Insider risk: Client survey insights 2026

2026

The insider risk challenge is evolving faster than organisational capability

Insider risk is changing rapidly and becoming more complex.

The convergence of employee pressure, access complexity, operational dependency and AI-enabled capability is creating a more interconnected and potentially more damaging threat landscape. Insider risk is no longer solely a cyber, fraud or conduct issue; it is increasingly a business resilience challenge requiring coordinated enterprise-wide management.

Our survey suggests organisations recognise this shift. Nearly half expect insider risk investment to increase over the next 12 months and 60% now view insider risk as an important or critical board-level issue. Yet organisational capability is not evolving at the same pace. Risk assessment, measurement, ownership and monitoring remain inconsistent, while confidence often exceeds demonstrated preparedness.

A gap is emerging between the pace at which insider risk is evolving and the maturity of organisational responses. Leading organisations are strengthening insider risk capabilities and governance, while others continue to rely on fragmented ownership, reactive processes and legacy controls.

The findings suggest three priorities for organisations:

1. Reassess insider risk through an enterprise-wide lens.
2. Accelerate preparedness for AI-enabled threats.
3. Build integrated insider risk capabilities and establish clear accountability.

Organisations that fail to adapt, risk leaving critical vulnerabilities unaddressed. As insider threats become more sophisticated and harder to detect, these weaknesses are likely to be exploited more frequently and with greater impact, increasing the potential for significant operational, financial and reputational harm.

60%

Now view insider risk as an important or critical board-level issue.

33%

Reported experiencing an insider-related incident in the last 12 months.

47%

Expect insider risk investment to increase over the next 12 months.

0%

Feel very well prepared for AI-driven insider risk.

Five signals shaping insider risk in 2026

PwC's survey of senior leaders across multiple sectors helped generate insights on how different organisations approach insider risk. Five key takeaways emerged.

01

Peer comparison: Most feel 'average' - but average isn't good enough.

02

Capability gaps are emerging: Risk assessment, ownership and monitoring are not keeping pace.

03

AI is the inflection point: AI is an emerging risk amplifier, yet 0% of respondents feel very well prepared.

04

Known incidents are only part of the challenge: One in three organisations have been hit in the last 12 months.

05

Investment is increasing – but not evenly: Nearly half plan to invest more, but a third are standing still.

How organisations are responding

Operating model enhancements

- Establishing clearer governance and executive accountability.
- Creating cross-functional coordination forums across HR, Security, Legal and Compliance.
- Introducing more formalised escalation and investigation processes.
- Aligning insider risk activities with wider cyber, conduct and operational risk frameworks.

Control and monitoring enhancements

- Expanding monitoring of privileged access and high-risk user activity.
- Improving visibility of behavioural and technical risk indicators.
- Strengthening access management and role-based control models.
- Increasing investment in insider-specific detection and analytics capabilities.

Workforce culture enhancements

- Enhancing insider risk awareness and behavioural training.
- Improving speak-up and reporting culture.
- Increasing focus on high-risk roles and sensitive access populations.
- Developing more proactive approaches to AI-related insider risk exposure.

Future state operating principles

Enterprise-wide ownership

- Insider risk owned as a business wide risk rather than a siloed cyber or HR issue
- Clear governance, escalation routes and decision-making accountability across functions
- Executive sponsorship aligned to broader operational, cyber and conduct risk priorities.

Human and technical signal integration

- Consistent standards and approaches applied across business functions and geographies.
- Better coordination between HR, Security, Legal, Compliance and Technology teams.
- Shared visibility of control gaps, investigations and emerging risk indicators.

Continuous risk reassessment

- Improved visibility of behavioural, operational and technical risk signals across the organisation.
- Use of integrated data and analytics to identify anomalous activity earlier.
- Continuous reassessment of insider risk exposure as workforce models and technologies evolve.

Five 'no regret' actions for firms wanting to enhanced insider risk management capability

01

Strengthen enterprise ownership of insider risk

Many organisations still manage insider risk through fragmented functions, resulting in inconsistent accountability, duplicated effort and limited executive visibility.

02

Reassess insider risk frameworks to capture the full breadth of the threat

Insider risk is often assessed too narrowly through isolated fraud, cyber or HR lenses. Organisations should broaden risk assessments to reflect the interconnected nature of poeple, process, technology and emerging AI-enabled risks.

03

Enhance monitoring and detection capability

Monitoring approaches are often siloed, partial or patchy, making it difficult to identify broader behavioural patterns, escalation indicators and cross-functional risk signals.

04

Build a more proactive insider risk posture

Many organisations still operate reactively, relying on incident response after issues emerge. Leading organisations are shifting toward continuous monitoring, prevention and early intervention.

05

Increase preparedness for AI-enabled insider risks

AI is increasingly viewed as a force multiplier for insider threat activity, yet preparedness levels remain relatively immature across many organisations.

