



The OneTrust 2026 AI-Ready Governance Survey Report

The AI Governance Gap Is Now An Operating Risk

How organizations are moving from governance programs to **connected operations** as AI scales

Research from 1,200 senior business decision-makers across eight markets



Table of Contents

AI Governance Is Moving Into Operations	03
Why We Did This and What Got Us Here	04
Chapter 1: Foundations Are In Place, But Maturity Is Uneven	06
Chapter 2: Agent Adoption Is Exposing the Next Governance Gap	08
Chapter 3: Governance Has Not Yet Become a Connected Operating Model	11
Chapter 4: Investing in Governance to Move Forward	16
What This Means for Enterprise AI Governance	19
Notes From The Field	20
Methodology	21

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document. OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.



Report at a Glance

AI Governance Is Moving Into Operations

AI governance now sits inside daily enterprise operations. AI adoption is broad, governance programs are active, and investment continues to rise. The survey also shows a gap between activity and a consistent operating model. Visibility into unsanctioned use remains incomplete and agent adoption is moving faster than oversight is being deployed. Only 5% of respondents say coordination and accountability are clear across the AI lifecycle.

The next phase of AI governance centers on connection. Organizations need governance that works across systems, teams, vendors, and agents, with controls and evidence that stay attached to AI as it moves from intake through deployment and ongoing use.

The next phase of AI governance is about connection across systems, teams, vendors, agents, and the full lifecycle.

74%

Departmental or scaled AI adoption

87%

Encourage AI agent use

47%

Have clear governance in place

5%

Clear coordination and accountability across the AI lifecycle

86%

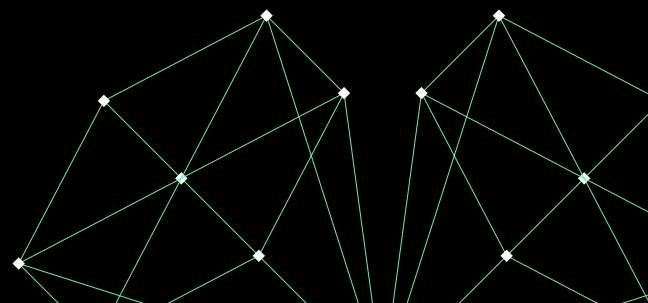
Experienced at least one AI-related incident

80%

Increased time spent managing AI-related risk

98%

Plan to increase budgets for technologies used to govern AI





Introduction

Why We Did This and What Got Us Here

AI governance now has an operational job to do. Organizations are moving AI into business functions and processes, while employees and teams continue to adopt new tools and agents. Governance has advanced alongside that adoption, but the work has become harder to coordinate as the number of systems, stakeholders, and decisions grows.

OneTrust surveyed 1,200 senior business decision-makers across eight markets to understand how organizations are adopting AI, governing its use, managing risk, measuring value, responding to incidents, and planning future investment. The audience included equal representation from privacy, data and AI, security and risk, and marketing leaders at companies with at least \$100 million in annual revenue.

The data describes an active market. Nearly three-fourths (74%) of respondents report departmental or scaled AI adoption. More than half (52%) use AI across multiple business functions or embed it into business processes and operations. Governance has also moved forward. Fifty-two percent describe their programs as integrated into the AI lifecycle or embedded by design.

That progress sits beside an almost even divide. Forty-seven percent still describe governance as reactive, fragmented, slow, or manual. Only 17% select the highest operating state, where governance is embedded by design and enables innovation. The market has built real foundations, yet consistent execution remains concentrated to a smaller group.

The strongest tension appears when governance activities need to work together. Organizations perform an average of four AI governance activities, and roughly three-quarters express confidence across the seven capabilities tested. Only 5% say coordination and accountability are clear across the full AI lifecycle. The issue is increasingly less about whether governance work exists and more about whether that work connects across teams, systems, vendors, and stages of use.

AI agents sharpen that tension. Eighty-seven percent encourage agent use, while only 47% have clear governance controls in place. The gap places new weight on action authority, human review, monitoring, and evidence.

Operational pressure is also visible. Ninety-six percent identify at least one type of AI initiative that was slowed, paused, or complicated by governance, risk, or review requirements. This report follows that progression. It starts with the foundations organizations have built, then examines the agent oversight gap and the broader coordination challenge. It closes with the investment organizations are making to turn individual governance activities into a connected operating model.

The market has built real governance foundations.
The next test is whether those foundations operate as
one connected system.



Chapter 1

Foundations Are In Place, But Maturity Is Uneven

AI Adoption and Governance Have Both Advanced

AI adoption has moved beyond isolated pilots for most respondents. Twenty-two percent use AI within individual teams or departments. Another 32% use it across multiple business functions, and 20% have embedded it into business processes and operations. The remaining 26% are planning, evaluating, or experimenting, with only 1% reporting no AI use.

This adoption profile matters because governance is being tested in active settings. Policies, reviews, and controls now need to support decisions that occur across departments and operating processes. The survey shows meaningful progress, but a clear split in how organizations execute.

Fifty-two percent describe governance as integrated into the AI lifecycle or embedded by design. Forty-seven percent describe it as reactive and fragmented or defined but slow and manual. The split provides a direct view of the market — many organizations have moved governance closer to the work, while nearly half still depend on processes that struggle with speed, consistency, or cross-functional execution.

Only 17% choose the highest maturity response, where governance is embedded by design and enables innovation. This places a practical limit on broad claims of market readiness. Governance has become established, however the most integrated operating state remains the exception.

52%

Integrated into the lifecycle
or embedded by design

47%

Reactive, fragmented,
slow, or manual



A Maturity Model Shows a Market Spread Across Every Stage

To add structure to that picture, the research measures how organizations perform governance, and how many governance activities they perform.

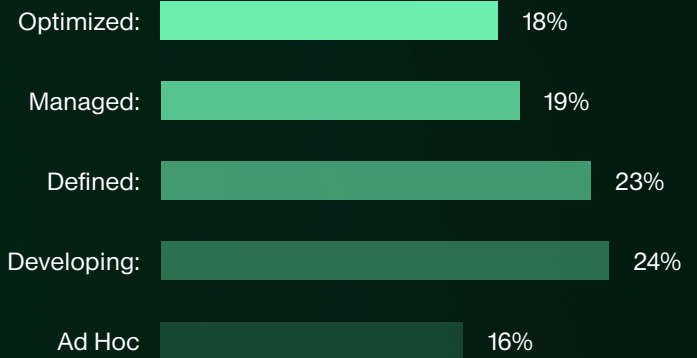
OneTrust's AI Governance Maturity Model was used as a basis to weigh the respondents' answers. Responses were grouped into five categories, and scored as such:

- Optimized = a score of 7 or 8
- Managed = a score of 6
- Defined = a score of 5
- Developing = a score of 4
- Ad hoc = a score of 1 to 3

Eighteen percent fall into the Optimized group, and 19% fall into Managed. Twenty-three percent sit in Defined. Twenty-four percent are Developing, and 16% are Ad hoc. That leaves 37% in the two most advanced groups, 23% in the middle, and 40% in the two earlier groups.

The distribution reinforces the report's central point. This audience has moved beyond a simple starting line, yet progress remains uneven. Some organizations have connected governance to the lifecycle and built a broad set of activities. Others have defined pieces of the program without reaching the same level of integration and scale.

