Risk Review

Risk management

The Board of Directors, supported by the Risk and Audit Committee, is responsible for defining the risk strategy, risk appetite and risk policy – along with approving any material changes to them and for ensuring that adequate internal-risk management and control systems are in place across the organization. The effectiveness of the design and operation of these systems is reviewed with the Risk and Audit Committee, together with the result of its annual evaluation, as well as any identified deficiencies, significant changes and planned improvements. In addition, other relevant matters may be considered to support the Directors' statements at the end of this section. For further information, see the Risk and Audit Committee Report included in this Annual Report.

The CEO and the senior management team are responsible for implementing the Board's guidelines, including the measures established to mitigate the risks taken within the approved risk appetite. They carry this out through a clear and segregated organisational model, supported by qualitative principles, indicators and thresholds, and by the limits set by the Board of Directors. The outcomes of the risk assessment process are incorporated into strategic planning, capital allocation and resource prioritisation decisions, ensuring consistent alignment with the approved risk appetite.

Risk management approach

Risk management involves identifying and measuring both direct and indirect risks, as well as potential and emerging risks. This approach is based on the analysis of internal and external risks associated with the Group's strategy and activities, including in all cases, strategic, operational, compliance and reporting risks. This analysis determines the Group's appetite for the identified risks – and whether the appropriate response is to accept, avoid, mitigate or transfer them. Effective risk-management also strengthens the Group's resilience, enhances its competitive position and helps identify new business opportunities.

Allfunds has a comprehensive risk-management and control model that is tailored to its business model, organizational structure, and its corporate governance framework. This model enables the Group to implement the risk-management and control strategy, as well as the policies defined by the Board of Directors, while adapting to a changing economic and regulatory environment. The model is designed, implemented and maintained on a Group-wide basis, integrated into relevant business processes and updated at least annually. The annual update includes a systematic assessment of the design and operation of internal risk management and control systems, considering observed weaknesses, cases of misconduct or irregularities, lessons learned and finding from internal/external audits, providing sufficient insight into any failings. Material deficiencies are defined as failures in key controls that could result in material financial misstatements, significant compliance breaches or material operational disruptions.

Improvement actions are implemented whenever necessary. The model consists of the following components: risk management framework, risk management strategy and objective, risk appetite framework and risk reporting. The assessment of the design and operation of these systems is conducted using recognised standards, including ISO 31000 and ISO 27005 for ICT Risk management, applied consistently across the Group.

We promote the development of a strong risk culture that ensures the consistent application of this model across the Group. This ensures that the risk-management and control model is well understood and applied by all employees for whom it is relevant, and that responsibilities are clearly understood and embedded at every level of the organisation.

The internal control systems provide reasonable assurance that financial reporting is free from material inaccuracies, and at least limited assurance to sustainability reporting. The ongoing evaluation of the Group's risk profile, liquidity position and control environment supports the preparation of the financial statements on a going-concern basis.

Risk management framework

The Group's risk management framework is built on three lines of defence model: the business, risk management functions and internal audit. This framework is designed to ensure effective and independent oversight of the Group's activities in line with the overall risk strategy, which is established by the Board of Directors and updated at least annually.

1 First line of defence

- Business and support functions (other than control functions).

Provides day-to-day risk management and control for the Group.

Implements and manages risk indicators or first level controls to identify potential risks and ensure an effective answer to mitigate them.

2 Second line of defence

- Compliance, Anti-Money Laundering (AML) and Risk Management teams.
- Act autonomously and independently of each other and with respect to the first line of defence.

Provides independent oversight of and challenges the risk management of the business.

Supports the first line of defence by defining and monitoring compliance with rules and limits needed for the business to stay within the overall Risk Appetite defined by the Board of Directors.

3 Third line of defence

- Internal audit function.
- Has the maximum level of independence and objectivity within the Group.

Ensures the effectiveness of the Group's control systems

Carries out independent reviews of the first two lines of defence to verify compliance with the Group's risk management framework and provides assurance to the Risk and Audit Committee on the effectiveness of the Group's risk management.