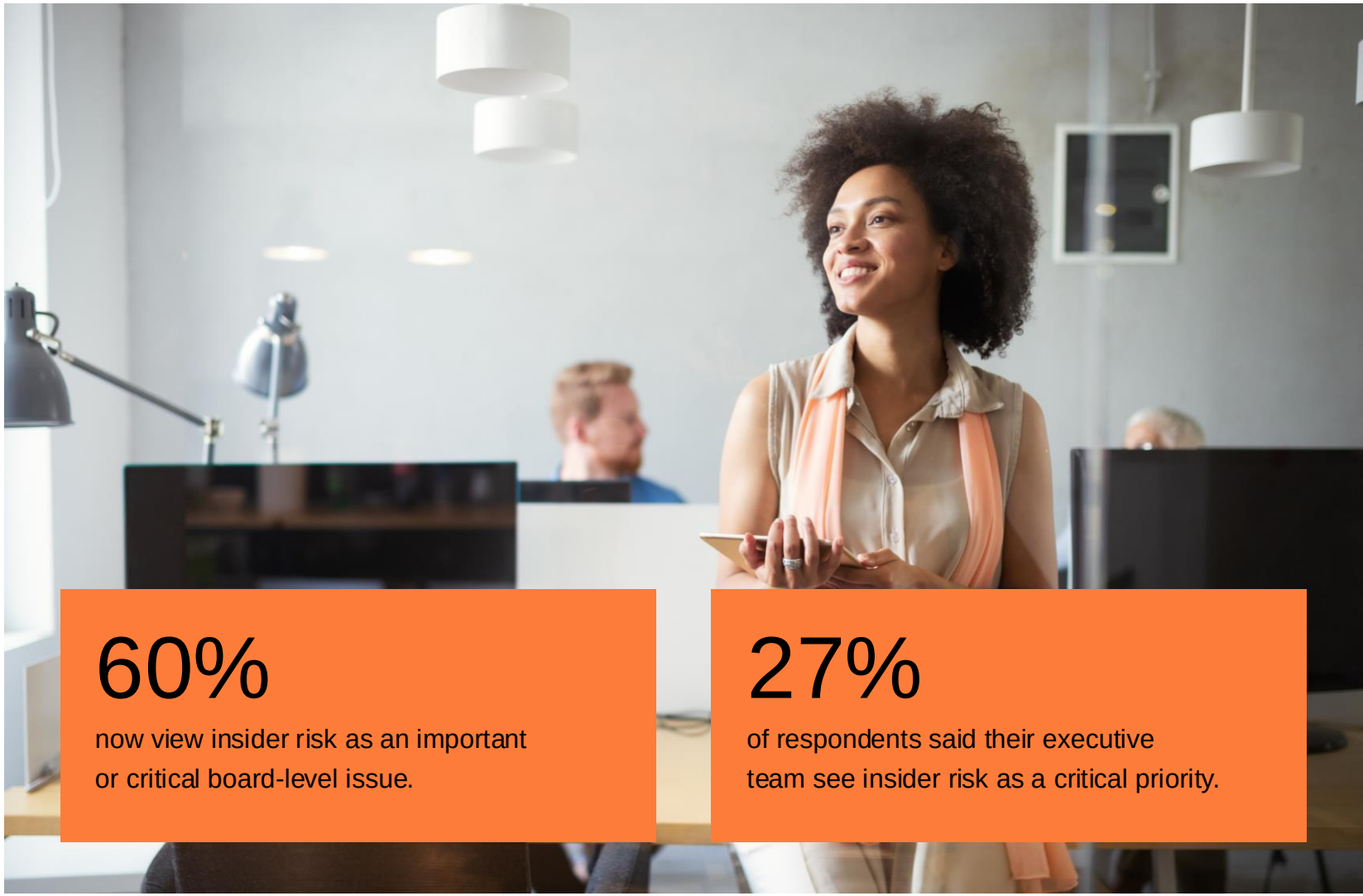
Appendix: Survey results

Methodology and respondent profile

Awareness is growing, but urgency is limited

Survey overview

The data and findings in this report is informed by a survey conducted between December 2025 and February 2026 by PwC UK's Enterprise Risk and Forensics practice. All data refers to results from the survey. The findings are anonymous, with aggregated results reported. Survey participants were senior leaders in Risk, Legal, Finance and Technology representing a range of industries including Financial Services, Retail, Sport and Leisure. Participants were drawn from organisations of varying scale and geographic scope, including global institutions, major UK-based corporates, and smaller high-growth and specialist organisations.



60%

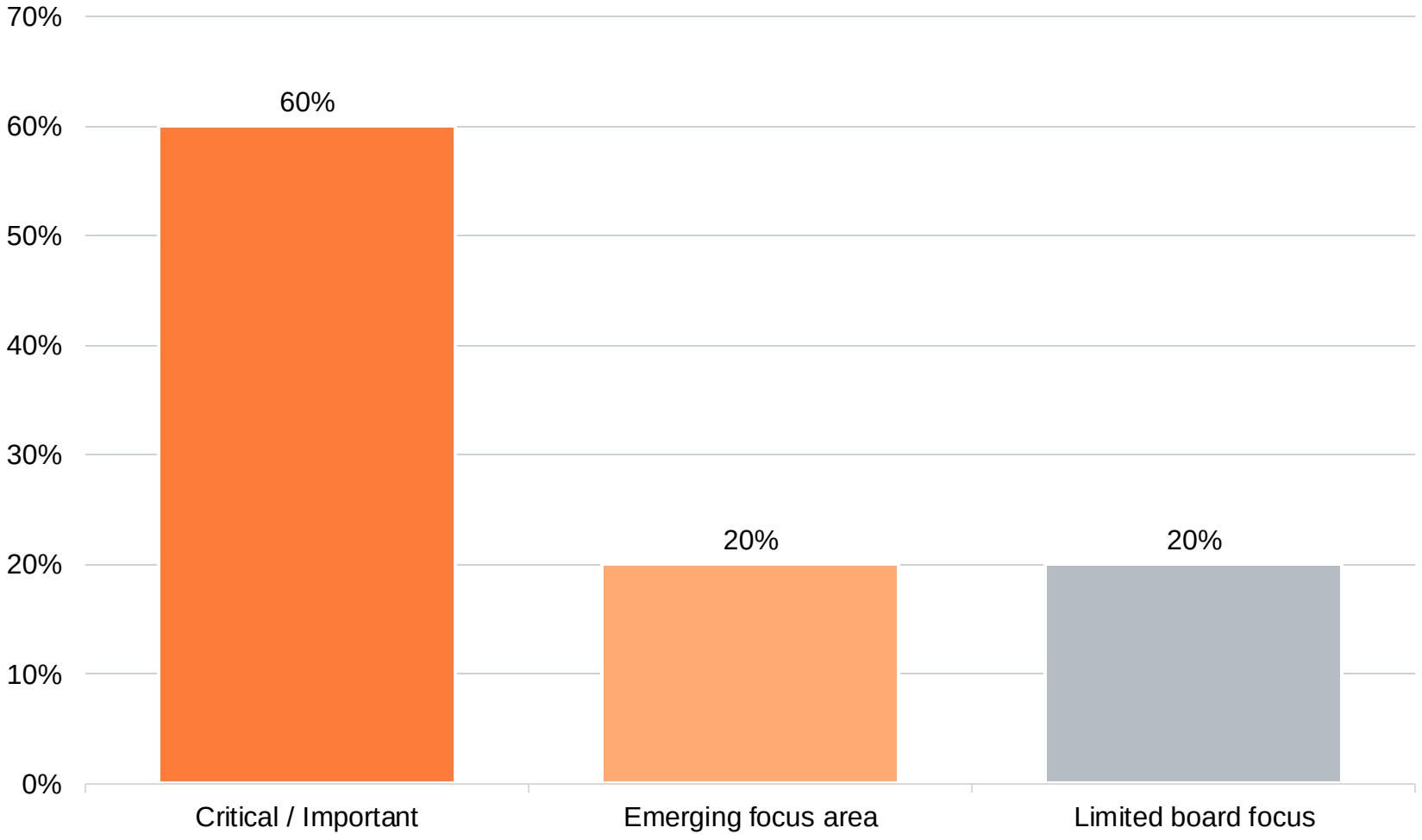
now view insider risk as an important or critical board-level issue.

27%

of respondents said their executive team see insider risk as a critical priority.