AI Governance Maturity Spans Every Stage





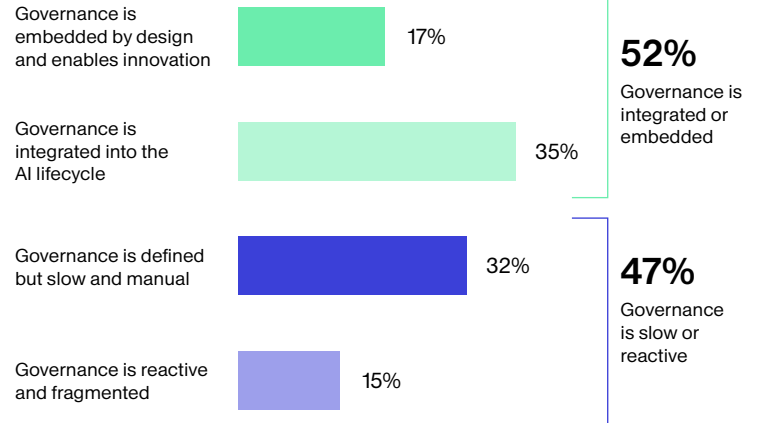
Governance Activity is Widespread, With Room for Greater Operating Depth

Organizations perform an average of four AI governance activities. Risk classification and impact assessments are the most common at 37% each. Employee AI usage controls follow at 36%, with policy and governance documentation at 35% and incident management at 34%.

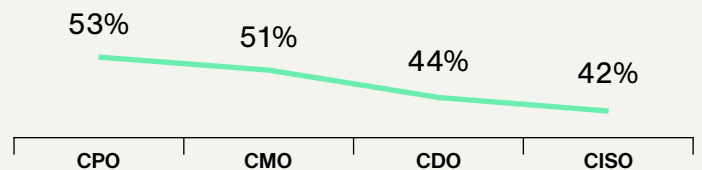
The activities that support ongoing operation appear less often. Less than a third (31%) report AI inventory and asset management. Thirty percent conduct monitoring after deployment, and 30% perform third-party AI vendor reviews. Governance evidence and audit trails rank lowest at 28%.

This pattern shows where many programs have concentrated their effort. Classification, assessment, policy, and employee controls establish a foundation. Inventory, continuous monitoring, third-party review, and evidence connect that foundation to day-to-day operations. Those capabilities become more important as AI moves across business functions and remains active after launch.

Which best describes how your organization currently performs AI governance?



% Slow and Manual / Reactive by Segment



Confidence is High, While Consistency Remains a Separate Test

Between 76% and 78% of respondents feel confident in their ability to perform each of the seven governance activities tested. The highest confidence response ranges from 29% to 33%. Teams believe they can classify risk, maintain documentation, demonstrate human oversight, monitor systems, respond to incidents, and preserve evidence.

That confidence reflects task-level capability. The 52% versus 47% governance split (integrated governance versus reactive and fragmented, respectively) and the five-level maturity model reflect how consistently those tasks actually operate together. Both views matter. Organizations have skilled teams and established practices, while lifecycle integration and coordination still vary.

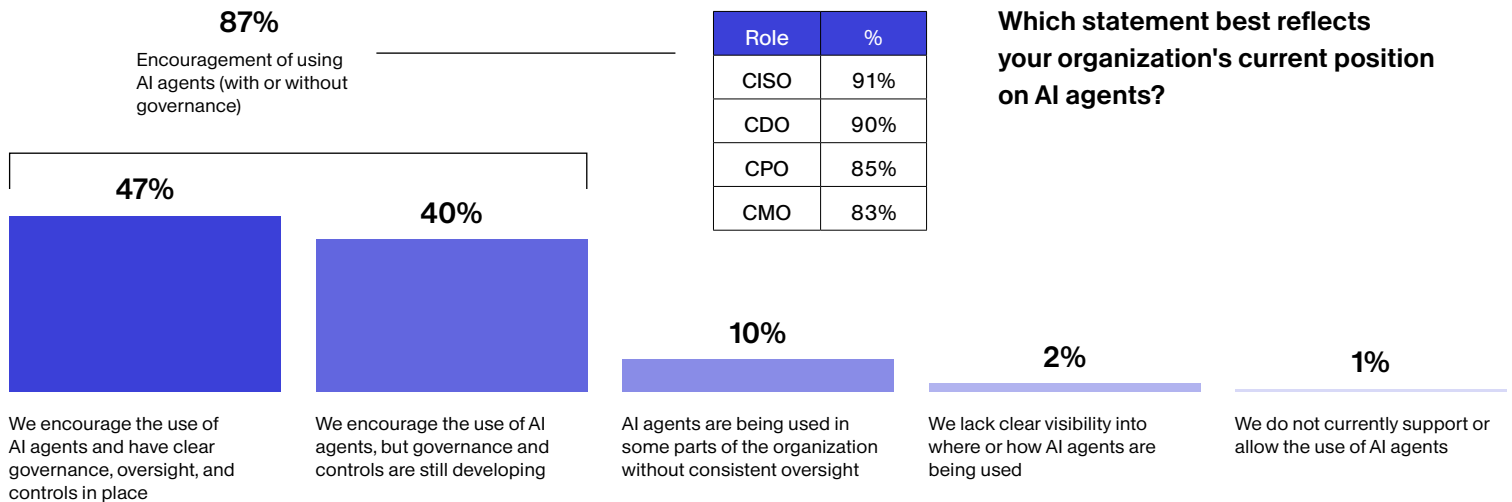


Chapter 2

Agent Adoption is Exposing the Next Governance Gap

Agent Use is Moving Ahead of Clear Oversight

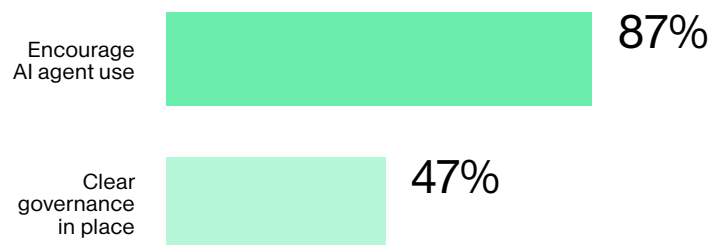
AI agents provide the survey's clearest direct comparison between adoption and governance readiness. Eighty-seven percent of respondents say their organizations encourage agent use, while less than half (47%) encourage use with clear governance, oversight, and controls in place. Another 40% encourage use while governance and controls continue to develop.



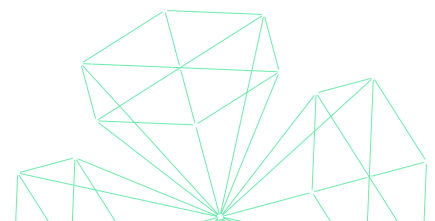
The remaining respondents describe a less consistent position. Ten percent say agents are used in parts of the organization without consistent oversight. Two percent lack clear visibility into where or how agents are even used. But one last measure of widespread adoption is that just 1% currently disallow agent use.

The 40-point difference between encouragement and clear governance shows the size of the readiness gap. Organizations are opening access to agents while they continue to define the rules that surround agent activity.

Agent Encouragement is Outpacing Clear Governance



They're building the plane while it's already in flight.



