Risks

Our risk management framework

The Group's risks are managed on a day-to-day basis within the businesses and functions across the Group's entities. Inherent risks are identified and assessed by "First Line" resources alongside controls and their proven or expected mitigating effects. This process is supported by the risk functions across the Group and is called the Risk and Control Self-Assessment ("RCSA"). Risk is aggregated across businesses, themes and functions as directed by the Executive Committee, to provide risk reporting for the Group and the qualitative and quantitative bases for determining risk appetite for the firm. The Executive Committee is responsible for endorsing the policies and procedures within the Group framework and motivating the business to take calculated risks. The "Second Line" risk function is responsible for the risk taxonomy and the Group's risk register as well as the management of risk events (recording, escalation, reporting) through the Risk Committee. The regional risk officers (Luxembourg and Australia) report to the Head of Risk and the Chief Risk Officer.

The Board believes the Group has an effective framework to identify, manage, monitor and report the risks the firm is or might be exposed to, or pose or might pose to others, and operates adequate internal control mechanisms, including sound administration and accounting procedures.

Three lines of defence

The Group operates a three lines of defence ("3LOD") model with risk management oversight owned by and managed within the second line of defence ("2LOD"). The Audit & Risk Committee of the Group receives quarterly reports on the risk profile of the UK, Luxembourg and Australian entities from the Head of Risk for Foresight Group LLP.

Members of the Foresight team

Risks continued

Board of Foresight Group Holdings Limited (the "Group")

- Accountable for the overall adequacy and effectiveness of the Group-wide Risk Framework and the Group's risk culture
- Delegates responsibility for Risk Management to the Executive Committee

↑

Executive Committee for Foresight Group

- Responsible for the overall adequacy and effectiveness of the Group-wide Risk Framework
- Approves risk policies and procedures, risk roles and responsibilities
- Sets "tone from the top" and establishes tangible risk appetite and strategy
- Monitors risk reporting and ensures actions are taken to mitigate risk

↑

Members Board for the Prudential Consolidation Group (the "Firm" – Foresight Group LLP and subsidiaries)

- Responsible for the overall adequacy and effectiveness of the Firm-wide Risk Framework
- Approves Firm risk policies and procedures, risk roles and responsibilities
- Stewardship of "tone from the top"
- Monitors risk reporting and ensures actions are taken to mitigate risk

↑

External oversight/assurance

- Verification of the adequacy of the Group Risk Framework
- Non-executive challenge of the overall adequacy and effectiveness of actions taken by the Risk Committee

Third line of defence

↑

Firm Risk Committee

- Periodic reviews of integrity and adequacy of risk reporting
- Independent review of adherence to risk policies/procedures
- Recommendations and verification of implementation for detailed process and control improvements
- Tracking and reporting of incidents, losses and breaches

↑

Risk & Compliance

- Day-to-day responsibility for implementation of Risk Framework
- Risk identification, scoring and prioritisation with input from first line of defence
- Preparation of risk reporting
- Implements and monitors risk policies and procedures
- Advises on risk impact of regulatory issues/other external changes
- Loss/incident analysis
- Monitoring of investment limits

Second line of defence

↑

Businesses, functions

- Primary responsibility for ensuring adequate control environment and adherence to risk policies and procedures
- Primary responsibility for managing investment risk in accordance with fund mandates
- Input into risk identification and scoring managed by Risk function
- Notification and escalation of losses and incidents
- Provision of data for risk reporting

First line of defence

Risks continued

Risk appetite

As a provider of regulated services, Foresight is required to document its risk appetite in relation to its entities within the Group. Foresight Group LLP has its principal office based in London and the risk appetite for this entity is considered the minimum standard for the Group. Foresight's risk appetite statement sets out the level and types of risk that it is willing to assume to achieve its strategic objectives and business plan.

The Risk Appetite Statement is an articulation of the aggregate level and types of risk that the Group is willing to accept, or avoid, in order to achieve its business objectives. It includes qualitative statements, quantitative measures expressed in relation to earnings, capital, concentration, liquidity, risk measures and other relevant measures (individual business or functional area appetite statements) as appropriate.

