UK Financial Services Chief Risk Officer Survey 2026

Teneo

Contents

Foreword

Risk and compliance leaders across UK Financial Services are operating in an environment defined less by novelty than by intensity. The risks themselves are familiar – cyber, resilience, conduct and technology change – but the pace, interconnectedness and scrutiny surrounding them have materially reshaped the Chief Risk Officer (CRO) role.

Cybersecurity now sits at the centre of the risk agenda, not as a discrete technology issue but as a persistent operational threat with real-world consequences. Alongside it, operational resilience has moved from a regulatory concept to a practical test of execution. Firms are no longer judged on whether frameworks exist but on whether they hold under stress.

What defines this moment is not the emergence of new risks but the expectation that existing risks are managed more visibly, consistently and with greater impact. Boards and regulators increasingly expect risk functions to influence decisions, not simply oversee process. The challenge for CROs is no longer defining the model but making it work across the organisation.

Teneo's survey of 40 UK Financial Services CROs during Q4 2025 shows a function in transition. Core governance structures and the three lines of defence remain in place, yet confidence weakens around embeddedness, first-line ownership and the effectiveness of challenge. At the same time, risk teams are absorbing growing expectations around technology, third-party dependency and AI, often without equivalent increases in capacity.

The response has been pragmatic rather than radical. Over the past year, firms have focused on strengthening foundations – updating frameworks, enhancing stress testing and refining measurement. Looking ahead, the emphasis shifts to industrialisation: clearer risk appetite, stronger monitoring and increased use of automation to scale oversight without diluting judgement.

Taken together, the findings point to a CRO agenda shaped less by transformation programmes and more by execution under pressure. Success will depend on turning frameworks into lived practice, combining technology with human judgement and ensuring risk management is effective where it matters most.

This is not the future risk function.

It is the one already being tested.

Matthew Francis
Senior Managing Director
Financial Services Risk and Regulation

02

Key Findings

Teneo

Cybersecurity has become the defining enterprise risk for CROs, shifting the focus from prevention and frameworks to resilience, response and decision-making under pressure

Priorities and Emerging Risks

35%

of UK Financial Services CROs cite **cybersecurity and incident response** as a top priority for 2026. **Operational resilience** (28%) and **risk culture** (25%) also feature prominently, reflecting a continued focus on protecting critical services and strengthening execution.

50%

cite advanced cyber threats as the leading emerging risk over the next three years. **Economic stagnation** (33%) and **geopolitical tensions** (33%) form a clear second tier of concern, indicating a broadening risk horizon beyond technology-driven threats.

Risk Function Mandate

85%

of CROs report clearly defined roles and responsibilities for risk in their organisations.

The risk function's mandate is generally viewed as well established. Most CROs report that the mandate is clearly documented and well understood within the risk function itself. CROs report high confidence that **the first line owns risk** (88%), with **roles and responsibilities clearly defined** (85%).

However, the data also highlights persistent weaknesses in the embedding of the three lines of defence model, rather than its design. This indicates a gap between formal definition and day-to-day application.

CROs are less confident that the **3LoD model is consistently understood by all stakeholders** (40%). They are also less confident that **the second line has comprehensively mapped and engaged its internal and external stakeholders** (25%), which can weaken effective challenge.

Remit and Team

Beyond the core remit, CRO scope frequently extends to adjacent second-line activities. **Compliance** (73%), **financial crime** (65%) and **regulatory affairs** (43%) are commonly included, while areas such as **information security** (20%), **data governance** (15%) and **legal** (15%) sit within the CRO remit less consistently, indicating variation in operating models across firms.

73%

of CROs report that **size**, **capability** and **capacity of the risk function meets their firm's needs.**

23%

of CROs have team members who are based outside the UK.

Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

Risk frameworks and operating models are largely in place, but effectiveness increasingly depends on embeddedness, first-line ownership and real influence on decisions

Transformation of Risk Function

Over the past 12 months, CROs have updated **risk frameworks** (48%), **enhanced stress** and **scenario testing** (41%) and **refined risk measurement** (34%).

Looking ahead to the next 12 months, CRO priorities shift decisively towards industrialisation and execution:

63%

plan to implement risk technology to automate risk processes.

55%

intend to improve risk reporting capabilities through better risk data and aggregations.

Talent

Talent and capability remain a strategic priority for CROs as risk expectations continue to expand.

76%

of CROs expect to need to recruit additional skillsets over the next five years to ensure their risk functions have the right capabilities.

The skills in greatest demand are increasingly non-technical. Over the next five years, the most important capability for the **first line** is the ability to **understand and use information and technology,** while for the **second line,** the strongest consensus centres on **communication, interpersonal leadership and critical thinking.**

This reflects a shift towards influence, judgement and technology fluency as differentiating factors for effective risk management.

Technology

45%

of firms currently use **automation or advanced analytics** in **incident and breach reporting,** indicating that adoption is most mature in operationally intensive risk activities.

58%

of firms have established **enterprise governance structures, roles and responsibilities** to manage risks associated with machine learning, AI and large language models.

Basic controls are more common than advanced safeguards.

Most firms report having **AI usage policies, model inventories or safeguards** in place. Far fewer have embedded **responsible AI practices** such as **bias monitoring, explainability, legal review or ongoing performance monitoring.**

Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

03

Priorities and Emerging Risks

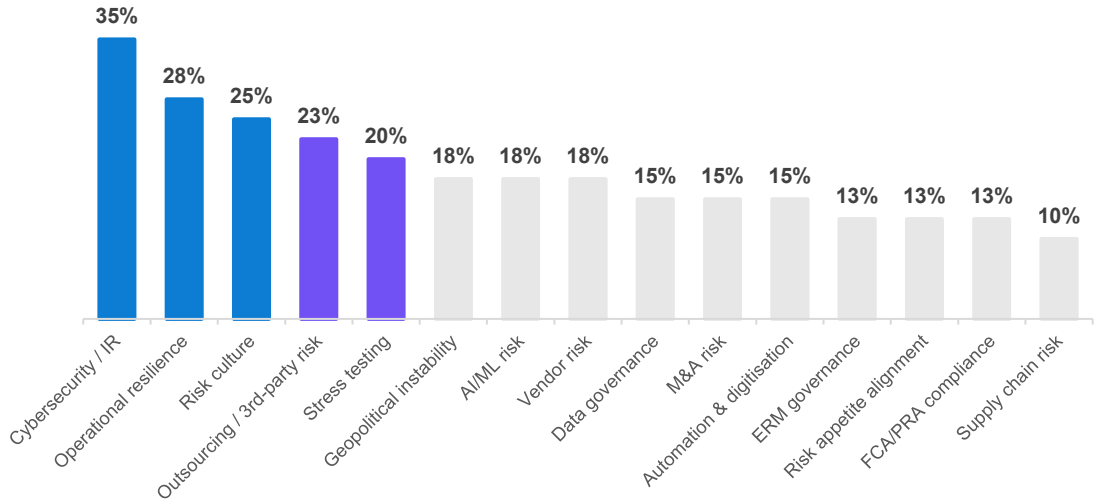
Teneo

Cybersecurity and incident response is the top priority for Financial Services CROs in 2026, followed by operational resilience and risk culture, reinforcing the focus on protecting critical services

Third-party and preparedness themes round out the top five, with outsourcing/third-party risk (23%) and stress testing (20%) both featuring prominently. Beyond that, responses quickly fragment into a long tail, suggesting CRO agendas are broad but anchored by a small set of non-negotiables.

Sector nuance sits in the supporting priorities. Banks tend to layer in structural change items (e.g., data governance, Basel-related change and geopolitical risk) alongside the core. Insurers skew more toward execution, pairing cyber with vendor/outsourcing control, resilience delivery and remediation of legacy systems and reporting constraints.

Question: What are your top risk priorities for the next 12 months?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

> In our cyber work, we are seeing a clear shift from a sole focus on prevention towards preparedness and response. Firms are increasingly judged on how they manage incidents in real time, including decision-making, communication and recovery, rather than on the existence of controls alone.