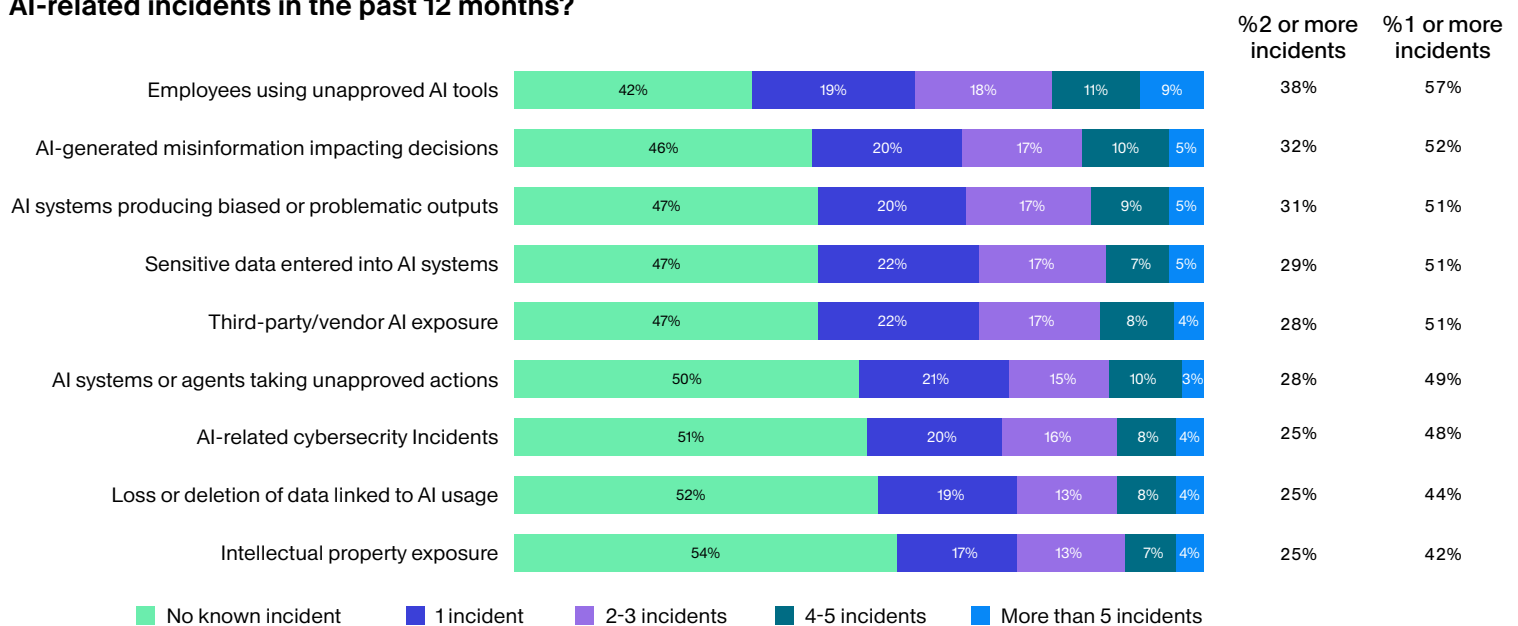


Agents Compress Several Governance Questions Into One Operating Challenge

Autonomous or agentic workflows take actions on behalf of users. That characteristic brings action authority, human review, technical controls, post-deployment monitoring, and evidence into the same governance decision. Each of those areas appears elsewhere in the survey as a point of friction or coordination difficulty.

Thirty percent of respondents say autonomous or agentic workflows are among the AI initiatives most often slowed, paused, or complicated by governance, risk, or review requirements.

Has your organization experienced any of the following AI-related incidents in the past 12 months?



The incident findings add another layer. Nearly half of respondents report at least one incident in which AI systems or agents took unapproved actions during the past year. More than a quarter (28%) report two or more such incidents. These results show that authority and oversight are current operating concerns rather than future design questions.

48%

Report at least one incident involving unapproved actions by AI systems or agents

28%

Report two or more such incidents



Preparedness Remains Uneven Across Agentic and Data Risks

Incident preparedness findings place data integrity at the top of the risk agenda. Twenty-nine percent say data loss, corruption, or misclassification is the incident their organization is most likely to experience. Thirty-four percent say it would create the greatest risk, and 34% say their organization is least prepared to manage it.

Unvetted automation or agentic action sits close behind on likelihood and preparedness. Twenty-seven percent select it as the incident most likely to occur, and 27% say their organization is least prepared to manage it. The response is defined as an AI tool, agent, or AI-enabled workflow taking an unauthorized action without appropriate human review or approval.

29%

Say data loss, corruption, or misclassification is most likely

27%

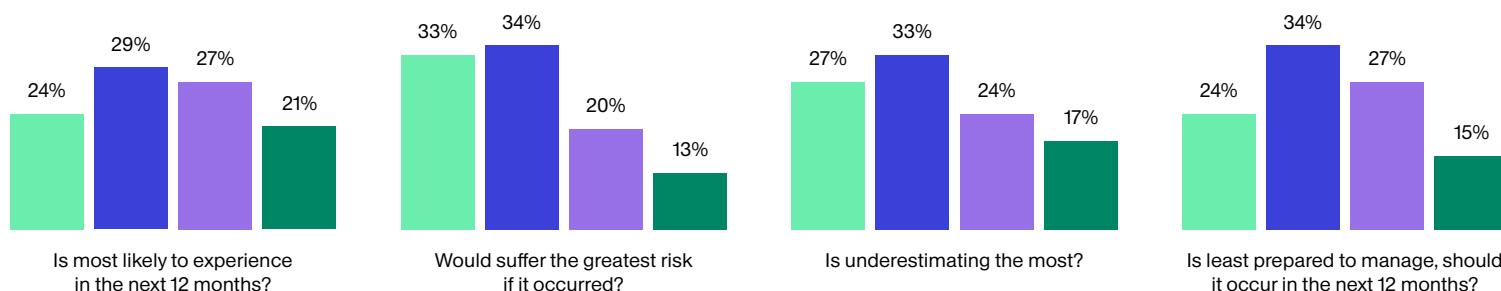
Say unvetted automation or agentic action is most likely

The connection between these results matters. Agent oversight involves both the action an agent takes and the data it accesses, changes, or classifies. Governance therefore needs to cover authority, review, data handling, monitoring, and response as one operating process.

Agents serve as a pressure test for the wider governance model. Organizations with separate policies, reviews, and monitoring practices still need those elements to work together at the moment an agent acts. Clear controls need to travel with the workflow, and evidence needs to show what happened, who approved it, and how the organization responded.

Which type of incident do you believe your organization...?

- Data leakage or unauthorized disclosure
- Data loss, corruption, or misclassification
- Unvetted automation or agentic action
- Flawed decision-making or unreliable output



Agents serve as a pressure test for the wider operating model.
Authority, review, controls, monitoring, and evidence need to work together at the moment an agent acts.

Chapter 3

Governance Activity Has Not Yet Become a Connected Operating Model

Coordination and Accountability Aren't Clear Across the AI Lifecycle

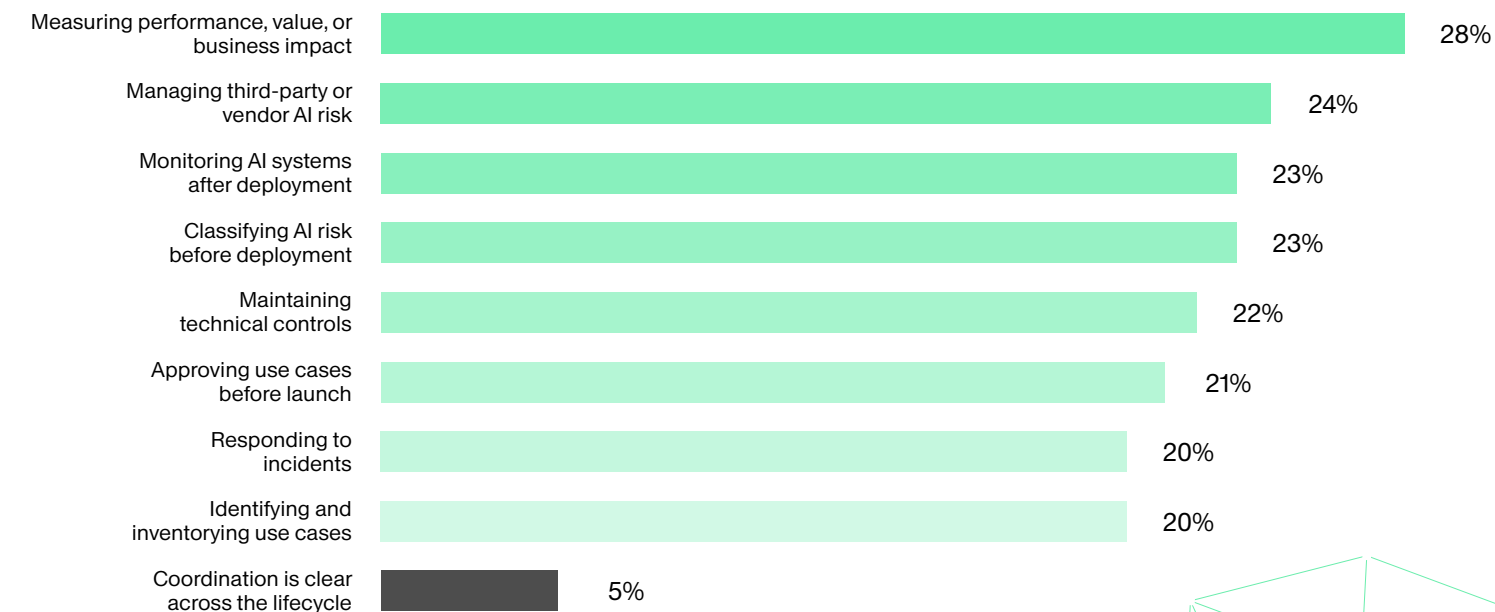
Organizations report active governance programs, an average of four governance activities, and high confidence in individual capabilities. But just 5% say coordination and accountability are clear across the AI lifecycle. The other responses cluster across a broad range of operating challenges.