Insider risk is gaining board attention, but remains inconsistently prioritised

Current board-level prioritisation of insider risk



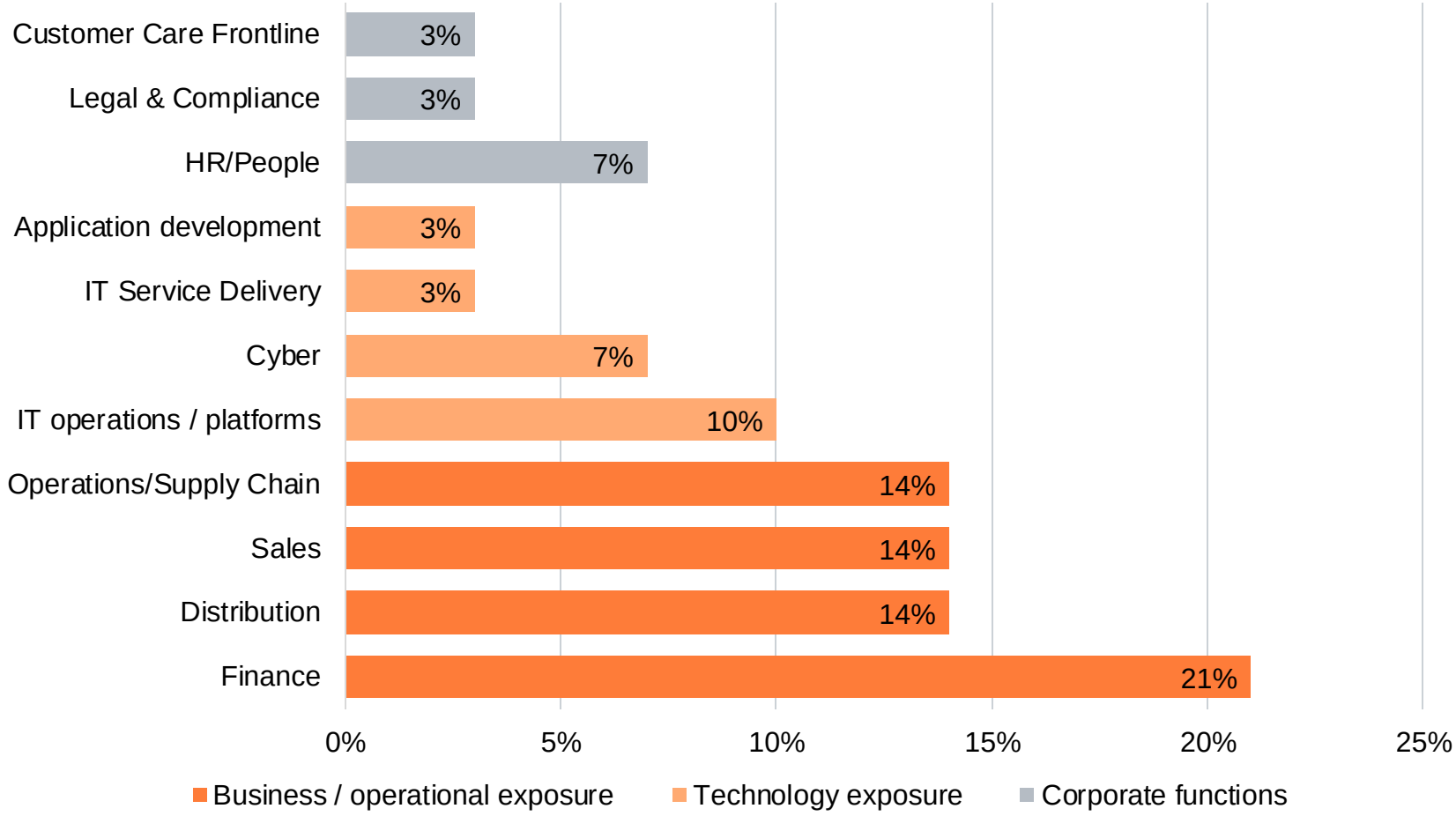
60%

now view insider risk as an important or critical board-level issue.

Board awareness is increasing, but maturity remains uneven. Without clear ownership, insider risk is often managed reactively and in silos rather than as a coordinated enterprise risk. As insider threats become more interconnected and AI-enabled, boards are increasingly expected to provide clearer governance and accountability.

Insider risk exposure is increasingly enterprise-wide

Functions viewed as most exposed to insider risk



63%

identified business and operational functions as the primary areas of insider risk exposure.

Organisations will increasingly require coordinated governance across Cyber, HR, Legal, Operations, Supply Chain and Risk functions.

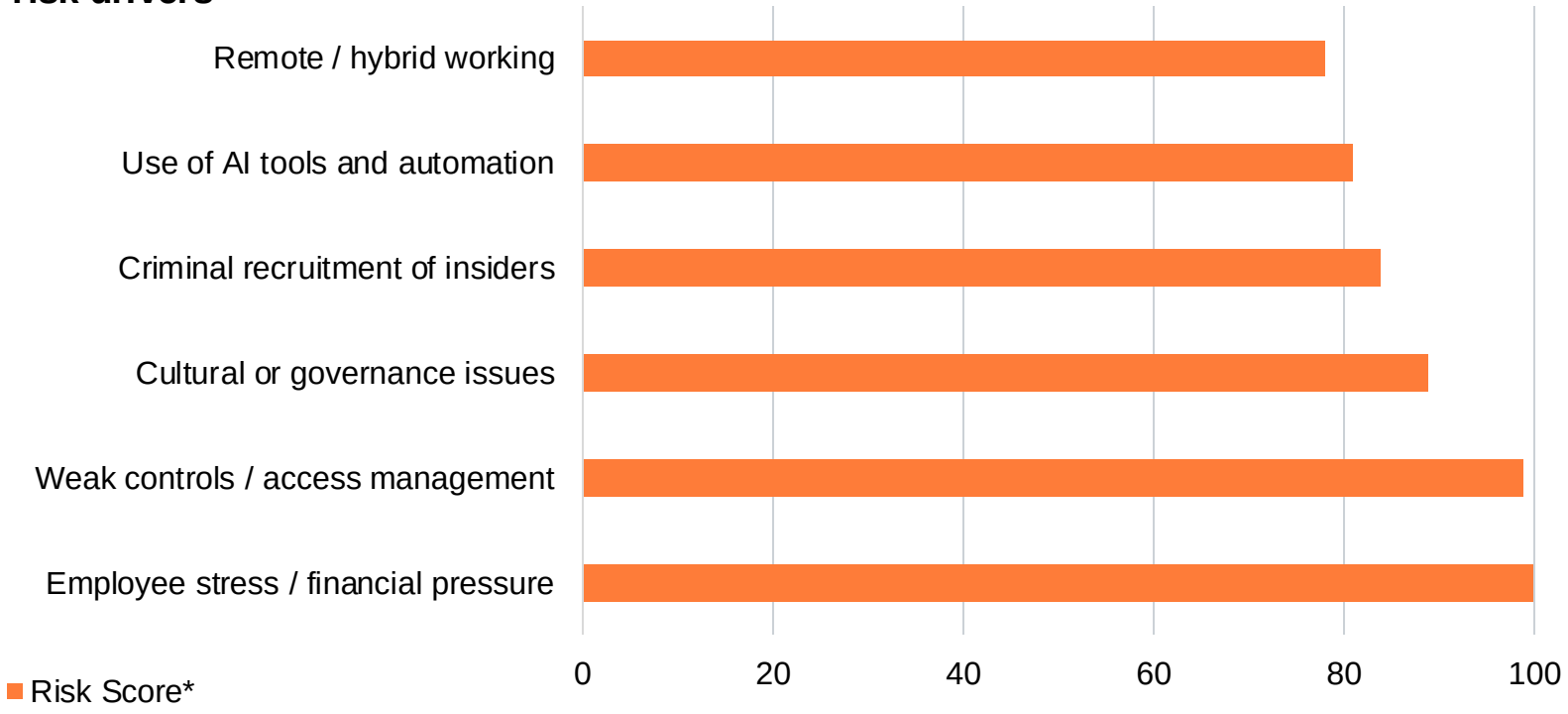
Insider risk exposure is increasingly enterprise-wide. Traditional siloed approaches are becoming less effective against increasingly interconnected and AI-enabled insider threats.