Courtney Adante
President, Security Risk Advisory

> From our experience supporting organisations through live cyber incidents, the technical response is only one part of the challenge. What often determines the outcome is how quickly leaders can make decisions with imperfect information, communicate clearly with regulators, customers and employees and maintain trust while the situation is still evolving. The firms that manage cyber events most effectively are those that have rehearsed not just the technical playbooks, but the governance, escalation and communications required when an incident becomes a business-critical issue.

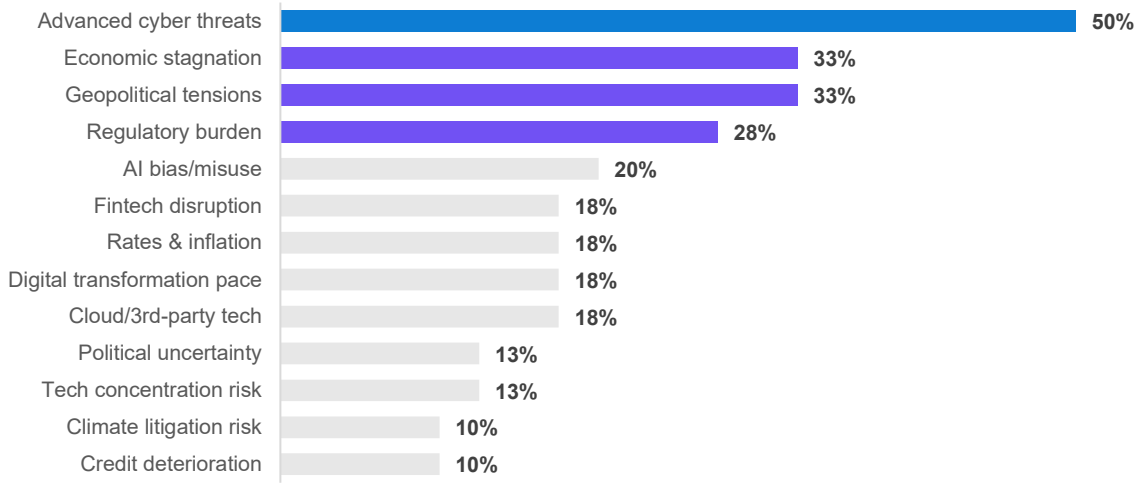
Louise Male
Senior Managing Director
Strategy and Communications

Advanced cyber threats are the clear standout emerging risk, where CROs see the threat evolving faster than traditional controls and requiring stronger detection, response and recovery capabilities

Macro and geopolitical pressures return to the centre of gravity, with economic stagnation and geopolitical tensions both at 33%, and regulatory burden not far behind (28%). Taken together, this reads as a "volatility stack:" growth uncertainty, policy shifts and a heavier supervisory perimeter reinforcing one another.

Technology risk is widening beyond cyber. AI bias/misuse is now a material theme (20%), while several tech-adjacent risks cluster at 18% (cloud/third-party tech, fintech disruption and transformation pace).

Question: What do you see as the main emerging risks facing your firm over the next 3 years?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

> Advanced cyber threats are no longer a future concern – they are a present-day business risk with tangible operational impact. We are seeing threat actors use increasingly sophisticated tools and tactics that bypass traditional controls, forcing firms to move beyond prevention to resilience-oriented strategies that combine real-time detection, rapid response and cross-functional coordination. This elevates cyber risk from an IT-centric issue to a core enterprise concern that touches operations, reputation and customer trust.

Elizabeth Buckley
Managing Director and Head of Cyber and Technical Solutions
Risk Advisory

> Our survey was conducted in late November and early December 2025, before a series of subsequent geopolitical developments that have since intensified global uncertainty. Even at that point, we were already seeing clear signs of strain on the rules-based international order, with rising tensions across multiple regions. We have evolved from decades of an economically driven global operating environment to one dominated by geopolitics. For firms, this reinforces the need to treat geopolitical risk as a core input into stress testing, resilience and strategic decision-making, rather than a peripheral scenario.

Kevin Kajiwara
Global Chair, Political Risk Advisory

04

Risk Function Mandate

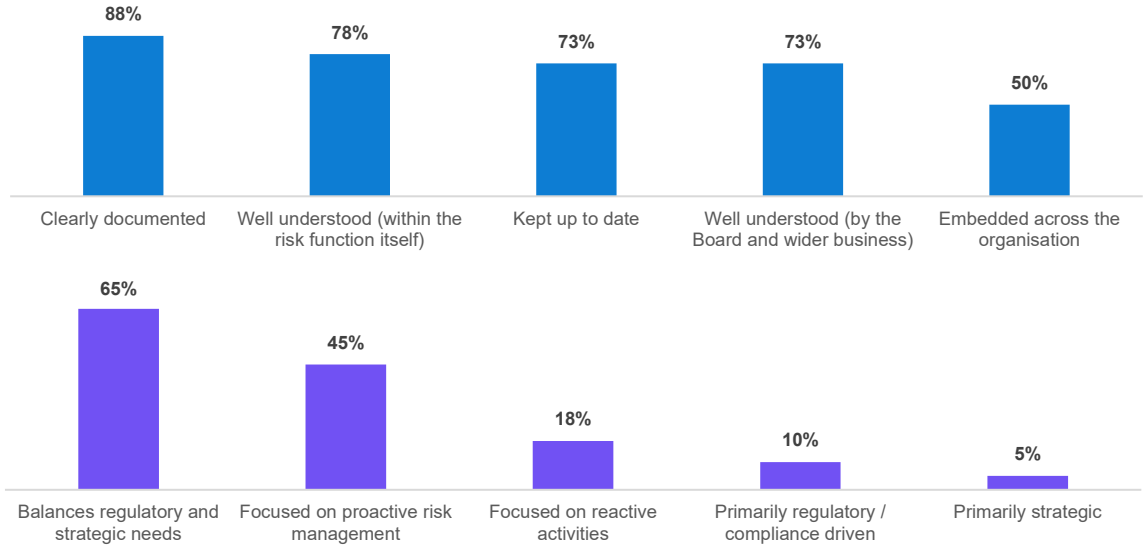
Teneo

There remains a gap between the risk function's mandate as designed and documented, and its embeddedness across the business

Respondents largely describe the function as "balanced" rather than polarised. 65% position it as balancing regulatory and strategic needs, while only small minorities see it as primarily compliance-driven (10%) or primarily strategic (5%). The tone is also more forward-leaning than reactive.

The implication is that the mandate itself is not the issue; operationalising it is. Turning "known and documented" into "routinely used," through clearer reinforcement, consistent training rhythms and more visible ownership in day-to-day decisioning.

Question: How would you describe the strategy and mandate of the risk function?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

Most firms have clearly defined CRO mandates and operating models. However, our experience indicates that understanding these roles is not yet consistent across the organisation. The priority has therefore shifted to embedment; ensuring the risk function is clearly understood, appropriately trusted and demonstrably effective in shaping day-to-day decision-making.