The Group uses staggered risk limits (Early Warning Indicators ("EWIs") and hard limits) as appropriate for each risk metric to monitor compliance with the approved risk appetite covering business and strategic risk, market risk, credit risk, operational risk, legal and regulatory risk, financial crime risk, conduct risk and information security risk.

Risk position versus risk appetite is reviewed annually, with any changes to key metrics reviewed, challenged and adopted by the Board if appropriate, through the risk appetite framework.

The Group continues to maintain strong liquidity across a range of scenarios, with the greatest threats to capital and liquidity positions represented by the risks of new and escalating conflicts and persistent inflation.

Sustainability Risk Management

A more detailed description of our climate risk assessment is included in the TCFD section of our Sustainability Report. Sustainability and operational resilience are synonymous. If our business activities are not sustainable, they will not be resilient, and this is as true of the impact of our social and governance activities as much as it is of our environmental or climate-related impact.

The Group Risk function ensures that there is a robust framework in place to identify and manage sustainability risks and opportunities as well as improve Board visibility of our activities. The management of the risks arising from our sustainability objectives focuses as much on the opportunities as the threats. Supporting a diverse range of financial products designed to satisfy our customers' sustainable investment objectives necessitates enhanced oversight not only of the investment process but also the marketing and promotion of those products.

Sustainability, within which we include environmental, social and governance ("ESG") practices, has become an important business driver over the last decade for most firms and is a key driver for Foresight. Foresight also focuses on wider environmental issues, such as nature and biodiversity, firstly because these form a core part of our sustainability strategy and secondly because we expect the regulator to follow the same path with TNFD (Taskforce for Nature-related Financial Disclosures) as it did for TCFD; voluntary disclosures become mandatory through their adoption into the rulebooks.

The success of our business depends on our ability to generate attractive risk-adjusted returns for our investors while meeting our sustainability objectives. Delivering any of the ambitious climate and social targets demanded represents a challenge for every business and in addition to aligning business strategies, requires significant investment in data frameworks and controls to support regulatory reporting requirements.

The Board requires assurances that significant ESG risks have been identified, are measured and managed and that Group businesses have enhanced their first line of defence risk management activities to integrate climate risk management. As approved by the Board, the Risk function is currently enhancing its set of Key Risk Indicators for the Risk Appetite Statement to monitor our progress towards our stated objectives in diversity and inclusion, as well as our emissions targets.

Our social risks are clearly a responsibility for all staff and our People & Sustainable Culture team continue to improve the data collection and analytical capabilities that will enable us to report most of the metrics mentioned in a recent FCA consultation paper and make sure that we can evidence our commitment to diversity, equity and inclusion.

Regulatory and legal risk, particularly with respect to the integrity of sustainability claims (including the risk of "greenwashing") is a feature of most top ten risk lists for product manufacturers and distributors. Foresight's sustainability focus necessitates additional controls and careful scrutiny of all of our sustainability claims in digital and print media. We expect that enforcement activity relating to specious sustainability claims will be a significant feature of the regulatory landscape over the short to medium term, as new regulations come into force while firms adapt to regulatory requirements and enhance their existing processes around longstanding requirements for "fair, clear and not misleading" communications.

Risks continued

Reputational risk

Foresight Group's growth strategy and value to its Shareholders depends on its sustainability credentials and, as such, the Board recognises that the controls in place to mitigate associated risks such as greenwashing and "Impact Washing" need to be robust and receive appropriate focus. Foresight Group communicates with clients through a variety of media channels, as we support the marketing and promotion of our products across a wide set of markets and jurisdictions.

The Board recognises the importance of being able to substantiate our sustainability claims wherever they are made, beyond the threshold standard of "fair, clear and not misleading". The Head of Risk is a member of the Sustainability Committee and is responsible for the oversight of sustainability risk management activities across the Group.

Operational resilience

Operational resilience is the state of being able to continue to offer our services in volatile and potentially disastrous situations (crises and emergencies) without disruption or reduction in the standards that our clients and counterparties expect from us.