As shown in the coordination challenges chart, there's a very narrow range separating individual programs' most pressing challenges.

The narrow range is the point. Coordination problems appear across the lifecycle rather than concentrating in one team or stage. Organizations are doing the work, but ownership, context, and evidence often move unevenly from intake through deployment and monitoring.

In which of the following areas is cross-functional coordination or accountability most difficult within your organization's AI governance process? Two selections permitted.

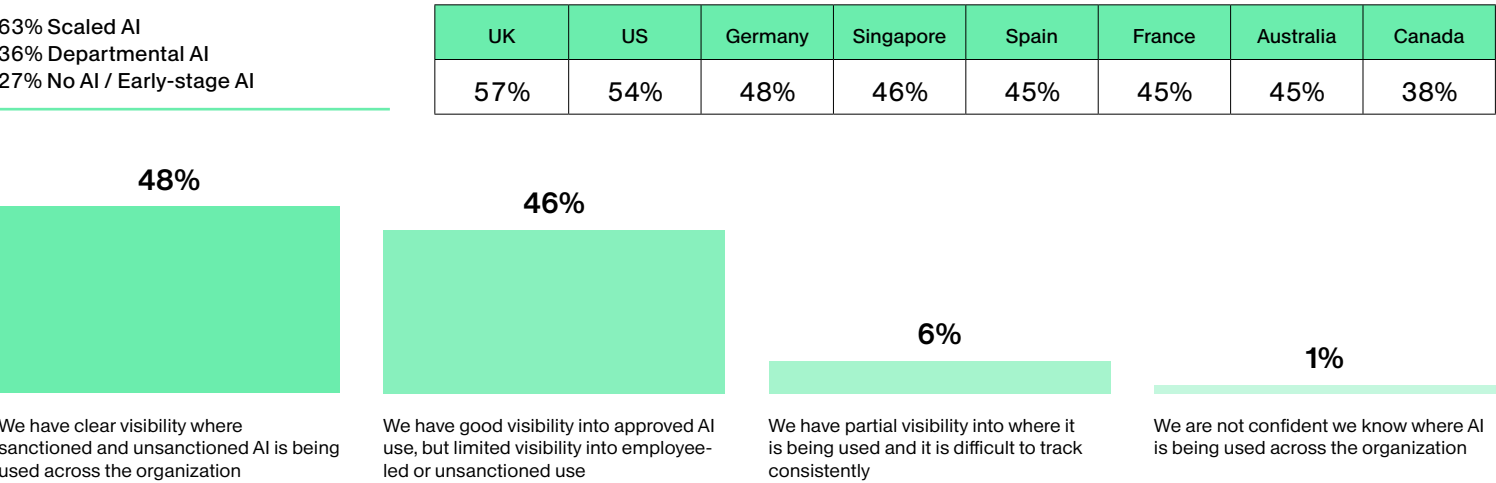
Coordination Challenges Span the AI Lifecycle



Visibility is Strongest for Approved AI

Forty-eight percent report clear visibility into sanctioned and unsanctioned AI use. Another 46% report good visibility into approved AI with limited visibility into employee-led or unsanctioned use. Six percent describe partial visibility that is difficult to track, and 1% lack confidence in knowing where AI is actually used.

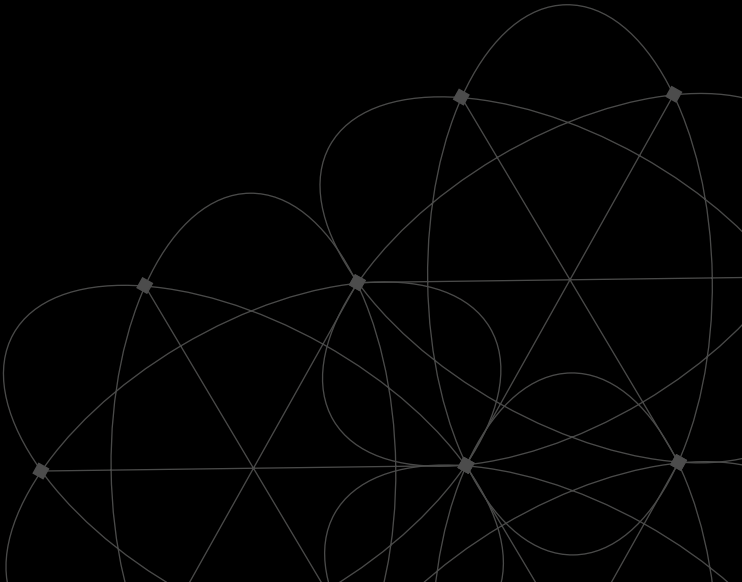
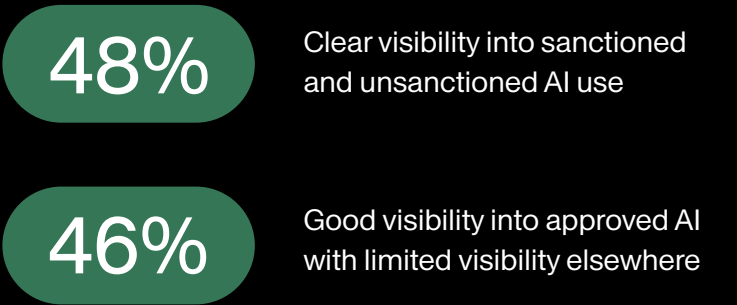
Which statement best describes your organization's current visibility into where AI is being used across the business?



The survey's workflow findings show how that visibility gap develops. Thirty-three percent experienced employees using unapproved AI tools because approved options or processes were not available quickly enough. Thirty-one percent identified use cases for review after they were already in use, while 29% saw projects move forward before risk review was complete. Another 29% said use cases move forward before being inventoried.

Taken together, these findings point to a broader visibility and process challenge. Slow access to approved tools can leave employees looking outside established channels, while late discovery means review may not happen until after adoption.

Missing inventory makes ownership, classification, and monitoring harder to maintain. Visibility therefore depends on both technology and process. Organizations need a current view of AI use, along with an intake path that employees and business teams can use at the speed of their work.



Operational Friction is Widespread and Comes From Several Sources

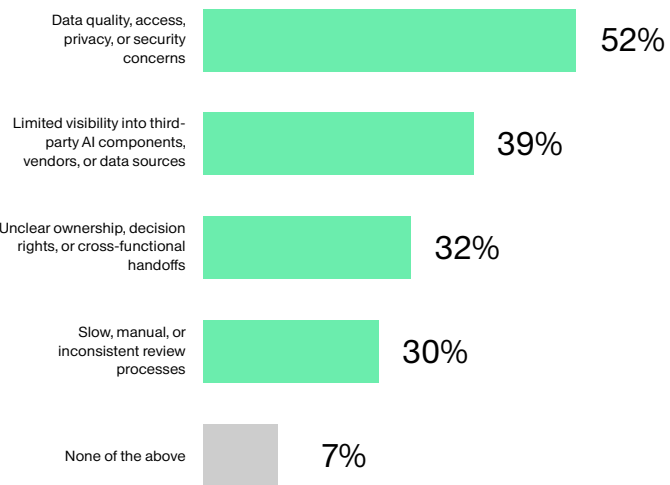
Governance friction has become a routine part of AI delivery. Ninety-six percent of organizations said at least one initiative was slowed, paused, or complicated by governance, risk, or review requirements. The impact reaches across data analysis, third-party tools, agentic workflows, customer-facing experiences, and employee copilots. This breadth points to fragmented execution across teams, systems, and stages of the AI lifecycle.