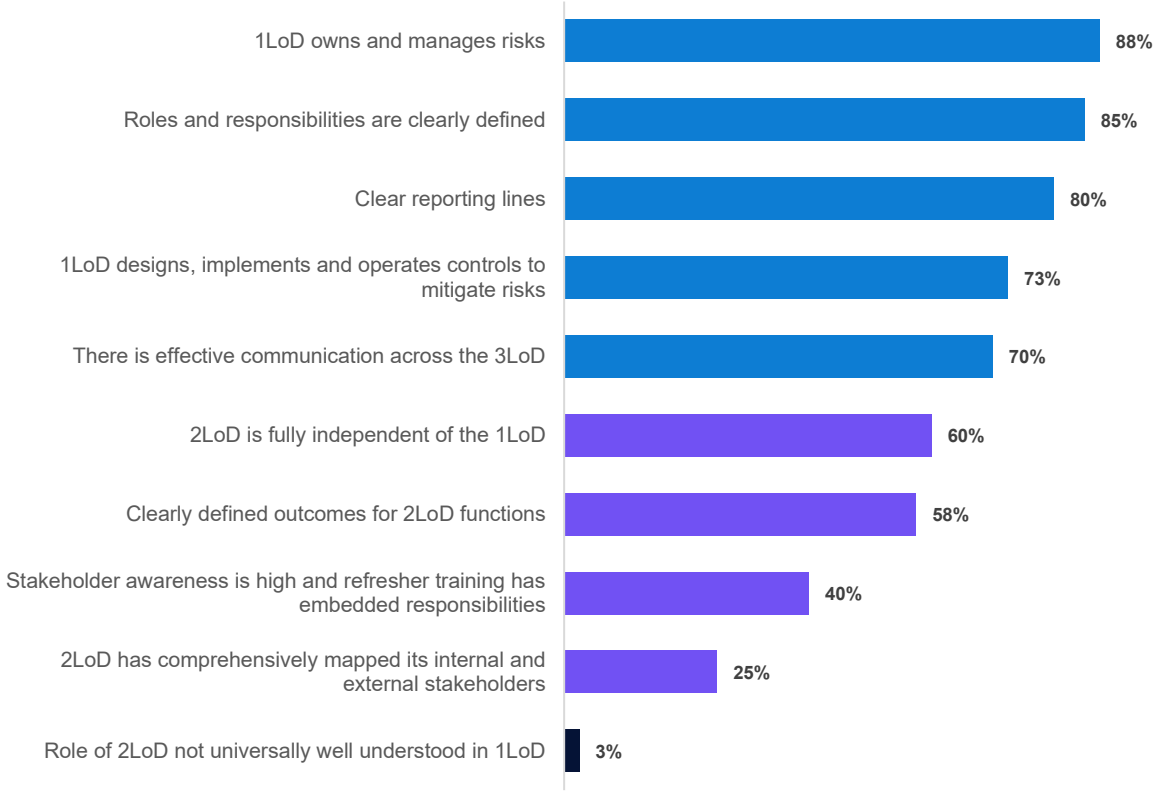
Amanda Rigby
Senior Managing Director and Global Forensic Leader
Financial Advisory

From our work with CROs, we see a clear split in how the role is lived day to day. A small minority remain heavily anchored to regulatory compliance and reactive issue management, often shaped by recent supervisory pressure or remediation. Far more commonly, CROs are seeking to operate proactively, balancing regulatory expectations with a strategic mandate focused on anticipating risk, influencing decisions and enabling the business to move with confidence.

Stephen Browne
Senior Managing Director
Financial Advisory

A well-defined three lines of defence model now places greater emphasis on the risk function's ability to drive ownership, challenge and preventative impact in practice

Question: How would you describe the assignment of roles for risk management across the business?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

Role fundamentals look well established in the first line. 88% say the 1LoD owns and manages risk, supported by clearly defined responsibilities (85%) and reporting lines (80%). Control ownership is also largely in place, with 73% saying the 1LoD designs and operates key controls.

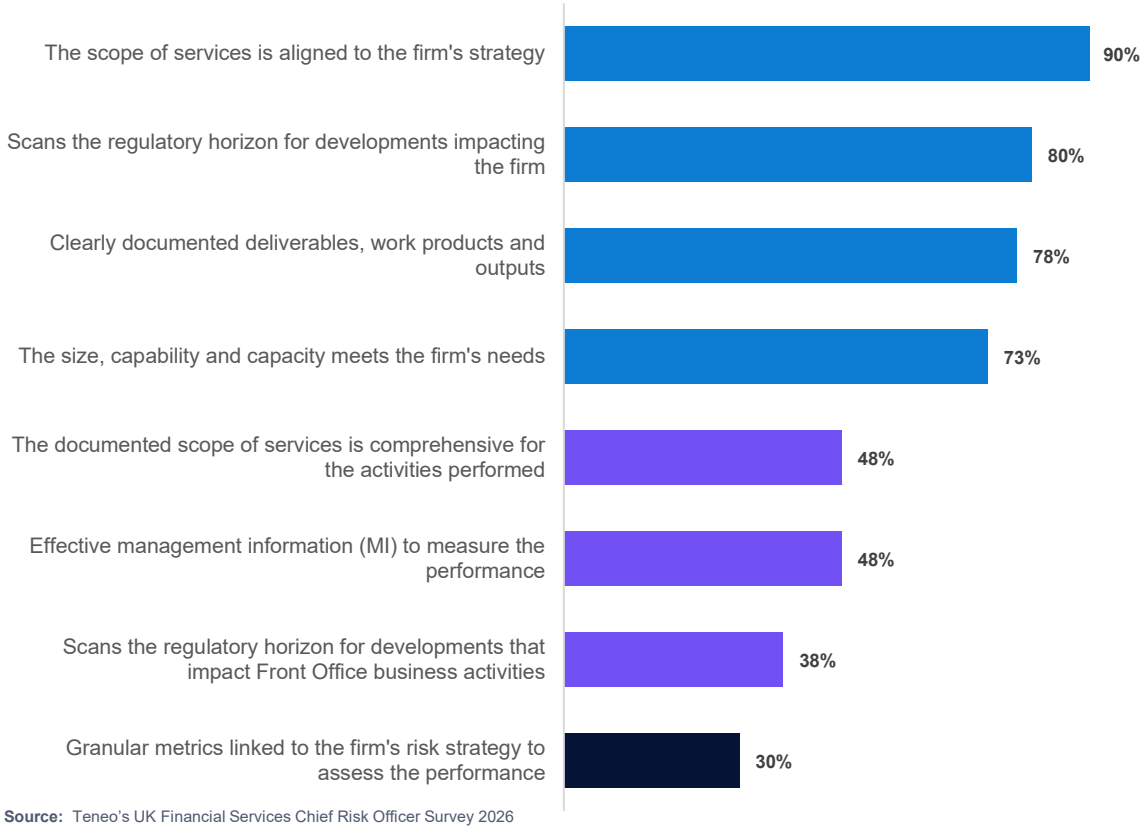
The second line story is more uneven. Independence (60%) and defined outcomes (58%) are not weak, but the "influence mechanics" lag: only 40% cite high stakeholder awareness supported by refresher training, and just 25% say the 2LoD has comprehensively mapped internal and external stakeholders.

> Geopolitical risk is now a live consideration for many firms, not a distant scenario. We are seeing organisations contend with its practical impacts on supply chains, regulation and market conditions, driving demand for more integrated horizon scanning and stress testing.

Carsten Nickel
Managing Director
Risk Advisory

The widening scope of risk services highlights growing expectations for the function to balance assurance, advisory and enablement roles simultaneously

Question: How would you describe the scope and levels of service that the risk function is expected to deliver?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

What we are seeing in practice is a steady expansion in what organisations expect the risk function to deliver. Beyond core oversight and assurance, risk teams are increasingly asked to provide advisory input, decision support, training and enablement across the business. The challenge for CROs is not the absence of demand, but prioritising which services genuinely add value while maintaining independence and ensuring the function remains focused on the risks that matter most.

David Soden
Senior Managing Director
Financial Advisory

We are seeing regulators place far greater emphasis on how risk functions respond to stress scenarios that test the viability of the business, not just its resilience. Exercises such as Dynamic GIST are pushing firms to think more realistically about how risks crystallise over time and what that means for capital, liquidity and operational continuity. In parallel, expectations around solvent wind down have become much more tangible, requiring risk teams to integrate recovery and resolution thinking into day-to-day risk management rather than treat it as a standalone regulatory exercise.