A perfect storm is amplifying insider risk

Headline hierarchy:

- Human pressure is rising – Employee stress and financial pressure is the highest-scoring driver.
- Weak controls create opportunity – Access management gaps remain a core enabler.
- AI is the emerging amplifier – Increasing the speed, scale and sophistication of insider activity.

Key risk drivers



No single driver dominates

The highest ranked factors span people, governance, controls and technology, reinforcing that insider risk is increasingly driven by a combination of interconnected risks rather than isolated issues.

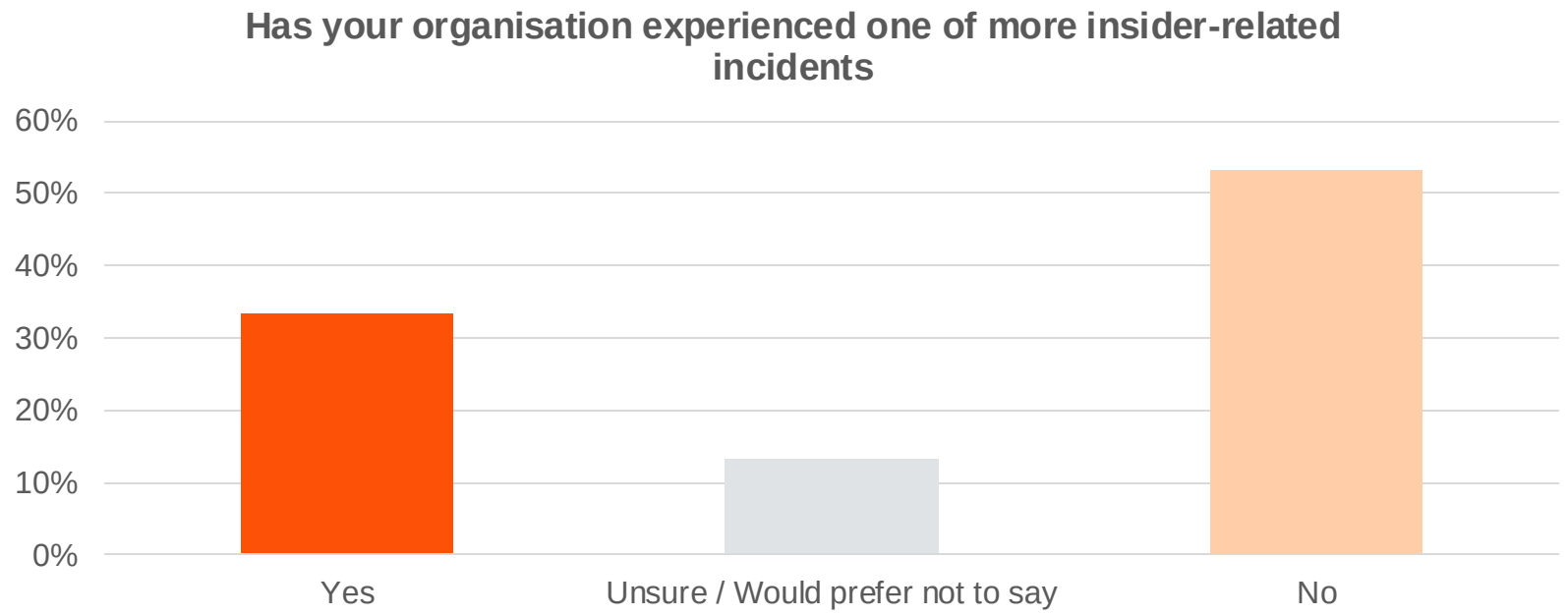
Insider risk is no longer just a people issue or a control issue.
It is a convergence risk where human pressure, access gaps and AI-enabled capability combine to amplify potential harm. Insider risk is therefore becoming more interconnected, more difficult to detect, and potentially more damaging.

*Risk priority index based on weighted respondent rankings; highest-scoring response indexed to 100.

Insider risk is often more prevalent than organisations recognise

Headline hierarchy:

- Insider-related incidents may be more common than organisations currently recognise or formally classify.
- One-third of respondents reported experiencing an insider-related incident, while uncertainty levels suggest visibility and classification challenges persist.
- Many organisations may be identifying operational, fraud or cyber incidents without recognising the underlying insider contribution.



33%

reported experiencing an insider-related incident.

The level of uncertainty (13%) also suggests that many organisations may lack a consistent framework for identifying and classifying insider-related incidents.

Insider risk is frequently under-recognised. Client conversations consistently suggest that insider risk is rarely an isolated incident category. When significant cyber, fraud, conduct or operational events are examined in detail, a direct or indirect insider element is often present somewhere in the chain of events.

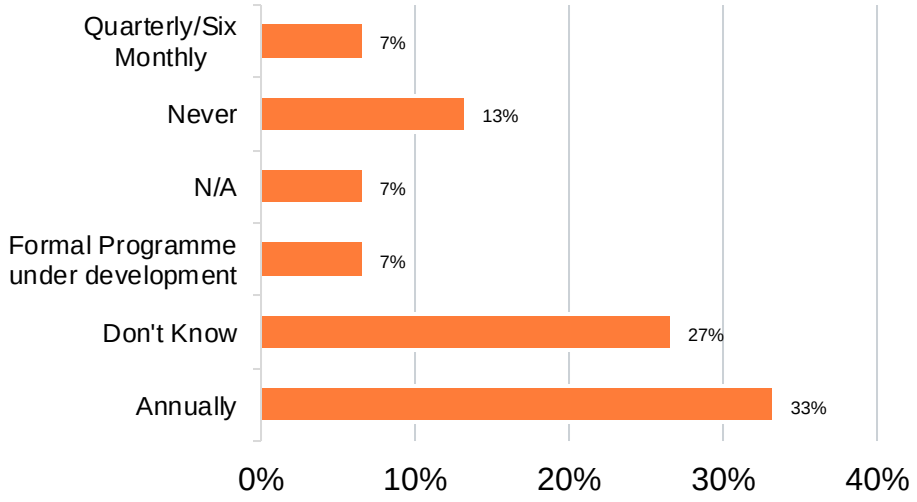
As a result, organisations may underestimate their true insider risk exposure because incidents are frequently categorised by outcome rather than by the human factors that contributed to them.