Risk management strategy and objective

Prudence in risk management is a fundamental pillar of the Group's activities and services. The Group's organisational structure establishes a system of clearly defined delegations that support effective risk management. The guiding principles for the identification, monitoring and management of risks are as follows:

a. Risks undertaken must be compatible with the Group's assets and aligned with its target solvency level

b. Commitment to maintaining a low-risk profile, achieved through:

i. Maintaining a focus on distribution activities while limiting exposure to proprietary positions that could create risks beyond the Group's desired risk profile

ii. Seeking a high degree of diversification of structural risks, establishing concentration limits by customer, sector, market and/or geography that could jeopardise solvency objectives, liquidity and the stability of results

iii. Ensuring continuous attention to risk identification and monitoring, providing all areas with adequate and dynamic systems that support optimal risk management and control

c. Implementing robust procedures for the control and monitoring of all risks incurred by the Group in the course of its activities

d. Maintaining sound mechanisms for managing and mitigating operational and reputational risks

Risk appetite framework

The Risk Appetite Framework (RAF) is a Group-wide corporate management framework designed to determine risk appetite (the type and amount of risk to be willingly taken to achieve the business strategy) within the limits of the Group's risk-taking capacity. It is supported by management strategies formulated by the senior management team based on the Group's management principles – together with the internal control system underpinning that process.

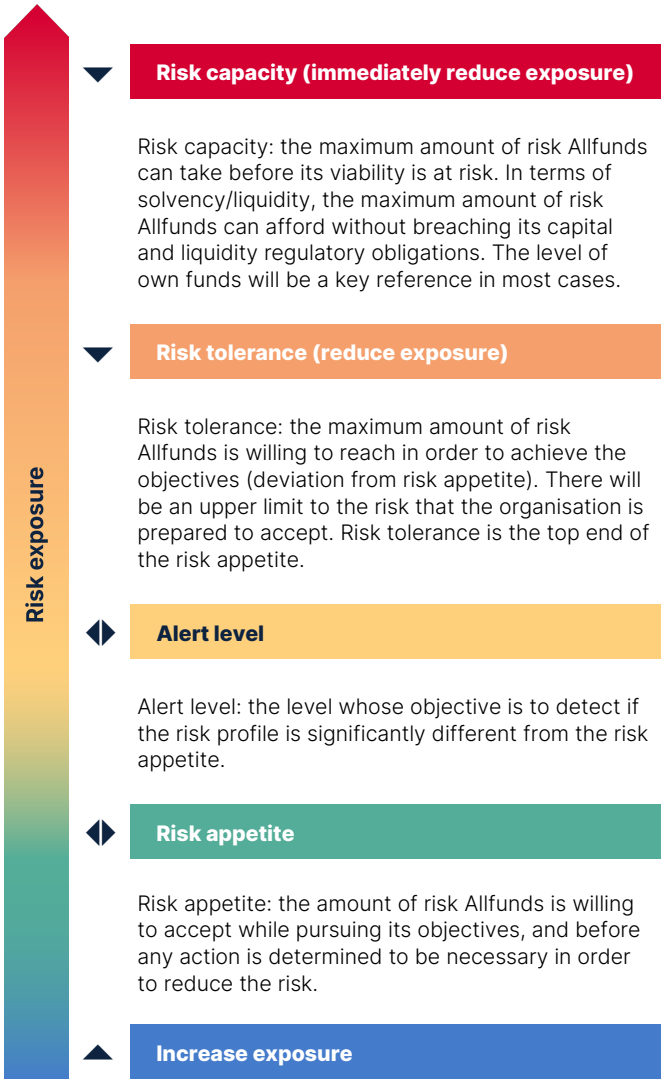
The primary objectives of the RAF are to strengthen profitability, enhance risk management and promote transparency in the overall risk-taking policy for capital allocation and profit maximisation. This is achieved through the establishment, communication, and oversight of risk appetite, as well as the optimisation and speed-up of allocation of management resources. Overall, the RAF reinforces the effectiveness of the Group's risk-monitoring system.

The Board of Directors approves the risk strategy on an annual basis, including the RAF, promoting sound internal governance, the establishment of limits and objectives and the implementation of monitoring and surveillance mechanisms for the different types of risk. The most recent update was completed in March 2026 and the Board of Directors confirmed that the Group's risk appetite is maintained at a low level. This risk appetite level provides the foundation for the development of calculation and control methodologies for the risks incurred by the Group, which are implemented through its Risk Management Department.

The Board of Directors reviews and discusses potential corrective measures should any of the risk tolerance levels be exceeded. The Group has identified and implemented a set of key risk indicators (KRIs) to monitor performance against its stated risk appetite. The key risk indicators report, covering all risk areas, is provided to the Board of Directors on a quarterly basis. The report identifies any deviations or potential breaches of established risk-tolerance levels and proposes mitigating actions where necessary.

Risk exposure

Risk profile: an assessment of the Group's exposure to each relevant risk at a given point in time, taking into account the current situation and future forecasts as reflected in dynamic and potential risk metrics. The risk profile must remain within the limits set by the Group's risk appetite and must not exceed its overall risk-taking capacity.



