams or spreadsheets. Only 22% say each application has a single named owner tracked in one centralized system of record.

Without clear, centralized ownership, accountability gets harder to track across applications, making it more difficult to consistently manage access risk and governance processes.

Figure 6 | Ownership of application access governance remains fragmented

Ownership and accountability for access governance across critical business applications. Base: 1,000 respondents.



What to examine

- Does every critical application have a single named owner in one system of record?
- Which governance controls are still manual, and what would it take to automate them without losing accountability?

Key finding 3

Gaps persist within and across applications

Business application ecosystems are changing quickly. Organizations are bringing more critical business applications into formal governance programs, but the number of business applications operating outside those programs is also increasing.

More than two-thirds of respondents (68%) say the number of critical business applications formally in scope for access governance or SOX compliance has increased over the past two years. At the same time, 60% say the number of critical business applications in use but outside their access governance or SOX program has increased as well.

That growth in scope is translating into heavier governance workloads. Sixty-eight percent report more users with privileged or elevated access, 65% report greater effort to complete user access reviews (UARs) and 58% report longer remediation times for access-related audit findings.

Falling outside formal scope does not remove risk. Those applications can still expose the organization, especially where they integrate with systems that are under governance. As the application estate expands, organizations need visibility into what users and AI agents can do, both inside individual applications and across the connections between them, not just in applications subject to regulatory requirements.

Figure 7 | Application scope is expanding, but gaps remain

Percentage saying each measure increased slightly or significantly compared with two years ago. Base: 1,000 respondents.



Figure 8 | Governance demands are increasing alongside application scope

Percentage saying each measure increased slightly or significantly compared with two years ago. Base: 1,000 respondents.



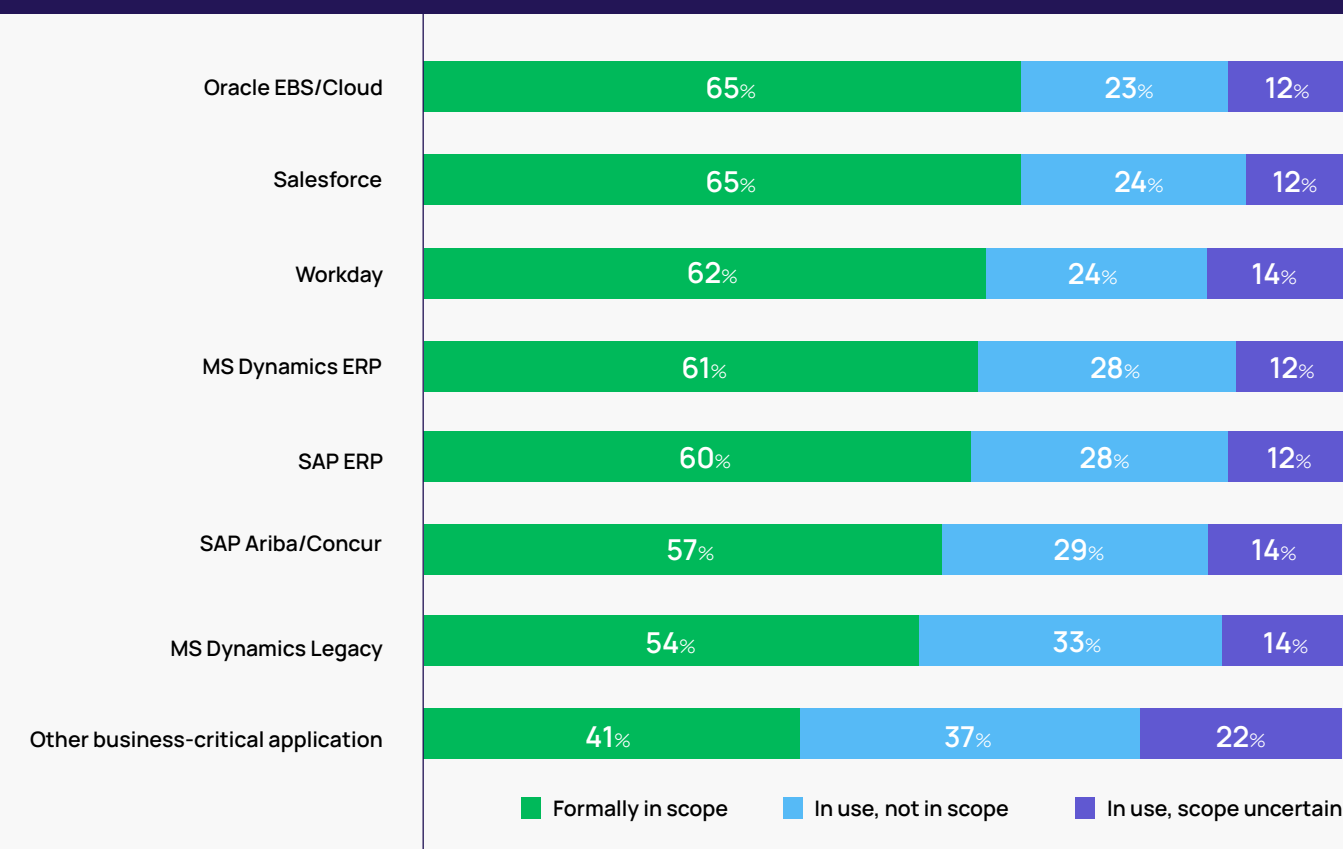
A larger business application estate creates more places for risk to hide

