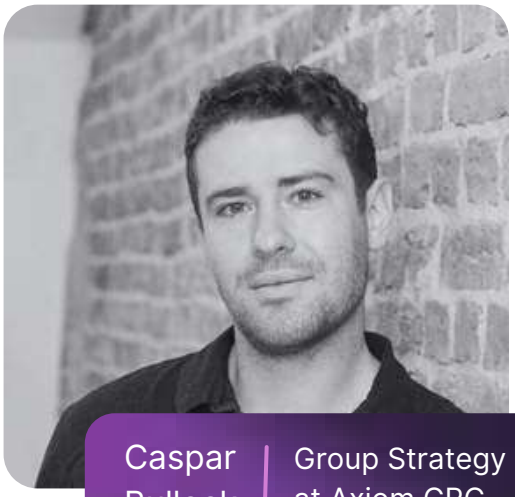
axiom grc

The Future of Governance, Risk and Compliance: **2026 Trends**

Foreword



Caspar Bullock | Group Strategy Director at Axiom GRC

Every year we rigorously survey our customer base. It's good for our business. Thousands of professionals: business owners, heads of risk, compliance, health & safety, InfoSec, cyber security or HR, all informing how we build our solutions and products. These thousands of clients have their ear to the ground on the most relevant forces affecting the governance, risk and compliance landscape, and who, like Axiom GRC, seek to respond to the signal of change before the noise. We recognise that these survey results are an invaluable insight into the forces shaping the GRC landscape. And so, in the hope that by distributing the key trends highlighted by our surveying, we are now publishing their results as part of annual whitepaper focussed on helping the GRC community navigate the challenges ahead.

Axiom GRC's findings highlight the potent trends affecting GRC professionals around the world. Two key themes ring particularly loudly this year: **AI & Cyber Risk**. AI is perceived with an uncertainty as to whether it poses more opportunity or risk for compliance professionals, whereas cyber threats are seen as the more immediate and real danger to business operations, requiring compliance professionals to manage all aspects of data, info and cyber security in increasingly compliant ways. Never has conformity to cyber security frameworks standards shown such a strong ROI.

We have combined all these surveys' results with the views of an expert selection of Axiom's 1,300 compliance specialists to bring you insights on the key GRC trends that could affect you as a compliance professional.

Axiom's survey results show advancements in technology and AI, growing cyber security risks and changing regulations have led to a perception of "riskflation" in the GRC community – driving them to rethink and readdress their approaches. For 2026 and beyond, compliance professionals recognise the need for an interconnected approach to managing risk where siloed approaches between departments no longer work.

AI is of course a key theme in this whitepaper, with the technology maturing at a much more rapid pace than GRC leaders could have anticipated when it exploded into the mainstream space in 2022. Specialist AI presents opportunity across the GRC space to optimise risk management, compliance eLearning and day to day operations. However, the adoption gap is stark. Axiom GRC research found that **84%** of workers across global organisations use AI tools at work. Yet only **13.5%** of organisations have a formal AI policy, and **41%** have not implemented preventative measures against the compliance challenges driven by AI. For enterprises and SMEs, it's a double-edged sword in the opportunities it presents, vs the risks it creates.

Cyber remains a defining external exposure for global organisations – with the volume of attacks outstripping historical levels. Threats are also evolving: RaaS lowers the barrier to entry; quantum-enabled risks loom; and supply chains are a primary attack path. Organisations must manage this risk more effectively; training teams is paramount – with **95%** of attacks caused by human error.

With the risk landscape increasing from all angles, Axiom GRC insights found that GRC leaders are prioritising single vantage point to mitigate these challenges. Research by Axiom GRC found that, currently, only **42%** of global organisations require **all** suppliers to follow their data and AI policies – leaving themselves open to attacks. The opportunities for health and safety risk management are vast, but organisations must have the right processes and platforms in place.

We hope the results prove helpful to you in navigating the risks and opportunities in the GRC world.

Why this paper is a must-read for GRC leaders

This white paper brings together market research from our GRC audiences and expert trend analysis to deliver a landmark resource for business leaders and senior teams.

Offering a strategic view of the evolving GRC landscape for 2026 and beyond, it explores four key themes set to shape the future of governance, risk, and compliance.

The four key themes set to impact the GRC landscape in 2026:

1. AI is outpacing GRC – amplifying future risks
2. Cyber security is the number one concern for GRC leaders
3. Single risk vantage point is a strategic imperative for modern GRC
4. New data and labour laws will impact GRC landscape

axiom grc

1.

AI and GRC

AI is expediting GRC processes – but causing an internal compliance headache

1.0 AI in action: adoption is happening at speed

AI represents a monumental shift for GRC. **Over 84% of our respondents to an Axiom survey** say they are already using AI tools. Adoption is accelerating, and as AI usage continues to grow, so too will the associated risks – alongside new opportunities driven by AI.

GRC leaders need to act now to manage AI effectively in the workplace. Without robust policies, strategies, and oversight, organisations risk exposing themselves to operational, compliance and reputational challenges over the long term. But our respondents don't have a consensus view on who is responsible for ensuring its compliant use – a key tension area in the GRC market.

Do you use AI tools for work (e.g. ChatGPT, DALL·E, Copilot)?

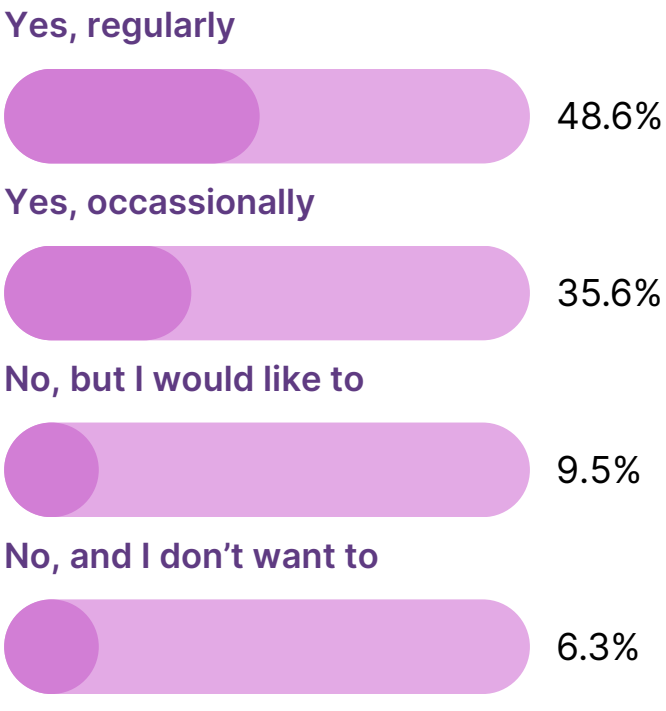


Diagram 1 – Use of AI tools in the workplace

1.1 Responsibility and accountability for AI is mixed

The mixed picture on AI's responsibility indicate many GRC professionals believe all employees should be responsible for the compliant use of AI (52%) while only **21% place primary responsibility with leadership** – highlighting the early and uncertain stage we are at with the technology's application in business.

Axiom GRC also found that the practical responsibility for setting rules and guidance varied – senior leadership held primary responsibility in **47% of organisations**, while in **22.5% no department or individual** was assigned responsibility at all. The processes governing AI's use in companies are not mature enough yet and this is a clear concern amongst our respondents.

Who is primarily responsible for setting rules or guidance on AI use in your organisation?

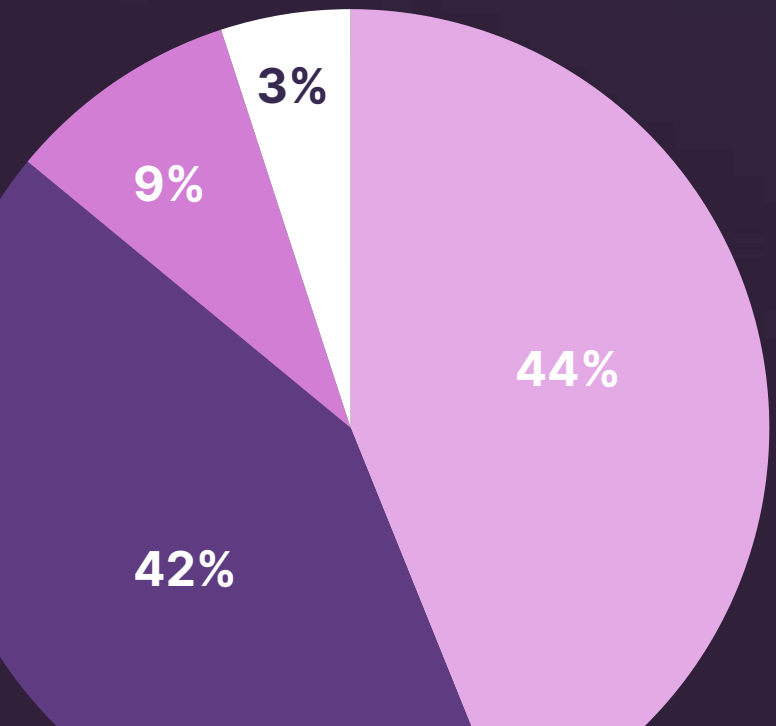
47% Senior Leadership | **12%** Legal/Compliance

5% HR | **14%** IT | **22%** No one currently

1.2 Many organisations yet to implement training and policies on AI

As AI adoption accelerates, understanding how organisations are responding - and what measures are in place to manage it responsibly – is critical. We asked organisations what procedures, training or other preventative measures they had implemented to protect against compliance breaches from AI. The results of this show a 50:50 picture of organisations who have put procedures in place to protect against AI compliance breaches. Overall it appears that even with the procedures in place, there is a lack of confidence in the respective measures.

Have you implemented any procedures, training or other preventive measures to protect against compliance breaches by AI?