Programme maturity – Measurement and reassessment

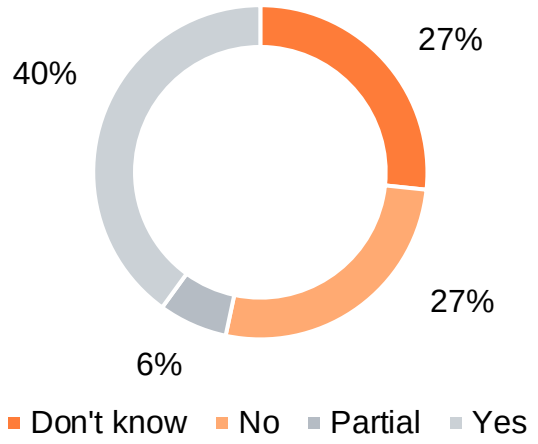
Headline hierarchy:

- Some organisations are demonstrating increasing maturity through reassessment and programme maturity activity.
- However, reassessment and effectiveness measurement remain inconsistent across the sector.
- Many organisations still lack structured mechanisms to validate whether insider risk controls and programmes are operating effectively.

How do you measure the effectiveness of your insider risk program today?



Have you undertaken a holistic reassessment of insider risk within the last 12 months?



40%

report conducting a holistic insider risk assessment within the last 12 months

The key findings suggest **organisations are increasingly recognising the need for formal insider risk reassessment** and programme measurement. However, approaches remain inconsistent, with many organisations still lacking mature mechanisms to validate effectiveness and drive continuous improvement.

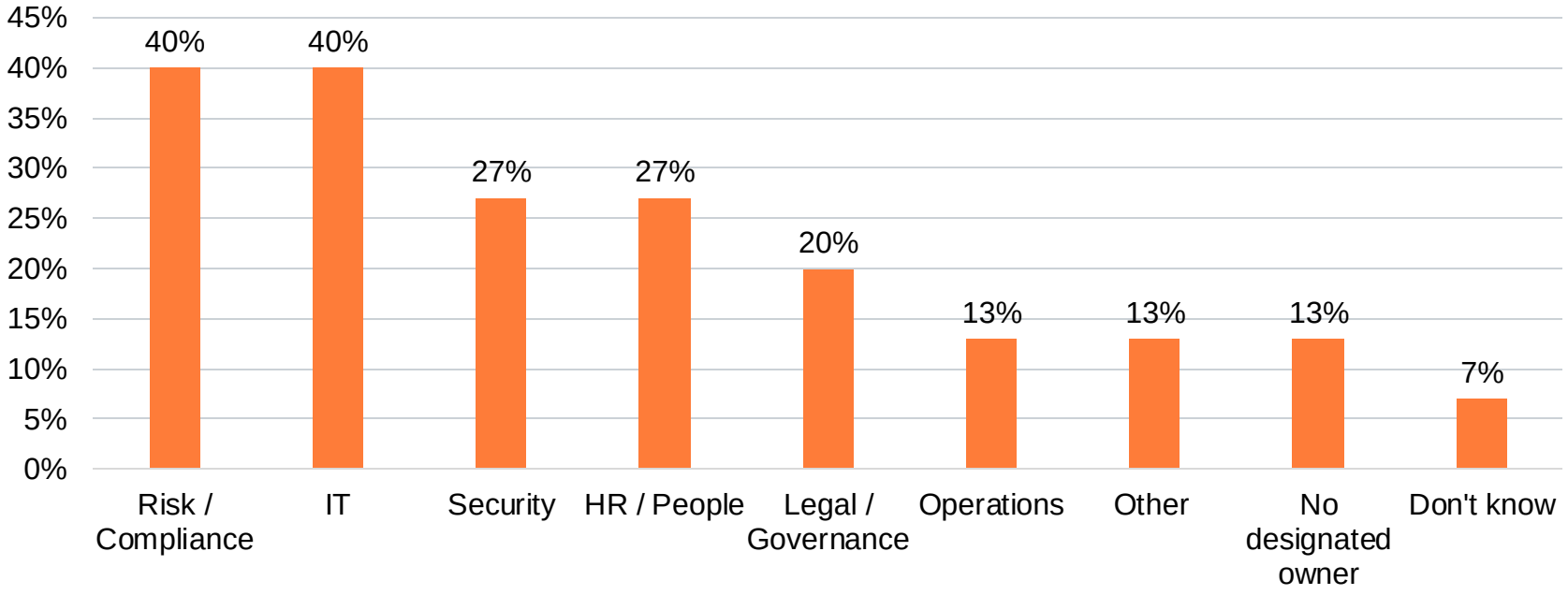
As insider risk drivers continue to evolve, periodic reassessment should become a core element of programme governance.

Who owns insider risk?

Headline hierarchy:

- Ownership of insider risk is typically distributed across Risk, IT, Security, HR and Legal functions.
- While shared ownership models can support broad coverage, fragmented accountability may create governance and coordination challenges.
- A notable proportion of organisations still report having no formally designated owner for insider risk management.

Which functions in your organisation currently 'own' insider risk management?



13%

report having no designated owner for insider risk management.

Insider risk ownership appears highly distributed across Risk, IT, Security, Legal and HR functions.

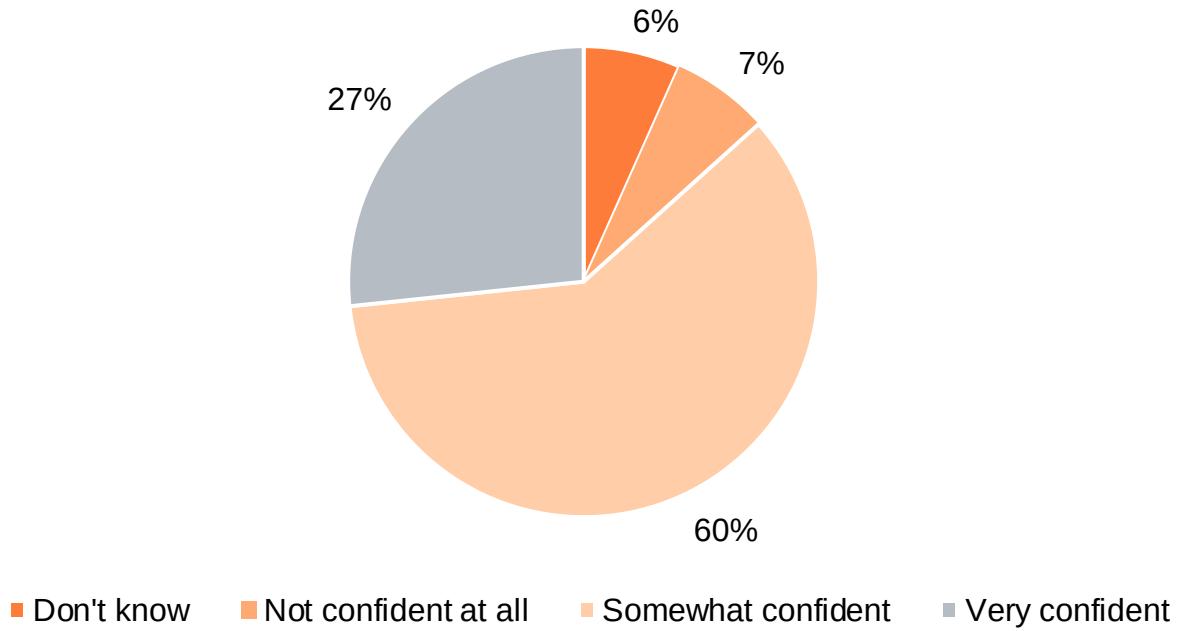
While shared ownership models can support cross-functional coverage, fragmented accountability may reduce coordination, clarity of ownership and governance effectiveness – particularly where no formal ownership model exists.