The scope gap is visible across widely used ERP, CRM and HCM applications. For example, among the 89% of respondents whose organization uses Salesforce, 24% say it is in use but not formally in scope for access governance, and another 12% are unsure whether it is in scope.

This isn't limited to one application. Similar patterns appear across SAP, Oracle, Microsoft Dynamics and Workday.

Figure 9 | Governance status among organizations using each application

Governance status among organizations using each application. Base varies by application and reflects only respondents whose organization uses it, ranging from 68% (other business-critical applications) to 89% (Salesforce) of the full sample of 1,000 respondents.



As the application estate changes, governance teams need to keep pace. Otherwise, an organization can improve controls over known systems while risk continues to accumulate elsewhere.



What to examine

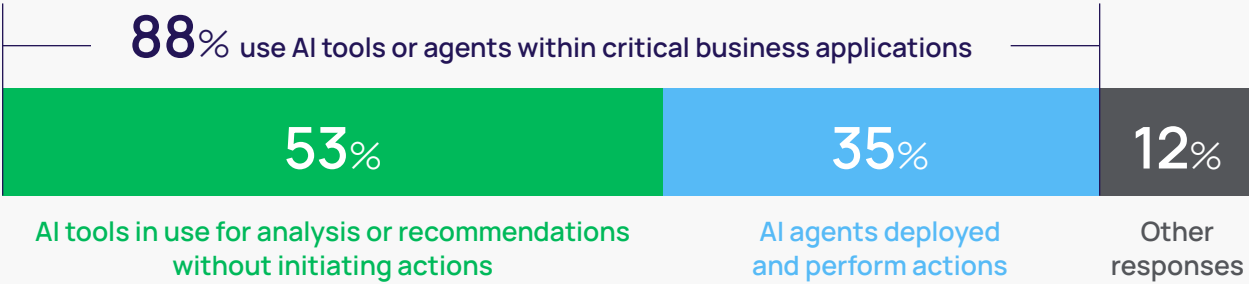
- ✓ Is every critical business application, including those outside formal SOX or governance scope, included in your access risk analysis?
- ✓ Can you identify SoD conflicts and excess access that span more than one application?

Key finding 4

AI agents already act inside critical applications, and oversight hasn't caught up

AI is moving into critical business applications faster than most organizations can govern it. Adoption is already widespread. Oversight of what agents can do is inconsistent and the consequences are already surfacing in day-to-day operations.

Figure 10 | AI agents and tools are prevalent
Current use of AI tools and agents in critical business applications. Base: 1,000 respondents.



AI tools or agents are already in use within critical business applications at 88% of organizations. Fifty-three percent use them for analysis or recommendations without initiating actions, while 35% have deployed AI agents that perform actions.

This distinction matters. An agent that can execute a transaction, change a record or alter permissions needs controls appropriate to those actions. Leaders need to understand what access it holds, who owns it and which decisions require human approval.

