UK Transparency Report 2022

# Principal risks

As at 30 September 2022

| Risk | Current risk landscape | Mitigations |
|---|---|---|
| **Reputation, Regulation and Legal risks** | | |
| **1. Trust**<br>(Trend: No change)<br>KPMG in the UK fails to maintain the trust of external stakeholders, due to a failure to embed trust into the firm's strategy, failure to define and communicate the standards of conduct expected by the firm, and failure to develop a culture aligned to the firm's core values, resulting in negative impact on the firm's reputation at local, national and international levels. | — Continued regulator, public and colleague scrutiny of the firm in the context of both audit quality and the outcome of historic regulatory investigations.<br>— A culture ambition centred on being Values-led, operating to the highest ethical and quality standards.<br>— Increasing importance of, and expectations surrounding, ESG.<br>— A need to embed and sustain improvement in our AQR results. | — A tone at the top which emphasises quality, ethics and integrity, with Ethics Champions embedded in the business.<br>— A culture ambition guided by Our Values, Our KPMG, Our Impact, a Culture Steering Committee and Conflicts of Interest Working Group. Measurement of progress using culture metrics (incl. regular colleague surveys) and oversight from a Culture Steering Committee.<br>— Global ethical health survey to identify successes and areas for continued focus.<br>— Implementation of a 'Trust index' to aid with monitoring of external reputation.<br>— A refreshed code of conduct (Our Code) (reviewed by the Institute of Business Ethics) and set of Values, on which all colleagues receive annual mandatory training.<br>— Appointment of a Head of Professional & Ethical Standards with appropriate scope and resources and a Partner Conduct Verification Dashboard process to support performance management of partners, ensuring an appropriate link between conduct and partner remuneration.<br>— Embedded whistleblowing processes and promotion of a Speak Up hotline overseen by a third-party ombudsman.<br>— An Inclusion, Diversity and Equity Policy, employee networks which host a range of diversity focused learning events throughout the year and published diversity target zones, with regular progress reporting. Firmwide training on inclusion, diversity and social equality provided to all KPMG partners and employees.<br>— A Global and UK Impact plan which set out our environmental, social and governance (ESG) commitments — holding us accountable for progress toward a more sustainable future.<br>— Continued focus on the environment, with all UK offices certified to ISO 14001:2015.<br>— A mandated Audit Quality Framework, encompassing global methodologies, mandatory training (including KPMG Audit University), accreditation requirements (including for specialists) and audit quality review programmes (see further detail in Principal Risk 6). |

| Risk | Current risk landscape | Mitigations |
|---|---|---|
| **Reputation, Regulation and Legal risks** (continued) | | |
| **2. Regulation**<br>(Trend: No change)<br>KPMG in the UK fails to meet the expectations of our regulators, due to poor relationships with regulators, regulatory non-compliance and lack of regulatory horizon scanning to prepare for incoming regulatory changes, resulting in regulatory sanctions and enforcement action. | — Continued enhanced supervisory approach as FRC transitions to ARGA.<br>— Incoming regulatory changes affecting multiple parts of the firm, including audit reform.<br>— FRC published updated principles and timeline for operational separation of the Audit practice. | — A dedicated Regulatory Affairs function, with constructive and proactive arrangements to meet our regulatory commitments introduced.<br>— Regular engagement with regulators and relevant government bodies to understand and plan for the developing regulatory landscape.<br>— Monitoring of regulatory compliance by relevant regulatory affairs specialists and the firm's Public Interest Committee, including the impact and implementation of changes in regulatory requirements, such as Operational Separation.<br>— Active participation in Global Governance and Committees to oversee network controls and potential reputational and other risks.<br>— Regulatory horizon scanning introduced with regular reporting to relevant governance groups.<br>— Money Laundering Risk Officer function to meet our obligations in relation to anti-money laundering and financial crime, and regular financial crime training provided on topics such as money laundering, bribery and corruption.<br>— Maintenance of firm-wide and personal independence policies and systems (Sentinel™), KPMG Independence Compliance System, etc.) to ensure compliance, and additional approvals required for PIEs (Public Interest Entities) and OEPIs (Other Entity of Public Interest).<br>— Annual mandatory firm and personal independence training and annual personal independence confirmation by all partners, colleagues and (where relevant) contractors.<br>— Rolling programme of personal compliance audits and compliance monitoring of certain key areas by the firm-wide independence team.<br>— ESG Corporate Reporting team, focused on ensuring timely adoption and compliance with developing ESG regulatory and reporting requirements. |
| **3. Legal**<br>(Trend: No change)<br>KPMG in the UK fails to comply with legal obligations, including contractual obligations with clients, audited entities, third parties and colleagues etc., due to a failure to identify and understand these obligations, or put in place appropriate controls and monitoring frameworks to ensure that these obligations are met, resulting in litigation, legal costs and reputational damage.<br>The UK firm fails to appropriately monitor and mitigate the impact of reputational damage arising from actions taken by other KPMG member firms. | — Increasing complexity of contracting environment, in particular in relation to long-term nature of large advisory engagements and increasingly complex legal and regulatory frameworks (e.g., in relation to liability caps and information security and data requirements).<br>— Increased complexity of global sanctions framework post Russia Ukraine conflict. | — In-house Office of General Counsel team to assist the business with contracting and compliance with regulation, including specialists in regulation, data privacy and employment law.<br>— Close liaison with KPMG Global through International Office of General Counsel and liaison with other network firms' offices of General Counsel.<br>— Legal input to both Deal Boards, Client and Engagement Acceptance and Continuance Committee and Conflicts Working Group, to ensure that the appropriate approvals are in place and legal/contracting risks are considered before pursuing new opportunities and agreeing scope and terms of engagement deliverables.<br>— Comprehensive client and engagement acceptance procedures, including in relation to contracting with all stakeholders and recipients of our services/deliverables.<br>— Framework of policies, underpinned by regular training, in relation to compliance with external regulation and legal requirements (including in relation to financial crime and fraud management).<br>— Engagement Quality Control Reviewers (EQCRs) and other 'first line' quality control processes, including in relation to legal and contracting matters.<br>— Annual 'second line' compliance processes (including QPR and Global RCP/KQCE) in relation to contracting and legal compliance.<br>— Specific policies, procedures and controls related to complying with sanctions. |