Confidence in detection and response may be overstated

Headline hierarchy:

- Only a minority of organisations express strong confidence in their insider risk response capability.
- Moderate confidence may mask underlying gaps in preparedness and governance maturity.
- Survey findings suggest a potential disconnect between perceived capability and operational readiness.

How confident are you that your organisation has effective measures to detect and respond to insider risk?



Only

27%

report being very confident in their organisations ability to detect and respond to insider risk.

Strong confidence in insider risk detection and response capability remains limited

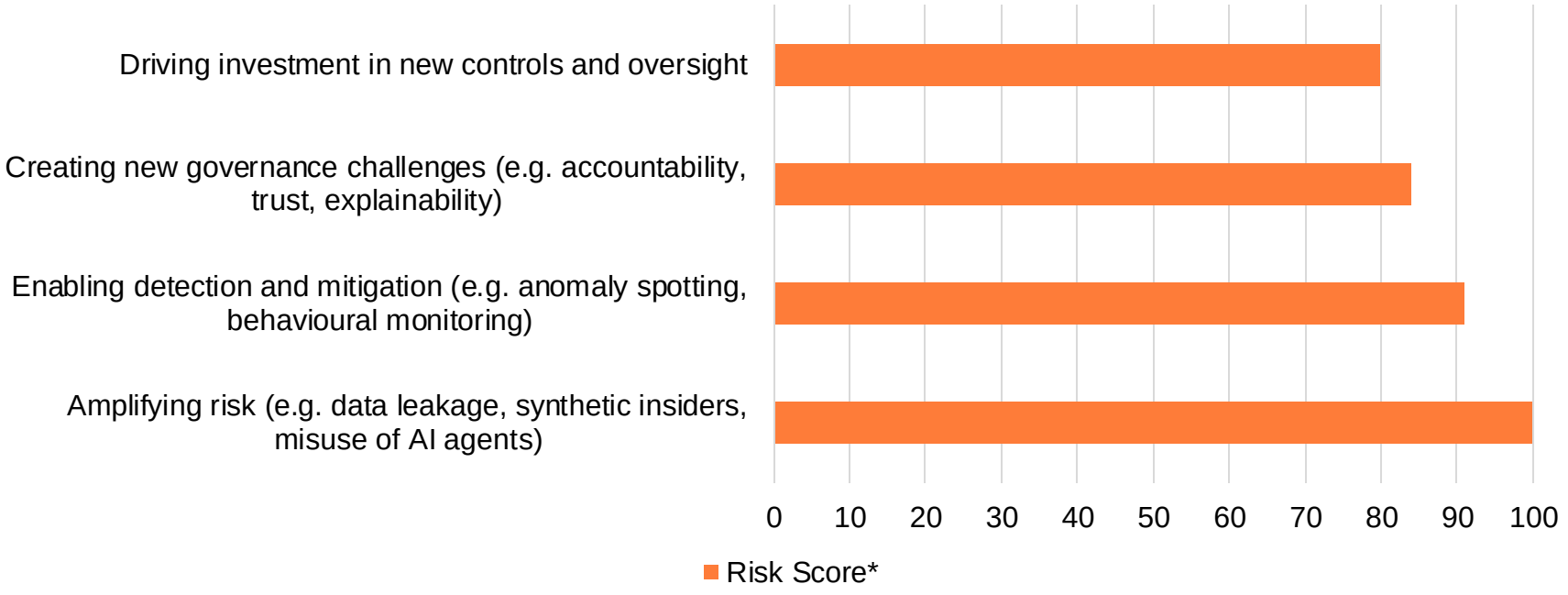
The large proportion reporting only ‘somewhat confident’ may indicate uncertainty or potential overconfidence, particularly given the maturity and assessment gaps identified elsewhere in the survey.

AI – The game changer

Headline hierarchy:

- AI is changing the scale, speed and complexity of insider risk.
- Emerging risks extend beyond technology into governance, workforce capability, and oversight.
- AI is likely to create a two-speed resilience landscape, where organisations with mature insider risk capabilities gain a disproportionate advantage in prevention, detection and response, while those relying on legacy controls face a rapidly expanding exposure gap.

Risk score[1]



Key insights:

- AI is viewed primarily as a risk amplifier.
- Detection and behavioural monitoring are emerging opportunity areas .
- Respondents also highlighted governance and accountability concerns.

AI is reshaping insider risk in two ways:

1. It lowers the barriers to insider harm, enabling greater scale and sophistication with less effort or expertise.
2. It is accelerating the divide between leaders and laggards, making governance, workforce capability and monitoring maturity key determinants of resilience.