- **44%** Yes, we have some but not extensively
- **42%** No, but we want to implement some
- **9%** Yes, we have comprehensive measures in place
- **3%** No, and we don't plant to

Diagram 2 - Research finds lack of confidence in preventive measures against compliance breaches

Axiom GRC surveys reveal a growing disconnect between the rapid adoption of AI and the governance structures needed to manage it effectively. While AI tools are already embedded in daily workflows, **only 13.5% of organisations have a formal AI policy**, with the majority either lacking clear guidance altogether or in the process of developing policies.

Does your organisation currently have a formal policy in place to govern employee use of AI tools? (e.g. ChatGPT)?

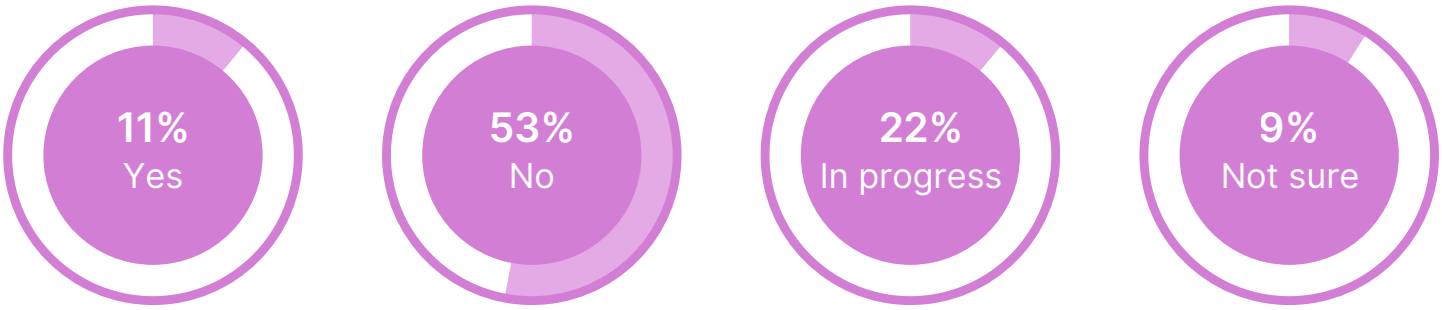
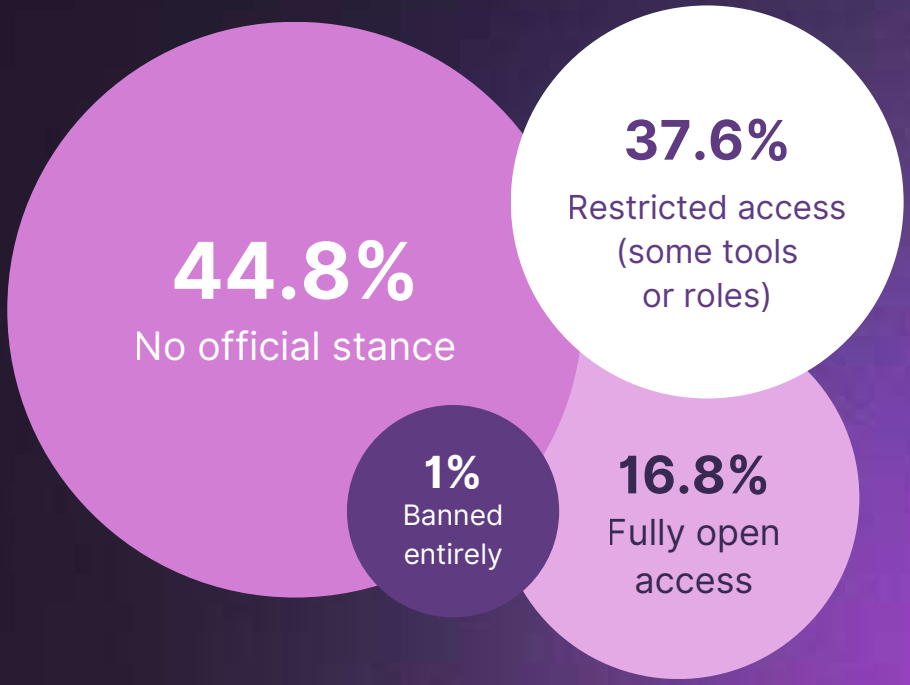


Diagram 3: Most organisations do not have a formal policy in place to govern AI use

Probing similar themes from different angles, our surveys found that nearly half of businesses actually have no official stance on AI tool access, creating inconsistency and fuelling the rise of Shadow AI - the term given to the unapproved use of AI tools. Shadow AI is a key GRC concern underpinned by the anxiety of sharing valuable corporate shared with public large language models.

What best describes your organisation's stance on employee access to AI tools?



Overall, the results highlight a clear governance lag: AI adoption is currently outpacing GRC's leadership's ability to manage it.

Diagram 4: Many organisations yet to establish an official stance on AI

1.3 So what? The risks of operating without AI policy

Angela Carter, Director of Legal Services at Axiom's Employment Law division (WorkNest) warns:

"Organisations that leave employees to interpret boundaries themselves increase risks around data protection, confidentiality, and intellectual property. Effective policies and guidance enable responsible use, ensure alignment with legal and ethical standards, foster innovation, and mitigate risks including data breaches and bias."

The ease with which employees can feed sensitive information into AI tools - whether for drafting documents, analysing datasets, or generating creative content – introduces serious exposure points for confidential and proprietary data. Without a clear policy, there is a very real danger that **trade secrets, client data, or commercially valuable insights** could be inadvertently shared, stored, or repurposed by third-party AI providers.

Angela adds: "AI's ability to generate content at scale raises complex questions around copyright and authenticity, blurring the lines between original and derivative work. In this rapidly evolving environment, organisations should act proactively - embedding robust AI usage policies, training employees on data handling, and implementing technical safeguards - to ensure that innovation doesn't come at the cost of compliance or competitive advantage."

Organisations already taking proactive steps - through formal policies, staff training, and controlled access - are better positioned to balance innovation with risk and secure long-term competitive advantage.

1.4 How to address the governance gap

While responsibility for AI varies between organisations, Lenitha Bishop, who heads Axiom GRC's data protection proposition (The DPO Centre), part of Axiom GRC's data protection division, **predicts an influx in AI Governance roles in 2026.**

"In many organisations, the responsibility for AI governance gets bounced between legal, risk and compliance, and IT teams, all of whom are still developing expertise needed in this fast-evolving area. AI governance is new territory for most, and its impact cuts across every business function.

"Our clients have found the most effective approach is appointing a dedicated individual to oversee AI governance across the organisation – someone who can align teams and provide clear direction to C-suites. As AI systems become more complex and integrated, AI governance will shift from 'nice to have' to a business-critical discipline."

In response to this demand, The DPO Centre now offers an outsourced AI Officer service. This role helps leadership teams embed AI across products and services responsibly, ensuring ethical, compliant adoption that strengthens trust while enabling confident innovation for businesses.

The positive: AI is enhancing GRC

1.5 The rise of narrow AI: specialisation, not generalisation

Shmuli Goldberg, Head of AI at VinciWorks, explains why GRC leaders leveraging AI specialisms are set to make the biggest gains.

"The most effective AI models today aren't those trying to do it all; they are designed to solve specific problems with precision. The more knowledgeable GRC leaders are about the tools available, the better they can implement them strategically."

"While the technology industry continues to focus on advancing Artificial General Intelligence (AGI), GRC is taking a more specialised approach. Instead of building single, generalised models, organisations are adopting targeted AI solutions developed to address specific compliance and regulatory challenges."

Specialised AI assistants are already emerging across core areas of GRC – from anti-money laundering and health and safety management to diversity, equality, and inclusion training. These targeted solutions deliver greater accuracy, contextual insight, and operational value, helping compliance teams automate high-volume tasks, identify patterns, and make better-informed decisions without losing human oversight.

Active learning methods can **90%** boost retention up to

AI is enabling compliance training to move beyond box ticking, making it more dynamic, personalised, and impactful.

1.6 AI is revolutionising compliance eLearning

AI is already transforming the way compliance eLearning is designed, delivered, and experienced. Rather than relying on static modules, **AI-powered training creates interactive learning environments** that employees remember and apply in their roles. Courses are built to encourage critical thinking and genuine behavioural change, with AI acting as a facilitator, coach, and guide throughout the process. Learners are engaged in conversation from the outset, for example, being asked to predict the outcome of a scenario before being guided deeper into the subject.

In June 2025, VinciWorks, launched 'Conversational Learning' – combining 20 years of compliance expertise with AI to create a learning experience that adapts to each individual's learning journey.

Shmuli Goldberg continues: "Research from the National Training Laboratory shows traditional lecture-based learning yields just **5% retention, while active learning methods can boost retention up to 90%**. Conversational Learning applies these principles through personalised, AI-driven experiences, significantly improving knowledge retention and engagement.

"The unanimous feedback we've received from tens of thousands of users highlights much higher engagement than traditional methods. Interestingly, the courses that perform best are those that involve ambiguity and real-world grey areas – such as equality, anti-money laundering, and online safety – where open dialogue and critical reasoning are most effective."

By embracing new delivery models that cater to different learning styles, AI is enabling compliance training to move beyond box-ticking, making it more dynamic, personalised, and impactful.

60% of global organisations identify AI and automated workflows/ tools as key investment areas for compliance and GRC functions.

1.7 AI-driven insights are driving smarter, faster, risk management

AI is transforming the way organisations approach risk management, shifting from manual, reactive assessments to continuous, real-time monitoring. By integrating AI into risk platforms, GRC leaders can analyse vast datasets far more quickly, identify emerging threats earlier, and allocate resources with greater precision. This not only strengthens resilience but also frees compliance teams to focus on strategic decision-making rather than administrative tasks.

Paul Cadwallader, Strategy Director at CoreStream GRC, explains: "AI integration allows risk management platforms to move beyond static reporting into dynamic, predictive analysis. Platforms should offer true customisation, flexing to how each organisation works and scaling with them as they grow. The focus will shift from tick-box compliance to delivering real business value, helping teams stay aligned, act faster, and make better-informed decisions. For GRC leaders, this creates a real opportunity to anticipate risks, respond faster, and demonstrate the value of governance and compliance as enablers of business growth, not just safeguards."