Risk reporting

Risk control and monitoring reports support the efficient and continuous oversight of the risks the Group incurs in its daily activities. The information contained in these reports enables the Group to monitor operating limits established for each counterparty and to oversee other operating aspects related to its intermediation activity.

The Risk Management unit relies on the following key reports to fulfil its responsibilities: progress reports on execution and settlement risk exposure limits; progress reports on overdraft limits; progress reports on liquidity and market risk; and statistical reports and stress-testing results. In addition, reporting also includes annual updates to the Risk and Audit Committee and the Board of Directors on: any major failings identified in the internal risk-management and control systems, any significant changes made to these systems, and any major improvements planned.

Principal risks and uncertainties

The Group's financial risks include credit risk, market risk, interest-rate risk, exchange-rate risk, settlement risk, liquidity risk, counterparty risk and concentration risk. Non-financial risks include operational risk, information and communication technology (ICT) risk (including cybersecurity risk), third-party risk and compliance-related risks, such as regulatory, conduct, reputational, legal, and anti-money-laundering and counter-terrorist-financing risks. Allfunds also integrates environmental, social and governance (ESG) considerations into its broader risk-management framework.

Regarding climate and environmental risks, Allfunds' aims to minimise the direct or indirect impact of its business, thereby limiting its exposure to such risks. It is important to note that the Group does not engage in lending activities, issue financial instruments, or provide portfolio management services. Consequently, its exposure to climate-related risks-based on the classifications of the Task Force on Climate-related Financial Disclosures is considered limited. Nevertheless, the Group continues to strengthen measures to control and monitor these risks within its sphere of influence.

The Group also monitors emerging risks, whose materiality or significance may be increasing and which could, over time, justify their inclusion in the RAF if their relevance has increased or they are expected to have a material impact in the medium term.

Risk and potential impact	Mitigation	Comments for 2025
Operational risk Risk of losses resulting from deficiencies or failures of internal processes, human resources or systems, or derived from external circumstances, which can lead to increased operational losses. Operational risk is inherent to all activities, processes and systems, and can be generated by all business and support areas	• The Board of Directors annually approves Operational risk limits to monitor losses • Risk and Control Self Assessments (RCSAs) to identify relevant exposures to Operational risk • Identification, reporting and tracking of operational risk events • Dedicated resources for the integration of new businesses acquired in the previous year • Existence of insurance policies against fraud and cybersecurity • Annual Operational Risk training	• The Board of Directors has reviewed and approved the Group's operational risk limits as well as its operational risk policy • The Group has continued to expand the scope and maturity of the RCSAs, including new businesses acquired in previous years • The Group has further enhanced the RCSA methodology to integrate ICT risk, with the corresponding assessment results expected to be delivered during 2026 • Enhanced systems for operational risk management with a new GRC solution
Information and Communication Technology (ICT) risk ICT risk is defined as any reasonably identifiable circumstance related to the use of the network and information systems that, if materialized, could compromise the security of the network and information systems, any technology-dependent tool or process, operations and processes, or the provision of services, producing adverse effects in the digital or physical environment	• Existence of a Group IT Security and Cybersecurity framework • Internal and external assessments of the ICT risk framework • Existence of a Global Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) that are tested annually • Definition and Operation of the Resilience Strategy • Identification, reporting and tracking of technological risk events (TKIs) • 1LoD & 2LoD Red team exercises • 2LoD Cloud Risk assessment • Event monitoring and response (Security Operations Centre, SOC) and Cyber Intelligence services • 2LoD ICT threats oversee • Annual training on ICT Risk	• Increased testing on ICT contingency scenarios and operating resilience • Satisfactory testing of the BCP and DRP • Renewal of Security Director Plan with DORA, Zero Trust and Security Cloud Strategy • The risk control framework has been updated to support the increasing adoption of cloud computing services, IA, and to comply with the mandates of the DORA regulation regarding digital operational resilience • Corporate cybersecurity framework maturity level above the average benchmark for financial institutions • Cloud security strategic roadmap
Credit and counterparty risk (including execution and overdraft settlement risk) Credit risk quantifies the losses derived from the potential failure of customers or counterparties to meet their financial obligations, which could impact our ability to settle trades with Fund Partners and Distributors	• Ex-ante and ex-post controls to monitor trades and settlements • Ongoing monitoring of large exposures limits • Approval of credit risk limits for each counterparty and use of alarms to prevent risk limit breaches	• The Board of Directors has reviewed and approved the Group's credit risk limits as well as its credit and counterparty risk policies • No defaults from our counterparties in the history of Allfunds • Risk profile remains comfortably below risk appetite thresholds
Liquidity risk Liquidity risk is the possibility of incurring losses when there are not sufficient cash or liquid resources to comply with the obligations assumed	• Daily monitoring of short-term liquidity to ensure that all trades can be funded • Ongoing analysis of net cash flows • Regular liquidity stress testing to simulate potential defaults by Distributors or Fund Partners • Additional controls have been implemented during the year to monitor daily inflows- outflows as well as concentration risk • Existence of a liquidity risk management procedure aimed at ensuring compliance with the liquidity risk limits approved by senior management • Strict compliance with regulatory obligations in terms of liquidity management (LCR, NSFR, ALMM) under the close supervision of Bank of Spain	• Allfunds has continued to have strong liquidity levels throughout 2025. The Group's LCR and the NSFR stood comfortable above regulatory levels at 31 December 2025 • Stress test shows strong buffer to cope with severe scenarios • The Board of Directors has reviewed and approved the Group's liquidity risk policy

