Managing our risks

Effective risk management is key to the success of delivering our strategic objectives. Our risk culture continues to strengthen; it ensures identification, assessment, and management of the principal risks to our business.

The overall level of risk we face continues to increase as a result of external market conditions; high volumes of regulatory change; an increasingly uncertain global political environment and associated market volatility; and increasing cyber criminality.

Our approach is to maintain a strong control framework to identify, monitor and manage the principal risks we face, adequately quantify them and ensure we retain sufficient capital in the business to support our strategy for further growth.

We assess our principal risks regularly to ensure that our risk profile is within our risk appetite which is set by the Board.

We categorise risks into risk groups covering potential impacts to clients, revenue, capital and reputation. The three risk groups are:

- Business Risk
- Financial Risk
- Operational Risk

We identify and assess specific risks within these risk groups, mitigate and manage these risks, and monitor and report against these risks, which provides the foundation to enable us to deliver against our strategic objectives.

Risk Management Objectives

The primary objectives of risk management at Brewin Dolphin are to ensure that there is:

- a strong risk culture so that employees are able to identify, assess, manage and report against the risks the business is faced with;
- an appropriate balance between risk and the cost of control;
- a defined risk appetite within which risks are managed; and
- a swift and effective response to incidents in order to minimise impact.

Risk Management Framework

The Board has established a Risk Management Framework to ensure there is effective risk governance.

We follow industry practice for risk management through the ‘three lines of defence’ model. The first line is the business that owns and manages the risk, the second line is the control functions, and the third line is independent assurance provided by audit.

The key parties involved in the risk management process within the Group and their respective responsibilities, and an explanation of how risk management is structured within the Group, is set out opposite.

The Board promotes a strong risk culture throughout the business by promoting and encouraging:

- A distinct and consistent tone from the top
- Clear accountabilities for those managing risk
- Prompt sharing and reporting of risk information
- A commitment to ethical principles
- Appropriate levels of conduct and considered risk taking behaviour
- Recognition of the importance of knowledge, skill and experience in risk management
- Members of staff at all levels to make suggestions for improving processes and controls
- An acceptance of the importance of continuous management of risk, including clear accountability for and ownership of specific risks.

Every employee within the Group is expected to adhere to the high standards established by the Board. The benefits of establishing a strong risk culture is evident; with our employees self-identifying and escalating risk events and potential issues to mitigate the probability of risks crystallising.

The Board reviews the effectiveness of this Risk Management Framework periodically, receiving reports on internal control from the Audit and Risk Committees and debating key risks for the Group following more detailed work by the Risk Committee.

Risk Management Framework

Top Down Risk Management

Board
- Responsible for ensuring there is an adequate and appropriate risk management framework and culture in place.
- Sets risk appetite and is responsible for ensuring alignment with the Group's business strategy.

Risk Committee
- Oversees the Risk Management Framework.
- Assists the Board in its responsibilities for the integrity of internal control and risk management systems.

Audit Committee
- Assists the Board in gaining assurance as to the integrity of the financial statements and the effectiveness of the system of internal controls.
- Monitors the effectiveness and objectivity of internal and external auditors.

Risk Management Committee
- Executive level day to day oversight and monitoring of the adequacy and effectiveness of the Risk Management Framework.
- Monitors current and emerging risks and themes.
- Oversees the Group's Policy Framework.

Business Risks

These are the risks that we do not set the right strategy, a material business decision fails or external market factors impact the viability of the business.

Financial Risks

These are the risks facing our business in terms of inadequate or failed management of finances and the risk introduced by external factors that could have a detrimental impact on our cash flow, capital and liquidity.

Operational Risks

This is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

Risk Identification and Assessment
- Risk and Control Self Assessments to identify the key risks for each department and for business change activities.
- Assessment of inherent (pre-control) and residual risk (post-control).

Risk Mitigation and Management
- Management of events that had a potential or actual financial, regulatory, operational or client impact.
- Agreeing action plans to mitigate risk issues.

Risk Monitoring and Reporting
- The business community is primarily responsible for monitoring risks.
- Risk trends are monitored and analysed.
- Key risk indicators are reviewed monthly.

Risk Assurance
- Annual audit plan to evaluate the adequacy of processes and systems, and test the operating effectiveness of key controls.

Bottom Up Risk Management

2017 Developments

Considerable uncertainty in the external environment has continued in 2017 both in the UK and globally, including ongoing Brexit negotiations and international political events. Whilst the Group is predominantly a UK domiciled business with a UK centric client base, this uncertainty and resulting increased levels of market volatility may have an impact on some of our principal risks. We are closely following the Brexit negotiations and will assess the ongoing impact of these on our principal risks over time.