CoreStream GRC, Axiom GRC's global risk management platform, includes an optional AI integration module that parses vendor documentation, leverages trust centre data, and maps findings to industry frameworks. Where gaps remain, teams can issue targeted questionnaires, only when needed. By streamlining reporting and generating improved insights for GRC leaders, AI makes risk management faster, more agile, and demonstrably valuable.

What technology are you planning to invest in for compliance?

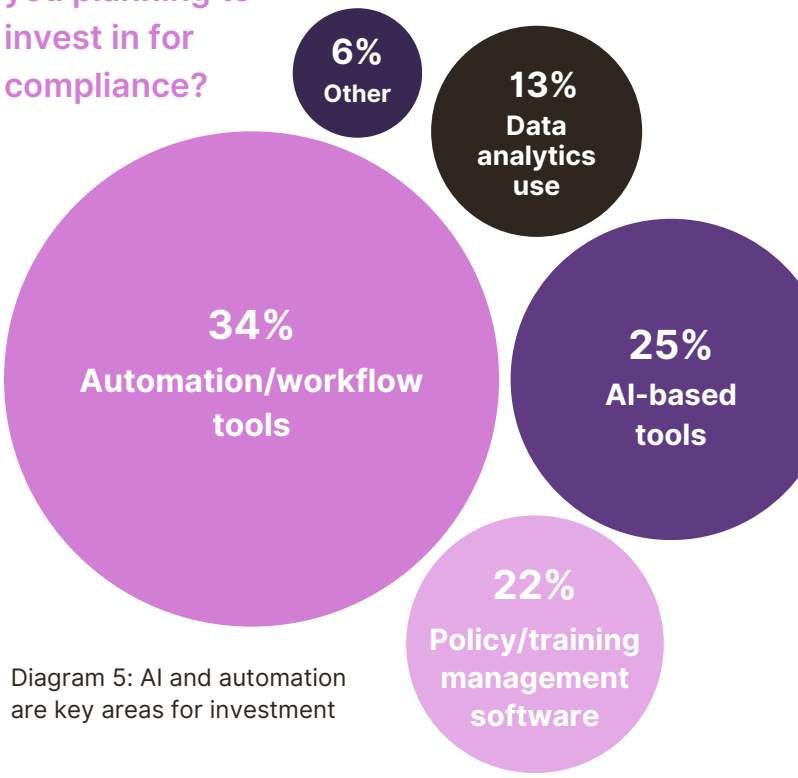


Diagram 5: AI and automation are key areas for investment

1.8 From risk to resilience: using ISO frameworks to govern AI

As AI becomes embedded in core business processes, GRC leaders must not only manage the risks AI introduces but also demonstrate to regulators, partners, and clients that these risks are managed in a structured, transparent way.

Existing and emerging ISO standards provide useful reference points:

ISO 42001 (published in 2023) is the first international management system standard specifically for AI. It offers a framework for addressing issues such as bias, explainability, and oversight, all of which are increasingly scrutinised by regulators and business partners alike.

In parallel, **ISO 27001** remains critical, as AI models rely heavily on data integrity and secure information flows. Embedding ISO 27001 controls into AI systems strengthens resilience against breaches and ensures that data used to train and operate models is safeguarded.

While not a silver bullet, these standards provide organisations with recognised mechanisms to align AI adoption with existing governance expectations. From a global competency perspective, ISO certification demonstrates validation and integrity, differentiation against competitors.

Olumide Alade, Lead Auditor at IMSM, Axiom GRC's ISO certification division, explains:

"Certification is often viewed as the finish line, but in reality, it's the foundation. The value of ISO frameworks lies in embedding continuous improvement into the organisation – creating a culture where AI risk is monitored, learned from, and adapted to in real time. Organisations that treat standards as living systems rather than checklists will be the ones that maintain trust as technology evolves."

The critical issues shaping AI governance

1.9 Risks from reliance and model degradation

Across industries, the use of LLMs for first-tier conversations is increasingly prevalent. Risks arise not only from a governance perspective around accuracy and output quality, but also when the underlying AI technology degrades. Few companies build AI in-house; most rely on external models, meaning when new models are released, it can impact performance quality.

The launch of AI agents – LLMs with the power to take action in the real world – increases the need for clear boundaries: where AI can operate independently, where human oversight is mandatory, and how to detect and stop incorrect behaviours.

1.10 The impact on business continuity

Beyond risks linked with policy and usage, **organisations must treat AI as a third-party service within their GRC frameworks**. Unlike traditional in-house systems, most AI tools rely on external providers, creating dependency on third-party infrastructure for critical business functions. This reliance introduces new business continuity risks that must be actively managed.

AI outages, whether caused by large-scale grid updates, capacity shortages, or technical failures in data cooling centres, can disrupt essential operations with little warning. The global concentration of AI computing power in a handful of providers amplifies systemic risk, as a single outage can cascade across multiple industries and geographies simultaneously.

> "Effective GRC frameworks should incorporate robust resilience strategies: supplier risk assessments, multi-vendor approaches, and contingency plans to maintain operational stability during AI service disruption."
>
> **Shmuli Goldberg | Head of AI at VinciWorks**

1.11 EU's AI regulation will lay regulatory foundations for others – but also underpins the regulatory divergence

While global legislation on AI is still in its infancy, the European Union's upcoming regulation is significant in its breadth and primacy as the first significant bill. The EU AI Act is the first of its kind and takes a risk-based approach. It categorises AI systems from minimal to unacceptable risk, placing the greatest obligations on high-risk applications such as those used in recruitment, law enforcement, and critical infrastructure. Nowhere will have introduced such wide-ranging conditions on corporates for the responsible use of AI. UK has proposals already in progress on its own legislation which are expected to sit somewhere between the US and EU's position. The USA has an intrinsic state-by-state variance in its approach to regulating AI. By comparison to Europe, the USA is not imposing stringent limitations federally but US states are anticipated to continue to release their own specific legislation – leading to intra-state regulatory divergence, which increases complexity for organisations.

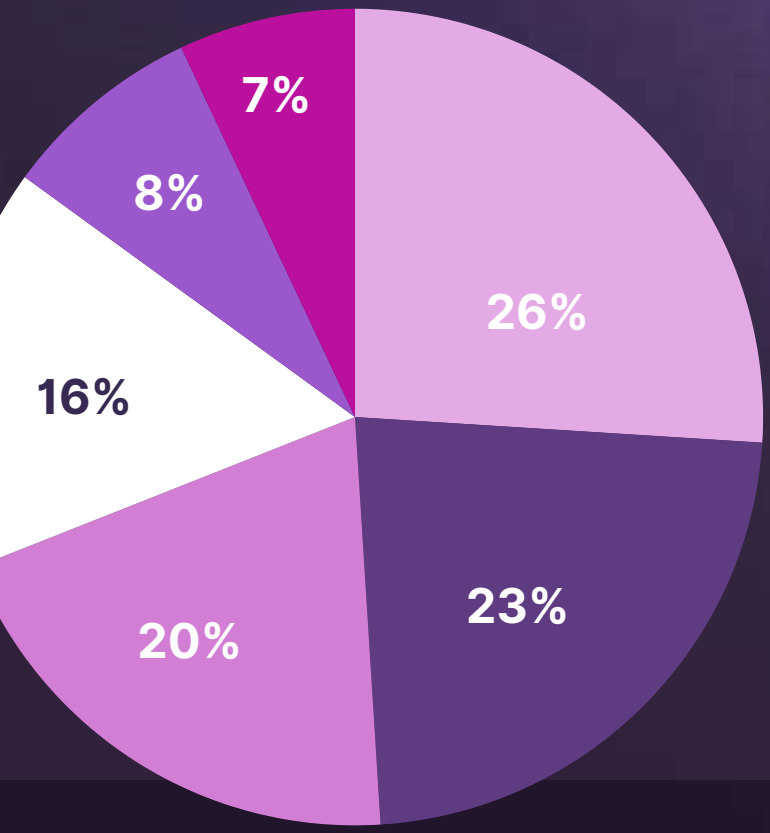
Not only do organisations need to develop clear GRC frameworks and policies on AI but they need to do so in a way which acknowledges the different political environments in which they operate. Reacting promptly, reading the EU AI Act closely, and understand the essence of its implications sooner rather than later will better position businesses to adapt to future regulations as they inevitably come into force.

1.12 Ethical conversations around AI

Axiom GRC observes that, as AI adoption grows, so do ethical considerations. Our research indicates that businesses must not go too far down the road of applying AI without the requisite ethical guardrails. To install such guardrails, our surveys also reveal organisations are employing or upskilling employees into ethical AI and compliances roles.

The core thrust behind compliance professionals' **reservations on using AI were largely down to bias and discrimination in automated decision-making (41%).** While many enterprise level AIs include bias disclaimers, there is a growing cultural awareness on ethical responsibility, which is driving customer decisions and informing internal strategies.

What are your main reservations about using AI in your role?



- **26%** Bias and discrimination in automated decision-making
- **23%** GDPR and data privacy concerns
- **16%** Lack of transparency or explainability
- **8%** Job displacement or deskilling
- **7%** None
- **20%** All of the above

Diagram 6: Bias and discrimination deter AI conscious individuals

Not far behind are understandable concerns (23%) around GDPR and data privacy and the perceived risk that data can be misused at scale by AI models. For a significant minority (1/5 of our respondents), "all of the above" concern them: transparency shortcoming, GDPR, job displacement and bias.

Noticeably, for GRC respondents, job displacement surprisingly ranks quite low in their worries. When it comes to the complexity of managing AI internally, the one department which stands to benefit seems to be risk and compliance, the department which is tasked with invigilating company-wide use of AI. This helps explain why job concerns in GRC are less pronounced than other departments. Organisations must demonstrate accountability and responsibility to avoid bias being introduced, as the risks can have significant costs to organisations from a financial and brand perspective. Effective training on AI bias and regular human monitoring can reduce risks.

