

# Risks

## Risk strategy

An effective risk management strategy is essential for the Group to achieve its objectives. Foresight's Risk leadership team are responsible for the risk culture across the Group and the effective implementation of our risk management frameworks.

Foresight receives the majority of its revenue from management fees for the investment products and services it provides. The risk management function supports the integrity and effectiveness of those products and services to provide a stable platform for further growth in the businesses and the returns for our Shareholders. Foresight's revenues and shareholder value are principally driven by the opportunities afforded from infrastructure and renewable energy asset investment management and investment in non-listed companies.

Foresight's risk strategy is implemented by the Chief Risk Officer, the regional Heads of Risk Management and the risk sponsors for departments where specialists with experience in particular risks reside, such as Information Security, Financial Crime, Conduct and Sustainability.

## Risk highlights – 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 the market for venture technologies, some ongoing conflicts have corollary if not direct effects on our businesses.

The actual and potential conflict zones for 2025-26 (Israel, China/Taiwan 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.

## Risk governance

Risk management governance starts with the Board of Foresight Group Holdings Limited ("Foresight", "Group") which both directly and through its Audit & Risk Committee ("ARC"), and the Executive Committee ("Exco"), oversees our approach to managing our risks through our Enterprise Risk Management framework. Exco is responsible for the annual review and approval of our risk appetite statement. The risk appetite statement describes the levels and types of risk we are willing to accept in order to achieve the objectives included in our strategy and business plan, while remaining in compliance with regulatory requirements.

Foresight accepts a certain amount of risk inherent in the activities and these include liquidity, market, credit, operational, cybersecurity, legal, compliance, conduct, regulatory and reputational risks.

As a provider of regulated services, Foresight is required to document its risk appetite in relation to its entities within the Group. These considerations are set out in the risk appetite statement and such decisions are made at Board and Exco level. 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.



Member of the Foresight team

# Risks

## Risk governance

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 the risk appetite for the firm. Exco is responsible for endorsing the policies and procedures within the Group framework and motivating the business to take calculated risks.

Risk mitigation and risk transfer are risk management activities performed by the second line and first lines of defence. Responsibilities are set out in the Group's three lines of defence ("3LOD") policy. The Board has authorised Exco to manage the day-to-day operation of the Group, which includes the performance of the risk management function. Exco has formal oversight of all matters in relation to the operations of the business, governance and risk.

The Risk function maintains the risk policies and risk procedures with clearly defined roles and responsibilities across the Group monitored through the Audit & Risk Committee, as well as the Risk Committee ("RC"). The RC is chaired by the Head of Risk, Jonathan Parsons, who is responsible for the risk management function, including updating the Executive Committee and Members' Board on risk-related matters of the business. The RC is guided by its own terms of reference and makes recommendations to the Executive Committee and Members' Board on any actions it considers are needed.

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.

## Risk culture

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

We continue to enhance our Risk and Control Self-Assessment ("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 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 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.

## Risk management framework

Foresight has established an Enterprise Risk Management ("ERM") framework to support a comprehensive, integrated approach to risk management across the Group. The ERM framework enables the risk management processes through which we identify, assess, monitor and manage the risks we assume in conducting our activities.

The Risk function is responsible for ensuring that Foresight's ERM framework provides the Board, our executive committees and our risk committees with a consistent and integrated approach to managing risks according to the risk appetite.

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.