In addition to our own activities, Foresight is dependent on third parties for some important business services. Disruption to these services may threaten the delivery of our own services. In order to manage this risk, our counterparties are assessed on an annual basis in terms of their importance to our operations, with our most important counterparties subject to annual on-site due diligence.

Stressed market conditions

Analysis is performed using scenarios that could result in the Board of FGHL and Exco determining that Foresight Group LLP, as the MIFIDPRU Investment Firm and principal regulated entity, must cease its regulated activity and surrender its permissions such that Foresight Group LLP is no longer authorised under Part 4A of FSMA 2000.

Wind-down may occur in normal market conditions, but the underlying assumption for the scenarios is that an orderly wind-down is executed under stressed market conditions. Wind-down would occur if the Group was unable to recover from an event or series of events, e.g. a failure of controls, business continuity and disaster recovery planning.

Crises

The Crisis Management Plan (Disaster Recovery Plan ("DRP")) is the process by which events categorised as crises are managed.

The DRP is activated when there is a catastrophe, including, but not limited to, property destruction and/or loss of life. The DRP may be activated upon a significant event or series of events that bear a heavy reputational risk payload to the Group, such as a "greenwashing" scandal.

Emergencies

The Business Continuity Plan ("BCP") is the process by which events categorised as emergencies are managed. The BCP is in place to ensure that our regulated activities can continue more or less uninterrupted given a variety of scenarios that would otherwise cause them to stop. The BCP may be activated upon cyber assaults, terrorist assault on or nearby office locations, or the next pandemic.

Geopolitical risks, business continuity and disaster recovery

We monitor our exposure to geopolitical risks and perform scenario analyses to work through potential consequences.

Geopolitical tension can create problems for our supply chains. Some of the regions have historically been active in venture technologies; some ongoing conflicts may have indirect if not direct effects on our businesses. The actual and potential conflict zones for FY25 (Israel, China/Taiwan, Iran and Russia/Ukraine) will likely see increases in sanctions activities which would precipitate changes to operational workflows. Tariffs on Chinese "green technology" imports by the United States may precipitate a shift in the global supply chain and put pressure on industries based in Europe. For example, a glut of solar cells may be commercially attractive over the short term to the detriment of competitive European alternatives over the medium to long term.

Cyber risk

The Technology and Data team leverage a wide array of leading technology solutions and industry best practices to maintain a secure perimeter and detect and respond to threats in real time. Additionally, senior management (including the Foresight Executive Committee) are actively engaged and regularly updated on the extent of the threats, the mitigations in place to counter threats, and the business continuity and response plans in place to manage cyber incidents. The Information Technology Steering Committee and the Risk Committee provide oversight of the management of cyber risk. Cyber risk is a standing agenda item of the Risk Committee. Our Technology and Data team tests our cyber defences regularly through simulated cyber-attacks (penetration testing).

Risks continued

Cyber risk continued

These exercises feed into a significant programme of work to continue to enhance the integrity and security of our digital estate. The Board is focused on the evolution of our cyber capabilities as part of our operational resilience and updates on the emerging and evolving cyber threat landscape are provided.

With respect to the operational resilience of our service providers, we are also focused on the risk that hackers might find a way into the Group's systems through a compromised third party. We include a detailed IT security assessment as part of our due diligence process on such providers and the outcome of this assessment feeds into the Third-Party Risk Assessment and is a significant factor in the decision to proceed with or retain the business relationship.

Cyber and information security remains a key risk due to the prevalence and increased sophistication of cyber-attacks. The emergence of simple Artificial Intelligence ("AI") tools has had a significant impact on the quality of phishing emails and therefore phishing attacks are becoming harder to recognise. Foresight continues to monitor these threats regularly alongside employee engagement with cyber security training. The cyber security training covers the latest phishing techniques to ensure our staff stay abreast of the latest attack techniques. Regular test emails have proved beneficial and enable Foresight to understand which staff required additional training across the business. An internal review and escalation programme was recently implemented to align the training and event response with Foresight's risk strategy.