1.13 Key takeaways on AI

Organisations need to address AI from a compliance perspective promptly before it can become a catalyst for growth.

Those that leverage the opportunities AI presents – balancing innovation with governance - will be best positioned to reap the rewards.

AI checklist for GRC leaders:

Clarify accountability

Assign clear responsibility at board or officer level to ensure oversight and escalation. AI governance cannot drift between departments.

Implement policy

Establish formal AI usage policies covering confidentiality, data handling, and approved tools to reduce ambiguity and risk.

Upskill employees

Train staff to use AI responsibly, challenge outputs, and recognise ethical concerns. Human error drives most compliance breaches.

Eliminate Shadow AI

Provide sanctioned alternatives, monitor adoption, and enforce governance consistently.

Integrate into GRC systems

Embed AI oversight into risk registers, audits, and incident processes to ensure accountability is systemic, not reactive.

Adopt global standards

Demonstrate robust, credible compliance frameworks.

Embed ethics

Position ethical AI as a core part of ESG and organisational culture.

Continuously validate

Test and monitor AI systems regularly, like any other critical system, to maintain accuracy and trust.

Plan for outages

Build resilience with supplier risk reviews, multi-vendor models, and continuity plans. AI is a service, not infrastructure.

Anticipate regulation

Monitor evolving AI regulations such as the EU AI Act and UK frameworks. Embed adaptability within governance to maintain compliance, manage cross-border differences, and respond swiftly to emerging global legislative changes.

Manage interdependencies

Map ecosystem risks across supply chains, data flows, and people.

Evidence value

Measure trust, culture, and compliance outcomes, not just efficiency gains, to demonstrate AI as a strategic asset.

2.

Cyber security and GRC

Cyber security is the number one concern for GRC leaders

2.0 Growth in cyber threats surpasses historical levels

Globally, the vended cyber security market is expected to grow 12.4% annually between 2024 and 2027, outstripping historical levels of growth[1]. In the UK, four in ten businesses reported experiencing a cyber attack in the last 12 months, with phishing attacks being the most prevalent – affecting 85% of businesses[2].

As the volume and complexity of cyber attacks increase, organisations must adopt a proactive approach to digital risk. Cybersecurity, data governance, and operational resilience should be embedded into broader GRC strategies. Media coverage frequently highlights significant data breaches and their detrimental effects. These threats are not limited to large enterprises; SMEs are equally at risk, with potentially business-compromising consequences.

2.1 Building a human-centred security culture

**According to Mimecast's 'The State of Human Risk Report'*

[1] McKinsey & Company. (2024). Global Cybersecurity Outlook 2024.
[2] UK Government. (2024). Cyber Security Breaches Survey 2024.

> "Cyber security starts with people. The biggest risk to businesses is their own teams"
>
> **Luke Peach**
>
> **Head of Information Security Operations at Axiom's cyber division**

Luke Peach, Head of Information Security Operations at Axiom GRC's cyber division (BulletProof Cyber Security), emphasises the importance of training as the first step in maintaining a secure organisation

The rise of AI-powered phishing and social engineering tactics have made it easier for malicious actors to exploit human vulnerabilities. Cyber attackers can easily generate highly professional, tailored emails using tools like ChatGPT, making scams harder to detect by the average employee.

"Invest in your people. Staff awareness training, phishing simulations, and ongoing education are essential to create a workforce alert to risks at work and at home.

"Hybrid and remote working increases risk further. Organisations with multiple security layers, such as VPNs and network usage guidance, improve protection, but ultimately rely heavily on their people in contrast to those operating from office-based roles. Training staff to be more security-conscious in general – whether managing their own bank accounts or social media – helps develop the instincts that safeguard company systems too. A culture of cyber responsibility starts at the individual level."

Building this culture requires consistent investment in both technology and people. Regular staff training, proactive threat detection, and clear reporting frameworks can dramatically reduce the likelihood of breaches. Without these safeguards, cyber threats can quickly escalate into significant financial, reputational, and operational damage. By embedding awareness into daily routines and aligning human vigilance with technical controls, organisations can transform their biggest vulnerability into their strongest line of defence.

2.2 Zero Trust as a solution to human error

As threats increase, Axiom GRC notes organisations are adopting a 'Zero Trust' approach, which assumes no user or device should be trusted by default – even within the network. While effective, it comes with operational implications. By definition, every access request - to a system or file - must be authorised, requiring a capable, 24-hour security team; otherwise the impact on productivity may be significant.

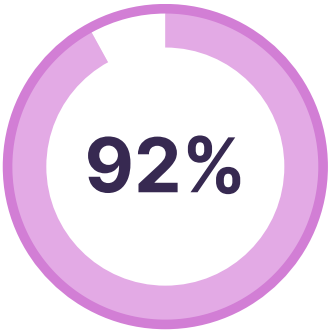
Zero Trust policies also extend to supplier onboarding and internal workflows. Mandatory verification at every login and rigorous supplier vetting can introduce delays, making it essential to balance security with practicality.

Luke Peach explains: "Rather than relying solely on strict Zero Trust frameworks, organisations can take a more nuanced approach by carefully managing access permissions and embedding cyber security into wider GRC processes. Establishing clear rules on who can access what, when, and why – supported by regular audits – protects critical assets without paralysing operations. Crucially, partnering with trusted cyber security specialists and integrating robust processes into enterprise-wide governance balances protection with practicality, ensuring resilience against threats while enabling business to move at pace."

2.3 Legacy technology: A breach waiting to happen

Outdated infrastructure is a common vulnerability often overlooked. Failure to review and update security solutions leaves businesses open to zero-day attacks, as attackers target older, unpatched systems.

Maintaining up-to-date systems - through security patches, retiring unsupported software, and upgrading infrastructure – should be central to any cyber resilience plan.



of organisations with UK Cyber Essentials are less likely to make a claim on cyber insurance

Achieving industry-recognised security standards should be the baseline for organisations. As an example, research from the UK's National Cyber Security Centre (NCSC) found that organisations who implement the UK government-backed Cyber Essentials scheme, were 92% less likely to make a claim on their cyber insurance (*NCSC, 2024*).

2.4 Hidden entry points through supply chain

As organisations strengthen their own cyber security posture, attackers are increasingly targeting softer entry points: the supply chain. Third-party providers, contractors, and service partners can all serve as conduits for cyber criminals, creating vulnerabilities that bypass otherwise robust internal systems. In reality, an organisation is only as secure as the weakest link in its supply chain.

Global organisations should embed supply chain cyber risk directly into their GRC frameworks, recognising it as both a compliance and resilience priority.

Step 1

Due diligence and verification:

Conduct cyber risk assessments for all suppliers, regardless of size, before onboarding.

Step 2

Contractual safeguards:

Embed requirements for recognised cyber security standards (e.g., ISO 27001, Cyber Essentials) within supplier contracts.

Step 3

Ongoing monitoring:

Move beyond one-off checks to continuous oversight, including mandatory incident reporting from suppliers.

Step 4

Scenario testing:

Use tabletop exercises to simulate supply chain breaches and stress-test response plans.

2.5 The next frontier of cyber risk: RaaS and quantum AI

The cyber threat landscape is evolving at a pace that challenges even the most resilient cyber security and GRC frameworks.

Ransomware-as-a-Service: Lowering the bar for attackers
What was once the domain of highly skilled cyber criminals has now become widely accessible.

Ransomware-as-a-Service (RaaS) operates like a commercial marketplace - malicious actors can purchase or subscribe to ransomware kits, often complete with customer support, tutorials, and even 'success guarantees.' This model significantly lowers the technical barrier to entry, expanding the pool of attackers and increasing the volume of incidents. For organisations, the implications are twofold: attack frequency is rising: small and mid-sized enterprises are no longer "too small" to target.

Supply chain vulnerabilities amplify risk: Attackers increasingly exploit smaller suppliers as a back door into larger enterprises, often using RaaS techniques.

> "Effective GRC requires building resilience through tabletop exercises, tested incident response plans, and investment in staff training to reduce the risk of a successful breach."
>
> **Luke Peach**
>
> **Head of Information Security Operations**

Quantum AI: A new era of cyber threats

While still emerging, quantum computing and AI pose potential risks that could fundamentally reshape cyber security. **Quantum-powered AI could:**

- Break traditional encryption methods, rendering current security protocols obsolete.
- Dramatically accelerate data-cracking capabilities, reducing the time needed to exploit vulnerabilities from years to hours.
- Automate and scale sophisticated attacks with unprecedented speed and precision.

Although mainstream quantum AI threats may be several years away, the window for preparation must begin now. Organisations integrating AI into their operations should start incorporating quantum risk scenarios into their long-term cyber strategies. This includes monitoring advances in post-quantum cryptography, building flexible infrastructure capable of rapid upgrade, and partnering with cyber experts who can track emerging risks.

Ultimately, the path forward requires both cultural and technical evolution. Cybersecurity cannot sit solely within IT - it must be embedded across GRC functions, and championed at every level of the organisation.

2.6 Top 8 cyber resilience measures for organisations

Enforce least-privilege and role-based access

Limit access so users, devices, and systems have only the permissions strictly needed for their function. This minimises internal exposure and reduces lateral movement risks by attackers.

Continuous identity validation and contextual access

Apply dynamic checks before granting access - considering device posture, user behaviour, and session risk.
Re-authenticate during sessions when anomalies are detected.

Rigorous third-party penetration testing

Engage external penetration testers to uncover blind spots, validate existing controls, and stress-test access logic under real-world conditions.

Managed threat detection and monitoring (24/7)

Implement, or outsource to, a trusted partner for continuous SIEM monitoring, threat detection, and alert triage to gain specialist expertise without overburdening internal teams.

Secure-by-design architecture

Embed security precepts at the design stage, not as an afterthought. Incorporate defence-in-depth, minimise attack surfaces, and compartmentalise systems rather than bolting on controls later.