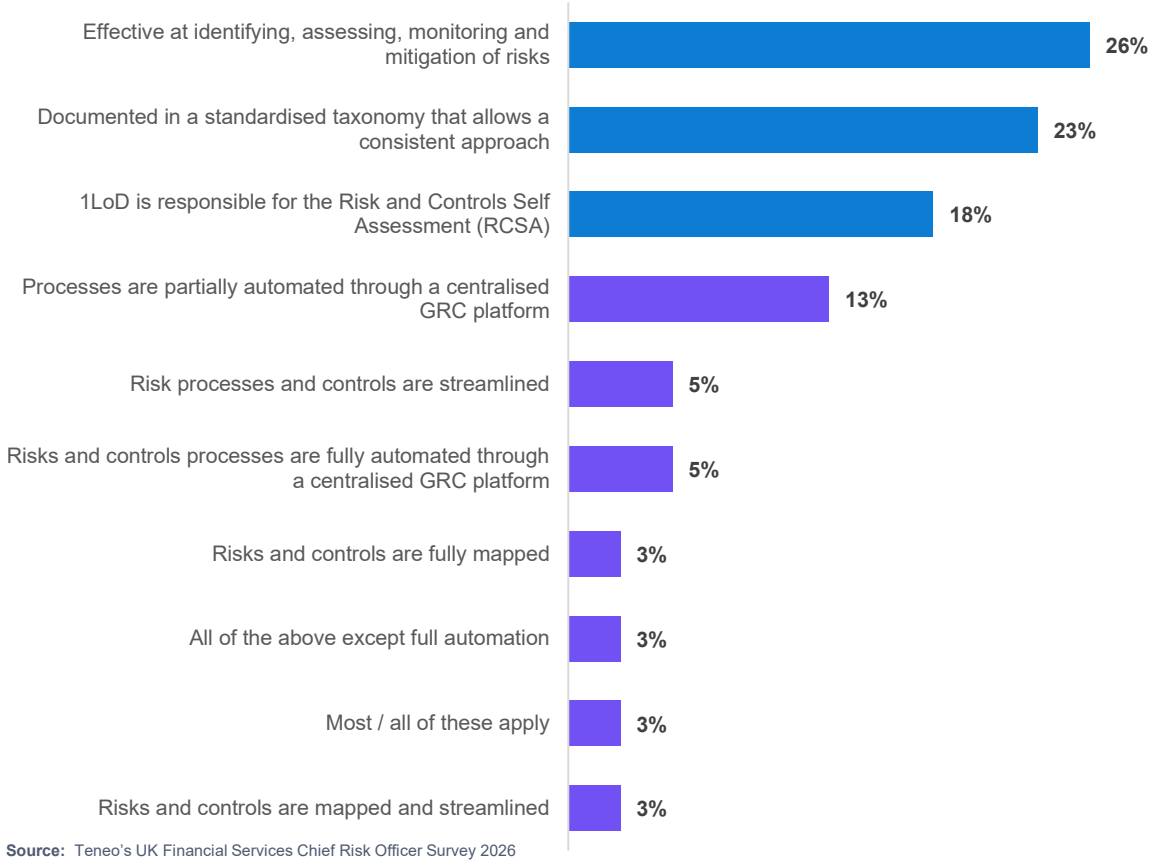
Michael Tagg
Senior Managing Director
Financial Advisory

05

Risk's Remit and Team

Risk and compliance processes are largely established, with embedment and effectiveness remaining the key challenge

Question: How would you describe risk and compliance processes?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

CROs describe risk and compliance processes as functional but still maturing in consistency and enablement. The most selected descriptor is end-to-end effectiveness (26%), followed closely by a standardised taxonomy for a consistent approach (23%) and first-line ownership of RCSA (18%).

Automation remains a differentiator rather than the norm. Only 13% report partial automation through a centralised GRC platform, and just 5% describe full automation. The very low selection of "fully mapped" risks and controls (3%) points to ongoing work on documentation, rationalisation and data quality before scale is achievable.

> In recent years, compliance failures – whether in financial crime, regulatory reporting or conduct oversight—have served as stark reminders that compliance controls are only as strong as their implementation and testing. What we are seeing in the market is less about isolated breakdowns and more about the systemic effects of weak embedment: missed risk signals, regulatory censure and, in some cases, erosion of client trust. Firms that have responded most effectively have doubled down on closing control gaps, strengthening second-line challenge and investing in monitoring and assurance that identifies weaknesses before they crystallise. The lesson from compliance failures isn't that frameworks are irrelevant, but that consistent execution, continuous testing and a clear line of sight from issue to resolution are fundamental to effective risk and regulatory outcomes.

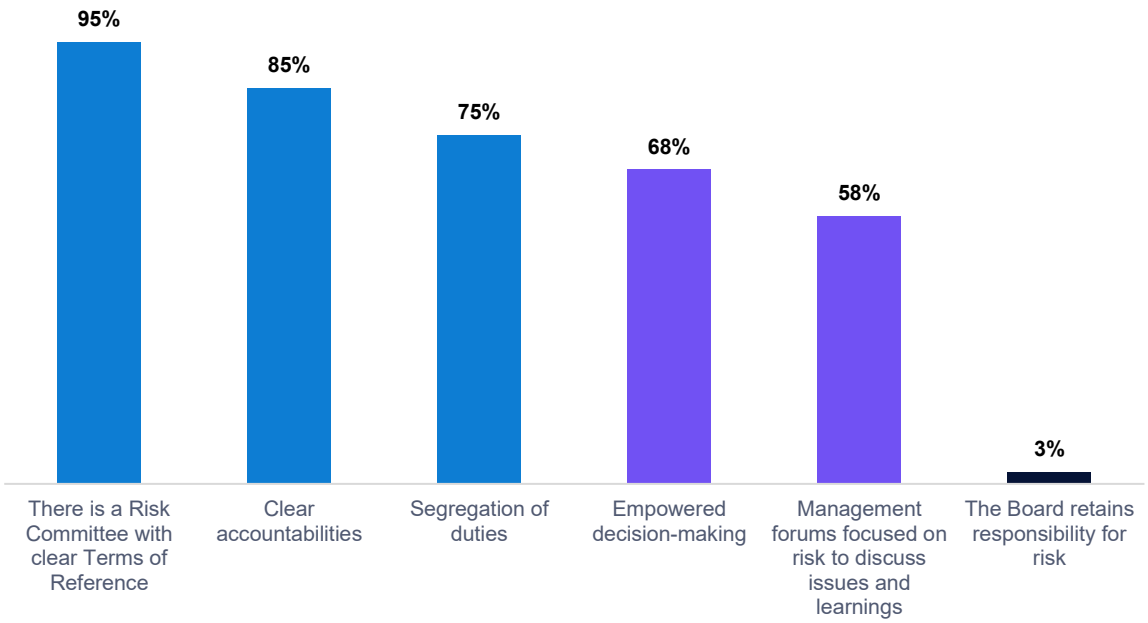
Duncan Perring
Senior Managing Director
Financial Advisory

Risk governance structures are firmly in place, but their effectiveness is increasingly defined by the quality of decisions they enable rather than by the forums themselves

Governance wiring is largely in place. Nearly all CROs point to a formal risk committee with clear terms of reference (95%), supported by clear accountabilities (85%) and segregation of duties (75%). The picture is of a framework that is established and broadly understood.

The weaker signal is the operating cadence. Empowered decision-making is cited by 68%, and only 58% highlight management forums focused on risk discussion and learnings, suggesting governance is stronger on structure than on consistent day-to-day application.

Question: How would you describe risk governance?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

Across the firms we work with, risk governance structures are largely well established, with clear committees, accountabilities and reporting lines in place. The challenge is less about design and more about effectiveness: ensuring governance forums drive timely decisions, surface emerging issues early and translate risk insight into action, rather than functioning as procedural checkpoints.

Alex Adam
Senior Managing Director
Financial Advisory

In real cyber incidents, the organisations that struggle most are not those without the right controls, but those without clarity on how to escalate and make decisions under pressure. We often see incident responses hampered by a lack of coordination between technology, risk, legal and communications teams. An effective response can depend on having rehearsed how those teams come together in real time, with clear ownership, rapid information flow and a shared understanding of priorities when systems, customers and regulators are all in play.

