EXECUTIVE PERSPECTIVES ON TOP RISKS AND OPPORTUNITIES

for the Near - and Long - Term

protiviti®
Global Business Consulting

Risk and compliance leaders face a new mandate: growth, governance, resilience

A strategic reset for R&C: Alliances and ecosystems on the 2027 agenda.

Risk and compliance leaders enter 2027 with a clear mandate: Enable growth without weakening resilience. New survey findings show that strategic alliances and ecosystems have overtaken revenue potential as the leading growth opportunity, even as third-party management remains near the bottom of investment priorities.

That disconnect is one of several revealing gaps in the data. Leaders recognise that AI value depends on workforce readiness, integration and governance, yet third-party AI risk and error prevention receive comparatively little attention. They are also more confident in their ability to protect enterprise value than to respond quickly when markets, technologies or threats shift.

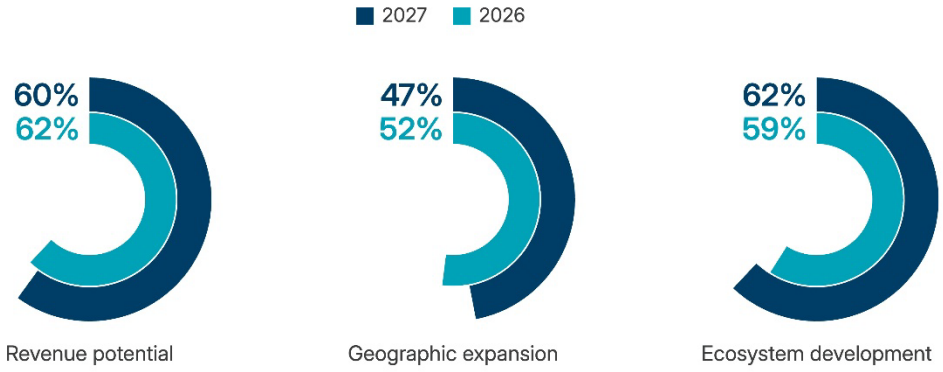
Together, these findings point to a changing risk and compliance agenda. Cybersecurity remains the leading near-term concern, but privacy, identity protection and disruptive innovation are gaining momentum. Internal audit also sees greater exposure than risk owners across several critical areas, raising questions about control effectiveness and assurance alignment.

Over the longer term, competitive position is giving way to security, resilience, talent and trust as strategic priorities. For leaders, the message is straightforward: Partnerships, AI and innovation can accelerate growth, but only if governance, decision-making and investment keep pace. The organisations that close these gaps now will be better positioned to move faster, respond with confidence and turn resilience into competitive advantage.

Where do R&C leaders see the greatest opportunities for their organisation over the next two to three years?

Ecosystem development is now the No. 1 growth story, and that is a genuine shift. Nearly two-thirds (62%) of risk and compliance leaders see significant opportunities to expand strategic alliances and partnerships, up from last year, and it has overtaken revenue potential to top the list. Meanwhile, revenue potential remains strong at 60% but dipped slightly from 62% last year. Geographic expansion is the outlier and a potential warning sign — only 47% see opportunities there, down 5 percentage points from last year, with 23% actively disagreeing.

Views about opportunities for growth – CRO/CCO



62%

view ecosystem development as an organisational growth opportunity in the near term.

Put all three of those together and the picture becomes clear: Risk and compliance leaders are betting on partnerships over passports. In a world of trade friction, regulatory fragmentation and geopolitical volatility, growing through someone else's footprint is faster and cheaper than building your own in a new jurisdiction. Ecosystems let you enter markets, add capability and reach customers without the capital and licensing drag.

Here is the part most organisations miss: Every ecosystem is a third-party ecosystem. **You cannot simultaneously make partnerships your primary growth engine and treat third-party risk as a procurement compliance exercise.** Yet third-party management ranks 10th out of 12 investment priorities at just 14%. That gap between growth strategy and risk investment is the single most exploitable weakness we see heading into 2027.