| Risk | Current risk landscape | Mitigations |
| --- | --- | --- |
| **Strategic risks** | | |
| **4. Growth**<br>(Trend: No change)<br>KPMG in the UK fails to define and execute a strategy that is supported by an appropriately resourced operational plan, that is underpinned by further development of relevant services and propositions, and which can be measured objectively. In addition, the UK firm fails to design its strategy to be able to adapt or respond to changes in the external economic and regulatory environment, or to maximise opportunities from the KPMG global network, resulting in a failure to achieve the desired levels of growth. | — Continued levels of market uncertainty in relation to the external environment: including the impacts of ongoing global conflicts, the wider political landscape, growing economic uncertainty, economic recession in the UK and the impact on specific markets of regulatory action.<br>— Impact of operational separation of audit on our growth strategy.<br>— Increasing importance of, and stakeholders' expectations surrounding, ESG. | — Board approved three-year planning exercise with yearly refreshers and regular review.<br>— Defined strategies (at Firm and Capability/Market level) approved by leadership with Board input and oversight and aligned with Global strategy and Our Impact plan (see below).<br>— Executive Committee sponsorship of strategic growth initiatives with an investment allocation and governance process to prioritise and monitor investment.<br>— Enterprise-Wide Risk Management Framework with matrix reporting across Capability, Market and Firm-wide risks to support Board and Committee governance and Executive decision-making. Capability, Market and Regional risk officers in place to support second line management/ oversight of risk policies, practices and decision-making.<br>— Separate governance for Audit, including Audit Board, with impact of operational separation on delivery of the firm's strategy reflected in both Audit and firm-wide business planning.<br>— 'Our Impact' ESG strategy and plan, with Head of ESG supported by dedicated ESG Centre of Excellence. |
| **5. Clients and audited entities**<br>(Trend: No change)<br>KPMG in the UK fails to work with the right clients and audited entities, maintain a balanced portfolio across sectors and industries, optimise its use of strategic alliances and build both a unique and innovative brand proposition and a holistic go-to-market strategy, resulting in declining market share or over-concentration in specific sectors and a failure to achieve its strategy and ESG commitments. | — Audited entities and clients' changing business models and service needs, arising as a result of their responses to the current external and economic environment, increasing digitalisation and growth in importance of the ESG agenda.<br>— Impact of the firm's ESG strategy on the acceptance and delivery of services to clients and audited entities. | — Comprehensive acceptance procedures undertaken before engaging with clients and audited entities for the provision of services, including KYC checks and global conflict checking to support the management of independence when working with audited entities or potential audit targets.<br>— Client and Engagement Acceptance and Continuance Committee consideration for higher risk clients and engagements to ensure that risks are considered, and appropriate internal approvals obtained, before pursuing new opportunities.<br>— Conflicts Working Group established (as sub-committee of the Risk Executive) and mandatory annual firm-wide Conflicts of Interest training rolled out to support adherence to conflicts of interest policy.<br>— Continued challenge of audited entities where improvements to systems, controls and governance are required and careful management of transition where we decide to resign from audited entities, with reference to our public interest responsibilities.<br>— Introduction of the ACCEPT framework to further support colleagues in making decisions about who we work with and what work we do in line with Our Impact plan, supported by firm-wide and engagement leader training and communications.<br>— Monitoring period of audit tenure for audited PIEs in order to comply with mandatory tendering and rotation requirements.<br>— Extensive independence policies, guidance and processes supported by annual mandatory firm-wide training on Personal and Firm independence and regular compliance monitoring (see further details in Principal Risk 2).<br>— Regular portfolio strategy and account planning, with Executive Committee oversight of plans for major accounts.<br>— Investment programme to oversee the development of new service lines and propositions, in line with Our Impact plan and reflecting market and client need developments.<br>— Regular review of Client Insights programme feedback, including to inform development of future service propositions.<br>— Investment in technology and specialists e.g., climate, IT audit and data scientists to ensure our audit approach is responsive to changes in the external environment and new markets. |