Agents may use permissions inherited from user accounts or shared accounts. Those permissions should be assessed against the agent's intended task, rather than assumed to be appropriate because an existing account has already been approved.

Visibility has not kept pace with AI adoption. Fewer than half of respondents with AI tools or agents in critical business applications have full, centrally tracked visibility into their deployment, access, permissions, ownership and approval. Roughly four in ten report only partial visibility.

Consequential AI actions need consistent controls

Among the 879 respondents with AI tools or agents in critical business applications, those tools and agents do far more than read data. Some respondents report tools and agents can autonomously execute or approve transactions, modify business data, change user permissions, access sensitive data or alter application configurations. Approval, traceability and permission limits become essential when actions happen without human review.

Fewer than half of AI-using organizations consistently apply each common governance control measured to all AI tools and agents.

Figure 11 | Share of AI-using organizations where tools/agents can act autonomously

Percentage of AI-using organizations saying tools or agents can perform each action autonomously with no human review. Base: 879 respondents.

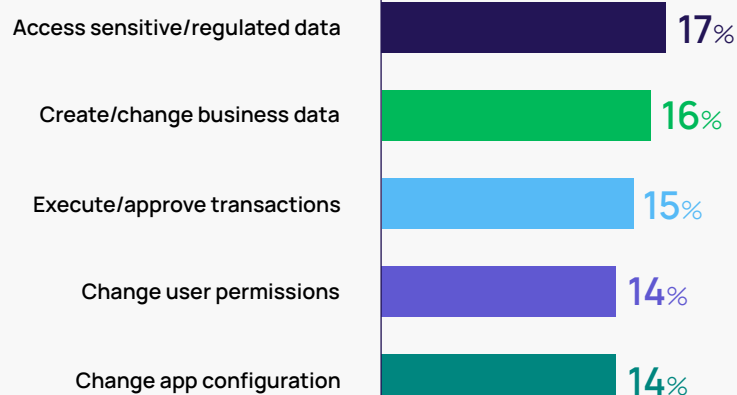
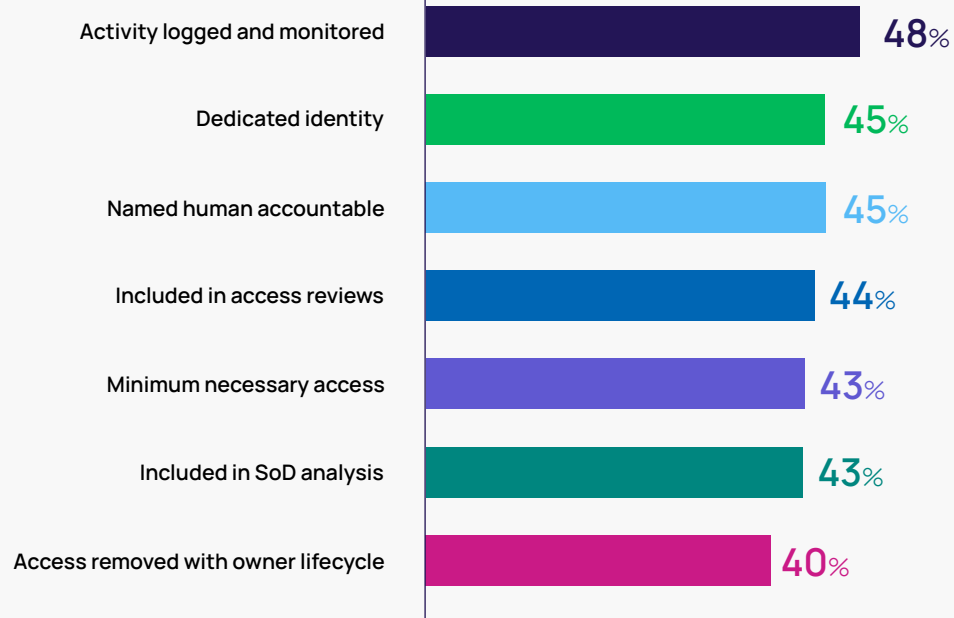


Figure 12 | Access controls applied to AI tools/agents

Percentage consistently applying each control to all AI tools and agents. Base: 879 respondents.