Data quality, access, privacy, and security concerns lead the list of delay factors at 52%. The wider pattern shows how those concerns become operational delays. Teams lack complete visibility into third-party AI, ownership and handoffs remain unclear, and review processes are often manual or inconsistent. When these elements remain disconnected, risk decisions happen later and delivery slows.

A connected operating model brings visibility, decision rights, and review workflows together earlier, helping organizations manage risk with greater consistency while keeping AI initiatives moving.

Governance affects delivery. The operating question is how to address data and risk concerns with less process drag, clearer ownership, and stronger context at the point of decision.

Which of the factors, if any, have most delayed your organization's ability to launch or scale AI initiatives? Two selections permitted.

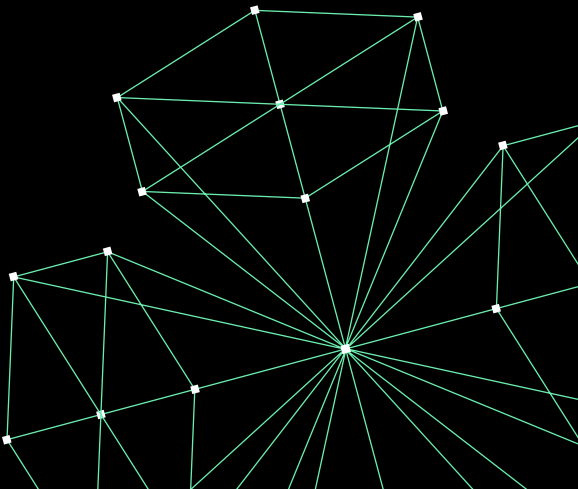


Third-Party AI Runs Through the Full Operating Model

Third-party AI appears at several stages of the survey. Thirty-nine percent identify limited visibility into third-party AI components, vendors, or data sources as a delay factor. Thirty-one percent say third-party or vendor AI tools are among the initiatives most often slowed, paused, or complicated. Nearly a quarter (24%) identify third-party AI risk as a coordination challenge.

The issue also appears in incident experience. Twenty-nine percent report third-party or vendor AI exposure two or more times during the past year. Separately, 28% say vendor AI tools were adopted before full assessment.

Together, the findings show a lifecycle issue. Third-party AI enters through procurement, business adoption, embedded product features, and data flows. Governance needs a consistent way to identify those relationships, assess risk, set conditions, monitor ongoing use, and preserve evidence. A review at the point of purchase covers only part of that cycle.

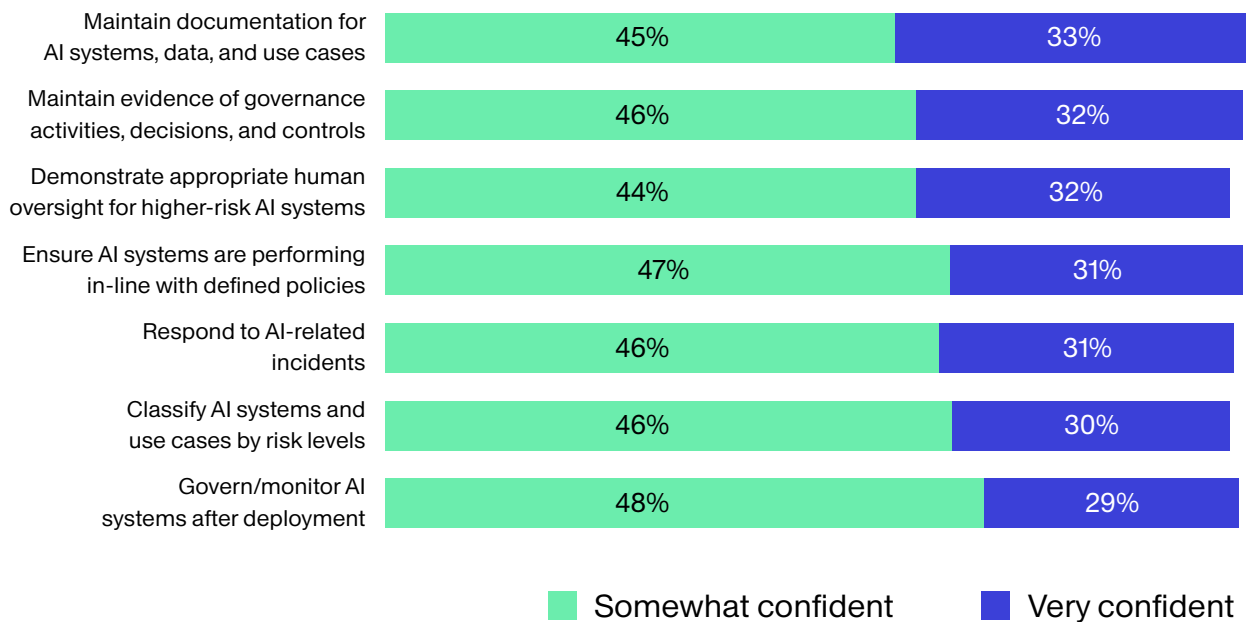




High Confidence and Connected Accountability Tell Different Stories

The contrast between confidence and coordination captures the operating challenge. Roughly three-quarters of respondents feel confident in individual governance activities. Only 5% report clear coordination and accountability across the lifecycle. Teams can be capable within their own responsibilities while the handoffs between them remain unclear or inconsistent.

How confident are you in your organization's ability to perform the following AI governance activities?



The operating gap is between connection and coordination. Governance work exists, while context, ownership, controls, and evidence still move unevenly across the lifecycle.