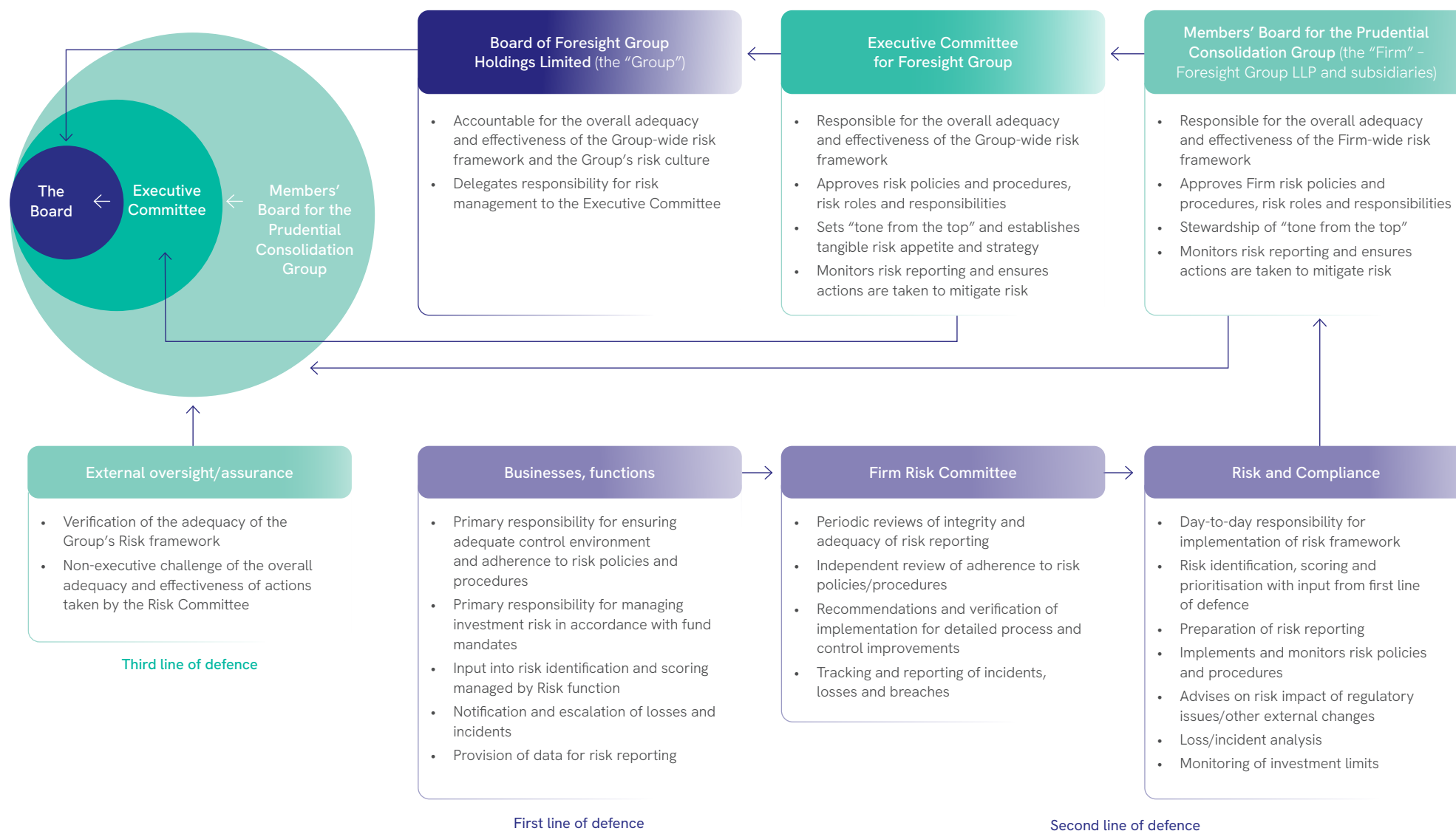
Our first line of defence consists of our revenue-producing units, our Technology & Data team, Group Finance and certain other corporate functions. The first line of defence is responsible for its risk-generating activities, as well as for the design and execution of controls to mitigate their risks.