Resilience and continuity planning for cyber disruption

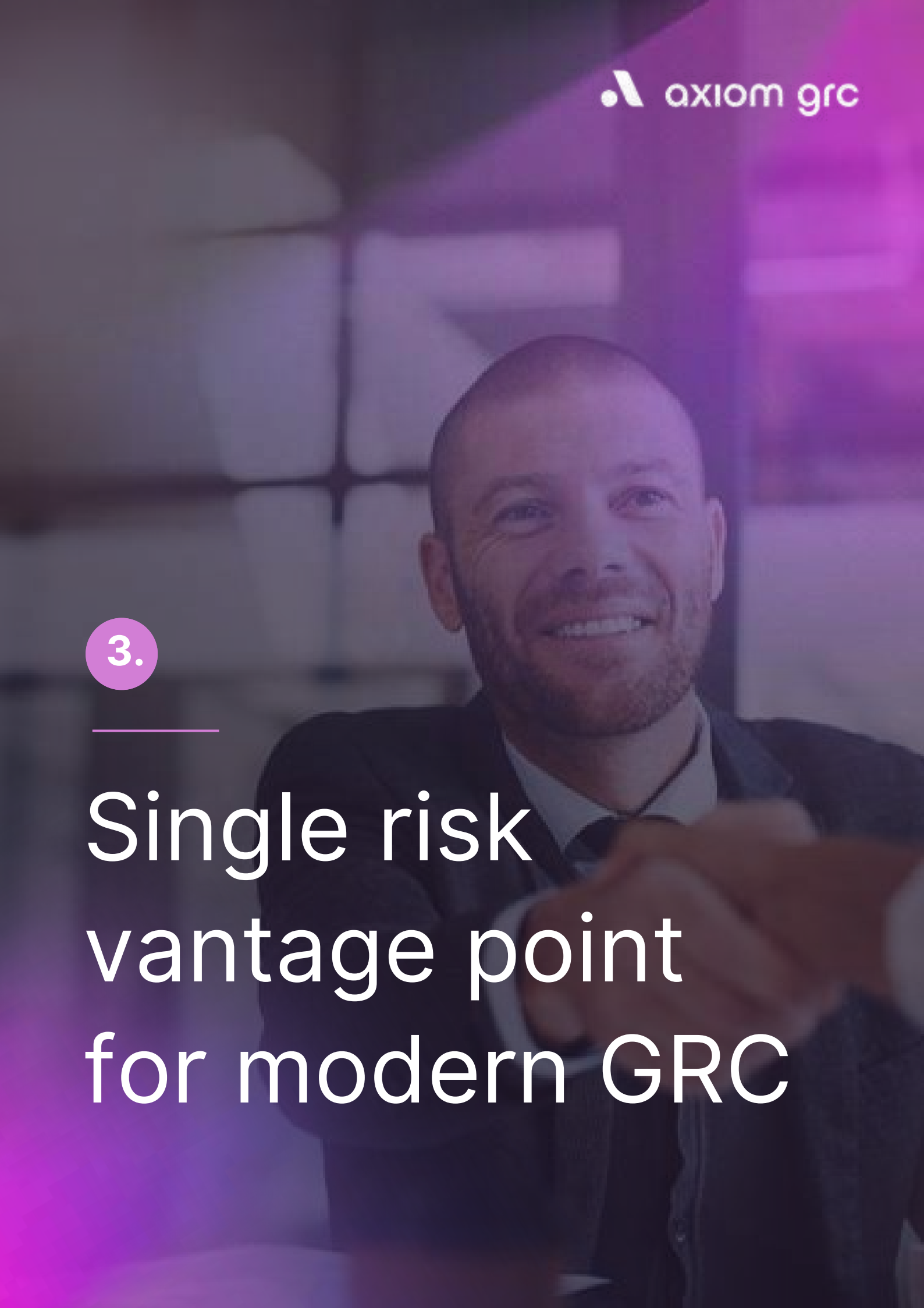
Prepare for infrastructure failures, cloud outages, or coordinated attacks by establishing fallback systems, maintaining tested backups, and building multi-vendor dependencies.

Supply chain and vendor security demands

Extend security expectations to suppliers. Enforce access controls, audit rights, and compliance standards – recognising that weak links in your supply chain are frequent entry points for attackers.

Partner with trusted security expertsoutages

Leverage external capabilities for holistic protection, strategic oversight, and rapid incident response. Axiom GRC's cyber division supports organisations of all sizes globally to proactively protect their data, ensure compliance, and stay ahead of evolving threats.



Single risk vantage point for modern GRC

Single risk vantage point is a core priority for GRC leaders

3.0 Why siloed approaches create risk mismanagement

Managing GRC in isolation - with separate teams, systems, and reporting lines - creates blind spots, drives inefficiencies, and amplifies risk exposure. In today's complex regulatory and risk environment, disconnected GRC frameworks are no longer sustainable.

Siloed GRC approaches can lead to:

- **Missed insights:** Isolated GRC programmes fail to share data, preventing organisations from identifying interconnected risks and trends across the enterprise.
- **Operational inefficiencies:** Disconnected systems and manual processes create redundancies, wasting time and resources while driving up operational costs.
- **Increased security threats:** Disparate systems create more multiple potential entry points for cyber threats, heightening the organisation's exposure to breaches and other security incidents.
- **Reactive decision-making:** A fragmented GRC approach shifts decision-making from strategic and proactive to reactive, limiting the organisation's ability to anticipate issues or capitalise on opportunities.
- **Incomplete risk coverage:** Without cross-functional collaboration, risks are not always linked to the assets they influence, leading to unknown vulnerabilities and an increased likelihood of unforeseen challenges.
- **Slower communication:** Silos impede rapid information sharing and collaboration between departments, slowing down decision-making and weakening responses to emerging risks.
- **Regulatory non-compliance:** Inconsistent policies and fragmented data across siloed platforms make it difficult to enforce standards and maintain alignment with industry regulations, potentially resulting in fines and legal complications.

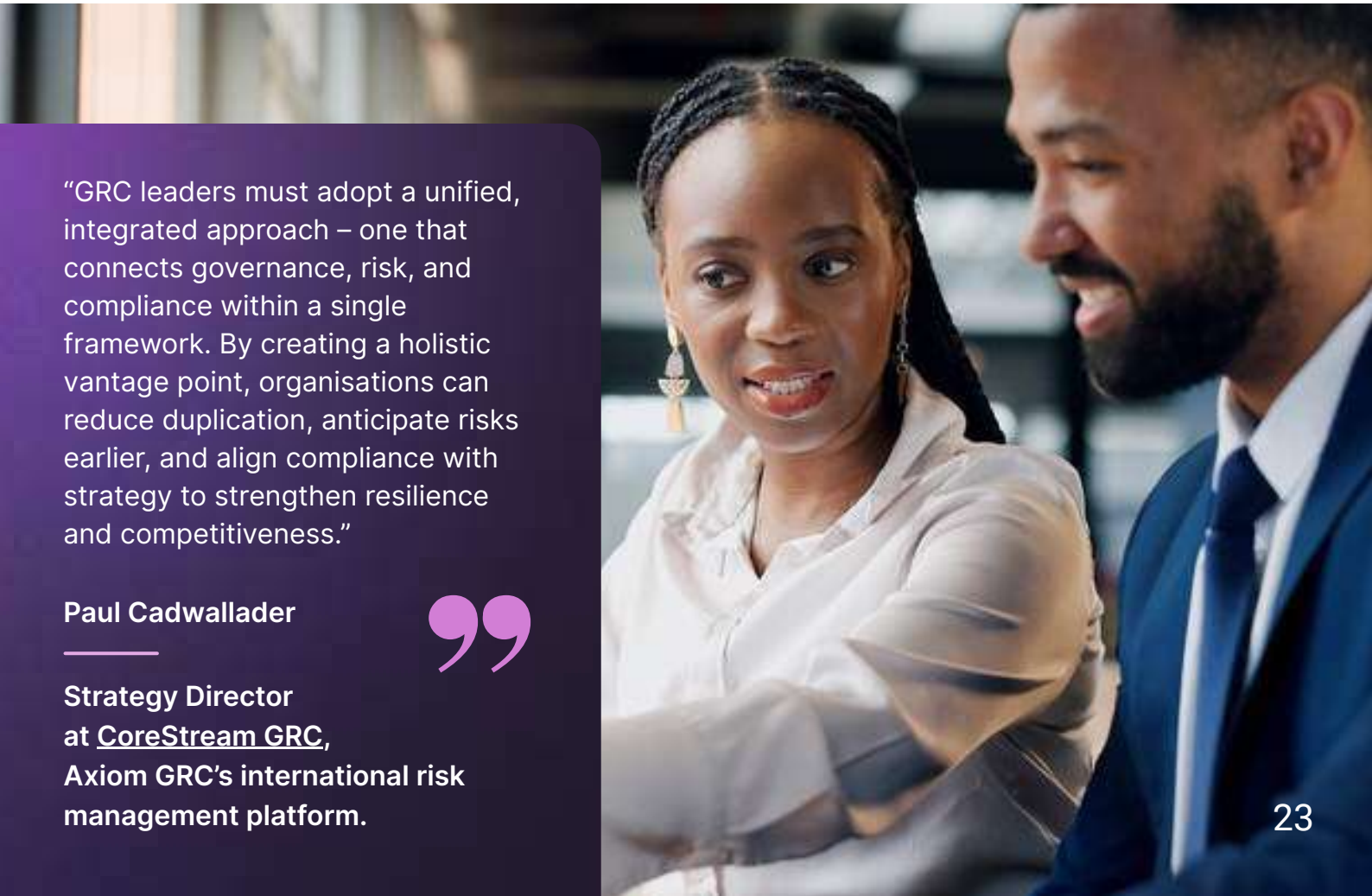
3.1 Regulatory intelligence as a catalyst for integration

As the regulatory landscape continues to expand across AI governance, ESG reporting, data protection, environmental compliance and health and safety, the need for real-time visibility has never been greater. Regulatory intelligence sits at the centre of this challenge, enabling organisations to track, interpret and respond to evolving laws and standards through a single, unified lens.