| Risk | Current risk landscape | Mitigations |
|---|---|---|
| **Operational risks** | | |
| **6. Execution – Quality**<br>(Trend: No change)<br>KPMG in the UK fails to meet the expectations of clients, audited entities, regulators and other interested parties in relation to the quality of work delivered. | — Sustained public and regulatory scrutiny of the firm's ability, independence and qualification to deliver engagements to a high standard.<br>— Impact of changing ways of working on the ability to deliver quality services. | — Programme to implement ISQM1 as part of the firm's System of Quality Management, in advance of mandatory adoption date in December 2022, including close liaison with KPMG International's ISQM1 Programme team and creation of newly established System of Quality Management team to support the annual ISQM1 risk assessment and oversee our compliance post implementation.<br>— Continued investment in our Audit Quality Plan which prioritises actions with the biggest impact on audit quality, and the Banking Audit Quality Improvement Plan, supported by the development and implementation of the KPMG Clara Audit workflows.<br>— Mandated Audit Quality Framework, encompassing global methodologies, mandatory training (including KPMG Audit University), accreditation requirements (including for specialists) and audit quality review programmes.<br>— Mandated engagement quality controls including the use of standardised methodologies and tools, accreditation requirements, targeted involvement of Engagement Quality Control reviewers, Accounting and Auditing specialists, Risk Panels and Deal Boards. Enhanced processes for complex, longer-term engagements.<br>— Newly established Audit Regulatory Compliance function, with remit to deliver a dedicated audit compliance programme, testing outcomes to provide assurance that the processes, procedures and controls in place to meet regulatory requirements are operating effectively.<br>— Regular review of Client Insights programme and requests for feedback in relation to quality of delivery.<br>— Engagement watchlists maintained at Capability and Risk Executive Committee level, with escalation of issues as appropriate.<br>— Firm-wide quality compliance programmes including QPR and Annual Root Cause Analysis programme. Established quality function in Consulting, with appointed quality leads for each performance group. |
| **7. Execution – Delivery**<br>(Trend: No change)<br>KPMG in the UK experiences failures in its delivery of services to clients and audited entities due to taking on inappropriate clients or engagements, ineffective engagement setup, poorly managed projects, contracting and financials, lack of adequate resourcing or identification and management of third parties in its supply chain, resulting in preventable losses and missed opportunities. | — Increasingly competitive market for recruitment of talent.<br>— Increased reliance on reliable and appropriate technology and connectivity due to hybrid working.<br>— Increased complexity of contracting in particular in relation to multi-year framework services and work delivered for the public sector.<br>— Increased use of third parties in engagement delivery in particular of long-term compliance projects. | — Global Quality & Risk Management Manual supplemented by UK requirements set out in Capability-specific risk management manuals, policies and guidance.<br>— Comprehensive client and engagement acceptance procedures, including ACCEPT framework for decision-making, Client and Engagement Acceptance and Continuance Committee and Conflicts Working Group as described under Principal Risk 5: Clients and Audited Entities.<br>— Template engagement letters and OGC/risk review requirements for contracting.<br>— Inter-firm contracting protocols when working with other KPMG International member firms.<br>— Input from Commercial teams on pricing and terms, as well as Deal Boards for non-audit engagements, and controls in place when working with sub-contractors and alliance partners.<br>— Significant investment in our colleague proposition, Our KPMG, and recruitment, performance management and wellbeing support, to ensure we can continue to attract and retain the talent we need to meet demand now and in the future (see further detail in Principal Risk 8).<br>— Compliance programmes including Global GCR, QPR and Compliance Assurance Programme, with appropriate root cause analysis undertaken and action plans implemented and monitored. |