The organisations that win will treat partner onboarding as a growth capability, not a control gate, with these benefits:

- Faster, risk-tiered due diligence
- Concentration analysis at the ecosystem level, not the contract level
- Exit and substitution planning before you need it

Here's a question risk and compliance leaders should be asking the board: If partnerships are how we grow, is our third-party function built to accelerate that growth or to slow it down? Most leaders we talk to already know the answer. And few have a plan.

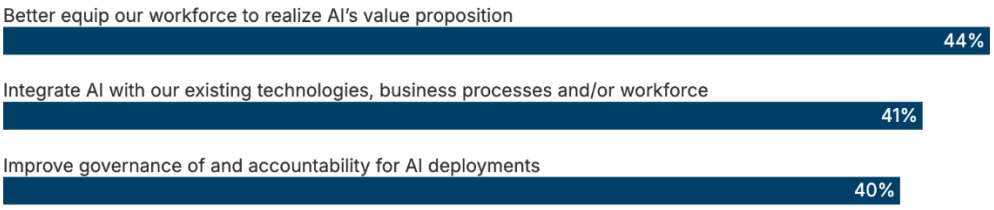
What priorities do leaders see as most important to maximising the value of AI deployments?

The answer is refreshingly unglamorous. It is people and plumbing, not models. The top three priorities for risk and compliance leaders are:

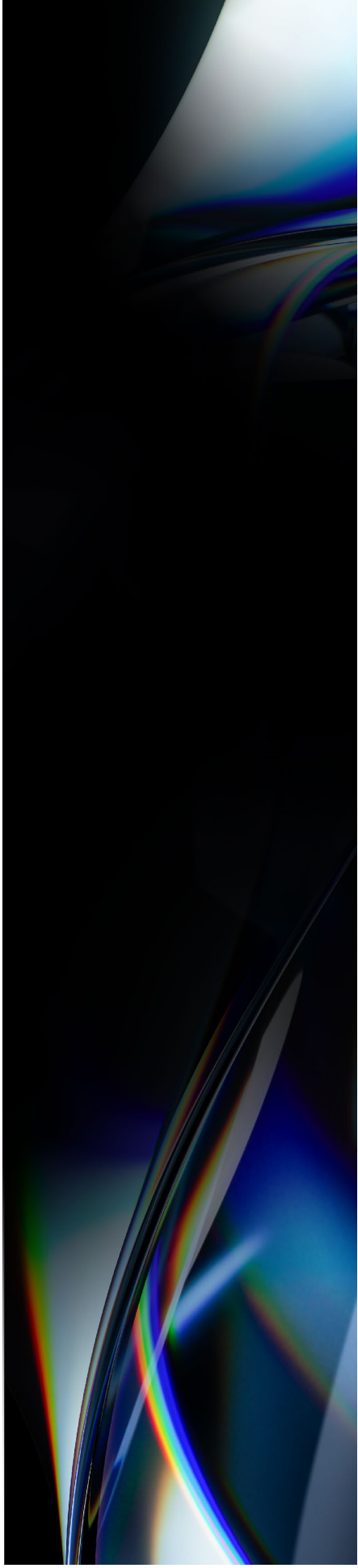
- Better equip the workforce to realise AI's value (44%)
- Integrate AI with existing technologies and processes (41%)
- Improve governance and accountability for AI deployments (40%)

Deploying AI at a more competitive pace (26%) and data security (24%) are far behind, and that ordering tells you something important about priorities. Leaders have stopped treating AI as a race and started treating it as an operating problem. The constraint is no longer access. It is whether your people can use it, whether it connects to the systems you already run and whether, when a regulator asks, you can prove it is governed.