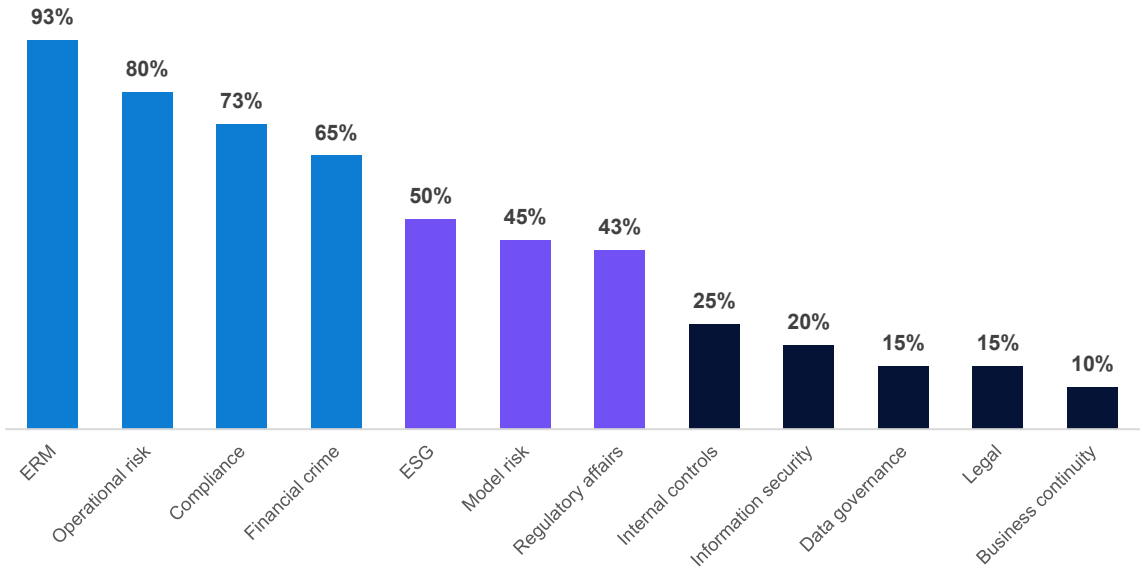
Arjan Keshavarz
Director
Strategy and Communications

An expanding CRO remit, with more functions reporting in, reflects rising expectations for enterprise-wide risk ownership but places growing pressure on governance, capacity and prioritisation

Bank CRO reporting lines look relatively tight, concentrated around ERM, operational risk and compliance, with only a small minority also owning information security, data governance or legal.

Insurance CROs operate a much broader remit, with ERM at 70% and many adjacent second-line functions commonly reporting in, suggesting a more centralised risk model. Business continuity appears similar across both sectors.

Question: Which functions report into the CRO?



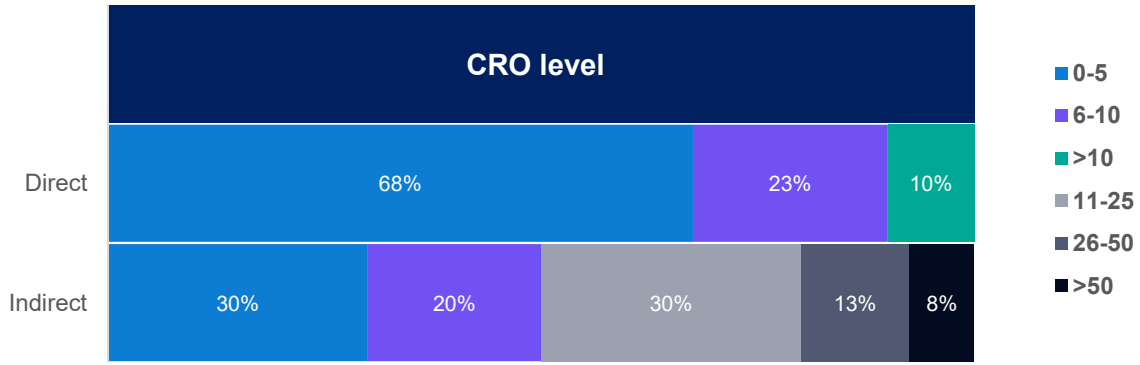
Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

What we are seeing across UK Fnancial Services is a broadly consistent core CRO remit, typically encompassing enterprise and operational risk, with compliance and financial crime also reporting into the function in many firms. Beyond that core, there is far greater variation, particularly around areas such as information security, data governance and legal, reflecting different operating models and choices about how firms balance centralisation with specialist ownership.

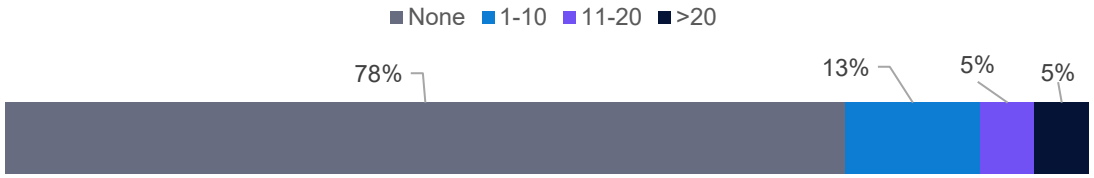
Matthew Francis
Senior Managing Director
Financial Advisory

CROs are reflecting on the size of their teams and their span of control to deliver their widening remit in a cost-conscious and proportionate way

Question: Considering all the functions that report into the CRO, how many direct/indirect reports (FTE) does the CRO have?



Question: Of direct reports and indirect reports, how many of these are located offshore?



Direct reporting lines are typically lean. Most CROs sit with a small direct leadership team (68% with fewer than six direct reports), with a smaller cohort at 6-10 (23%) and only 10% above 10, consistent with a "tight top team" model.

Indirect span is materially larger. Indirect reporting quickly scales, with around half reporting more than 11 indirect reports (30% at 11-25, 13% at 26-50 and 8% above 50), pointing to layered management of sizeable risk organisations.

Overseas reporting remains the exception. 78% report no overseas direct reports, with only 22% having any overseas span (13% at 1-10; 10% above 10). Even where firms operate internationally, CRO operating models appear primarily domestically anchored, relying on matrix structures for global coverage.

> What we are seeing in the market is that risk team size is generally viewed as adequate on paper but increasingly stretched in practice. As CRO remits broaden and expectations around resilience, technology and regulatory engagement intensify, the challenge is less about headline headcount and more about whether teams have the capacity and skills to absorb additional demand without diluting effectiveness.

Sumrana Saleem
Managing Director
People Advisory

Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

06

Transformation of the Risk Function

Teneo

CRO focus will shift towards industrialising delivery over the next 12 months, with greater emphasis on automation and risk technology, strengthened data and reporting capabilities and improved monitoring

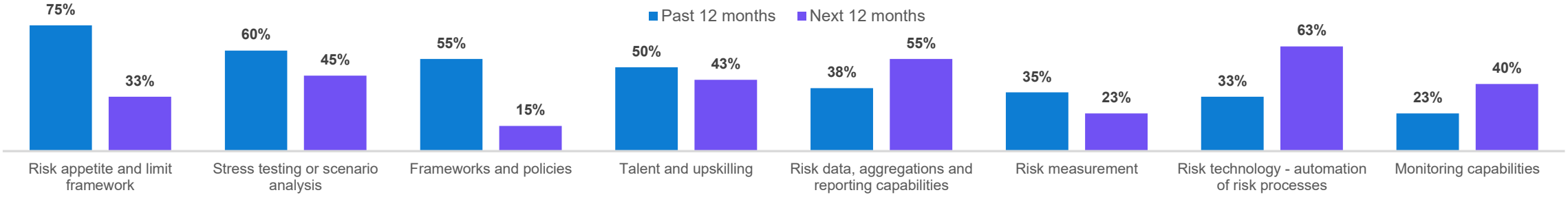
The past 12 months were about tightening the core framework. Enhancements skewed toward risk appetite and limits (75%), stress testing and scenario analysis (60%) and frameworks and policies (55%), signalling a focus on definitional clarity and control design.

The next 12 months shift from “define” to “mobilise.” Risk technology and process automation becomes the standout priority (63%, up from 33%), alongside risk data aggregation and reporting (55%, up from 38%) and stronger monitoring (40%, up from 23%).

> Over the past 12 months, we have seen firms strengthen core risk management practices, with particular attention on enhancing stress and scenario testing, tightening control frameworks and improving monitoring across operational and regulatory risk areas. In the client money and safeguarding space, this has translated into more rigorous reconciliation processes, clearer end-to-end controls and enhanced oversight of third-party custodians – all of which have been essential as new digital asset and payment services firms enter the ecosystem.