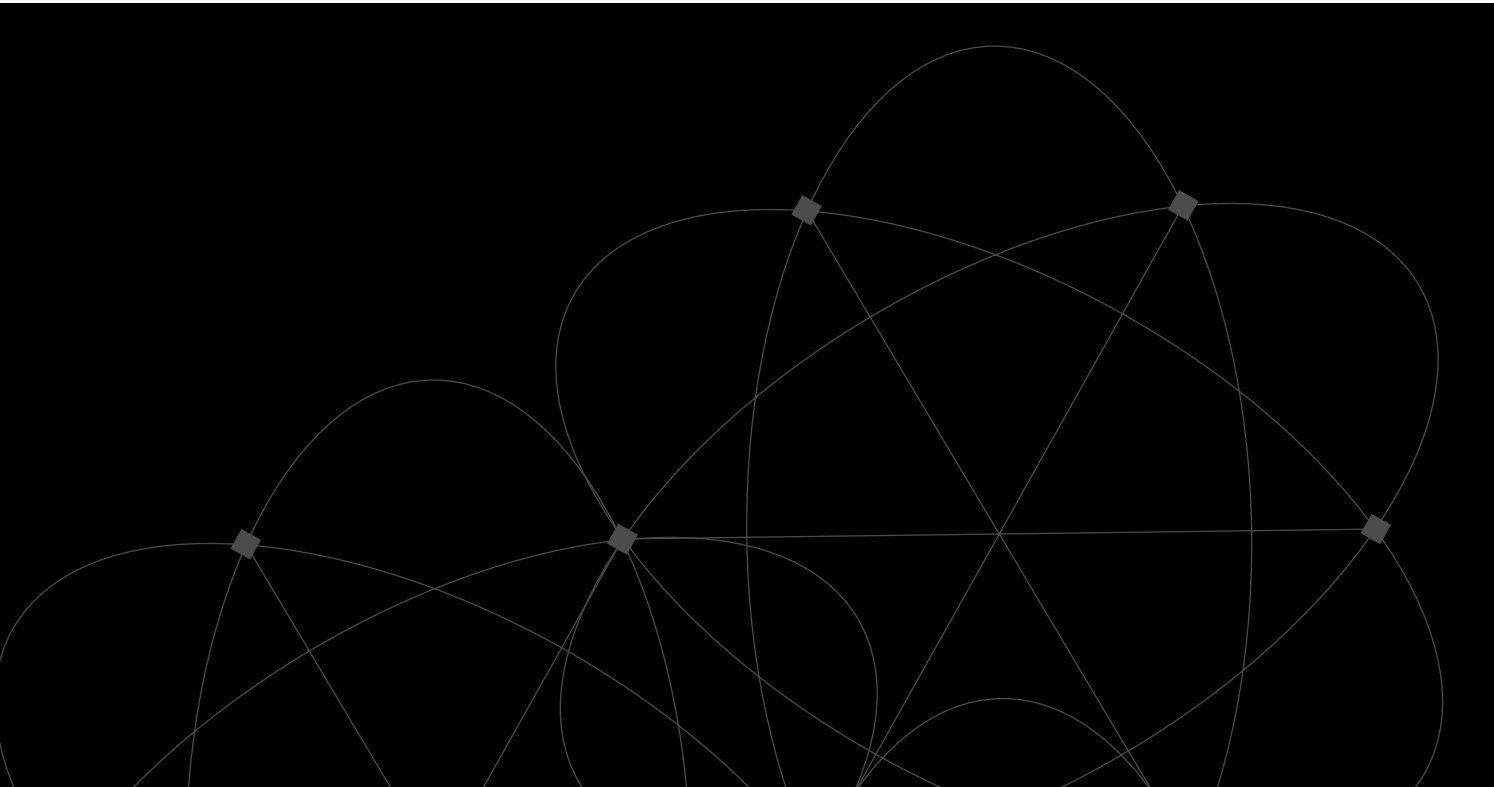
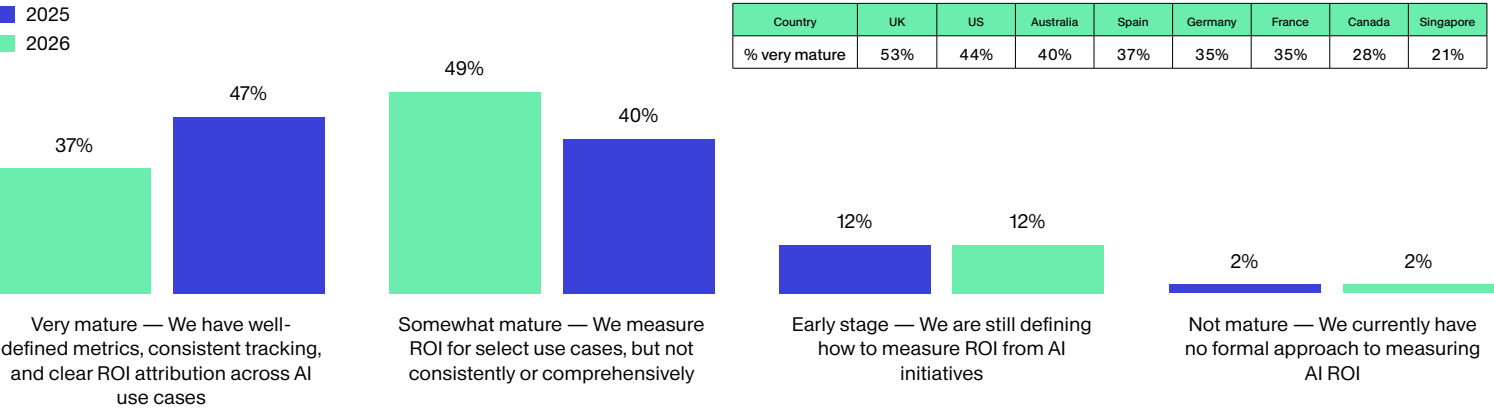
The ROI data reveals a similar tension. Eighty-six percent rate their approach as at least somewhat mature, yet nearly half say measurement is limited to selected use cases and is not consistent or comprehensive. Measuring AI performance, value, or business impact is also the most frequently cited coordination challenge. This suggests that ROI measurement may be established in parts of the organization without yet being consistently connected across teams and use cases.

A connected operating model links the work. Inventory provides a shared record of systems, use cases, agents, vendors, and owners. Classification supplies a common

view of risk. Review and approval translate that context into decisions, and policies become technical and workflow controls. Monitoring continues after deployment and evidence stays attached to decisions.

The survey shows that many organizations have several of these elements. The next step is making them operate as one system. That connection reduces repeated work, clarifies accountability, and gives teams the context they need to make timely decisions.

How mature is your business in measuring the value and return on investment (ROI) of its AI system?





Chapter 4

Investing in Governance to Move Forward

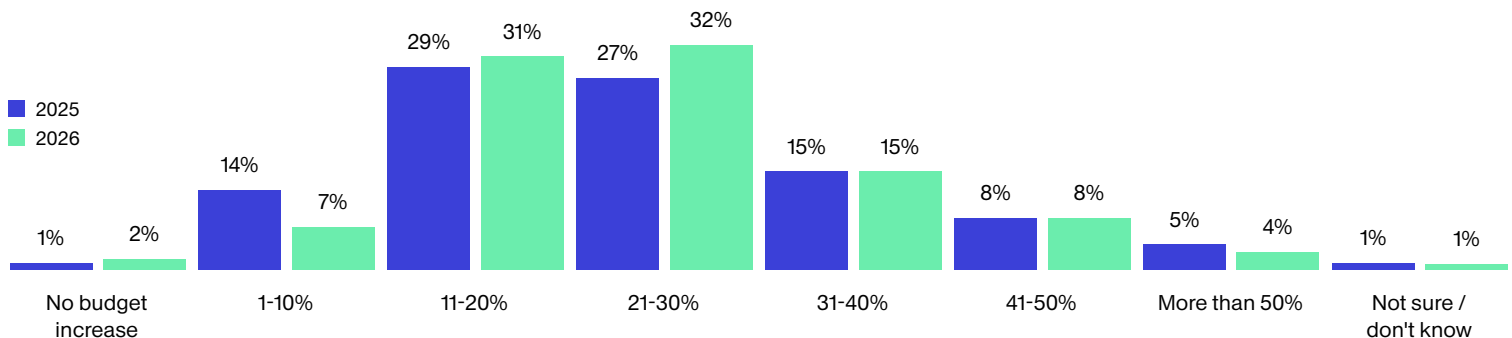
Risk Management is Taking More Time

The overwhelming majority of respondents (80%) say their function spends more time managing AI-related risk than it did 12 months ago. Among respondents overall, the average net increase in time spent managing AI-related risk was 26%. This measures a growing operating workload that includes review, coordination, monitoring, incident response, and evidence.

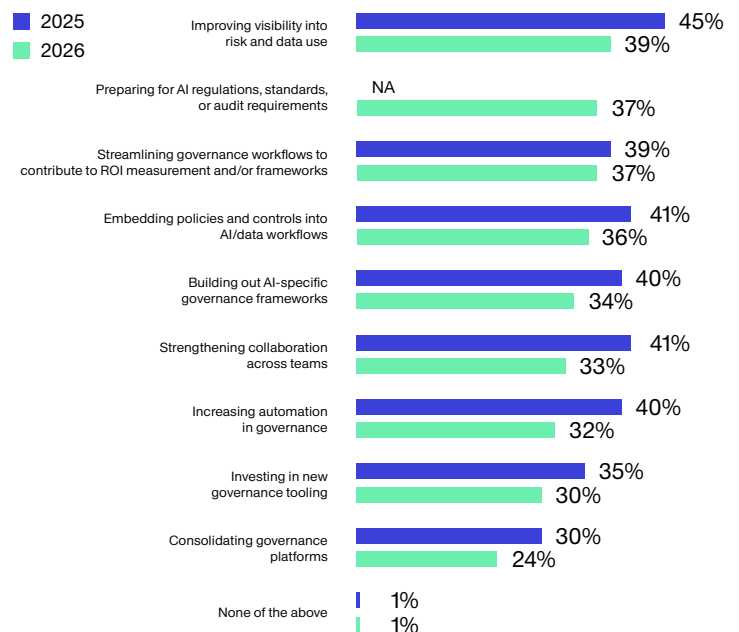
In 2025, 86% reported an increase, with an average of 37% lift in working hours. This year's results still show broad growth in effort, but a lower average increase. The distribution points to more incremental increases as AI risk management becomes part of ongoing operations.