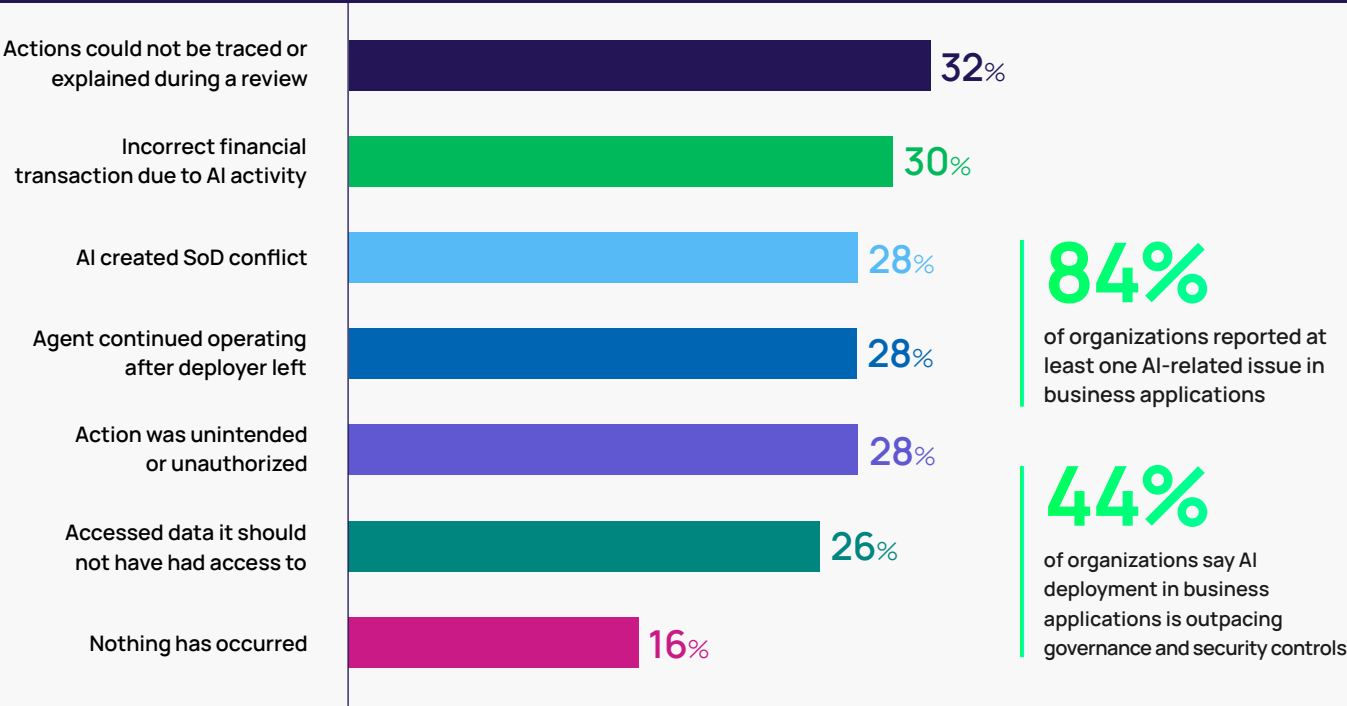
AI governance gaps are already producing observable problems

Eighty-four percent of organizations using AI tools or agents in critical business applications report at least one AI-related issue in the past 12 months. Only 16% say nothing has occurred. The most frequently reported issues include actions that could not be traced or explained during a review (32%), incorrect financial transactions from AI activity (30%), SoD conflicts (28%), agents continuing to operate after the person who deployed them left (28%) and unintended or unauthorized actions (28%). Twenty-six percent report that an AI tool or agent accessed data it should not have had access to.

Organizations are struggling to keep AAG aligned with AI adoption. Among AI-using organizations, 44% say AI deployment is outpacing governance and security controls. Only 11% say the two are keeping pace.

Figure 13 | AI-related issues reported in critical business applications

AI-related issues reported in the past 12 months. Base: 879 respondents with AI tools or agents in critical business applications. Multiple responses permitted.



What to examine

- Which actions require approval, which permissions are restricted and can every consequential action be traced to an accountable owner?