Top AI opportunities – CRO/CCO



Two other data points deserve more attention here: Managing the impact of AI on third-party partners (10%) and avoiding AI errors (18%) both sit near the bottom, and both are exactly where supervisory attention is heading. Meanwhile, vendors are embedding AI into products you already consume,



often without even telling you. **Your AI risk is increasingly someone else's AI risk.**

The pattern Protiviti sees globally is clear: Organisations that lead with governance are now deploying faster than those that led with pilots. Governance is not the brake; it is what lets you scale without stopping to relitigate every use case. Practically, that means three things will be critical as we head into 2027:

- An AI inventory that includes third-party embedded AI, not just what you built
- Clear accountability for each deployment, named and documented
- Workforce enablement measured by adoption, not training completions

If you cannot currently list every AI system touching your customers, that is the first conversation to have.

We asked CROs and CCOs three questions about their views on the organisation's ability to transform the enterprise, protect enterprise value, and respond with agility to market opportunities and risks. What did they tell us?

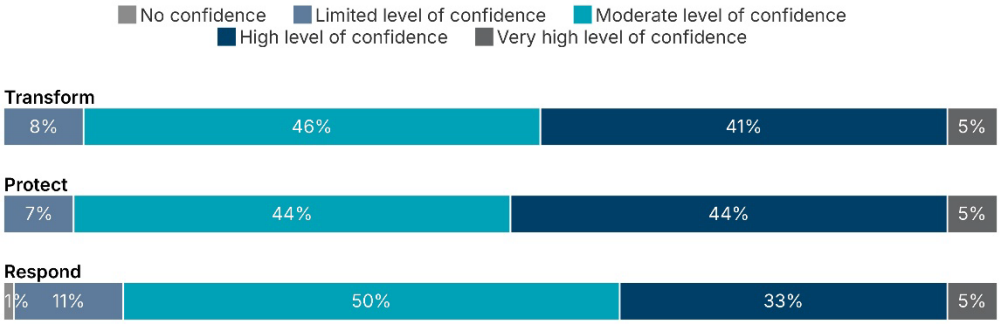
Risk and compliance leaders told us the gap is agility, and it is the most actionable finding in the survey.

Confidence in the ability to protect enterprise value is highest, with nearly half (49%) reporting high or very high confidence. Confidence in the ability to transform follows at 46%, while confidence in the ability to respond — meaning the ability to move with agility on emerging opportunities and risks — is 38%. Meanwhile, 11% say they have limited confidence in their ability to respond. That 11-point gap between protect and respond is the story.

Organisations have spent a decade building defences: They have frameworks, controls, three lines of defence and testing regimes. What they have not built is speed. The takeaway is that organisations can absorb a hit, but they struggle to move when the ground shifts.



Views about the ability to transform, protect and respond – CRO/CCO



This matters more than it sounds. Every risk topping the near-term list is a speed problem, not a strength problem. Cyber incidents are won or lost in hours. A critical third-party outage is measured in minutes of customer impact. **AI failures compound while you are still deciding who owns the decision.** Regulatory divergence across jurisdictions punishes organisations that need six months to change the process.

Here's the uncomfortable truth: A strong protect score can mask a weak respond capability, right up until the moment it matters. Controls tell you what should happen. They do not tell you how fast your organisation makes a decision.

What separates confident organisations from the rest is rarely more control. It is clearer decision rights under pressure, preauthorised playbooks and scenario testing against the specific disruptions at the top of their own risk registers.

We suggest you ask your executive team a simple question: In a live third-party outage, who makes the call on what happens next, and how long does that take? If nobody can answer that simple question clearly, you have found your top 2027 priority.

49%

have a high level of confidence in the organisation's ability to protect enterprise value.

What are the most significant near-term concerns and risks on the minds of CROs and CCOs?

It is interesting that the top three near-term concerns have not changed from last year: cyber threats, AI implementation risk and third-party risk. But what has changed is the intensity behind each of them.

Nine of the top 10 near-term risks were flat or lower year over year. Cyber remains the top concern but has eased. Regulatory change and fragmentation fell the farthest of any risk yet still ranks sixth. Economic conditions and third-party risk both softened but stayed in the top four. Do not misread that as relief — near-term risks are not receding.