The comparison provides context rather than a strict trend line. The 2026 study added Australia and Singapore, replaced the CIO audience with CMO respondents, and included a larger share of companies with more than \$500 million in annual revenue.

By how much is your organization planning to increase its budget in the next financial year to support modernization of technologies for governing AI?



Which of the following, if any, reflect governance related priorities of your organization for the next 12 months? Select all that apply.





Year-Over-Year Context

The contrast between confidence and coordination captures the operating challenge. Roughly three-quarters of respondents feel confident in individual governance activities. Only 5% report clear coordination and accountability across the lifecycle. Teams can be capable within their own responsibilities while the handoffs between them remain unclear or inconsistent.

Measure	2025	2026
Respondents reporting more time managing AI-related risk	86%	80%
Average change in time spent managing AI-related risk	+37%	+26%
Respondents planning an AI governance technology budget increase	98%	98%
Average planned budget increase	+24%	+25%

Source: OneTrust 2026 AI Governance Survey, Q4 and Q16. 2026 base: n=1,200. 2025 base: n=1,250. Comparisons provide context because the audience and market mix changed between studies.

Incidents are Prompting Stronger Governance Action

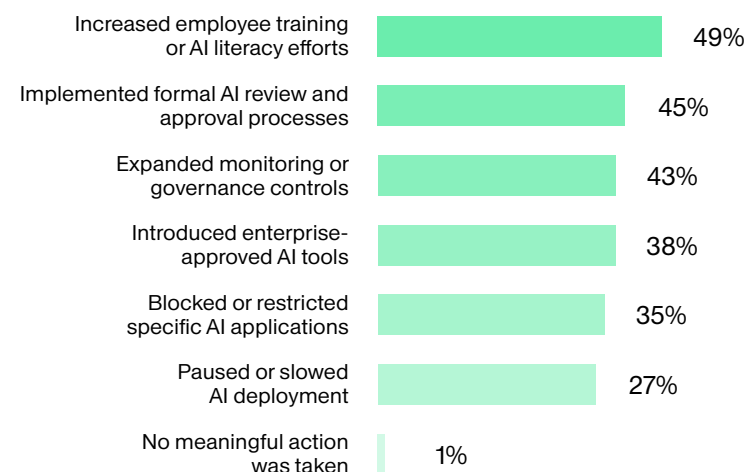
Eighty-six percent of organizations experienced at least one of the nine AI-related incident types tested during the past year. Among those respondents, 99% took meaningful action.

Employee training and AI literacy lead the remediation efforts at 49%. Nearly half (45%) implemented formal AI review and approval processes. Forty-three percent expanded monitoring or governance controls, and 38% introduced enterprise-approved AI tools. More than a third (35%) blocked or restricted specific applications, and 27% paused or slowed AI deployment.

The response pattern is important. Organizations are strengthening the capabilities that support continued AI use. Training addresses employee behavior. Formal review creates a repeatable decision path. Monitoring and approved tools increase oversight. Restrictions and pauses remain part of the response, but they appear less often than actions that improve governance capacity.

Incidents Prompt Stronger Governance Action

After experiencing an AI-related incident in the past 12 months, which of the following actions did your organization take? Select all that apply.





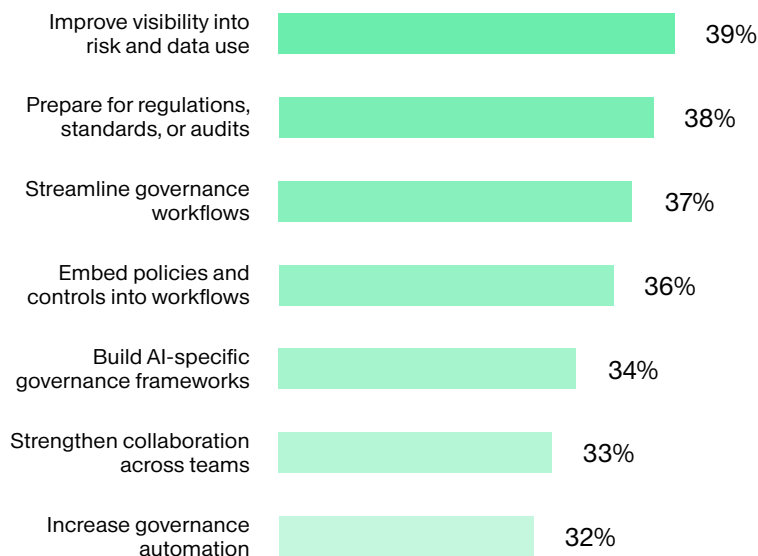
Investment Priorities Show What the Next Operating Model Looks Like

The leading priorities align closely with the gaps reported elsewhere in the survey. Visibility and preparedness lead the way, closely followed by embedding policies and controls into AI workflows.

The next group focuses on program depth and connection, where building AI-specific governance frameworks and strengthening cross-team collaboration are high priority.

Priorities Focus on Visibility, Readiness, and Workflow Integration

Which of the following, if any, reflect governance-related priorities of your organization for the next 12 months? Select all that apply.



Budget growth is broad and sustained

Ninety-eight percent plan to increase budgets for technologies used to govern AI during the next financial year. The average planned increase is 25%. Nearly six in ten expect increases above 20%, including 32% planning a 21% to 30% increase and 27% planning increases above 30%.

The year-over-year benchmark shows sustained commitment. Ninety-eight percent also planned an increase in 2025, with an average of 24%. The share planning an increase holds steady while the mean remains nearly unchanged.

Planned budget growth also stays consistent across the five maturity groups. Average increases range from roughly 24% to 26% across Optimized, Managed, Defined, Developing, and Ad hoc organizations. Investment therefore extends across the market. Earlier-stage programs are building foundations, while advanced programs are improving connection, automation, and scale.

The combination of workload, incidents, priorities, and budget points to a common direction. AI governance is becoming a funded operating capability. Organizations are investing in the people, processes, controls, and technologies needed to keep AI moving with clearer accountability and stronger evidence.

AI governance is becoming a funded operating capability. Investment spans every maturity group, with advanced programs continuing to **modernize visibility, workflows, controls, and evidence.**



Conclusion

What This Means for Enterprise AI Governance

AI governance has entered its operational phase. Adoption is broad, governance activity is established, and investment is sustained. The next challenge is making those elements work together as AI scales across business functions, third parties, and agents.

The survey shows meaningful progress. Fifty-two percent describe governance as integrated or embedded. Organizations perform an average of four governance activities, and confidence in individual capabilities is high. The maturity model places 37% in the Managed or Optimized groups. In those segments, the market is moving in the right direction.

The survey also shows where the operating model needs to advance. Nearly half still rely on reactive, fragmented, slow, or manual processes. Full visibility into sanctioned and unsanctioned use reaches 48%. Agent encouragement reaches 87%, while clear agent governance reaches 47%. Only 5% report clear coordination and accountability across the lifecycle.

Five capabilities define the work ahead:

Continuous visibility	A current view of approved, unapproved, third-party, and agentic AI use.
Scalable governance	Review and decision paths that keep pace with business adoption.
Enforced guardrails	Policies and risk decisions translated into controls within AI and data workflows.
Connected accountability	Clear owners, decision rights, and handoffs across functions and lifecycle stages.
Ongoing evidence	Documentation, monitoring history, approvals, and incident records that support decisions and external requirements.

