



Operating ethically

At Menzies, we recognise that ethical conduct is fundamental the safe running of our operations, to building trusted relationships with our business partners, and to supporting our All In commitments for a sustainable and resilient future. Upholding the highest standards of integrity is not only a moral imperative but also essential for building trust with our stakeholders and ensuring the long-term success of our global business.

By conducting ourselves and our business activities ethically at all times, we keep our business safe, our people safe and play our part in supporting a fair and just society and creating an ethical culture. We adhere to all applicable legal and regulatory requirements, as well as our robust internal policies and procedures, to ensure compliance with ethical standards and promote good governance practices. We lead by example, setting the tone from top of our organisation, modelling the values and behaviours expected of all employees, including acting with integrity, honesty, and respect. We communicate our values, ethical standards, and expectations through our policies, learning, guidance and regular updates for every area of our ethics wheel, as well as our wider All In plan.



Code of Conduct

Menzies Code of Conduct forms the cornerstone of our compliance programme and sets the expectations and behaviours for a full suite of ethics and compliance related policies. It covers awareness of topics including but not limited to: labour, human rights, discrimination, harassment, modern slavery, anti-bribery/corruption, conflicts of interest, cyber security, data protection and privacy, sustainability, safety, wellbeing, environment, financial integrity e.g. AML, protecting assets, social media, ethical conduct and Speak Up. Our Code of Conduct was significantly updated and shared to all employees in 2024, and is available in 16 languages. Employees will commence refreshed Code of Conduct training based on this new version early in 2025.

Zero tolerance for bribery or corruption

We have zero tolerance for any form of bribery or corrupt business practices anywhere in or organisation. In 2024, Menzies was not subject to any investigations or convictions related to bribery and corruption. Within our own organisation, we received four localised reports of bribery/corruption incidents via our SpeakUp platform, all of which were investigated and confirmed as unsubstantiated.

We have been a partner of TRACE for many years and utilise their best practice methods, training programs, and risk assessment data, to continuously develop and bolster our internal protocols. This includes conducting specialised and targeted virtual and in-person training sessions for our employee cohorts at heightened risk, as well as senior management and business partners (new and old), covering topics such as bribery, corruption, gifts and hospitality and conflicts of interest.



Anti-competitive practices

During 2024 we introduced a comprehensive global competition law policy to reinforce our stance on promoting fair business practices, compliance with anti-competitive regulations and increase our understanding of the essential principles in this area across our management cohort. In conjunction with the introduction of this policy, a number of virtual training sessions were delivered across the Group's senior leadership functions, led by our specialist legal advisors, providing practical legal guidance on key regulatory issues and commercial conduct advice to ensure our management functions understand their responsibilities in this area. During 2025, we aim to further extend implementation of this policy by introducing an obligatory anticompetitive practices online training session, which will sit within our existing compliance programme, applicable to all graded managers.

Cyber security and data privacy

As part of a critical supply chain, depended upon by our customers and the wider public, we take our commitments to data privacy and information security seriously, ensuring we have appropriate

controls in place. We take a risk-based approach to data privacy controls and cyber security, continuously monitoring and evolving threats, as well as the development of new threat areas resulting from AI technologies. During 2024, we undertook a deep-dive risk assessment on cyber security and continue to assess the vulnerabilities and continued to invest in our cyber security programme with the key aims of keeping the information we are trusted with secure and our business processes robust. We also achieved ISO 27001 accreditation further demonstrating our commitment to strengthening our standards and information security protocols.

We continue to educate and test our employees' cyber awareness, addressing the risk of human error through training, phishing simulations and improved reporting systems.

We experienced 20 reports/incidents of data privacy breaches in 2024, one of which was cyber-related, and five reports later confirmed as non-breach events. Only one event was reported to a local regulator, and none were deemed significant.



Training, awareness and controls

We provide continuous learning, and regularly review and improve our policies, practices, and training programmes to address emerging risks and challenges, as well as changing legislation and best practice guidance. We aim to make them understandable and accessible at all levels, translating them into multiple languages aligned to the geographies we operate in. Code of Conduct training and many of our other ethical and compliance courses are taken by every employee, and other more specific training is role-based.

Training is completed on a cycle of every 1, 2, or 3 years, dependent on the topic. To further support embedding ethical understanding and behaviours, we provide guidance and prompts via other communications on all ethics and compliance topics.

Whistleblowing system and reporting

We encourage all our employees or third parties we work with to report any concerns including breaches of our Code of Conduct or Third Party Code of Conduct (Codes). Our confidential and independent SpeakUp hotline enables employees and third parties to report any instances of unethical conduct via phone

or online, in their local language, safely and without fear of reprisal. Reports are treated seriously, confidentially and investigated appropriately in line with published procedures and service levels. We can communicate confidentially with reporters via the SpeakUp platform without compromising anonymity where this should be preserved. All reporters receive a recorded outcome and resolution for their case.