Elaine Sutton
Director and Head of Client Assets and Safeguarding
Financial Advisory

Questions: What key enhancements to risk management has your organisation made over the past 12 months?
What key enhancements is your organisation planning to make over the next 12 months?



Source: Teneo’s UK Financial Services Chief Risk Officer Survey 2026

07

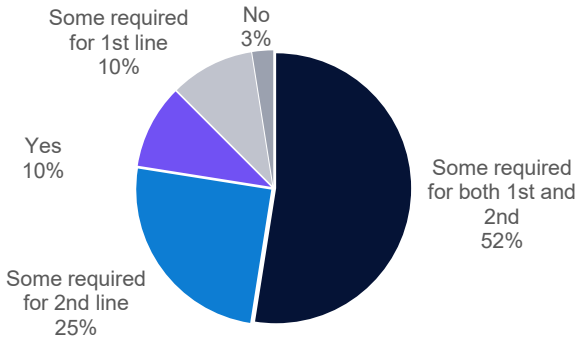
Talent

More than three quarters of CROs anticipate increasing the number of risk professionals in their organisation, with almost a third expecting to increase headcount by more than 16% over the next five years

The dominant message is “not broken, but not ready.” Only 10% say the talent pool is fully fit for the next five years, while 87% see some level of capability gap (52% across both first and second line, 25% in the second line, 10% in the first line).

The gap is broad, but it isn’t framed as a crisis. With just 3% saying “no,” the signal is targeted build, with uplift where requirements are changing fastest rather than wholesale replatforming of the function.

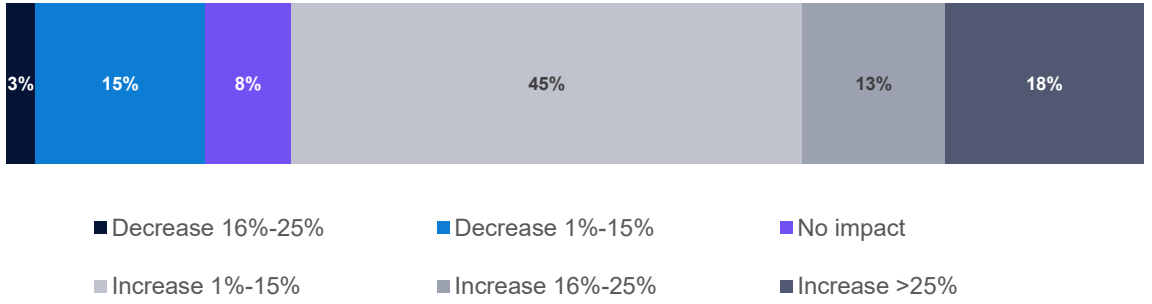
Question: Does your talent pool have the right capabilities to respond to the changing needs of the risk management function over the next five years?



Most CROs expect risk capacity to increase. 76% anticipate headcount growth, led by modest expansion (45% at 1-15%), but with a meaningful “step change” tail (18% at more than 25%).

Downsizing is not the base case. Only 18% foresee reductions (15% at 1-15%, 3% at 16-25%), with just 8% expecting no change, suggesting risk is still viewed as a build area driven by resilience, technology and regulatory expectations.

Question: How do you expect the total number of full-time equivalent (FTE) risk management professionals across the business to change over the next five years?



> As risk functions evolve, the skills gap is less about knowledge and more about application. CROs are increasingly looking for people who can work in commercial alignment with the business, interpret risk, challenge constructively and translate complexity into clear decisions, especially as technology and regulatory demands continue to intensify.

Freddie Williams-Thomas
Senior Managing Director
People Advisory

Source: Teneo’s UK Financial Services Chief Risk Officer Survey 2026

CROs report that communication and interpersonal leadership are the most important skills for risk professionals in the future, signalling that translating complex risks into clear decisions is now more important than technical depth

Influence skills dominate the podium. Communication, interpersonal leadership and critical thinking is the only capability with real consensus (48%), underlining that the differentiator is judgement and decision shaping, not technical depth alone.

The next tier is fragmented but telling. AI-based model risk management (10%) and the ability to understand and use information and technology (10%) sit alongside operational resilience and business continuity (8%) and cybersecurity (8%). The implication is that CRO teams win by integrating specialists, bridging risk, technology and business outcomes rather than trying to "own" every technical domain.

Question: What are the most important skill sets required in the risk management function over the next five years?

Podium	Risk skills	CRO selected as most important in the next 5 years (n=40)
🥇	Communication, interpersonal leadership and critical thinking skills	48%
🥈	AI-based model risk management	10%
🥈	Ability to understand and use information and technology	10%
🥉	Operational resilience/business continuity	8%
🥉	Cybersecurity	8%

> What we are seeing in the market is a shift in how firms define strong risk talent. Technical expertise remains important, but the real differentiator is the ability to exercise judgement, communicate clearly and engage credibly with the business in an environment shaped by technology change and regulatory scrutiny.

Christine Loughrey
Senior Managing Director
People Advisory

Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

08

Technology

Teneo

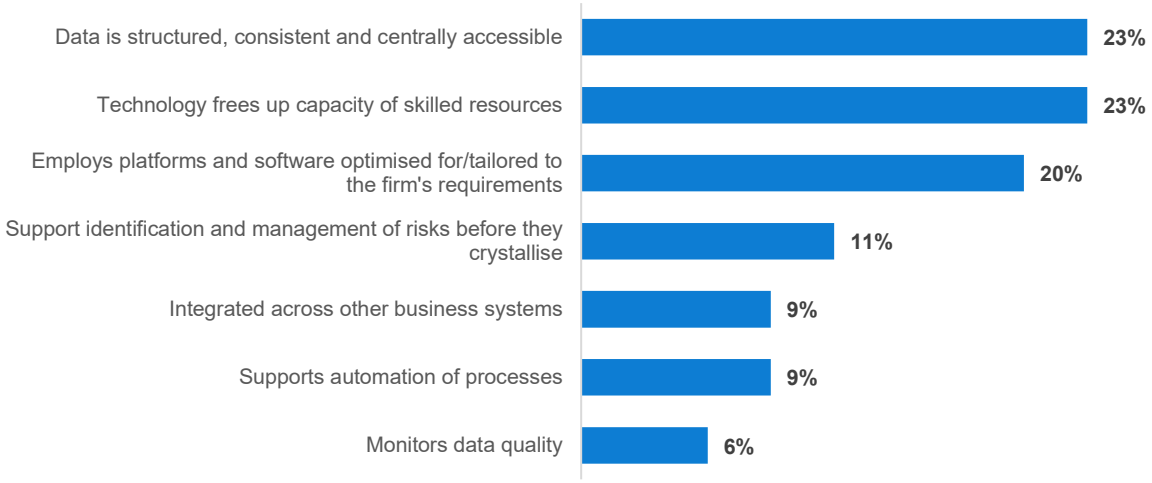
CROs are increasingly using technology to unlock productivity by freeing up the capacity of skilled resources where data is structured, consistent and centrally available

Risk technology is still framed as a productivity and data access lever. The most common descriptors are structured, centrally accessible data (23%) and freeing up skilled capacity (23%), with tailored and optimised platforms close behind (20%).

The higher ambition use cases remain minority views. Only 11% describe technology helping to identify and manage risks before they crystallise, while integration across other business systems (9%) and process automation (9%) are cited less often, suggesting many firms are still building the plumbing rather than running end-to-end digital workflows.

Data quality is the clearest gap. Just 6% point to technology actively monitoring data quality, reinforcing that foundational data control and stewardship is still catching up with investment in tools and platforms.

Question: How would you describe the firm's use of technology for risk management purposes?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

> In forensic and investigations work, automation is increasingly being used to manage scale and complexity rather than replace judgement. Technology is helping teams surface patterns and anomalies more quickly, allowing experienced practitioners to focus on interpretation, decision-making and client outcomes.