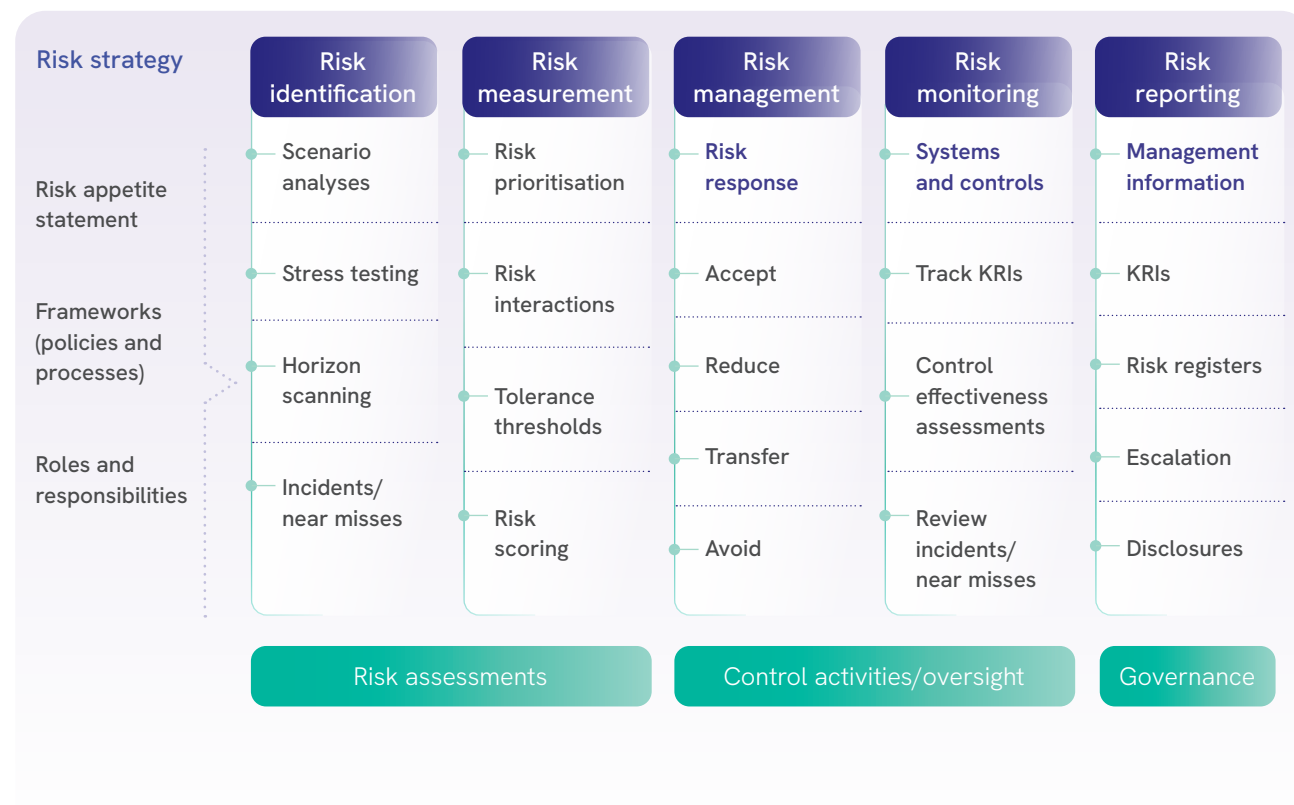
The second line of defence consists of our Risk and Compliance functions. These provide independent assessment, oversight and challenge of the risks taken by our first line of defence, the effectiveness of the control environment as well as leading and participation in the Risk Committee.

Our third line of defence is performed externally. Further to guidance from the Board, an Internal Audit strategy was set out in FY25. Internal Audit will be responsible for independently assessing and validating the effectiveness of key controls, including those within the risk management framework. Internal Audit will provide timely reporting to the Audit & Risk Committee of the Board and Senior Management and will support the activities for the implementation of Provision 29 of the 2024 revision to the UK Corporate Governance Code, relating to the effectiveness of internal controls.

The 3LOD model promotes the accountability of first line risk takers, provides a framework for effective challenge by the second line of defence and empowers independent review from the third line.

## Risks





## Risks

### Cyber risk – Information security and technology infrastructure

Cyber risk represents a significant risk across the Group since, apart from direct exposure, there are risks to many of the underlying infrastructure portfolio assets themselves. The risks of facility failure arising from attacks by hostile state or state-adjacent groups on renewable energy facilities has increased and precipitated a review of our risk assessment and control effectiveness.

The Group Technology and Data team leverages a wide array of leading technology solutions and industry best practice to maintain a secure perimeter and detect and respond to threats in real time. Additionally, Senior Management (including the Executive Committee) are actively engaged and regularly updated on the extent of the threat, the mitigations in place to counter this threat, 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). 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 cybersecurity training. The cybersecurity 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 what areas required additional training across the business.

### Cybersecurity risk management process

Our cybersecurity risk management processes are integrated into our overall risk management processes. Foresight has an Information Security Officer and a framework to identify, assess, document and mitigate threats as well as prevent, detect and respond to security incidents. The Risk team, which reports to the Chief Risk Officer, provides oversight and challenge of the Cybersecurity Programme and assesses the operating effectiveness of the programme against risk appetite-approved operational risk limits and thresholds.

Our process for managing cybersecurity risk includes the critical components of our Enterprise Risk Management framework as well as a comprehensive training and education programme, to prepare our staff to recognise information and cybersecurity threats and respond accordingly. A number of important controls and activities support the framework, including robust identity and access management, real-time monitoring of our network for known vulnerabilities and signs of unauthorised attempts to access our data and systems, as well as vendor management within our third-party risk management which includes cybersecurity and business resiliency assessments on vendors.

In conjunction with third-party service providers, we perform risk assessments to gauge the integrity of our security arrangements, to estimate our risk profile and to assess compliance with relevant regulatory requirements.

Foresight performs periodic control effectiveness assessments through our internal risk and control self-assessment process, as well as a variety of external technical assessments, including external penetration tests and "red team" engagements where third parties test our defences. The results of these risk assessments, together with control performance findings, are used to establish priorities, allocate resources, and identify and improve controls. We use third parties, such as outside forensics firms, to augment our cyber incident response capabilities.