Internal Capital Adequacy and Risk Assessment ("ICARA")

Our Prudential Consolidation Group is comprised of our principal regulated entity, Foresight Group LLP, and its subsidiaries. The Group is in scope of the FCA's Investment Firms Prudential Regime ("IFPR"). The regulation is implemented through the MIFIDPRU rulebook which came into force on 1 January 2022. As well as capital and liquidity requirements, the rulebook sets out governance requirements and revised remuneration standards that apply to the Collective Portfolio Management Investment firm but also represent best practice for the Group. In October 2023, the ICARA was approved by the Executive Committee.

Risk culture

By fostering a strong risk culture, businesses can seize opportunities, mitigate threats and create a sustainable path for long-term success.

We continue to enhance our RCSA activities as part of our process of supporting the Group's risk culture. The RCSA process is a core part of our risk management framework and helps us manage risk across the Group. The Risk team meets with the heads and risk owners of the businesses and core functions on a monthly basis to assess existing, emerging and evolving risks. These meetings also provide exposure and training on our enterprise risk management platform as we continue our migration from our former RCSA processes and towards more regular assessments as part of day-to-day business activities.

RCSAs are used to identify inherent risks arising from activities conducted by businesses and functions across the Group. We record and assess the controls in place to mitigate risks as well as the risks themselves, which enables us to maintain ongoing oversight of the overall risk profile of the Group.

Financial crime risk assessment

Foresight Group must ensure that there are adequate systems and controls in place to manage any potential financial crime ("FC") risks within the business and combat the potential misuse of its services and products in the furtherance of FC.

The Group aims to meet its responsibilities in carrying out its activities in accordance with the laws and regulations of the UK and the overseas jurisdictions in which it operates. The Group and its subsidiaries must comply with FC laws and regulations related to, but not limited to, money laundering, terrorist financing, financial sanctions, proliferation financing, fraud, anti-bribery and corruption, market abuse and tax evasion.

The Group has established a framework to manage FC risk effectively and proportionately, underpinned by five key pillars: Governance, Risk Assessment, Due Diligence & KYC ("Know Your Customer"), Training & Awareness and Monitoring & Surveillance.

Risks continued

Financial crime risk assessment continued

These pillars go across all three lines of defence; however, the key second line of defence ("2LOD") activities undertaken to deliver this framework for Foresight are as follows:

Governance	Risk Assessment	Due Diligence & KYC	Training & Awareness	Monitoring & Surveillance
The Money Laundering Reporting Officer ("MLRO") is responsible for oversight of Foresight Group LLP's ("Foresight") compliance with the FCA's rules as well as systems and controls to manage FC risk. The Compliance function meets monthly to discuss FC matters affecting Foresight and reports to the Executive Committee.	An annual risk assessment specific to each of the principal regulated Foresight entities is produced. Identification of inherent risks, controls and an assessment of residual risk areas requiring focus to ensure all financial crime risks are identified, understood, and managed/mitigated.	Initial risk-based KYC due diligence on prospective and existing clients, investors, transactions and counterparties is supported by periodic risk-based KYC reviews, with enhanced initial and periodic reviews where there is a higher financial crime risk (e.g. PEPs). In addition to the 1LOD quality assurance reviews, the 2LOD reviews a sample of KYC files via the compliance monitoring programme ("CMP").	Annual financial crime training for Foresight employees is supported by periodic FC refresher training via e-Learning and classroom sessions, as well as regular communications on topics such as how to escalate issues to Compliance.	Reporting of potential higher risk circumstances, issues and breaches to the Risk Committee and the Executive Committee which includes the MLRO. Reporting of suspicious activity to the MLRO in accordance with the Anti-Financial Crime Guide. Periodic review and assessment of the Firm's FC monitoring systems and controls in accordance with the compliance monitoring programme.

These pillars are supported by policies and procedures including the AML Policy and Anti-Financial Crime Guide, Anti-Bribery & Corruption Policy, Anti-Market Abuse Policy, Anti-Tax Evasion Policy and Record Keeping Policy.