| Risk | Current risk landscape | Mitigations |
|---|---|---|
| **Operational risks** (continued) | | |
| **8. People, Talent and Culture**<br>(Trend: No change)<br>KPMG in the UK fails to appropriately attract and recruit, engage, develop, retain and reward talent at all levels of seniority, resulting in a lack of expertise, capability and capacity (onshore and offshore) to meet the medium- and long-term demands of the business, loss of top talent and gaps in key leadership roles and succession plans. In addition, the UK firm fails to define and develop a culture in alignment with its core values and strategy. | — Intense competition for talent and skills shortage, impacting on ability to recruit at all colleague levels. Evolving expectations of employees risks the attractiveness of the firm reducing over time.<br>— Increased immigration complexity.<br>— Management of, and ability to meet, expectations in relation to the medium-to-long-term changing ways of working, including the move towards hybrid working.<br>— Downturn in economic environment and impact of increased cost of living on employee wellbeing and morale.<br>— Continued focus on developments in Inclusion, Diversity and Equity (IDE) and ability to meet IDE improvement objectives.<br>— Increasing importance of reaching our culture ambition and maintaining an environment where poor employee or partner conduct is identified and addressed. | — Significant investment in colleague reward, and an attractive employee value proposition, Our KPMG, against results of annual salary benchmarking. Range of projects ongoing to ensure we are able to recruit and retain the skills we need in the current environment, including in relation to improving our people systems and addressing complexities in immigration and onboarding.<br>— Defined performance management cycle and processes which includes goal setting, feedback and performance appraisal. Regular training delivered to Performance Managers and 360 feedback programme for leaders across the firm.<br>— Inclusion, Diversity and Equity Policy and firm-wide mandatory training for all KPMG partners and employees. Black Lives Action Plan, Black Heritage reverse mentoring, Black Lives Allyship programme and IDE Talent programme.<br>— Comprehensive wellbeing offering including mental wellbeing, bereavement support, a Domestic Violence and Abuse Policy statement, an employee assistance programme, remote GP, private medical insurance (for relevant colleagues), counselling service and number of wellbeing apps.<br>— Employee networks to support and engage with the various communities across the firm and an Employee Business Forum, which represents the views of the firm to leadership.<br>— Regular feedback on People strategy and practices sought through annual Global People Survey and regular Pulse Surveys, with action plans in place where required.<br>— Culture Ambition guided by Our Values, and a refreshed code of conduct (Our Code) (reviewed by Institute of Business Ethics). Firm-wide Culture Steering Committee responsible for approving and steering the firm-wide culture strategy, plan and priorities – which include a firm-wide Values Week and People Awards, building trust through developing a speak-up culture and a psychologically safe environment and building out our leadership and management capability to support our magnet for talent agenda.<br>— Succession plans in place for members of Executive leadership. Board succession monitored and managed through Nominations Committee. |

| Risk | Current risk landscape | Mitigations |
|---|---|---|
| **Operational risks** (continued) | | |
| **9. Technology and information management**<br>(Trend: No change)<br>KPMG in the UK fails to provide the technology solutions required by the business to support its operations, reputation and growth, or to adequately protect existing technology solutions, resulting in a breach of the confidentiality, integrity and availability of these solutions. This may lead to an inability to provide key services to internal and external stakeholders, and reputational or financial loss. | — Increased risk of cyber-attacks as a result of global political conflicts.<br>— Increasing complexity of technology solutions provided to clients.<br>— Increased importance of developing and investing in IT infrastructure for the future to support changing business needs.<br>— Continued reliance on technology and increased complexity of managing information risk in hybrid working environment.<br>— Increasing technology and security requirements.<br>— in contractual arrangements with clients and audited entities. | — Governance/approval requirements in place for technology investment and changes: Technology Assurance Group, DMTAP (Demand Management and Technology Assurance Process) and CTO Forum.<br>— Appointed Data Protection Officer and Chief Information Security Officer, each with specialist teams.<br>— Range of projects ongoing to improve technology inventory and protections (Backup & Restore, Data Centre Exit, Smart Networks, etc.).<br>— Ongoing programme of training and awareness of the end-to-end Technology Assurance process and refreshed Technology Assurance Policy.<br>— Multi-year Information Security Transformation Programme, introducing and embedding a new set of information security capabilities and services that can provide a more effective response to evolving cyber security threats and changes in regulations.<br>— Three lines of defence model for management of information risk, including a central Information assurance team and an Information Governance Oversight Committee.<br>— Ongoing mandatory training, covering information security, data protection and information management.<br>— Widespread use of Information Protection Plans in engagements and introduction of Data Champions.<br>— Programme of ongoing phishing resilience testing, security awareness focused on a range of themes including passwords, patching, phishing and social engineering.<br>— Rolling compliance programme (as part of second line assurance activities) in relation to Information Protection Controls and Policy Compliance. |