Key finding 5

Confidence in your controls doesn't mean they are working

Confidence is widespread, but so are persistent findings. Passing an audit does not mean access risk has actually been resolved, and the gap between the two matters whether or not an audit is scheduled.

Ninety-five percent of respondents say they are mostly or very confident their access controls for critical business applications would withstand scrutiny in an external audit today. That confidence does not hold up on its own: 26% say the same or similar access findings have recurred in consecutive years, and 25% say the same findings have remained open for three or more years.

Figure 14 | Confidence and outcomes tell different stories

Audit confidence compared with reported history of access-related audit findings. Base: 1,000 respondents. Percentages rounded.



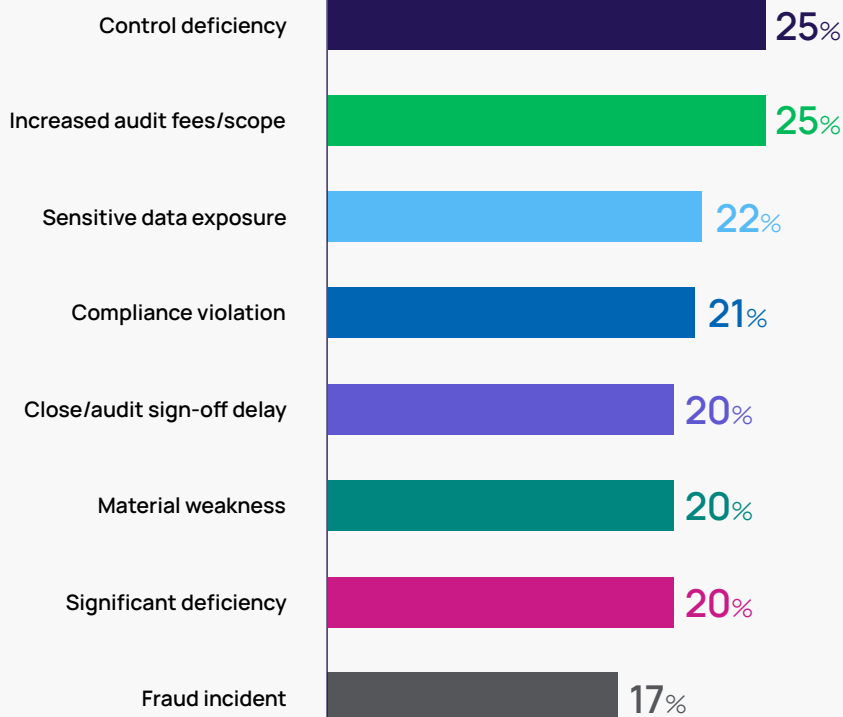
Controls may exist and evidence may be available, but access risks can still persist. New access issues may emerge as users, roles and applications change.

Consequential business application issues are commonplace

Seventeen percent report a fraud incident in a business application in the past year. About one in five report sensitive data exposure, a regulatory or compliance violation or a delay to financial close or audit sign-off. One-quarter report a control deficiency, and the same proportion report audit fees or expanded audit scope. The survey does not prove that access governance weakness causes these outcomes. It does establish the business context in which application controls must operate.

Figure 15 | Business application issues reported in the past 12 months

Issues experienced in a business application in the past 12 months. Multiple responses permitted. Base: 1,000 respondents.



Audit and access-review work consumes meaningful resources

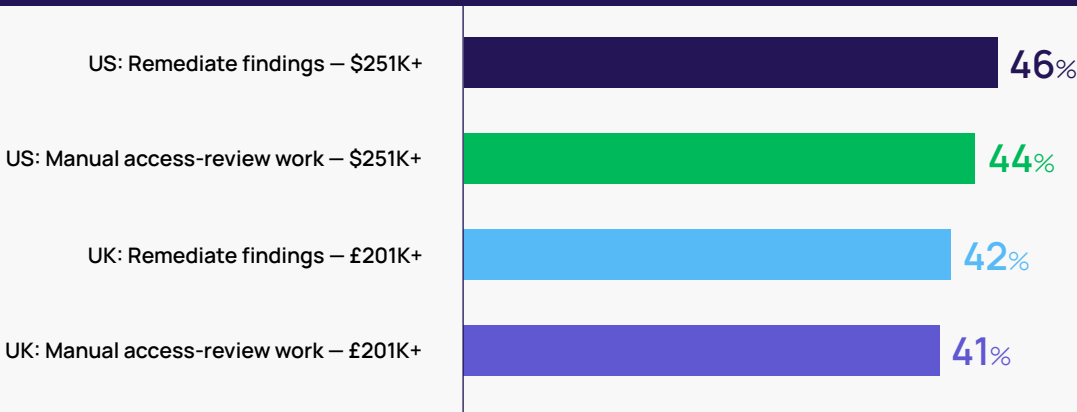
Strengthening AAG takes time and resources. Organizations report substantial expenditures to remediate access-related audit findings and perform the manual work required for user access reviews and certifications.