Conduct risk

Foresight Group defines conduct risk as the risk from improper behaviour or judgement by our employees, associates or representatives that results in negative financial, non-financial or reputational impact to our clients, employees, the firm and/or the integrity of the markets. This is a Group-wide definition and sets the foundation for the conduct risk framework. Confirming appropriate standards of conduct is a key aspect of the Group's culture.

In order to manage conduct risk we take the following approach:

a) Identify and analyse – Define potential key areas of conduct risks

b) Mitigation – Operation and assessment of existing management controls (processes, procedures and documents) that are key in ensuring the sound conduct of the business

c) Monitoring and management – Analysis of potential gaps and formulation of remediation recommendations where appropriate

d) Reporting – Discussion of content and potential actions with senior management

We look to identify potential conduct risks through regular review of the key risk areas across the business. We evaluate any conduct breaches and put in place mitigating measures to avoid further occurrences.

As the conduct risk framework matures, we reduce the opportunity for behaviour that could result in harms to our clients, harms to the integrity of the financial markets and harms to the Group itself.

Consumer Duty

The Consumer Duty came into effect on the 31 July 2023 and sets higher standards in the industry for consumer protection in financial services. Successful implementation of the new Consumer Duty rules ahead of the regulatory deadline to ensure Foresight Group LLP delivers good outcomes for retail customers and our ability to measure this, necessitated updates to existing policies and processes as well as the introduction of additional policies and processes. The Compliance Team has incorporated the Consumer Duty Implementation Plan and ongoing initiatives into its periodic reporting to the Compliance Officer, Risk Committee and Foresight Group LLP Members Board.

Risks continued

Top 10

The following table represents the Top 10 risks to the execution of the Group's strategic goals, as of 31 March 2024. The threat landscape is evolving, and debated at the Risk Committee, which convenes on a monthly basis. The principal risks are discussed at the Audit & Risk Committees, where our assessment and control framework is challenged.

Risk	Description	Causes	Consequences	Preventative and responsive controls and activities
Principal risks				
Cyber risk: information security (Increase)	Staff and asset managers are vulnerable to data breaches from cyberattacks, which can result in financial losses, regulatory fines and reputational damage.	• Phishing attacks • Malware and ransomware • Insider threats • Unpatched software	• Data breaches and unauthorised access to sensitive information • Expensive data recovery and security remediation exercises • Reputational damage • Confidential information distributed with potential harms to clients, markets and firm • Breaches of data protection laws • Potential vulnerabilities exploited more easily	• Robust firewall and intrusion detection systems • Employee security awareness training • Secure and resilient IT systems • Strong access controls and authentication mechanisms • Additional encryption and data protection measures
Macro-economic conditions (No change)	The opportunity for investment in the markets in which Foresight operates is highly competitive. Identifying and committing capital to investment opportunities over the long term involves a high degree of uncertainty and our profitability is sensitive to many factors, including power price volatility. Persistently high levels of inflation and uncertainty over central bank containment policies may have far-reaching consequences for investments. The Group recognises the need to balance competing aspects of wage inflation across capital requirements and talent retention.	• Price inflation and currency fluctuations • Interest rates • Political and geopolitical uncertainty • Regulatory changes and compliance complexity • Business disruptions and supply chain risks	• Reduced investment returns • Decreased market confidence • Regulatory non-compliance • Supply chain disruptions	• Business continuity and supply chain resilience • Diversification of investment portfolios • Active management of investment portfolios • Revision of hard and soft risk limits, risk appetite • Cost reduction and policy/process reviews
Third-party risk (No change)	The Group may rely on third-party service providers for various functions, which can introduce additional operational risks that need to be managed and monitored.	• Supplier quality issues • Ethical and social responsibility concerns • Lack of supply chain transparency • Geopolitical and natural disasters	• Business disruptions and financial losses • Reputational damage • Compromised product quality or safety • Compromised cyber security • Impact on investment performance	• Vendor and supplier evaluation and selection criteria • Supplier financial risk assessment • Increase supply chain visibility and transparency measures • Business continuity and disaster recovery planning review and test • Active third-party risk management