Top five near-term risks – CRO/CCO

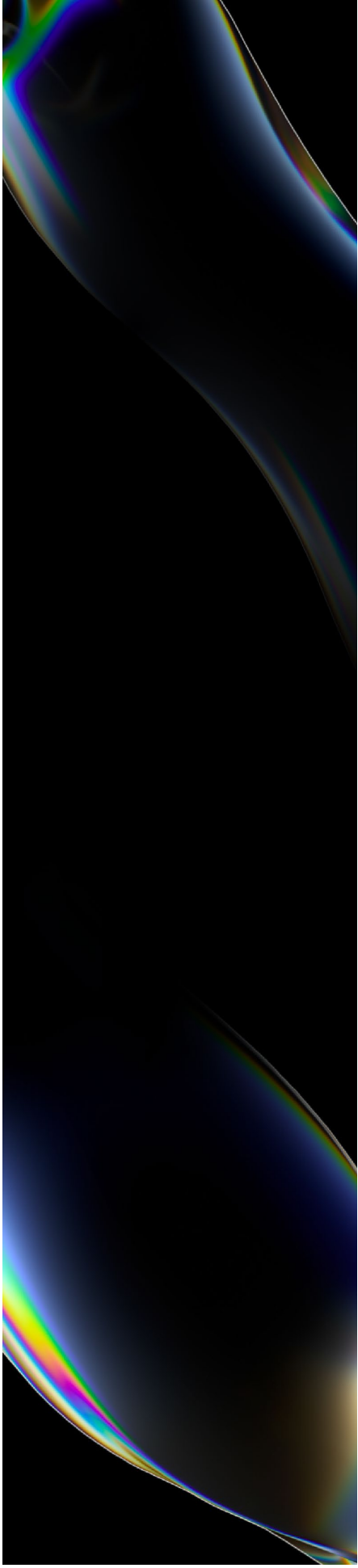
Risk description	2027	2026
Cyber threats	3.57	3.72
Emergence of new risks from implementing AI	3.46	3.43
Third-party risks	3.38	3.49
Economic conditions, including inflationary pressures	3.37	3.50
Skills and talent acquisition and retention, leadership development and succession challenges	3.35	3.29

Based on a five-point scale assessing agreement/disagreement.

Risk and compliance leaders ran hot in 2026 and are now recalibrating. This is a risk register maturing, not a threat landscape improving. Two indicators cut against the calming trend. Privacy and identity-protection compliance are the only top 10 risks climbing with conviction. Concern about the speed of disruptive innovation is also building. Taken together, they point to something specific: The worry is shifting from macro volatility toward data, privacy and technology outrunning the control environment.

Perhaps the most revealing finding is not in the CRO and CCO data at all. Internal audit ranks every protect-oriented risk materially higher than risk and compliance leaders do. Third-party risk shows the widest gap. AI and cyber follow closely behind. When your assurance function is consistently more concerned than your risk owners about the same exposures, one of two things is true: Either the controls are weaker than the first line believes, or internal audit is working from an outdated view. Both are worth knowing, and neither resolves itself.

That reconciliation is a two-week exercise with an outsised payoff, and it is the conversation we are having with most clients right now. The organisations that deliberately close that gap now are the ones avoiding uncomfortable conversations with regulators later.

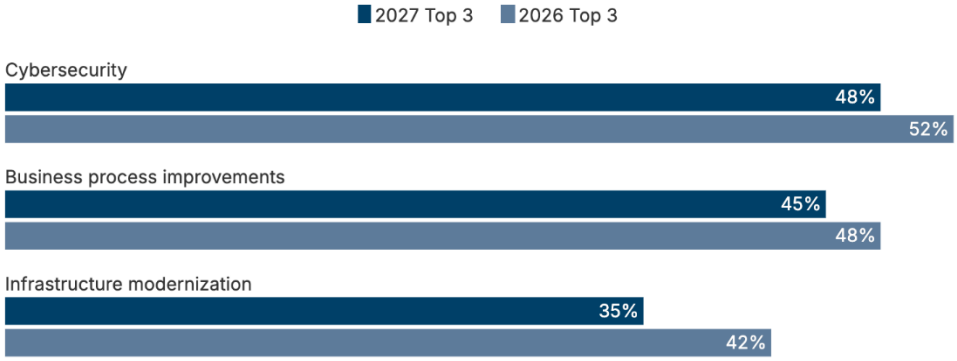


Given these near-term risk issues, where do organisations plan to invest most?