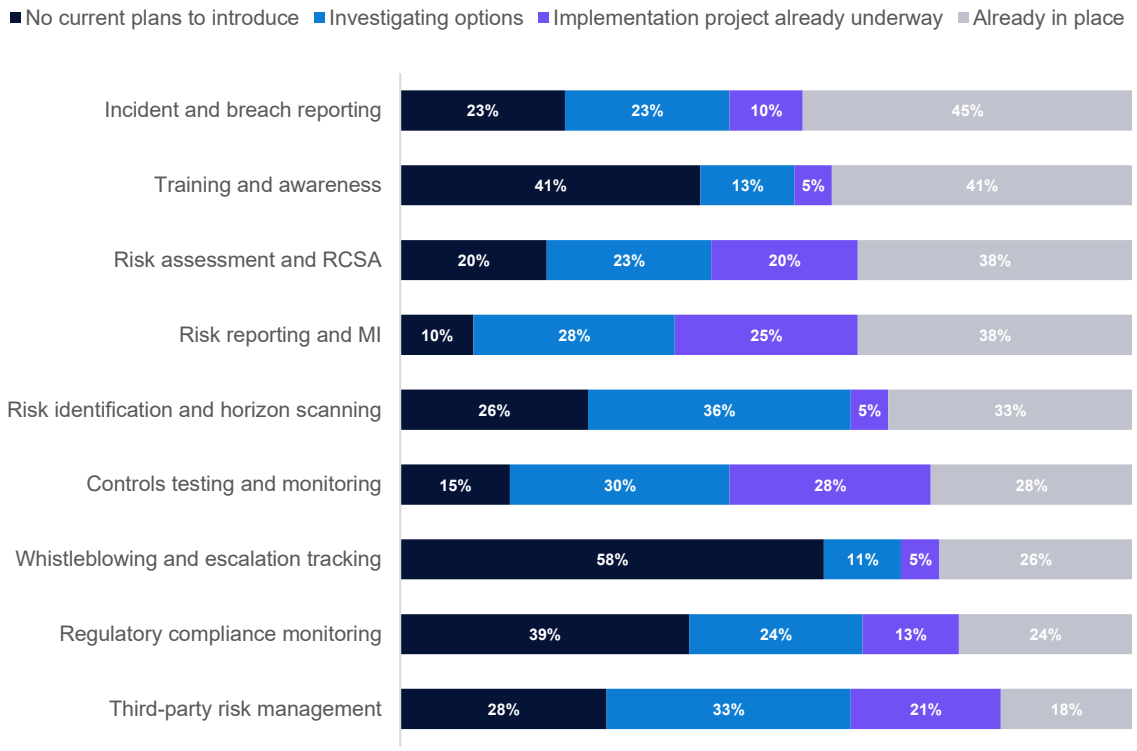
Christian Butter
Senior Managing Director and Head of Forensic UK & EMEA Financial Advisory

> The emergence of Regtech is helping firms strengthen monitoring, reporting and compliance at scale, but only where it is properly integrated into governance and oversight. The firms managing this best are those treating these relationships as critical business services, with clear accountability, resilience testing and ongoing assurance, rather than assuming technology alone mitigates the risk.

Simon Hemsley
Managing Director
Management Consulting

Automation is most mature in core control activities, with incident and breach reporting largely in place and growing use in training and risk assessment. Gaps remain in relation to whistleblowing and escalation tracking, where most firms have no plans to implement

Question: For which risk management activities does the organisation apply automation or advanced analytics?



Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

A two-speed profile shows up across the mid pack. Controls testing and monitoring is almost evenly split between already in place and implementation (28% and 28%), while risk identification and horizon scanning is as likely to be under investigation (36%) as deployed (33%) – more experimentation than industrialisation.

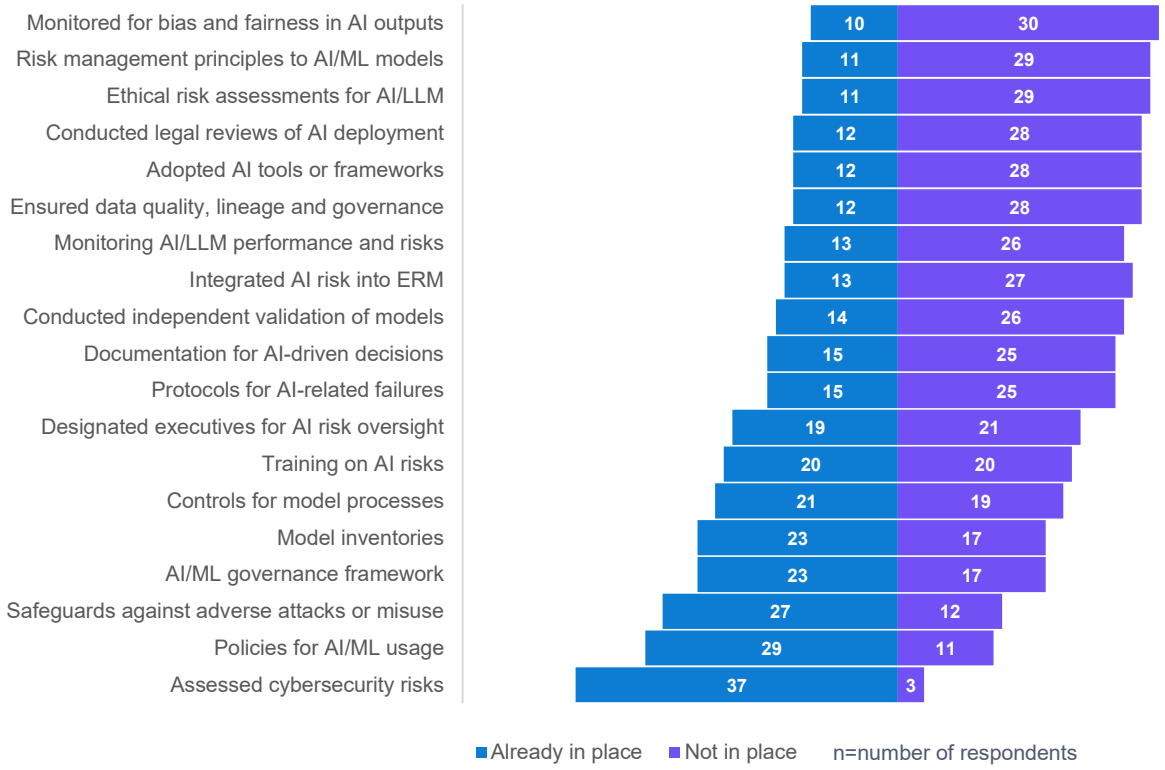
Conduct and compliance use cases lag furthest behind. Whistleblowing and escalation tracking has the strongest "no plans" signal (58%), and regulatory compliance monitoring remains underdeveloped (24% in place, 39% no plans). Third party risk management stands out as the build area, with only 18% in place but 54% investigating or implementing, reflecting rising dependency and vendor concentration pressures.

> What we are seeing in practice is that effective risk management increasingly depends on the quality of underlying technology, data and management information. Across recent engagements, firms have used technology not just to automate controls but to improve the timeliness, consistency and usability of MI, giving senior leaders a clearer line of sight from risk identification through to decision-making. Whether modernising core platforms under intense scrutiny or embedding analytics into day-to-day oversight, the common differentiator is MI that supports judgement and action rather than reporting for its own sake.

Jenny Brand
Managing Director
Management Consulting

While many firms have assessed cybersecurity risks and implemented policies for AI and machine learning usage, far fewer have embedded responsible AI practices such as bias monitoring, ethical assessments, explainability, legal review and performance monitoring

Question: Which actions has your organisation taken to manage and mitigate the risk associated with the implementation and use of machine learning, AI and large language models in your operations?



Guardrails are strongest at the perimeter and in baseline governance. Cybersecurity assessment is near universal (37 of 40 in place), supported by AI and machine learning usage policies (29) and safeguards against attacks or misuse (27), with around six in ten also maintaining model inventories and an AI or machine learning governance framework (23 each).

Responsible AI execution is materially less embedded. Only around a quarter monitor bias and fairness (10) or run ethical risk assessments (11), and fewer than half have performance and risk monitoring in place (13), highlighting a clear gap between policy and continuous assurance.