In 2024, we transitioned to a new version of the SpeakUp platform. This upgrade allowed us to update our SpeakUp Policy and Guidance and reintroduce SpeakUp details to our global employee population. Over the year, we received 941 cases through the platform. We categorise reports and monitor their statuses and outcomes, ensuring robust investigations and appropriate actions are carried out.

The SpeakUp hotline has become an essential tool in upholding our ethical standards and fostering a culture of accountability across the organisation. By encouraging open communication, we empower individuals to help us address misconduct, mitigate risks, and identify actions, improvements, or training opportunities. This enables us to

continually enhance our practices and drive positive change throughout Menzies.

Tax strategy

As a good corporate citizen, Menzies is committed to being a responsible and transparent tax payer, paying the right amount of tax in accordance with the laws and regulations of the countries in which we operate. Our Group Tax Policy is available on our company website.

Business Partner engagement

In 2024, we updated our Third Party Code of Conduct to better reflect the evolving expectations we have for our partners, aligning it with our internal Code of Conduct. This document is translated into multiple languages and available on our website. We require all suppliers to confirm their acceptance of the Third Party Code of Conduct, either as a standalone document or embedded within contractual agreements. The Code sets safeguards addressing critical areas such as human rights (including modern slavery and fair labour practices), anti-bribery and anti-corruption, environmental commitments, and more.

We continue to execute a comprehensive business partner due diligence process



in collaboration with a leading consultancy firm when entering acquisition, divestment, or joint venture discussions. When needed, we also engage external experts across various specialisms to conduct due diligence on our behalf.

Our **Third Party Risk Management (TPRM) system** and procedures enhance our engagement with our global

supplier network, which includes approximately 14,000 suppliers. This system enables us to perform auditable risk assessments and due diligence across ESG criteria, supporting our All In goals and sustainable growth agenda. In 2024, we conducted a supplier risk assessment across our global supplier population and continued to refine our due diligence and onboarding procedures.

Looking ahead, in 2025, we will further support these efforts with new sustainable procurement policies and onboarding criteria. Additionally, we are delivering supplier training and driving sustainability improvements across our supply chain by inviting suppliers to participate in the UN Sustainable Suppliers Training Programme.



Our risk framework

The **Menzies Enterprise Risk Management (ERM)** framework takes a proactive approach to risk, driving value and sustainable growth through accountability, governance, oversight, and strategic integration. Our ERM system enables the active identification, tracking, and management of risks, providing a dynamic, real-time view of risks, impacts, and actions across our global business, maintained by designated risk owners.

Risks are identified and raised throughout the organisation, and we conduct **horizon-scanning** to detect emerging risks that could significantly impact our business. This allows us to address potential threats as they develop, considering external factors brought about by technological and societal evolution.

We continuously monitor and review our risk exposure. Senior regional leadership and central teams assess risks within their respective business areas, while the **Risk Committee** regularly evaluates top-down, emerging, and principal risks. This includes assessing aggregated impacts, root causes, risk appetite, and mitigation actions to ensure validity and alignment with our objectives.

Risk identification, assessment, and management are also integral to new business opportunities, strategic decisions, investment considerations, and business changes. By consistently testing and improving our risk framework—including management, controls, and oversight—we ensure resilience, responsible growth, and the ongoing protection of our business and stakeholders.

Risk Committee

Our Risk Committee provides enterprise-wide governance and skilled business assessment, focusing on top-down, emerging, and principal risks. These risks include strategic, change, financial, regulatory, climate, political, IT, legal, reputational, and others. The Committee performs deep-dive analyses on emerging risk topics.

Chaired by the Chief Governance & Sustainability Officer, the Committee includes the following role-holders, along with specialist roles as required:

- Head of Sustainability & Corporate Responsibility
- Chief People Officer
- Head of Financial Planning & Analysis
- SVP Operational Risk
- Chief Information Officer

The Committee meets regularly to review risks related to new business opportunities, alongside the executive management board. It is responsible for instilling enhanced awareness and corporate risk governance in a meaningful way, informing our strategy and action planning.

During 2024, the Committee completed two deep-dive risk workshops on AI and on business integrations. Both pertinent topics as we continue

to grow our business and as we consider the risks associated with sophisticated AI technology and its role in increased privacy and cyber threats.

The Committee most recently undertook a thorough assessment of all top-down and emerging risks, finalised in early 2025. This includes finalising principal risks were for presentation to the Audit & Risk Committee to be ratified by them.

Climate risk is integrated into our ERM procedures. This includes the identification, assessment and mitigation of risks from climate change on our business, as well as the impacts of our own business and supply chains on climate change, whether they be physical, transitional or liability related. By making this part of our ERM procedures we can continue to engage and bring to life climate-related risks for our senior teams and how these are directly

related to our strategy, decision-making and procurement. Most recently, we have undertaken a refresh review of climate scenario modelling and climate risk with support from external ESG and climate experts ESG360°, with participation from our EMB and regional EVPs.

Risk Framework and Governance structure