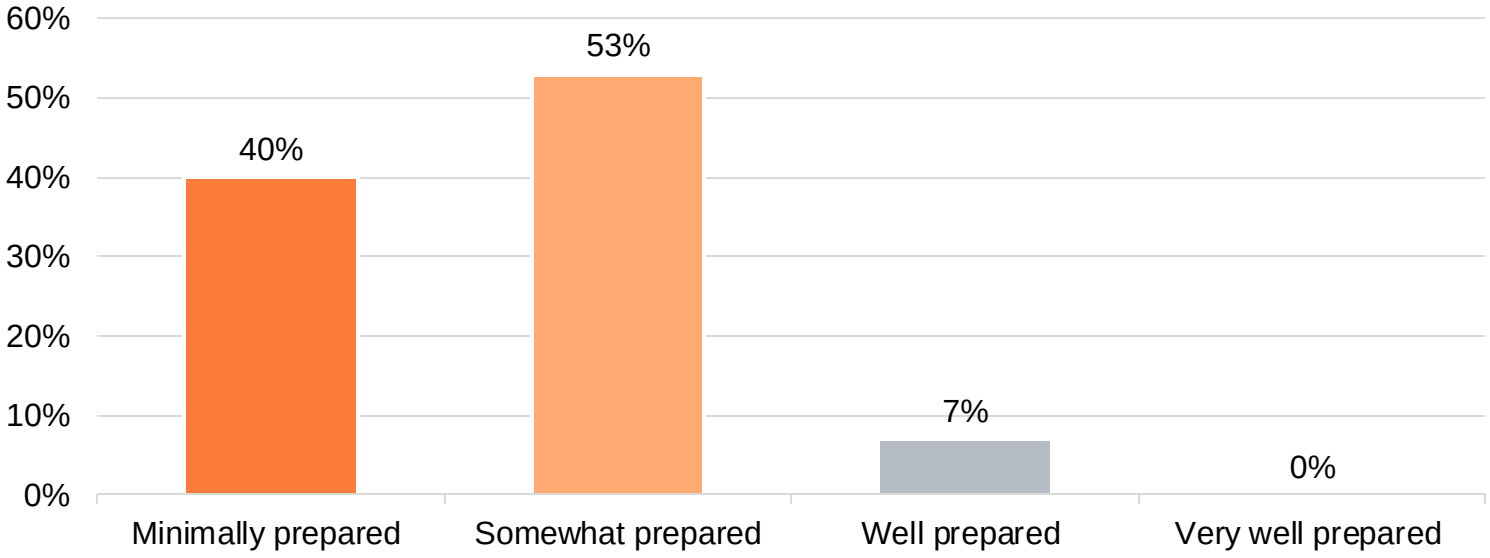
*Risk priority index based on weighted respondent rankings; highest-scoring response indexed to 100.

Preparedness for AI-Driven insider risk remains low

Headline hierarchy:

- Organisations recognise AI-driven insider risk, but few believe they are well prepared to manage it.
- Preparedness appears immature, with many respondents reporting only limited formal action or capability development.
- AI adoption may be outpacing governance, monitoring and workforce readiness.

How prepared do you feel your organisation is to address the potential increase in insider risk driven by AI



Minimal: We are aware of the issue but have not taken formal steps.
Somewhat: We have started to put in place initial policies, procedures, training or monitoring.
Well prepared: We have clear governance, controls, and response mechanisms in place.
Very well prepared: We have a mature and proactive approach, with continuous monitoring and adaptive controls specifically for AI-related risks.

0%

feel very well prepared.

40%

minimally prepared.

AI related insider risk is widely recognised, **but organisational preparedness remains immature**.

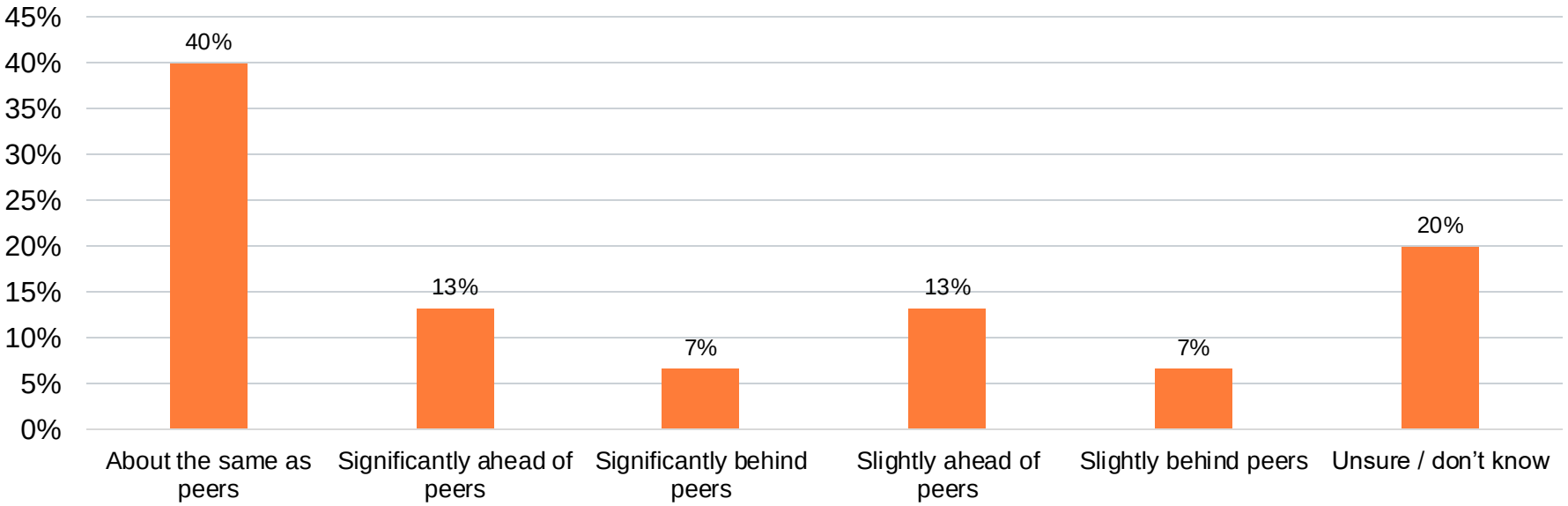
This reinforces broader survey findings showing gaps between perceived confidence and actual readiness.

Peer benchmarking may be masking maturity gaps

Headline hierarchy:

- Many organisations believe they are performing in line with peers, despite broader evidence of low sector-wide maturity.
- Benchmarking against an under-prepared market may create false assurance around insider risk readiness.
- Relatively few respondents acknowledge being materially behind peers, despite widespread gaps elsewhere in the survey.

How do you believe your organisation's approach to insider risk management compares to others in your sector?



14%

acknowledge being behind peers on insider risk management maturity (7% slightly behind, and 7% significantly behind peers).

Benchmarking against peers may be creating false assurance.