Increase · Trending up · Decrease · No change

Risks continued

Top 10 continued

Risk	Description	Causes	Consequences	Preventative and responsive controls and activities
Principal risk				
Sustainability risk (Increase)	The risk associated with environmental, social and governance factors that can affect investment performance, regulatory compliance and reputation.	• Climate change and environmental impacts • Regulatory changes and compliance complexity • Changing customer preferences and market shifts • Social inequity and human rights violations	• Regulatory non-compliance • Reputational damage • Stakeholder disengagement • Decreased market share	• Maintaining climate impact as part of due diligence • Social responsibility policies and programmes • Supply chain sustainability management • Compliance monitoring and reporting • Crisis management and disaster recovery planning
Regulatory compliance (No change)	The risk of changing regulations or compliance failures that could result in fines, penalties or reputational damage. Foresight must comply with a variety of regulatory requirements, including Sustainability Disclosure rules, which can result in significant penalties if violated.	• Changes in government policies, industry standards and best practices • Shifts in regulatory enforcement practices, increased penalties and legal consequences • Updates to compliance requirements and increased compliance costs • International regulatory harmonisation	• Non-compliance • Reputational damage • Increased costs • Business disruptions	• Regulatory monitoring and compliance programmes • Engagement with regulatory bodies and trade associations • Compliance training and awareness programmes • Legal and compliance firm consultations
Resilience risk (Trending up)	Impact on investment performance.	• System or technology failures • Natural disasters • Cyber security attacks • Third-party service provider failures	• Service outages • Financial losses • Reputational damage • Regulatory penalties	• Redundancy and backup systems • Business continuity and disaster recovery plans • Staff training and competency development • Supply chain diversification and contingency planning

Increase | Trending up | Decrease | No change

Risks continued

Top 10 continued

Risk	Description	Causes	Consequences	Preventative and responsive controls and activities
Emerging risk				
Geopolitical risk (Increase)	The risk that political, social or economic events in a specific country or region may have a negative impact on the performance of investments in that area.	• Political instability and regime changes • Trade wars and tariffs • Economic sanctions and embargoes • Terrorism and political violence	• Business disruptions • Financial losses • Reputational damage • Compromised cyber security	• Geopolitical risk assessment and monitoring, political and country risk analysis • Contingency and crisis management plans • Diversification of markets and supply chains • Reputational risk management strategies
Evolving risk				
Data and records management (Decrease)	The risk that the Group's processes, systems and controls relating to the management, storage and protection of data and records are not sufficient to support the growth in the Group's business.	• Inaccurate data entry and errors • Data duplication and redundancy • Data breaches and security incidents • Lack of record retention and destruction policies	• Compromised data integrity • Legal and regulatory consequences • Business disruptions • Data loss and unavailability	• Data governance framework and policies • Data privacy and compliance programmes • Backup and recovery systems • Cyber security measures and access controls
Conduct and culture (No change)	Conduct risk is the risk of harm to our clients arising from misconduct by our employees or by third parties or other counterparties engaged by the Group.	• Ethical misconduct and fraud • Inadequate training and awareness programmes • Poor governance and oversight • Conflicts of interest and insider trading	• Reputational damage • Loss of customer trust • Legal and regulatory consequences • Decreased employee morale and productivity	• Code of conduct and ethics policies • Regulatory compliance programmes • Whistleblowing policy • Conduct and culture assessments/audit
Human capital risk (No change)	Foresight relies on skilled personnel to manage investments and run its businesses, so human capital risks such as key person risk and talent retention risk can be significant.	• Talent attrition and staffing shortages • Skills gaps and inadequate workforce planning • Training and development gaps • Succession planning and key person risk	• Business disruptions • Decreased productivity • Loss of critical knowledge • Talent retention challenges	• Talent acquisition and retention strategies • Workforce planning and skill development programmes • Succession planning and knowledge transfer • Training and development requirements

Increase | Trending up | Decrease | No change