Organizations are investing because AI adoption is scaling, while agent use, incidents, and growing risk workloads place new pressure on governance operations. Their priorities show a practical response: better visibility, regulatory readiness, streamlined workflows, embedded controls, collaboration, and automation.

The next challenge is connecting existing governance activity into an operating model that can keep pace with AI. The shift from individual governance activities to continuous, connected operations is what AI-Ready Governance requires. It treats readiness as an ongoing operating capability, with context, controls, accountability, and evidence that remain connected as AI changes and expands.

The next challenge is no longer creating governance activity.
It's connecting that activity into an operating model that can keep pace with AI.



Notes From The Field

Real-world use cases of governance implementation show what it takes to move at the speed of AI. BBVA, a OneTrust customer, shared their perspective on AI governance in financial services. The responses below to OneTrust's questions, from the company's Head of AI Governance, Marta Sanz, reflect BBVA's experience and considerations as they advance their AI governance program.

OneTrust: What concrete steps have you taken to operationalize AI governance, and what has worked best so far?

BBVA: Our approach to operationalizing governance is to embed it into the AI lifecycle rather than treating it as a final approval step. We start by understanding the intended use case, the data, models and systems involved, the level of autonomy and access, and the potential impact on customers, employees and the business. This enables us to apply governance proportionately: a low-risk experiment should not follow the same path as an AI solution that supports a material process or can take actions in connected systems.

OneTrust: Where have you felt the most governance friction and how have you adjusted your approach to keep innovation moving while staying responsible?

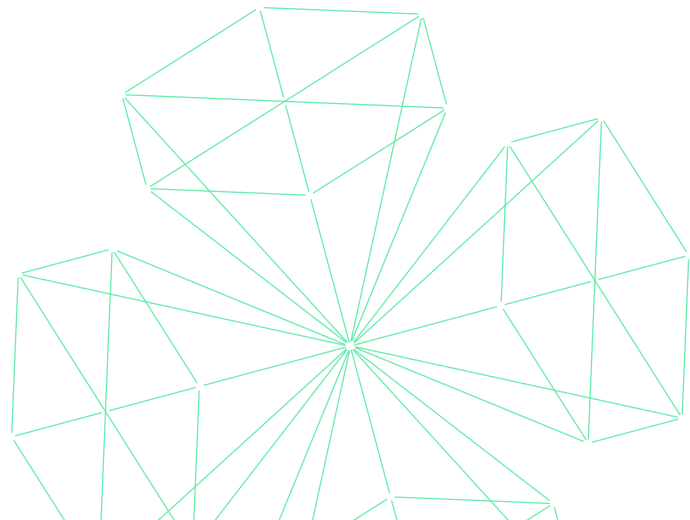
BBVA: We have learned that friction increases when questions are addressed too late, after key design choices have already been made. Our response has been to bring governance earlier into use-case ideation and design, helping teams identify the relevant risk and requirements from the outset. This avoids late redesigns and allows teams to make an informed choice about the appropriate level of autonomy, access, and human oversight.

OneTrust: Looking across the AI lifecycle, how are you clarifying ownership and accountability, and what lessons or advice would you share with peers trying to do the same?

BBVA: We believe accountability must remain meaningful after deployment. AI systems evolve in practice: usage patterns change, new risks emerge and performance can degrade. Monitoring, traceability, human intervention mechanisms, and well-defined escalation paths are therefore as important as the initial assessment.

Our advice to peers is to start with a simple, common language for classifying AI use cases and cases and assigning accountability. The objective is to make accountability clear and governance predictable, so teams can scale innovation with greater confidence and stronger control.

BBVA was named the "World's Most Innovative Bank" by Global Finance in 2026 for its technology use and AI-driven solutions. The publicly traded company now operates in 25 countries globally, serving more than 81 million customers.





Research Notes

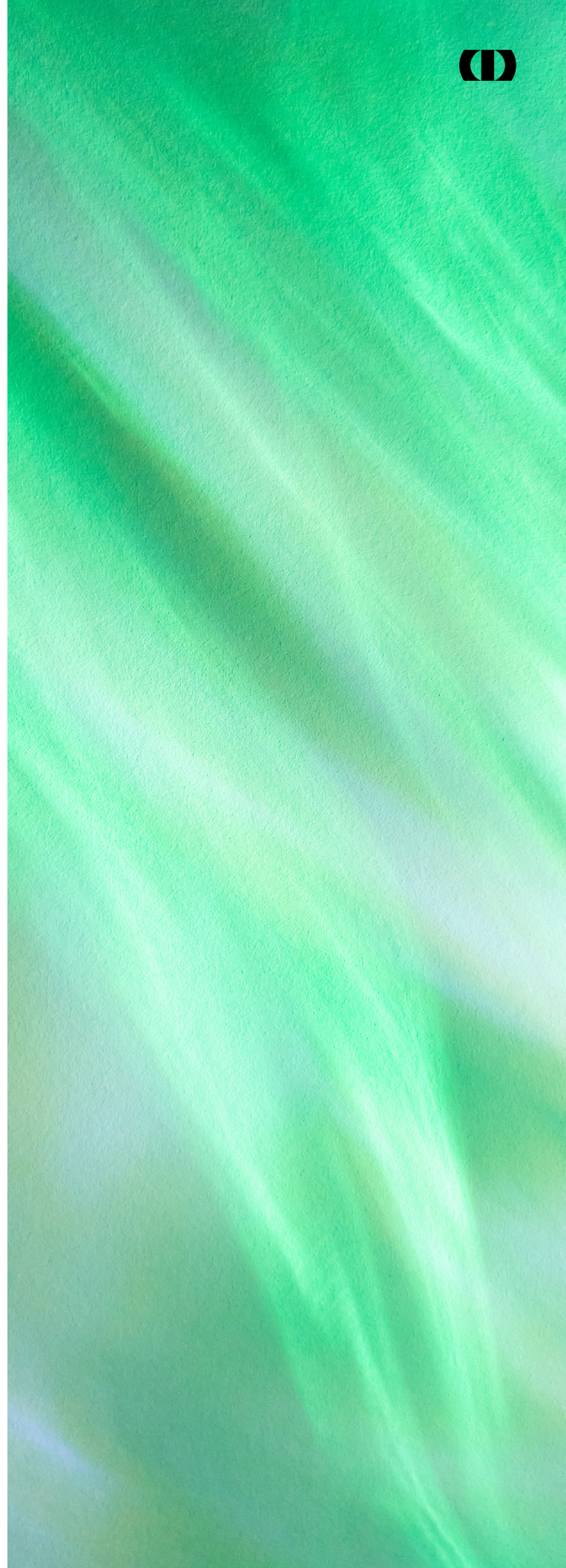
Methodology

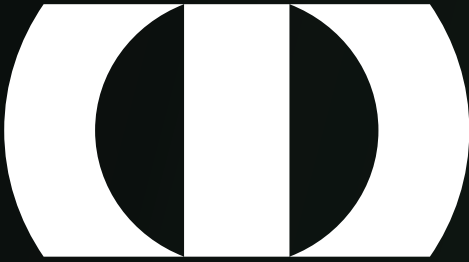
Together, OneTrust and Sapio Research conducted an online survey of 1,200 senior business decision-makers in June and July 2026. Respondents worked in Australia, Canada, France, Germany, Singapore, Spain, the United Kingdom, and the United States. The sample included 300 respondents in each of four audience groups: CPO, CDO, CISO, and CMO. All respondents worked at organizations with at least \$100 million in annual revenue, and 55% worked at organizations with more than \$500 million in annual revenue.

******Unless stated otherwise, results use a base of 1,200.

Question 12 used a base of 1,034 respondents who experienced one or more of the incident types tested in question 11 of the survey. At the 95% confidence level, the overall sample has a margin of error of plus or minus 2.8 percentage points. All percentages are rounded. Totals can differ from 100% because of rounding and multi-select questions.

Year-over-year comparisons use the 2025 study as context. The 2026 report added Australia and Singapore, replaced the CIO segment with CMO respondents, and included a larger share of organizations above \$500 million in annual revenue.





Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document. OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.