Risk and potential impact	Mitigation	Comments for 2025
Compliance risks Compliance risks are defined as the risks of regulatory breaches of the obligations defined by the applicable regulatory framework and the risks of breaches of ethical codes, codes of conduct and internal policies and procedures, which may result in sanctions, material or financial losses or damage to the Group's reputation	• Existence of a comprehensive, risk-based Compliance Monitoring Programme to assess the effectiveness of the controls implemented to mitigate regulatory, conduct and reputational risks as well as the risk of criminal liability, and to promote the necessary improvement actions. The results of the Compliance Monitoring Programme are reported to the management body • Advise senior management on the measures to be taken to ensure compliance with applicable laws, rules, regulations and standards • Implementation of an Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) framework	• The programme was developed in all its stages during 2025. It was updated and amended in terms of applicable regulation and organizational changes. Likewise, the controls and measures identified to mitigate the compliance risks were assessed by the departments responsible for such tasks (first line) and reviewed by Compliance. In this regard, over 2025, the programme was updated with: • In terms of regulation: mainly with the inclusion of (i) the Digital Operational Resilience Act (DORA) and its RTS and ITS; (ii) Artificial Intelligence Act; (iii) EMIR3; (iv) Instant Payment Regulation (IPR), and (v) at local level, the UK Economic Crime and Corporate Transparency Act (ECCTA). • In terms of organisational changes: Allfunds Middle East Ltd, based in Dubai Financial Service Centre and regulated by DFSA, was included in the group monitoring programme for the first time. • Allfunds compliance model was awarded in 2022 of the ISO 37301 Compliance Management Systems certification granted by AENOR. In 2025, following a full audit of the function, the certification was renewed for the period 2025-2028. This certification confirms that our model fulfils the highest industry standards
Climate-related and environmental risk Allfunds identifies the environmental aspects and impacts associated with the services provided in accordance with the organisation's environmental management system	• The Group has an environmental precautionary approach articulated through the Environmental Management System, Environmental and Climate Change Management Policy, ESG Policy and the commitment to the environment in the General Code of Conduct • ESG criteria (including environmental topics) have been established in the selection of suppliers, the onboarding of new Fund Partners and the procedure of approval of new services • Regular environmental training and awareness campaigns are conducted throughout the organisation	• Obtained Carbon footprint ISO14064 certification • Obtained Environmental Management System ISO 14001 certification at a Group level • Board approval of a revised Climate Change Management and Environment Policy, including the commitment to become Carbon Neutral in 2030, and of a Decarbonisation Plan as part of the ESG Strategic Plan that includes specific emission reduction targets • 93% of total electricity as of 31 December, 2025 came from renewable sources.

Directors' statement

In accordance with Best Practice Provision 1.4.3 of the Dutch Code, Directors are of the opinion that:

I. This report provides sufficient insights into the risks and into any failings in the effectiveness of the internal risk management and control systems with regards to strategic, operational, compliance and reporting risks

II. Systems provide reasonable assurance that the financial reporting does not contain any material inaccuracies.

III. In the same way, they provide limited assurance that the sustainability reporting does not contain any material inaccuracies.

IV. Considering the Group's risk profile and the inherent limitations associated with internal risk management and control systems, these systems provide an appropriate and reasonable level of confidence that operational and compliance risks are managed effectively and within the established risk appetite.

V. Based on the current state of affairs, it is justified that the financial reporting is prepared on a going concern basis

VI. This report states the material strategic, operational, compliance and reporting risks and the uncertainties to the extent they are relevant to the expectation of the Company's continuity for the period of twelve months after the preparation.

Strategic Report sign-off

This Strategic Report has been prepared in accordance with the UK Companies Act 2006. It was approved by the members of the Board of Directors and signed on its behalf.

Marta Oñoro
General Counsel and Company Secretary
30 March 2026