Without this integration, compliance functions risk working in isolation - interpreting legislation differently, applying inconsistent controls, and reacting to change rather than anticipating it. Centralising regulatory intelligence within a unified GRC ecosystem connects compliance insights with operational data, policies, and training. This ensures that every function is aligned, every update is actioned consistently, and compliance evolves in step with organisational risk.

Matt Reid, Managing Director at Barbour EHS, Axiom GRC's regulatory intelligence platform, explains: "Trust is the foundation of effective governance, and it depends on consistency. When every department operates from the same verified regulatory intelligence, leaders gain the confidence to make decisions that stand up to scrutiny – internally and externally. True regulatory intelligence doesn't just inform compliance; it unites it. It creates a single source of truth that enables organisations to act with clarity, anticipate change, and build lasting confidence among regulators, employees, and clients alike."

By embedding regulatory intelligence into the GRC ecosystem, organisations transform compliance monitoring from an administrative task into a strategic capability - one that strengthens transparency, accountability and enterprise-wide resilience.



"GRC leaders must adopt a unified, integrated approach – one that connects governance, risk, and compliance within a single framework. By creating a holistic vantage point, organisations can reduce duplication, anticipate risks earlier, and align compliance with strategy to strengthen resilience and competitiveness."

Paul Cadwallader

Strategy Director at CoreStream GRC, Axiom GRC's international risk management platform.

3.2 Supply chain visibility is more crucial than ever

Global supply chain disruptions have reinforced the importance of resilience and strategic sourcing across the GRC landscape. Following a series of high-profile 'weak link' failures, strengthening supply chain GRC is expected to be a defining priority for organisations in 2026.

Findings from our surveys highlighted a significant gap in supply chain and third party compliance, particularly in how organisations enforce their own governance frameworks to suppliers, with only **42% of organisations demanding that all suppliers must adhere to their data protection and AI policies**.

As highlighted in Section 2.5, weak links in supply chains create significant risk across all areas of GRC – from cyber security and data protection to health and safety.

Organisations which fail to demand full adherence from their suppliers risk undermining their own resilience and regulatory standing.

Axiom GRC's very own supply chain compliance expert Phil Jones provided further insights on the importance of achieving supply chain visibility:

"Companies often know their Tier 1 suppliers, but not Tier 2 or 3. Hidden vulnerabilities can cause cascading disruptions, so visibility must extend over multiple tiers."

Using a fully-integrated risk and compliance ecosystem enables organisations to achieve a single vantage point across all aspects of compliance - including supply chain management.

Do you require all third parties or suppliers to adhere to your data protection and AI policies?

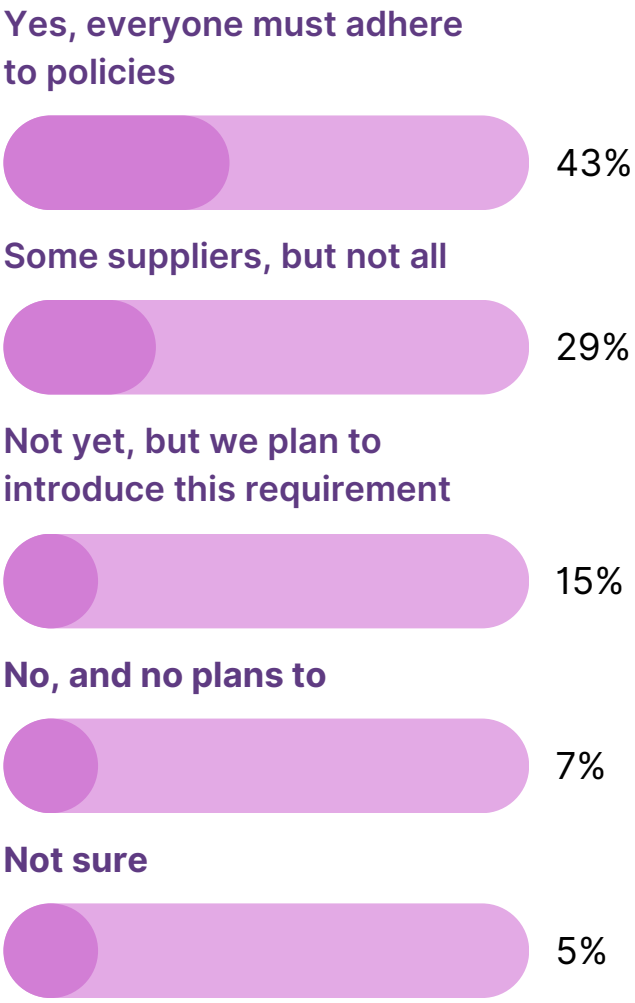


Diagram 7: Gaps in supply chain policies and data protection

3.3 Interdependency risk and the impact on supply chain

Axiom GRC notes that: “One of the biggest underestimated risks for facilities and supply chain that we see across our client base is interdependency risk - the cascading impact of a disruption in one part of the system on seemingly unrelated parts.

“From a health and safety perspective, facilities teams often view risk locally (general and specialist risk assessments, fire safety, emergency preparedness and training), while supply chain functions view risk more broadly (e.g. supplier failure, transport delays). Most organisations treat risks in silos, rather than as an interconnected network.”

Phil Jones

COO, Vantify

3.4 Key takeaways on creating more resilient supply chains

A joined-up approach to health and safety is essential for supply chain resilience. When standards, systems, and responsibilities are aligned across internal operations and external partners, organisations can reduce disruption, protect people, and build greater trust with regulators and stakeholders alike.

Adopt a unified risk framework

Align supply chain and facilities risk assessments under a common standard such as ISO 45001. Map risks on the same scale, whether they originate internally or externally.

Extend health and safety standards to suppliers

Conduct supplier audits that go beyond quality and cost, ensuring health, safety and ethical labour conditions are met. Apply the same expectations across all tiers of your supply chain.

Share data and visibility

Use integrated EHS and supply chain risk systems, such as the Vantify Ecosystem, to track incidents, near misses and disruptions. Use insights to improve collaboration and prevent recurrence.

Create joint governance

Form cross-functional committees and shared KPIs that unite supply chain, procurement, and health and safety leaders, ensuring joint accountability for both performance and safety outcomes.

Build a shared safety culture

Equip supply chain managers with health and safety knowledge, and vice versa. Reinforce a safety-first mindset across all partners to embed consistent behaviours.

Stay ahead of regulation

Integrate regulatory tools like Barbour EHS to monitor evolving legislation. Use this insight to anticipate change and maintain compliance proactively.

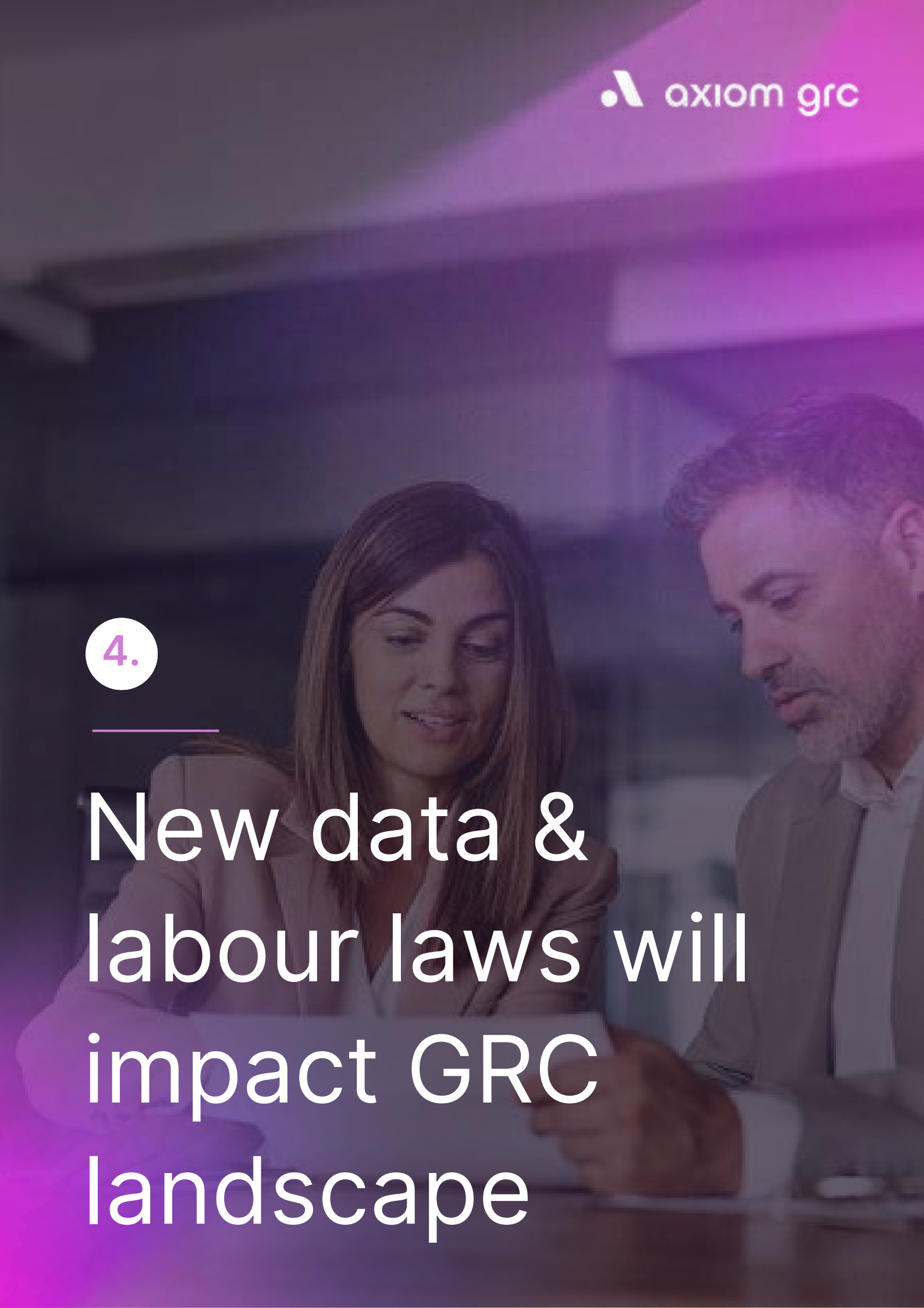
Leverage technology

Use predictive analytics to identify emerging risks and AI-driven supplier scoring to assess performance across safety, sustainability, and financial stability.