Among US respondents, 46% report spending \$251,000 or more in the past 12 months to remediate access-related audit findings. Forty-four percent report spending \$251,000 or more on manual user access reviews and certifications.

UK respondents report similar levels of spending. Forty-two percent report spending £201,000 or more to remediate access-related audit findings. Forty-one percent report spending £201,000 or more on manual user access review work.

Figure 16 | Reported substantial expenditures

Percentage of respondents reporting spending at or above the stated threshold. Base: 1,000 respondents.



What to examine

- ✓ Are the same access findings recurring year after year, and can you show why prior remediation didn't hold?
- ✓ What would it take to close a finding permanently rather than reopening it at the next audit?

Next steps: Close the gap

Centralize and automate controls across critical business applications and AI agents

Our research reveals a gap between confidence and control. Organizations report more applications in scope, high levels of automation and strong confidence in their access controls, yet recurring audit findings, persistent access risk and inconsistently governed AI agents tell a different story. For AI specifically, that gap is measurably widening.

These gaps become more consequential as AI takes on a greater role in business processes. As AI agents gain access to critical business applications and begin taking action, organizations must govern not only what people can do, but what agents can do on their behalf. That means understanding agent access and permissions, identifying new access and SoD risks and maintaining evidence of appropriate oversight.

As your business application ecosystem expands and evolves, you need greater visibility and control over who and what has access, including AI agents. You need to know what they can do and where risk exists across critical business applications. By centralizing and automating access controls across all identity types, you can identify and address risk, strengthen internal controls and reduce the manual effort required to maintain them.

Best practices for stronger application access governance

Keep critical applications in scope.

Sixty percent of respondents say critical applications outside governance has increased, and only 22% have a single named owner per application. Regularly identify critical business applications and bring them into governance programs as the application environment changes.

Automate repeatable governance processes.

Manual review effort has increased for 65% of organizations. Automate access reviews, provisioning and other repeatable workflows to reduce manual effort while maintaining appropriate approvals and accountability.

Analyze access risk across applications.

More than half lack continuous visibility into cumulative access risk across applications. Maintain a centralized view of access and evaluate cumulative permissions and SoD risk across ERP, CRM, HCM and other critical business applications.

Monitor changes to critical data and configurations.

Thirty percent experienced a critical change made without review or detection. Track changes to critical data, configurations and settings, including who made the change and whether it was authorized.

Identify and remediate access risk.

More than half do not continuously monitor and remediate excess access. Monitor for excess access, SoD conflicts and sensitive permissions, then track identified risks through remediation.

Extend access governance to AI agents.

Fewer than half consistently apply core controls to all AI agents. Maintain visibility into agent access and permissions, apply least privilege and SoD controls, include agents in access reviews and maintain appropriate human oversight.

| How Delinea Fastpath can help

Application access risk and audit readiness ultimately comes down to three questions: Who has access to your business applications? What are they doing with that access? Where are you vulnerable? Delinea Fastpath helps answer all three with a set of solutions that deliver cross-platform visibility and automated controls that make governance easier to manage.