During 2025, we did not identify any cybersecurity threats that have materially affected or are reasonably likely to materially affect our business strategy, results of operations or financial condition.

Our Information Security Officer and all Senior Management within the Technology and Data team have relevant expertise in the areas of information security and cybersecurity risk management.



# Risks

## Sustainability risk management

The success of our business depends on our ability to generate attractive risk-adjusted returns for our investors while meeting our sustainability objectives.

A more detailed description of our climate risk assessment is included in the TCFD 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 Taskforce for Nature-related Financial Disclosures ("TNFD") as it did for TCFD; voluntary disclosures become mandatory through the adoption into the rulebooks.

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.

The Risk function has enhanced its set of Key Risk Indicators for the risk appetite statement to monitor our progress towards our ESG objectives.

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 discussion paper and make sure that we can evidence our commitment to diversity 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 sustainability claims will be a significant feature of the regulatory landscape over the short to medium term.

## 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 additional 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

Foresight's ERM framework is designed to improve our operational resiliency, which is defined as our ability to deliver products and services with no discernible disruption or harms to clients by adapting and responding effectively to challenges through periods of volatility and change.

Operational resilience covers the control frameworks that prevent risks becoming issues in normal and stressed market conditions, as well as business continuity and disaster recovery situations during which some of those controls may not have been sufficient and additional activities are needed to minimise disruption.

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-attacks, terrorist assault on or nearby office locations, or the next pandemic. The Disaster Recovery Plan ("DRP") is the process by which events categorised as "crises" are managed. This is activated when there is a catastrophe, including, but not limited to, property destruction and/or loss of life.

Our BCP is tested by an external firm on an annual basis, on site, with the engagement of the Emergency Response Team and other senior managers. Our performance is discussed at the Risk Committee with recommendations provided to Exco with the report.

## Risks

### Operational resilience

For situations where operational resilience is not sufficient, analysis is performed using severe but plausible scenarios that may 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.

### 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 2024, the ICARA was approved by the Executive Committee.

### 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. 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 Group Head of Compliance and Head of Compliance UK meet weekly with the MLRO to provide updates on the Compliance Function including FC matters affecting Foresight and reports to the Members' Board and 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.

## Risks

### 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, aligned with the Group ERM processes:

Identify and analyse	Define potential key areas of conduct risk
Mitigation	Operation and assessment of existing management controls (processes, procedures and documents) that are key in ensuring the sound conduct of the business
Monitoring and management	Analysis of potential gaps and formulation of remediation recommendations where appropriate
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 continues to mature, we are reducing 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.








Members of the Foresight team



# Risks




## Principal risks

Principal risks are the key risks currently faced by the Group, which are recognised as having significant and potential impacts ranging from the short to the long term.

Risk	Description	Consequences	How we manage this risk	Impact
<b>Business risk – fundraising</b> 	Our ability to effectively raise funds is essential for business growth and meeting strategic objectives. Fundraising risks involve challenges in attracting investor capital due to economic uncertainty, market volatility, shifts in investor preferences and competition.	If Foresight is unable to raise sufficient capital, this may result in missed investment opportunities, reduced market competitiveness and could potentially impact our long-term financial viability.	Foresight fundraises through a variety of channels, actively engages with our investors and continuously innovates our product offerings. Our investor relations teams proactively monitor investor sentiment.	<div>Low</div> <div>Medium</div> <div>High</div>
<b>Business disruption and system failure</b> 	This risk involves interruptions to our critical business systems, technology infrastructure and operational capabilities, potentially due to cyber-attacks, IT system failures or physical disruptions.	Operational downtime, compromised client services, financial loss and reputational damage could occur if sufficient frameworks are not in place to support the services Foresight provides.	We have robust business continuity plans and cybersecurity defences. Foresight undertakes regular system testing, both internally and with external parties. Incident management processes and dedicated response teams are established to rapidly restore operations.	<div>Low</div> <div>Medium</div> <div>High</div>
<b>Strategic risk – asset concentration</b> 	Asset concentration risk arises from holding a significant portion of our Assets Under Management in specific markets, sectors or investment strategies, increasing vulnerability to economic or market downturns and policy shifts.	Policy shifts, for example in energy subsidy regimes or fiscal policy, could significantly impact overall investment performance, asset values and revenue.	Foresight regularly monitors and manages asset diversification, with limits and controls on exposures. Our Investment Committee evaluates asset allocations to ensure prudent diversification across portfolios.	<div>Low</div> <div>Medium</div> <div>High</div>
<b>Regulatory change and compliance</b> 	Regulatory compliance risk involves failure to adhere to laws, regulations and industry standards, potentially due to evolving regulatory environments, complexity in cross-border activities or ineffective internal controls.	Non-compliance could lead to fines, legal action, regulatory scrutiny, reputational harm and operational disruptions.	Foresight maintains a robust compliance framework, with regular training, compliance monitoring programmes, and proactive engagement with regulators. Dedicated compliance teams ensure adherence to existing regulation and guidance and support the regulatory change programmes.	<div>Low</div> <div>Medium</div> <div>High</div>
<b>Operational resilience</b> 	Operational resilience involves the ability to prevent, adapt, respond to, recover and learn from operational disruptions, including technological, operational or external events.	Poor resilience may lead to significant operational downtime, financial losses and damaged client confidence.	Foresight has a comprehensive operational resilience framework, which includes scenario testing and incident response processes, including enhancements to our resilience capability arising from events and near-misses.	<div>Low</div> <div>Medium</div> <div>High</div>