For risk and compliance leaders, the top three investment priorities are cybersecurity, business process improvement and infrastructure modernisation. Steady, sensible and unsurprising.

The interesting numbers are the movers. Data privacy nearly tripled, jumping from 7% to 20%. That is the sharpest rise in the entire investment list, and it aligns precisely with privacy being the fastest rising risk. Leaders are putting money where the concern is.

Top strategic investment priorities – CRO/CCO



48%

rank cybersecurity as a top strategic investment priority.

Two others should raise red flags. Third-party management sits at 14%, 10th out of 12. Crisis management sits at 4%, dead last and down from 8% last year. That is alarming, especially considering ecosystem partnerships are the top growth opportunity. Meanwhile, third-party risk is the third-highest near-term concern and shows the widest gap between internal audit and risk owners of any risk measured. Confidence in responding under pressure is the weakest of the three capabilities tested. **The areas with the largest strategic exposure and the weakest confidence are receiving the least investment.** You read that right. That is not a rounding error; it is a structural misallocation, and it is remarkably consistent across regions.

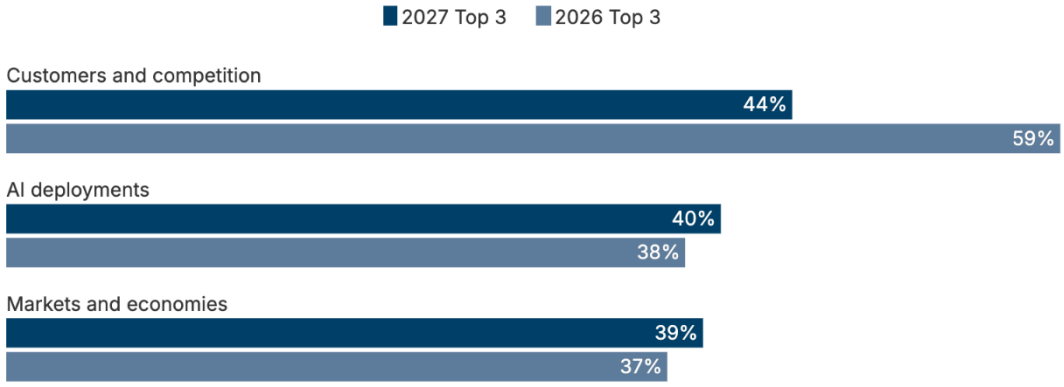
The likeliest explanation is that third-party and crisis capability get treated as compliance overhead rather than growth infrastructure. They do not have an obvious revenue story, so they lose the budget argument to things that do. The reframe is worth making internally: If partnerships drive your growth and resilience protects your license to operate, neither is overhead. Both are enablers.

Our advice going into 2027 planning is to stress-test the investment slate against the risk register. Where a top-four risk is drawing bottom-quartile investment, fix it.

How do CROs and CCOs view the 10-year risk outlook for their organisation?

The long-term picture is shifting from market position toward structural resilience, and the changes are significant. Customers and competition still rank first at 44%, but the figure fell sharply from 59%. That is the single biggest drop in the 10-year view. Security and privacy surged from 23% to 35%. Organisational resilience and culture climbed from 28% to 34%. Talent moved from 30% to 34%. AI deployments held near the top at 40%. Geopolitical challenges rose from 20% to 25%.

Top long-term risks – CRO/CCO



The long-term picture is shifting from market position toward structural resilience, and the changes are significant.

Here is a data point that stopped our team in its tracks: Quantum computing jumped from 1% to 8%. The figure is small in absolute terms but eight times as large as it was a year ago. That is what an emerging risk looks like just before it stops emerging. For anyone holding long-dated encrypted data — and that is every financial institution we can think of — harvest now, decrypt later is a live planning assumption, not science fiction.