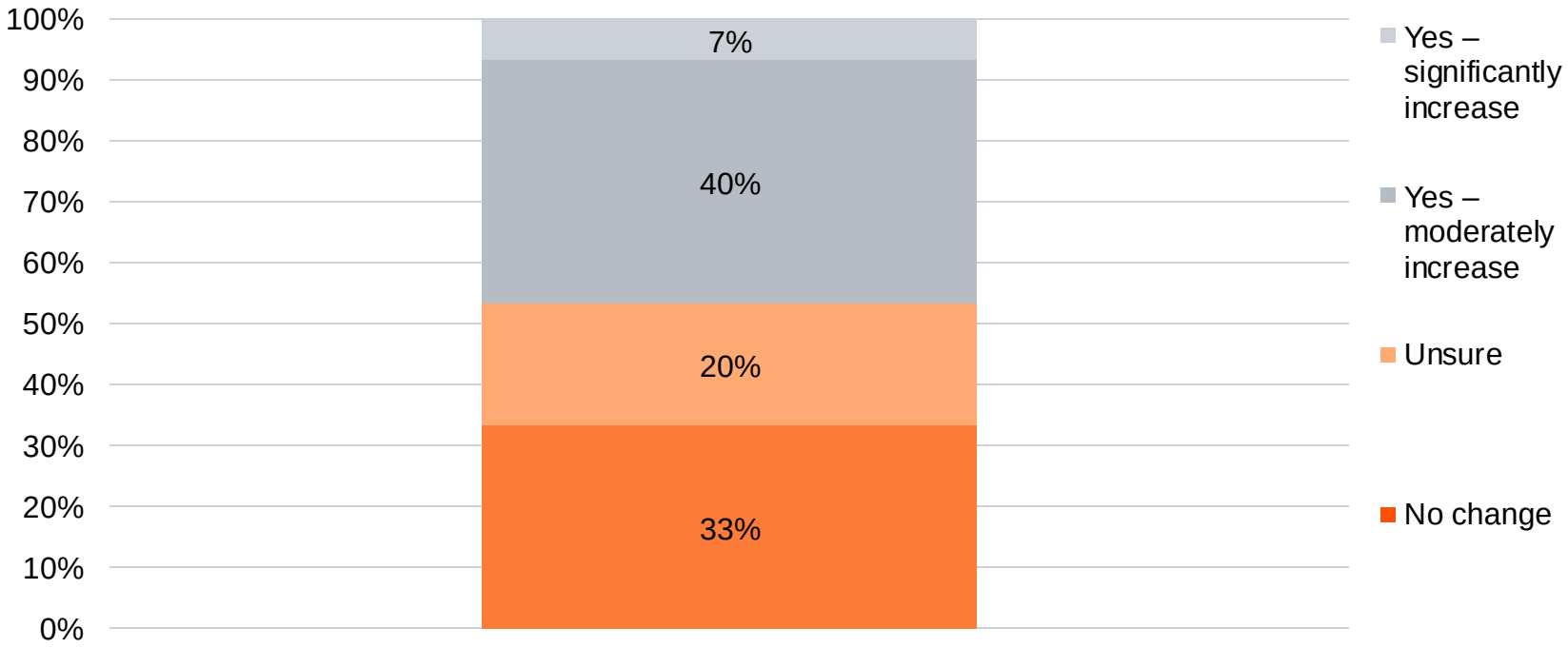
In a sector where broader survey findings indicate limited preparedness and governance maturity, being perceived as 'average' may still represent elevated insider risk exposure.

Investment divergence may widen maturity gaps

Headline hierarchy:

- Nearly half of organisations expect insider risk investment to increase over the next 12 months
- Investment growth suggests rising recognition of insider risk as a strategic issue.
- However, a significant proportion report no planned increase in investment, potentially increasing the risk of falling behind more mature peers.

Do you expect to increase investment in insider risk management over the next 12 months?



47%

expect insider risk investment to increase over the next 12 months

Rising investment suggests organisations increasingly recognise insider risk as a growing strategic and operational issue.

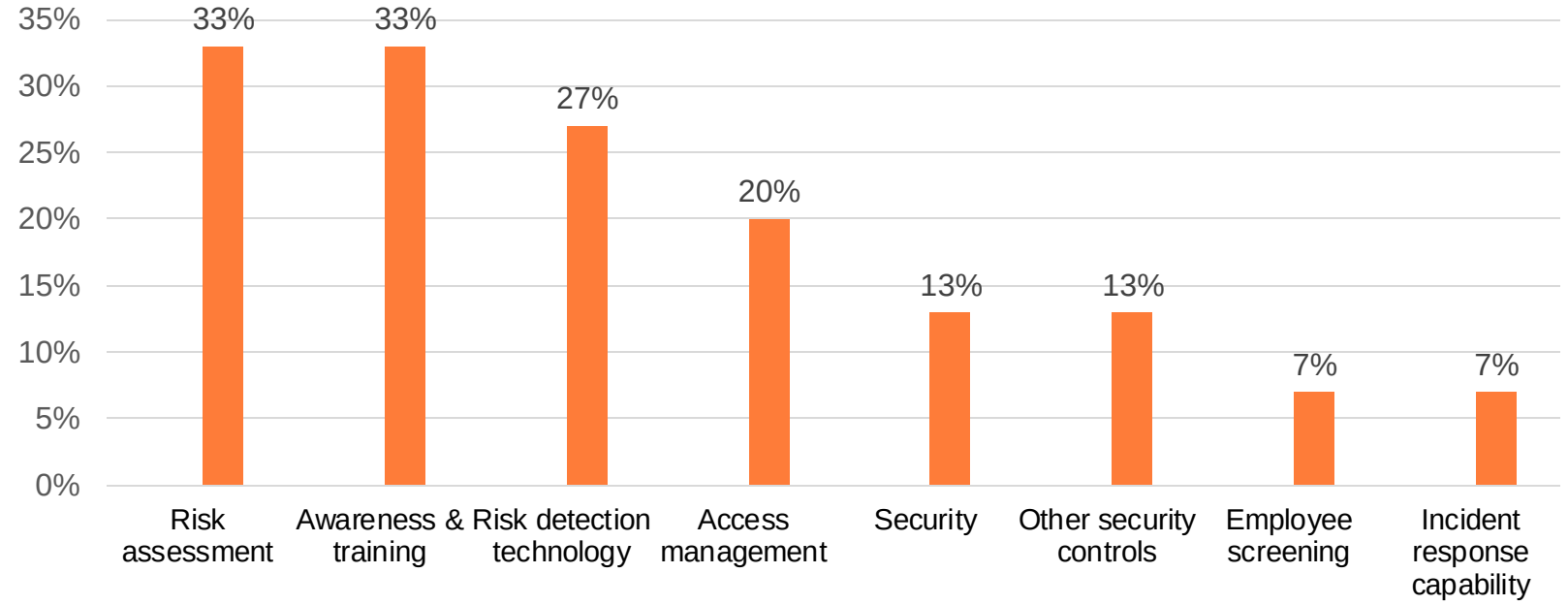
However, **firms maintaining flat investment levels may risk falling behind peers** as insider risk programmes, governance expectations, and AI-related threats continue to evolve.

Where will the investment go?

Headline hierarchy:

- Organisations are prioritising foundational insider risk capabilities rather than isolated technical controls.
- While risk assessment, awareness and detection attract the highest levels of investment, respondents indicate a need to strengthen capabilities across the insider risk lifecycle, including governance, access management, security controls and response.
- The spread of investment priorities reflects a shift from isolated controls towards integrated insider risk programmes that connect governance, people, process and technology capabilities.

Where will the investment go?



33%

Prioritised investment in risk assessment.

This reflects a broader shift toward integrated insider risk programmes that connect people, process, governance and technology capabilities.

Effective insider risk management depends on joining the dots across the organisation. The spread of investment priorities highlights the need for coordinated governance, people, controls and technology capabilities rather than reliance on any single function or toolset.

Thank you

pwc.com