Fastpath capability	Business value
Access control	Automates SoD and sensitive access risk analysis, down to the lowest securable object. It reports conflicts and risks so teams can remediate them or apply documented mitigating controls. Customized reports, scheduled and signed off by owners, help maintain continuous audit readiness across financially significant applications.
Access review	Automates the user access review process from data collection and distribution through delegations and sign-off. Reviews can be scoped by application, role, or risk, with the context reviewers need to make informed decisions. Rejected access can be automatically deprovisioned or routed to IT for removal, with post-review reconciliation providing a complete audit trail.
Access provisioning	Replaces manual email chains and ticketing systems with automated access request workflows and configurable approval routing, analyzing every request for SoD conflicts and appropriateness before approval. Once approved, access can be provisioned directly or routed to IT, with a complete audit trail from request to fulfillment.
Change tracking	Provides visibility into changes to critical data and configurations, including who made the change, with before-and-after values and key metadata to determine appropriateness, using out-of-the-box templates or a scope you define. Integrations with popular ITSM platforms map changes to tickets and approvals, providing a complete audit trail.



See how Delinea Fastpath can help you identify access risk, automate repeatable controls and strengthen audit evidence across critical business applications. [Request a demo](#) today.

Demographics and methodology

We surveyed 1,000 senior finance and finance technology decision-makers across the United States and United Kingdom from September 8 through September 16, 2026. The sample included 500 respondents in each country.

Respondents had direct hands-on responsibility for application access governance or responsibility for strategy, policy or budget. The survey covered critical business applications including ERP, CRM, HCM and related systems.

Figure 17 | Roles of respondents

Base: 1,000 respondents.