"Siloed approaches can no longer deliver the resilience businesses need. By integrating supply chain, health and safety, and wider governance functions into a single framework, organisations gain transparency, agility, and stronger assurance for boards and stakeholders."

Phil Jones

COO, Vantify



4.

New data & labour laws will impact GRC landscape

The new laws set to have significant impact on business landscape

4.0 Speed of regulatory changes causing concern for GRC leaders, particularly with respect to labour laws

Keeping pace with regulatory change has emerged as the single biggest compliance challenge for organisations today – particularly in the UK.

Research conducted by Axiom GRC's compliance eLearning platform, found that **44.3% of organisations** identified this as their top concern - ahead of embedding compliance culture (**24.8%**), staff engagement and training (**19%**), and resource constraints (**11.9%**).

This concern is well-founded. The **Employment Rights Bill,** expected to deliver sweeping reforms to workplace protections, and the **Data Use and Access Act (DUAA)**, which introduces stricter data protection, digital identity, and automated decision-making rules, are just two examples of the new legislation set to redefine compliance obligations in the UK.

Both carry significant implications for HR, legal, data, and risk teams - creating a rapidly shifting compliance landscape that demands agility and foresight.

For GRC leaders, the message is clear: regulatory change is no longer episodic, but constant. Organisations must build frameworks that can adapt to new rules while fostering a culture of compliance, ensuring that policies, training, and governance practices evolve in step with the law.

Diagram 10: 44.3% of organisations cited "keeping up with changing regulations" as their primary concern

4.1 Employment Rights Bill: Preparing for the most significant shift in UK employment law in decades

The Labour Government's Employment Rights Bill (ERB) is set to deliver one of the most significant overhauls of UK employment law in recent decades, affecting organisations of all sizes.

While the exact timelines and details continue to be shaped through consultation, the risks for employers are already clear. Stronger worker protections are expected to drive an increase in tribunal claims, new requirements for evidence gathering and reporting will add compliance pressure, and leadership teams will need to adapt business models and people strategies accordingly.

Axiom research highlights a clear readiness gap. In a survey of UK organisations, only **2% said they were "very prepared" for the reforms**, while **52% were neutral and 22% admitted to being unprepared**.

This underlines a growing governance challenge as businesses face new obligations on zero-hours contracts, expanded trade union powers, and restrictions on non-disclosure agreements – all of which are set to reshape employment practices and workplace relations.

Diagram 9: Insights reveal a lack of readiness for the Bill

4.2 How can organisations and GRC leaders prepare for the reforms?

Efficiently managing the impact of the ERB will be essential, with legal experts anticipating a surge in tribunal claims as worker protections expand. Strengthening reporting systems, implementing digital platforms for evidence gathering, and setting clear escalation routes to HR, legal teams, or external advisors will help organisations meet the increased need for accurate record-keeping and defined protocols.

From a culture perspective, the implications of the ERB extend beyond HR and legal teams. People leaders will need training and guidance to ensure consistent application across the organisation and reduce risk. Boards should consider the impact of increased trade union powers, changes to zero-hours contracts, and revisions to non-disclosure agreements when shaping future business strategies.

> "One of the most significant impacts of the Bill is the proposed changes to Day One rights. Organisations will no longer have a two-year buffer, so recruitment and probation will come under greater scrutiny. Businesses are likely to make hiring and restructuring decisions more cautiously, and many are already speeding up workforce changes in anticipation of the Bill."

Angela Carter

Director of Legal Services at WorkNest

Key steps to manage the impact of the reforms:

Step 1 - Undertake policy and contract reviews – Ensure contracts, handbooks, and HR policies reflect upcoming changes, including worker protections and union powers.

Step 2 - Upskill managers and leaders – Provide training so people managers understand the new requirements and apply them consistently.

Step 3 - Strengthen governance and reporting – build or refine frameworks for record-keeping, escalation, and evidence gathering to manage the expected rise in tribunal claims.

Step 4 - Scenario planning – Assess how changes to zero-hours contracts, NDAs, and union powers may affect business models and workforce planning.

Step 5 - Partner with experts – Engage specialist HR and employment law advisors for practical guidance, ongoing support, and assurance of compliance.

The ERB is one of the most far-reaching employment reforms in decades, requiring strategic foresight. Organisations that proactively adapt governance and compliance frameworks will be better positioned to manage risk, maintain stability, and protect workforce relationships as these changes unfold.

Axiom GRC Solution: Employment Law and HR Support

Part of Axiom GRC, WorkNest's Employment Law and HR specialists help organisations manage an increasingly complex employment landscape. From day-to-day HR challenges to guiding organisations through major reforms like the ERB through a combination of practical training, policy and contract reviews, and tailored advice. By combining compliance frameworks with people-focused practices, WorkNest helps businesses reduce risk, adapt to change, and build long-term resilience.

4.3 The Data (Use and Access) Act: organisations are unprepared for change

The introduction of the Data (Use and Access) Act 2025 (DUAA) represents the most significant update to UK data protection since GDPR. While the it does not replace existing legislation, the Act introduces new requirements around subject access, automated decision-making, consent, cookies, and legitimate interests, reshaping how organisations process and protect personal data.

Axiom GRC research highlights a significant preparedness gap. Fewer than **2% of organisations report being fully ready**, while **almost half are only partway through preparations** or yet to begin. The biggest challenge identified is updating governance, training, and vendor management (47%), pointing to the need for systemic changes that extend beyond compliance teams. Human error remains the greatest perceived risk (56%), reinforcing the need for broad-based staff training and awareness.

Over the next six months, **training is the top compliance priority for nearly four in ten organisations**, alongside updating SAR and incident response procedures. However, many organisations are adopting a cautious approach, with over a third saying it is "too early to tell" how the DUAA will impact them, given the ICO's expanded oversight and new enforcement powers.

For leadership teams, the message is clear: DUAA compliance cannot be managed in isolation. It requires board-level engagement, investment in culture and capability, and robust frameworks that span governance, risk, and supply chain management.

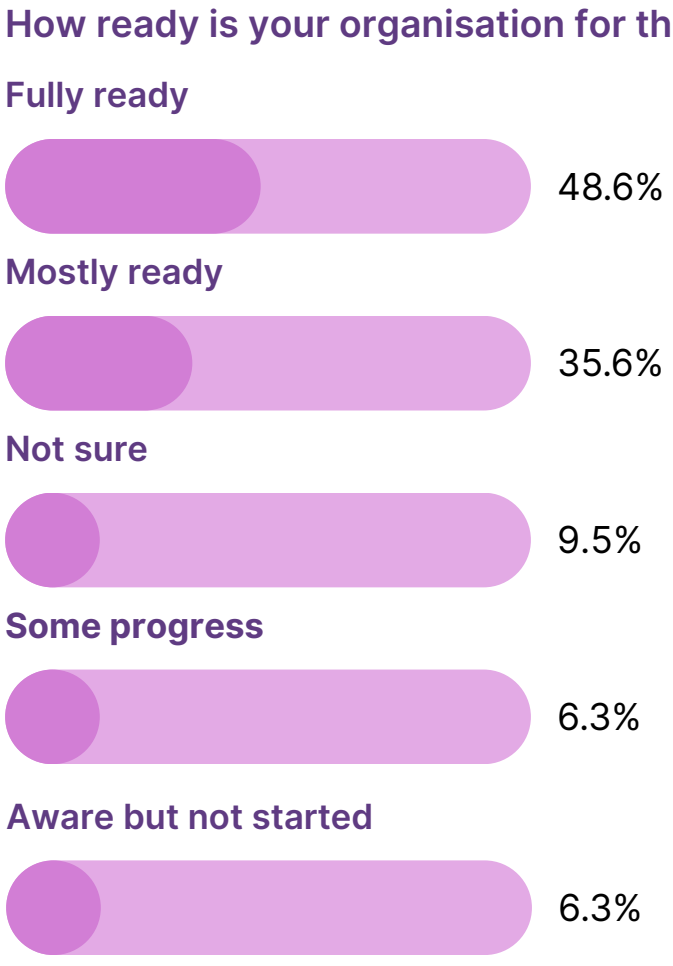


Diagram 10: Preparation for the DUUA is mixed

What do you see as your organisation's biggest data protection risks?

55.8% Human error | **25.3%** Data accuracy errors | **11.9%** Phishing/hacking

3.7% Breach reporting failures | **2.7%** DSAR disputes | **1.1%** Other

How do you view the DUAA overall?