Step back, and the 10-year story is coherent. A decade ago, the strategic question was, how do we beat the competition? Today, it is, how do we stay standing and trusted while the operating environment keeps moving? Security, resilience, talent and AI are all answers to that second question.

One tension is worth naming. Supply chains and third-party ecosystems slipped in the 10-year view, down to 19%. That sits awkwardly against ecosystem partnerships being the top near-term growth opportunity. **Leaders are betting on partnerships to grow while deprioritising the ecosystem risk that comes with them.** That inconsistency will resolve itself one way or another, and it is better to resolve it on your own terms.

The strategic implication for 2027 planning: Resilience and trust are becoming competitive differentiators, not cost centres. The organisations treating them that way are already pulling ahead.



Calls to action for CROs and CCOs

- **Confirm third-party risk findings with audit.** Run a joint review of your most critical suppliers with internal audit. Internal audit rates it materially higher than risk owners do, the widest divergence in the data. Either residual risk is understated or the assurance view is stale. Find out which and document the answer.

- **Move privacy up the agenda now.** It is the fastest-rising risk, and investment has already nearly tripled. Convert that spend into something concrete: a review covering AI data use, training data provenance and identity protection. Do it before a regulator defines the scope for you.

- **Strengthen incident response readiness.** Test response plans for the most likely incidents, including cyberattacks, third-party outages and AI failures. Close the response gap. Confidence in the ability to respond trails confidence in the ability to protect by 11 points. Fix it with decision rights, not more controls. Use preauthorised playbooks, named decision-makers and scenario tests against the three risks at the top of your own register: cyber incidents, third-party outages and AI failures.

- **Wire assurance into AI governance from day one.** Your AI priorities are already governance-led, which is right. Make internal audit a design partner rather than a downstream reviewer, and the concern gap narrows on its own. Start with an inventory that captures third-party embedded AI, not just what you built.

- **Reframe regulatory fatigue as operating discipline.** Regulatory concern fell more than any other risk. That is not a reduced obligation; it is familiarity. Convert the volume into a standing regulatory change capability so cross-jurisdictional divergence stays background noise instead of becoming a fire drill.

- **Redesign the risk target operating model.** Map where automation is absorbing effort, then redeploy that capacity against AI governance, third-party oversight and privacy, the areas where demand is climbing fastest.

Six moves, all achievable inside a quarter, and none of them require a transformation program. They require deciding that the gaps between how audit, the business and the market see the same exposures are worth closing deliberately. Where does your organisation sit against these six, and which one would move the needle most? That is your 2027 conversation.

About the survey

Our 15th annual **Executive Perspectives on Top Risks and Opportunities Survey** contains insights from 1,330 board members and C-suite executives around the world regarding their views on:

- Ability to transform and protect the enterprise and respond to market opportunities and risks;
- Opportunities for growth considering the current environment;
- Priorities perceived as most critical to maximising the value of AI deployments;
- The top risks on the horison for the near-term (two to three years ahead) related to 30 specific risks across three dimensions (transform, protect and respond);
- A discussion of their organisations' near-term strategic investment priorities, given the opportunities and the risks they face; and
- The long-term horison based on 11 risk themes that encompass the 30 near-term risk issues.

Our survey participants shared their views through an online survey conducted in June and July 2026.

About the author



Brian Kostek is a managing director and Protiviti's global CRO/CCO solutions leader. With nearly 20 years of experience consulting for financial services organisations, Brian also serves as the financial services industry leader for Protiviti's risk and compliance capabilities, where he focuses on solving clients' challenges in designing and implementing third-party risk, compliance management and operational risk management programs. His expertise spans third-party vendor risk, regulatory compliance risk, operational risk, operational resilience and control optimisation. Brian also leads the third-party risk management solutions within Protiviti's risk and compliance capabilities.

Contact Brian at brian.kostek@protiviti.com.

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

© 2026 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. 1026

protiviti®