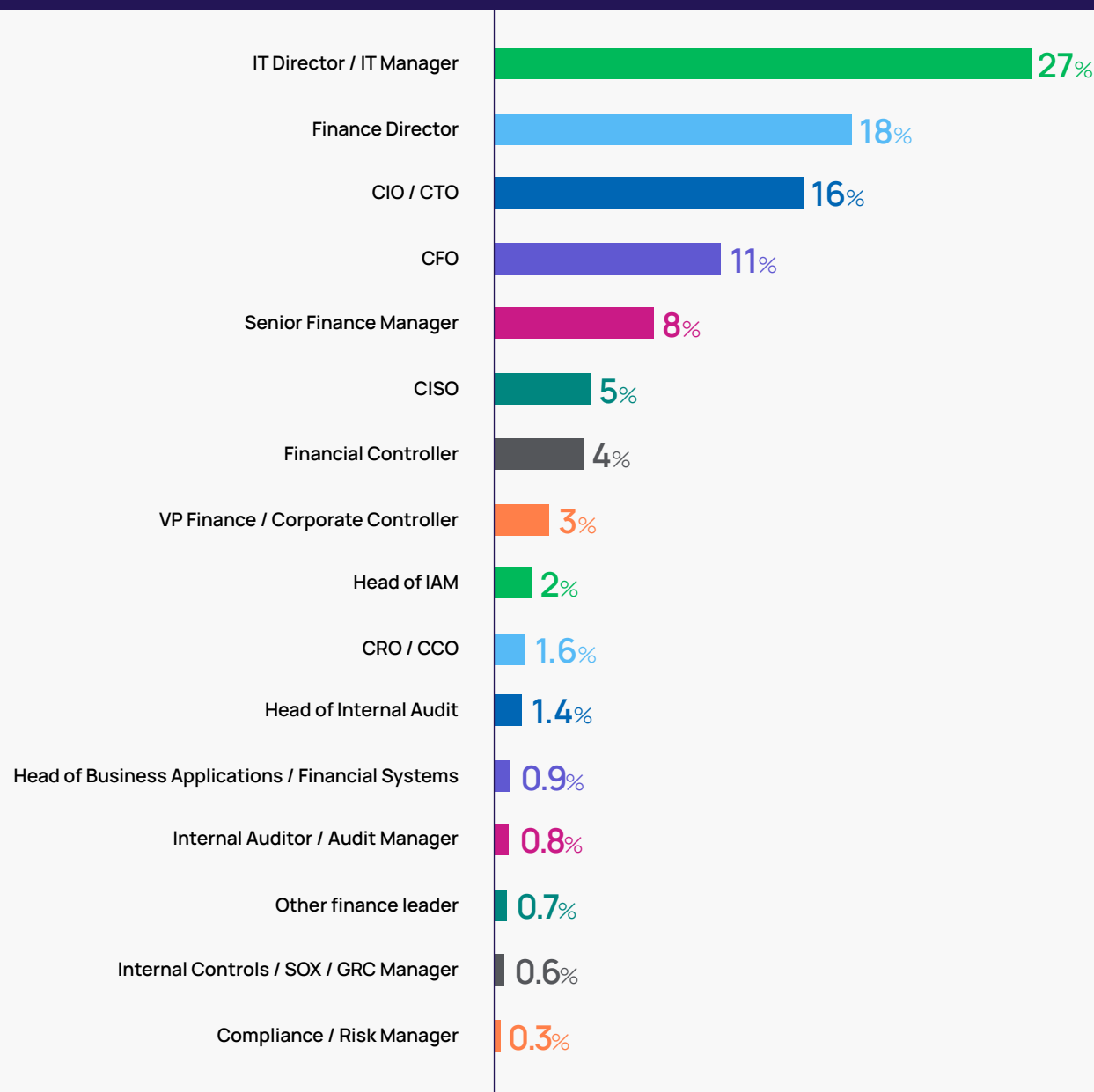
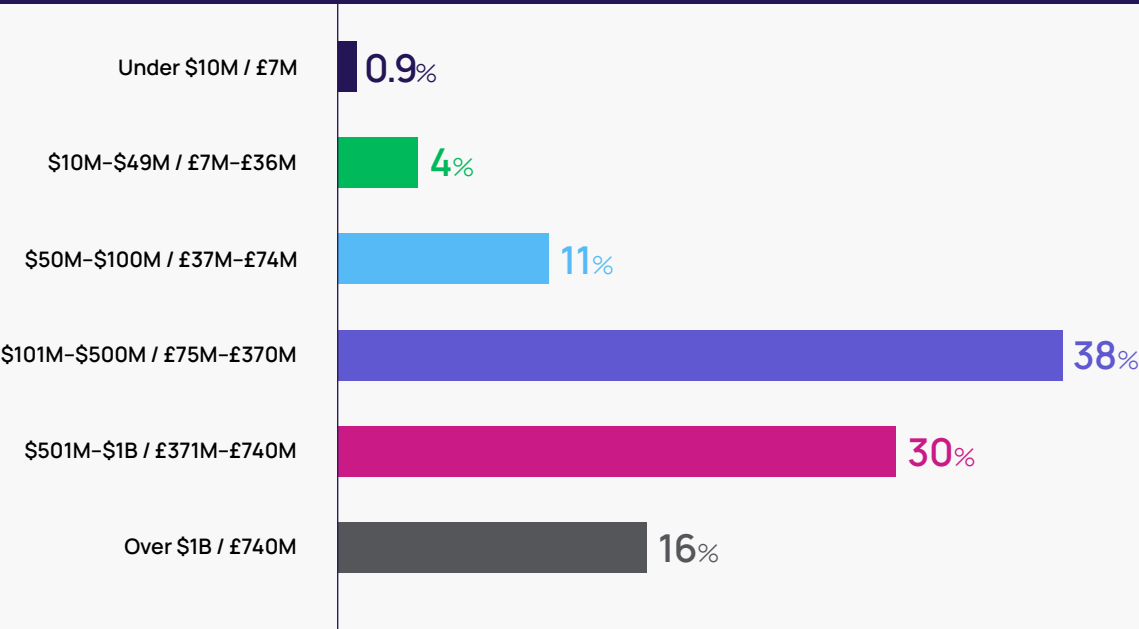


Figure 18 | Organization size by annual revenue or turnover

Base: 1,000 respondents.



About the data

Some questions applied only to certain respondents, including those whose organizations use AI in critical business applications and those whose organizations had been audited. Some questions allowed respondents to select more than one answer. Percentages in this report are rounded to the nearest whole number unless otherwise noted.



Delinea Fastpath

Delinea Fastpath is a leader in application access governance, helping organizations automate governance of human and agentic access across business applications to maintain continuous audit readiness. By automating key IT General Controls, including segregation of duties (SoD) risk analysis, Delinea Fastpath helps organizations reduce risk, simplify compliance, and strengthen oversight of sensitive applications and data. Organizations can govern access across 100+ cloud and on-premises applications, with more than 30 out-of-the-box native direct connections that enable fine-grained risk analysis down to the lowest securable object.