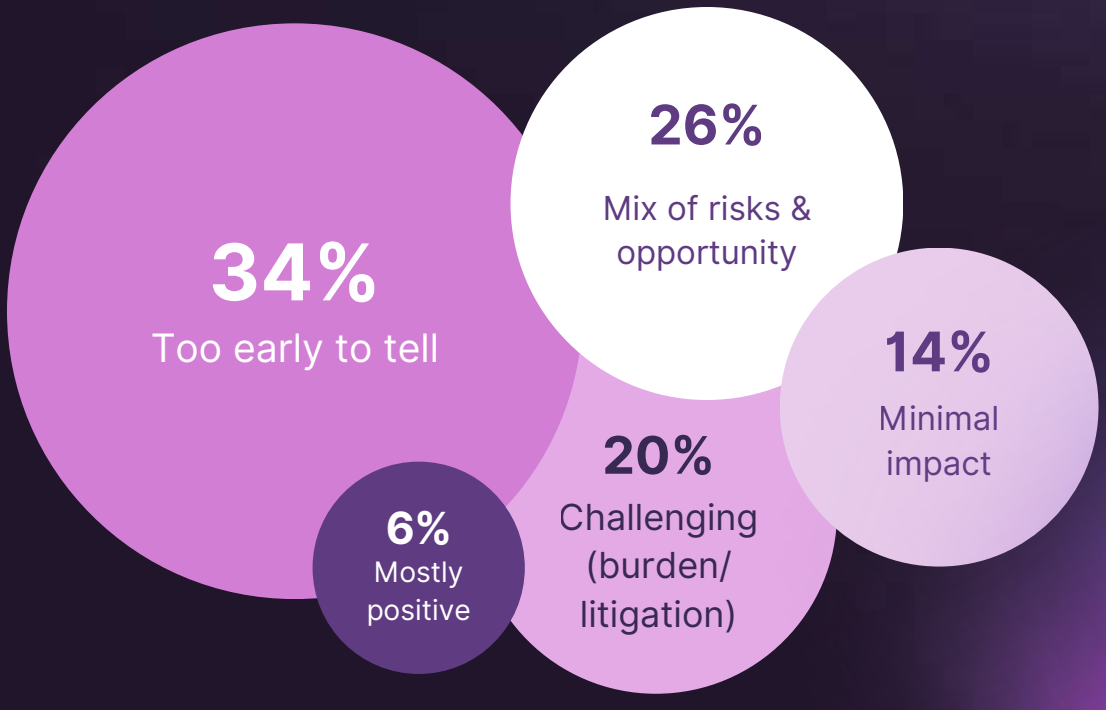


Diagram 11: Organisations see both risk and opportunity from DUUA

What will be your organisation's top DUAA compliance priority over the next six months?

39.2% Training staff across the business

25.3% Updating SAR and incident response playbooks

18.9% Board level engagement and strategic buy-in

8.9% Vendor contracts/supply chain

4.7% Regulator engagement/litigation

2.9% Other

4.4 DUUA checklist for leaders:

Update DSAR procedures

Apply the new proportionality rules, introduce the "stop-the-clock" mechanism, and prepare for potential court-level inspections.

Embed staff training

Deliver DUAA-specific training to all teams handling personal data – including HR, finance, marketing, operations - not just IT or compliance functions. VinciWorks provides training to organisations on the DUAA, in addition to further resources and checklists.

Review governance and policies

Refresh privacy notices, retention policies, and contracts to reflect new lawful bases, recognised legitimate interests, and enhanced protections for children's data.

Strengthen vendor management

Extend DUAA compliance requirements to suppliers and third parties through robust contract reviews and due diligence checks.

Plan for regulator engagement

With the ICO now empowered to compel staff interviews and access documentation, ensure audit-ready records and clear escalation playbooks.

Consider international data flows

Review cross-border transfers, particularly where Smart Data schemes or digital identity frameworks are involved.

Secure board-level buy-in

Position DUAA compliance as a strategic governance issue - not just a technical update - ensuring leadership engagement, oversight, and adequate resourcing.

The next chapter for GRC...

Over the next 12 months, compliance professionals need to proactively address four key issues: the **AI opportunity-risk spectrum, immediate cyber threats, lack of GRC connectedness** and **an array of specific new laws.**

Never has it been more important that compliance professionals are on the front foot of changes. Axiom GRC's research reveals a landscape sensitised to key changes, but also uncertain about how to accommodate technology changes in the most ethical way.

We hope that this research helps you as a compliance professional understand how the rest of the market is responding to key issues and highlights the key tension areas.

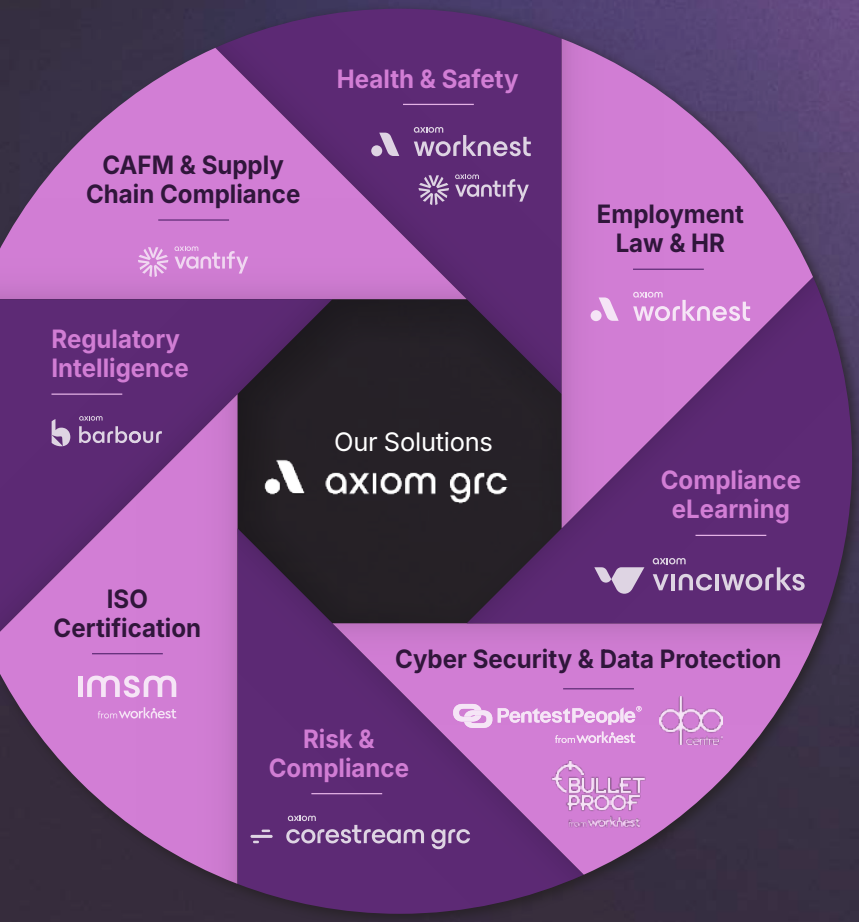
If you have any questions or want to understand the deeper implications of our research, please don't hesitate to get in touch.

Axiom GRC is a powerful force in the world of Governance, Risk, and Compliance (GRC). We're redefining how businesses worldwide approach resilience, responsibility, and growth. Our platform brings together the tools, expertise, and support to help organisations navigate complexity with greater clarity and confidence.

axiom grc

50 market-leading compliance products	**1,300** specialists	**10** countries	**2 million** software users	**40,000** happy clients	**90%+** retention levels

Axiom is the GRC platform of choice delivering a blend of software and advice that ensures your business resilience.



Health & Safety
EHS software and expert consultants delivering tailored Health & Safety support, compliance management, and risk reduction for safer, legally compliant workplaces.

Employment Law & HR
Expert guidance in Employment Law and HR through a unique, commercially focused approach, offering tailored support and clear actionable advice across 48 sectors.

Cyber Security & Data Protection
Expert cyber security and data protection services and software to help organisations proactively protect their data, ensure compliance, and stay ahead of evolving threats.

Compliance eLearning
Compliance eLearning with customisable, multilingual courses and interactive training to boost knowledge, reduce risk, and drive behavioural change across key areas.

ISO Certification
World-class consultancy, audits, and software to simplify ISO certification, turning compliance into a strategic advantage that builds trust and competitiveness.

Risk & Compliance
Comprehensive risk management software to identify, assess, and mitigate risks in real time, streamline processes, and ensure accountability and efficiency.

Regulatory Intelligence
Intuitive platform powered by expert insights delivering regulatory information and risk solutions - simplifying compliance, protecting employees, and safeguarding the environment.

CAFM & Supply Chain Compliance
A unique compliance ecosystem, simplifying the management of complex property portfolios through integrated CAFM, Supply Chain and Risk Management products.

World class clients rely on Axiom for GRC solutions:

savills · Unilever · L'ORÉAL · Walmart · AIRBUS · SONY · TESCO · BBC

www.axiomgrc.com · Axiom GRC

Contributors

Caspar Bullock,
Group Strategy Director
at Axiom GRC

Phillip Jones,
COO at Vantify

Shmuli Goldberg,
Head of AI at VinciWorks

Paul Cadwallader,
GRC Strategy Director at
CoreStream GRC

Lenitha Bishop,
CEO at The DPO Centre Ltd

Angela Carter,
Director of Legal Services
at WorkNest

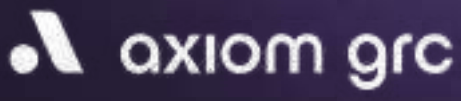
Luke Peach, Head of Information
Security Operations at
Bulletproof (Cyber Security)

Olumide Alade,
Lead Auditor at IMSM

Matt Reid,
Managing Director at
Barbour EHS

Index

1. AI compliance and ethical practices – Ensuring the responsible use of AI in your organisation. Hosted by VinciWorks. [7 May 2025]. 260 global employers surveyed. Available: AI compliance and ethical practices – Ensuring the responsible use of AI in your organisation
2. AI and GDPR Compliance in 2025. Hosted by VinciWorks. [14 Jan 2025]. 160 global employers surveyed. Available: AI and GDPR Compliance in 2025
3. AI in the Workplace. Leveraging opportunities while avoiding legal risks. Hosted by WorkNest. [14 August 2025]. 505 employers and HR professionals surveyed. Available: AI in the Workplace
4. General Compliance Trends Webinar. VinciWorks. [17 Jan 2024] 210 global employers surveyed. Available: General Compliance Trends Webinar
5. Data (Use and Access) Act compliance – What's changed in UK data protection. Hosted by VinciWorks. [10 September 2025]. 373 global employers surveyed. Available: Data (Use and Access) Act compliance



Find out more at axiomgrc.com