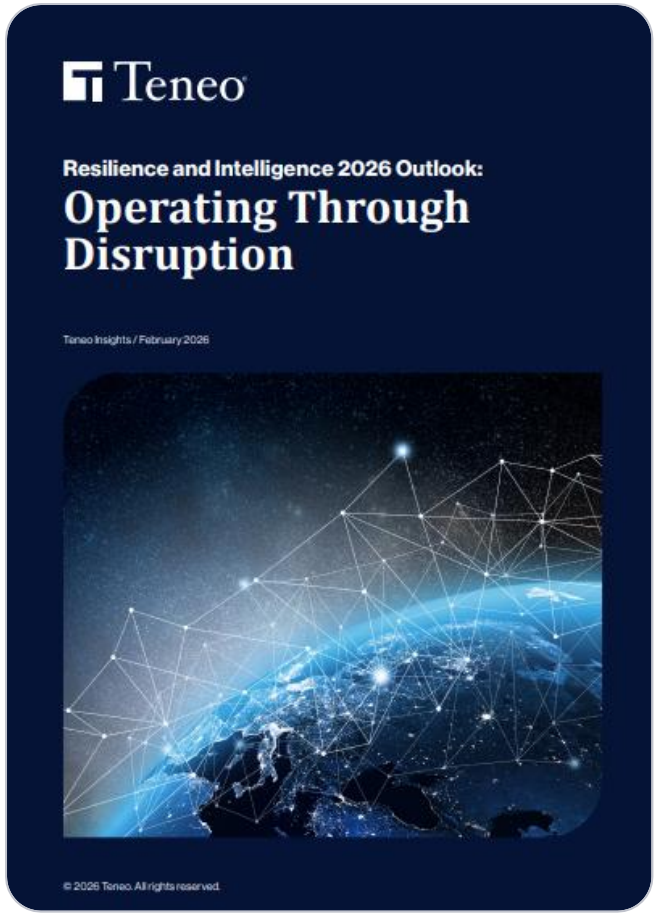
> Most organisations we work with now recognise the need for AI governance and have taken initial steps through policies and oversight structures. The challenge we see is moving from governance on paper to governance in practice, particularly around explainability, accountability and ongoing monitoring as AI use becomes more embedded.

Ryan Cox
Global Head of Artificial Intelligence

Source: Teneo's UK Financial Services Chief Risk Officer Survey 2026

The World in 2026: Selected Recent Insights from Teneo

teneo.com/insights



Contact Teneo's Financial Services team for more information

Financial Advisory

Stephen Browne
Senior Managing Director
Financial Advisory
stephen.browne@teneo.com

David Soden
Senior Managing Director
Financial Advisory
david.soden@teneo.com

Michael Tagg
Senior Managing Director,
Financial Advisory
michael.tagg@teneo.com

Matt Francis
Senior Managing Director
Financial Advisory
matthew.francis@teneo.com

Duncan Perring
Senior Managing Director
Financial Advisory
duncan.perring@teneo.com

Financial Advisory

Alex Adam
Senior Managing Director
Financial Advisory
alex.adam@teneo.com

Amanda Rigby
Senior Managing Director & Global Forensic Leader
Financial Advisory
amanda.rigby@teneo.com

Christian Butter
Senior Managing Director & Head of Forensic UK & EMEA
Financial Advisory
christian.butter@teneo.com

Andy Wood
Managing Director
Financial Advisory
andy.wood@teneo.com

Janine Catterson
Director
Financial Advisory
janine.catterson@teneo.com

Elaine Sutton
Director
Financial Advisory
elaine.sutton@teneo.com

Craig King
Director
Financial Advisory
craig.king@teneo.com

People Advisory

Toby Crosthwaite
Senior Managing Director
People Advisory
toby.crosthwaite@teneo.com

Freddie Williams-Thomas
Senior Managing Director
People Advisory
freddie.williams-thomas@teneo.com

Christine Loughrey
Senior Managing Director
People Advisory
christine.loughrey@teneo.com

Sumrana Saleem
Managing Director
People Advisory
sumrana.saleem@teneo.com

Strategy and Communications

Iain Dey
Senior Managing Director
Strategy and Communications
iain.dey@teneo.com

Louise Male
Senior Managing Director
Strategy and Communications
louise.male@teneo.com

Arjan Keshavarz
Director
Strategy and Communications
arjan.keshavarz@teneo.com

Risk Advisory

Kevin Kajiwara
Global Chair, Political Risk Advisory
kevin.kajiwara@teneo.com

Carsten Nickel
Managing Director
Risk Advisory
carsten.nickel@teneo.com

Courtney Adante
President, Security Risk Advisory
courtney.adante@teneo.com

Elizabeth Buckley
Managing Director & Head of Cyber and Technical Solutions
Risk Advisory
elizabeth.buckley@teneo.com

Artificial Intelligence

Ryan Cox
Global Head of AI
ryan.cox@teneo.com

Management Consulting

Simon Hemsley
Managing Director
Management Consulting
simon.hemsley@teneo.com

Jenny Brand
Managing Director
Management Consulting
jenny.brand@teneo.com

Regulatory & Risk Advisory Services

Teneo provides strategic and commercial regulatory advice to Financial Services firms, helping them shape, grow and optimise their businesses while navigating an ever-evolving risk and economic environment.

We work with clients across the Banking, Insurance, Asset Management, Payments and Trust and Corporate sectors. Our team has significant experience supporting Boards and management teams in managing crises and regulatory interventions, with the ability to mobilise capabilities at pace.

Implementing and Embedding Regulatory Change

Our team of regulatory professionals works with organisations facing regulatory scrutiny, sanctions or those needing critical operational changes to succeed.

We support regulated firms in implementing new regulatory initiatives, including:

- Developing remediation plans
- Conducting gap analyses
- Assessing and quantifying the firm's exposure
- Designing implementation or remedial action plans
- Supporting management with execution

Conducting Independent Reviews and Managing Risks

Our regulatory experts are appointed by global regulators to undertake skilled person and inspection engagements. These reviews assess the business activities and operating environment of regulated entities, identifying potential compliance issues with specific legislation and/or regulations.

We also support firms in considering their risk exposures and responses, including:

- Solvent wind-down planning
- Addressing climate change risks
- Enhancing operational resilience

Assessing Strategic Options and Executing Business Change

We assist firms in shaping, simplifying or optimising their legal entity, capital and operational structures to achieve transformational change and deliver corporate strategies.

We provide regulatory advice on the implications of a transaction or new business strategy, such as:

- Entering new markets
- Releasing new products
- Design solutions to mitigate risks

Enhancing Board and Functional Capabilities

We assess the effectiveness of a firm's Board or the capabilities of one of its functions and help management design a future target operating model.

Our team delivers generic and tailored training to Boards, senior executives and their teams on regulatory issues.

Methodology

Teneo's Chief Risk Officer Survey 2026 was conducted across UK Financial Services during late November and early December 2025.

Teneo's Chief Risk Officer Survey 2026 was conducted across UK financial services from 19th November to 12th December 2025.

Teneo designed an online survey to capture Chief Risk Officer perspectives on risk priorities, governance, operating models, transformation, talent and technology.

Senior risk professionals operating in UK Financial Services regulated firms were invited to respond.

There were 40 respondents included in the survey, of which nine were from the banking sector, 30 from the insurance sector and one broker.

Findings reflect a combined Financial Services sample (banking and insurance).Where sectoral differences are discussed, results have been segmented accordingly and are clearly labelled. The report does not seek to imply statistical representativeness at sector or sub-sector level.

Findings should be interpreted as directional insights, reflecting CRO sentiment and experience at a specific point in time. They are not intended to constitute a statistically representative sample of the UK Financial Services market. Percentages may not total 100% due to rounding.

The survey period preceded a number of subsequent geopolitical and macroeconomic developments in late 2025 and early 2026. As such, results should be read as capturing CRO perspectives prior to those events, rather than as a reaction to them.

Qualitative interpretation and commentary have been developed by Teneo, drawing on the survey results, Teneo's ongoing advisory work with Financial Services firms and observed market and regulatory developments.

Where interpretation is provided, it is clearly distinguished from underlying survey data.

Teneo is the global CEO advisory firm. We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance and ESG.

The firm has more than 1,800 employees located in 45+ offices around the world.

Teneo®