## Risks




### Principal risks

Risk	Description	Consequences	How we manage this risk	Impact
<b>People</b> 	People risk concerns Foresight's ability to attract, retain and develop skilled and motivated employees, essential for delivering strategic goals and maintaining business continuity.	Talent shortages, low morale or high turnover rates can disrupt operations, impact business performance and impair service quality.	We invest in employee engagement initiatives, development programmes, competitive compensation strategies and succession planning to retain critical talent and support career growth.	<div>Low</div> <div>Medium</div> <div>High</div>
<b>Sustainability</b> 	Sustainability risk encompasses environmental, social and governance ("ESG") factors, including climate change, impacting our investment portfolios and business reputation.	Failure to adequately integrate ESG considerations can lead to reputational harm, investor dissatisfaction, regulatory non-compliance and possible fines, climate litigation and investment under-performance.	Foresight integrates ESG criteria into investment decisions and processes, and applies its sustainability analyses to maintain transparency in ESG reporting and align with emerging global sustainability standards.	<div>Low</div> <div>Medium</div> <div>High</div>
<b>Conduct and culture</b> 	Conduct and culture risks relate to inappropriate behaviours, inadequate cultural alignment, or unethical practices within our organisation.	Misconduct or a weak corporate culture could lead to regulatory sanctions, reputational damage, loss of client trust and financial penalties.	Foresight's robust conduct risk framework, clear ethical guidelines, regular training, whistleblowing procedures and strong leadership engagement foster a culture of integrity and accountability.	<div>Low</div> <div>Medium</div> <div>High</div>

## Risks

### Emerging/evolving risks

Emerging and evolving risks are risks that carry a higher degree of uncertainty around their impact and likelihood. The Risk function prepares regular reports for the Board setting out scenarios and their potential impact on our assets and our operational resilience.

Risk	Description	Consequences	How we manage this risk
<b>Third-party risks</b> 	Third-party risks involve potential threats stemming from our reliance on external service providers, vendors and partners.	<p>Widespread adoption of third-party platforms by Group functions can create critical dependencies.</p> <p>Failures or security breaches by third parties could result in service interruptions, financial losses, regulatory breaches and reputational damage.</p>	We implement rigorous due diligence, continuous monitoring, robust contractual agreements, and establish clear accountability for third-party relationships, alongside contingency planning to minimise disruptions. We also plan for the unavailability of critical systems as part of our digital operational resilience.
<b>Geopolitical risk</b> 	Geopolitical risks continue to surface resulting from global political tensions, conflicts, trade disputes and changes in international relationships.	<p>Heightened geopolitical risks can lead to market volatility, operational disruptions, asset impairment and adverse impacts on global investment portfolios.</p> <p>Rapidly escalating tensions could have a significant impact on our supply chains.</p>	We conduct regular geopolitical risk assessments, scenario planning and proactive portfolio diversification. Our teams closely monitor geopolitical developments and adjust investment strategies to mitigate impacts.
<b>Artificial Intelligence</b> 	Alongside the many opportunities, Artificial Intelligence ("AI") represents a risk to the profitability and competitive advantage of the Group.	Misuse or poorly calibrated AI engagement could lead to biased decision-making, regulatory violations, loss of data, client and counterparty trust and financial losses.	Foresight's Risk and Compliance team's oversight over the implementation of AI-supported platforms and processes as part of an accountability and control framework to reduce the risk of harms to Foresight and its clients through adoption of this technology.