In 2017 we have focused on reviewing variances in the risks and controls across our offices. This process has identified opportunities to strengthen controls and improve operational efficiency, which will be implemented over the course of 2018.

A risk workshop was conducted during the period to review the risks facing the Group. For each risk, an assessment was undertaken of the relative willingness to take that risk to achieve the Group's strategic objectives. Key Risk Indicators used to monitor the profile of each risk against the risk appetite have been refreshed.

See page 37 for our Viability Statement, which relies on the evaluation of principal risks

Principal Risks

The tables below detail the principal risks and uncertainties we have identified. We have a process to regularly report key risk indicators and identify changes in the profile of these principal risks. We also consider emerging risks as part of this process.

Business risks

These are the risks that we do not set the right strategy, a material business decision fails, or external market factors impact the viability of the business. This could include an inability to introduce or enter into new business lines effectively, to expand organically or through merger/acquisition, or to enhance the effectiveness of our operational infrastructure.

Direction of change:

Business risks have increased over the past year as heightened levels of uncertainty in the external environment persist. Additional risk was taken on during the integration of DLAM to support the Group's growth objectives.

Principal Risk	Nature of the Risk	Key mitigants
Business Strategy	This is the risk that we fail to deliver against the strategic objectives.	– A strategic plan approved by the Board. – A risk appetite that is set against our strategic objectives, and monitored on a regular basis by our formal governance committees. – A robust governance structure that includes challenge from our independent Non-Executive Directors. – Branch and functional plans are set to achieve strategic priorities, which are subject to thorough challenge and review by the Board.
Geopolitical	The external environment continues to be marked by considerable uncertainty globally, as we are in a period of significant political change. Financial markets can be sensitive to geopolitical factors and market volatility can heighten in uncertain environments, impacting performance leading to the Group generating variable returns. Geopolitical uncertainties and external market factors are inherent risks to the financial services industry.	– We are focused on delivering long-term value to clients, positioning portfolios appropriately based on our clients' risk profiles and in line with our macroeconomic views.

Financial risks

These are the risks facing our business in terms of inadequate or failed management of finances and the risk introduced by external factors that could have a detrimental impact on our cash flow, capital and liquidity.

Direction of change:

Financial risks remain at a similar level to last year and are impacted by the continued uncertainty in the external environment. Economic uncertainty has the potential to impact profitability of our counterparties and their credit ratings.

Principal Risk	Nature of the Risk	Key mitigants
Counterparty	Default by our banking or trading counterparties could put our own or our clients' cash deposits or assets at risk.	– A Financial Risk Management Framework is in place which includes managing the Group's exposure to counterparty credit risk and setting and monitoring counterparty limits. – Diversity across our trading and banking counterparties. – Due diligence is undertaken for all banking and trading counterparties. – A Financial Risk Committee provides oversight of the Financial Risk Management Framework.

Operational risks

This is the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

Direction of change:

The volume of regulatory change and increasing occurrences of cyber attacks across industries has increased the inherent risk of change management and criminality. We focus on continually strengthening our monitoring and oversight of these risks.

Principal Risk	Nature of the Risk	Key mitigants
Regulatory & Legal Compliance	This is the risk that we are not compliant with all existing applicable regulation and legislation.	– Compliance and Legal functions monitor and oversee fulfilment of our regulatory and legislative requirements and interactions with our key regulators. – We are active in various industry and trade associations to help influence regulation and legislation.
Change Management	The risk that business and regulatory changes are not delivered which impact the Group's performance and ability to deliver strategic objectives.	– A Strategic Projects Committee is responsible for prioritising projects and reviewing their status and progress. – A Regulatory Change function within Compliance review new regulation as it is drafted to ensure we are in compliance when it is implemented.

Conduct	This is the risk of not delivering fair outcomes for clients.	– Tone from the top sets a culture which puts delivering fair outcomes for clients at the core of the Group's activities/ethos.
		– A conduct risk framework sets our approach to conduct risk governance, and the ongoing assessment and monitoring against key metrics and reporting of conduct risk.
		– A risk based client on-boarding process which ensures that we understand our clients' needs and attitudes to risk.
		– A quality assurance process to identify and address any instances where the best outcomes for clients are not achieved.
		– Robust investment governance supported by:
		  – an Investment Governance Committee;
		  – a dedicated research department to set the Group's asset allocation framework; and
		  – a restricted assets policy to prevent investment in unsuitable assets.

Criminality	The increasing external risk of criminality and the difficulty of complete prevention is recognised, as the volume and sophistication of information security threats (cyber risk) and fraud attempts across industries increase.	– Financial Crime, Information Security and Data Protection functions ensure we have robust preventative and detective measures to reduce this risk. – Dedicated Information Security and Data Protection team report directly to the Group Risk & Compliance Director. – Regular testing of our business continuity, disaster recovery and crisis management plans.