| Risk | Current risk landscape | Mitigations |
|---|---|---|
| **Operational risks** (continued) | | |
| **10. Business operations, resilience and controls**<br>(Trend: No change)<br>KPMG in the UK fails to define, implement and monitor the effectiveness of its policy, procedure and control framework, including in relation to its suppliers, and to ensure continuity in business operations. In addition, the UK firm fails to manage change effectively, resulting in control failure, and disruption to business operations and the services provided to clients and audited entities. | — Importance of maintaining robust business processes and controls and adapting where appropriate so that they remain fit for purpose in the current environment.<br>— Conclusion of ISQM1 implementation programme and transition to 'business as usual' System of Quality Management.<br>— Impact of rising global costs, Brexit and increasing global political conflicts on the ability of third party suppliers to deliver goods and service to KPMG.<br>— Planning for impact of operational separation of Audit.<br>— Importance of ensuring business processes and controls align to the firm's ESG strategy, as well as the expectations of external stakeholders.<br>— Ability to successfully manage multiple and significant transformation programmes, with appropriate governance and investment controls. | — Three lines of defence model, including internal audit, to review the design and operating effectiveness of key controls.<br>— Enterprise-Wide Risk Management Framework with matrix reporting across Capability, Market and Firm-wide risks to support Board and Committee governance and Executive decision-making. Capability, Market and Regional risk officers in place to support second line management/ oversight of risk policies, practices and decision-making.<br>— Regular updates to the Board on operational performance based on extensive MI; three-year business planning with yearly refreshers and regular review by Operations Executive and COOs.<br>— Operations Executive oversight of both internal and external audit quality reviews, recommendations and actions.<br>— Defined business continuity and crisis management plans, and controls in place to support IT, Third Party, People, Facilities & Data disaster recovery.<br>— Specialist Operational Resilience team which follows business continuity best practice guidelines and complies with ISO22301 (as confirmed by independent internal audit).<br>— EPMO (Enterprise Project Management Office) to manage investment and transformational change programmes.<br>— Supplier management centre of excellence.<br>— Focused preparation for the implementation of ISQM1, in close coordination with KPMG International. Newly established System of Quality Management team to support the annual ISQM1 risk assessment and oversee our compliance post implementation.<br>— Compliance programmes including Global GCR and Global RCP/KQCE, with appropriate root cause analysis undertaken and action plans implemented and monitored. |
| **Financial risks** | | |
| **11. Financial management**<br>(Trend: No change)<br>The UK firm fails to execute against financial targets or manage medium- to long-term financial position and performance, for example due to delivering unprofitable services, poor investment decisions, and failure to ensure a resilient balance sheet, resulting in poor business performance, inability to achieve growth and negative impacts to the financial health of the firm. | — Need to continually invest in our services, people and processes to ensure that the business model is fit for the future.<br>— Expected deterioration in external economic environment with potential impact on demand for KPMG services, increasing cost base and ability to collect payment for the services delivered to clients and audited entities.<br>— Inherent uncertainty with respect to any outstanding regulatory investigations and civil litigation matters. | — Budgets which are subject to various levels of approval, through a thorough budgeting process, with appropriate sensitivity analysis and planning based on emerging economic landscape.<br>— Board role in budget and performance oversight and Executive Committee budgetary challenge.<br>— Monthly financial analysis at firm and functional level, including regular refresh of downside scenario planning based on early warning indicators.<br>— Pricing panels, pipeline monitoring, WIP management processes and regular tracking of overdue invoices. Tools available across the firm.<br>— Approval and monitoring controls over investments, investment decisions and capital retention strategy.<br>— Closely controlled procurement process and approvals, via technology platform.<br>— Finance policies, including the Spend Control Policy, Timesheet Policy and Expenses Policy.<br>— Professional Indemnity Insurance in place. |

This principal risks content forms part of our UK Transparency Report 2022, which can be found **here**.

kpmg.com/uk



Designed by CREATE | CRT141935 | January 2023