Deloitte.

Deloitte's Internal Audit Insights

THIRD EDITION

Investment firms

September 2026

Internal audit of tomorrow

The investment firm landscape is evolving rapidly. New products, automated and algorithmic trading, retail investor platforms, embedded wealth solutions, open data interfaces, and an expanding network of outsourced service providers are reshaping how firms operate. At the same time, regulatory expectations continue to increase across governance, investor protection under MiFID, conduct risk, market abuse prevention, and anti-money laundering (AML) controls.

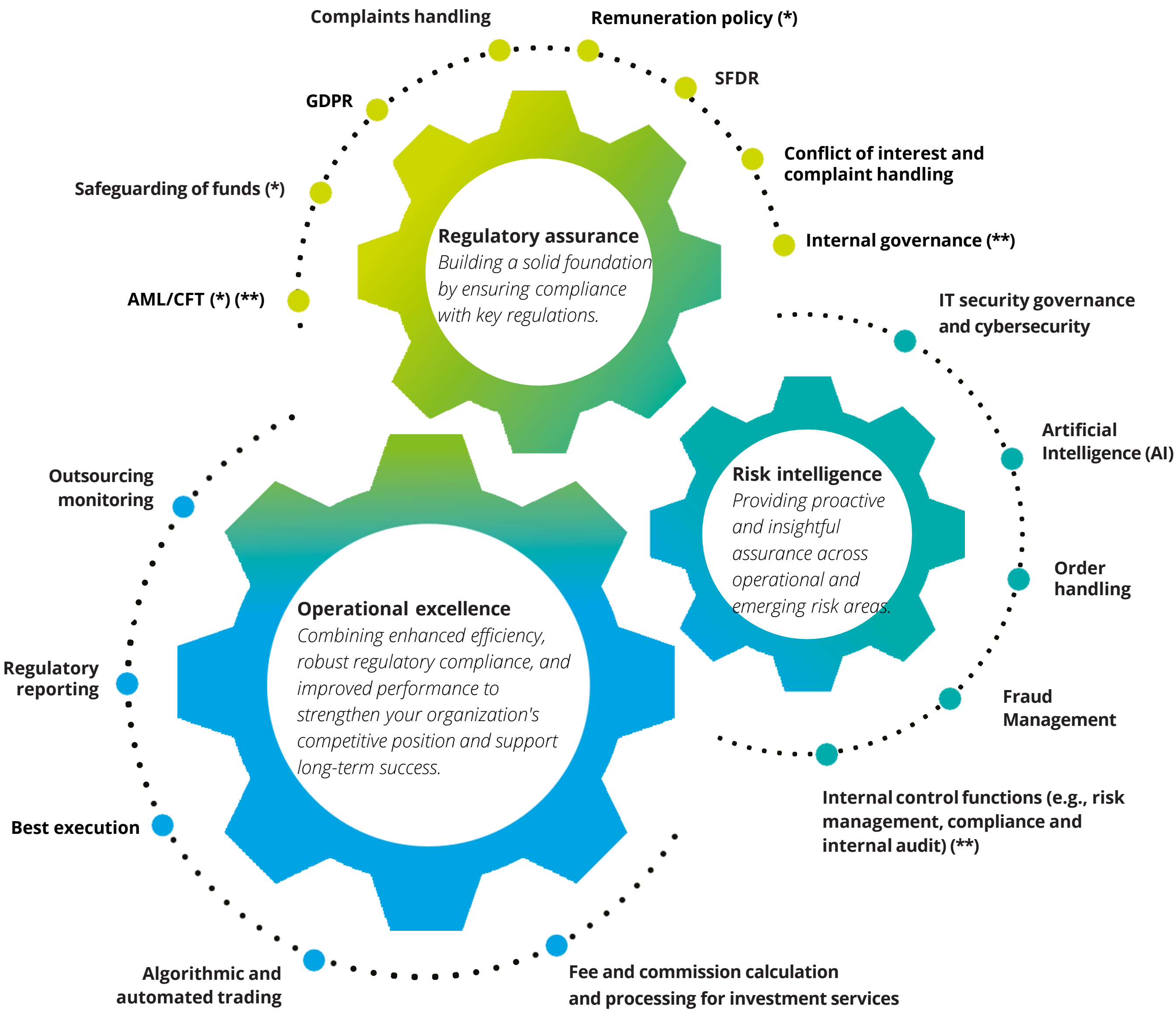
In this environment, a robust and strategically positioned Internal Audit function is a critical component of an effective control framework. By providing independent assurance, Internal Audit helps firms assess whether controls are operating effectively and risks are being managed appropriately across the value chain.

A risk-based, forward-looking internal audit plan enables firms to anticipate regulatory developments, identify control weaknesses early, and prioritise remediation efforts. Beyond supporting compliance, Internal Audit can provide valuable insights into portfolio management, trading activities, information technology, data governance, and outsourcing arrangements, helping organisations strengthen risk management, improve efficiency, and support sustainable value creation.

Internal Audit functions are also evolving. The Institute of Internal Auditors (IIA) introduced the new Global Internal Audit Standards (the “2024 Standards”), effective from January 2025. Internal Audit teams are adapting their methodologies, tools, and reporting frameworks to align with these requirements while continuing to deliver effective assurance in an increasingly data-driven and highly regulated environment.

Does your internal audit function truly address your investment firm's most significant risks?

Turning regulatory complexity into opportunity with Deloitte internal audit services



On-site inspections and thematic reviews conducted by the CSSF

In 2024, the CSSF conducted 17 on-site inspections of investment firms, focusing on AML/CTF, corporate governance and business model assessments, MiFID compliance, and IT risk management. As a result of these inspections, the CSSF imposed four administrative fines, ranging from EUR 14,000 to EUR 45,000. The sanctions were notably linked to failures to promptly notify the CSSF of changes in direct and indirect shareholding structures, non-compliance with prudential rules and professional obligations under the MiFID II framework, breaches of AML/CFT requirements, and failures to immediately report non-compliance with liquidity requirements. In addition, the CSSF issued 10 injunction letters addressing a range of regulatory and operational shortcomings. These included significant deficiencies in IT risk management arrangements, weaknesses in corporate governance frameworks, non-compliance with regulatory deadlines for the submission of 2023 year-end closing documents, and shortcomings identified through self-assessment questionnaires.

(*) Requires mandatory annual reviews (**) As per CSSF Annual Report 2024, these topics were subject to on-site inspections and thematic reviews by the CSSF

While Internal Audit focus areas should be tailored to an investment firm's strategy and risk profile, certain key topics warrant consideration across the sector. These are summarized below.

INVESTMENT FIRMS

Emerging regulatory priorities

1. DORA
Investment firms are required to establish a comprehensive ICT risk management framework, underpinned by effective governance, clearly defined roles and responsibilities, robust security and resilience measures, incident reporting, resilience testing, and appropriate oversight of ICT third-party service providers. The objective is to safeguard the continuity and resilience of critical business functions.

2. Governance
Investment firms are expected to maintain sound and effective governance arrangements, with clear organisational structures, defined responsibilities, robust decision-making processes, and effective management body oversight. Strong governance supports prudent and transparent management, effective risk oversight, and regulatory compliance.

3. Sustainability
Investment firms are expected to integrate sustainability risks into investment and advisory processes, while providing clear, accurate and consistent sustainability-related disclosures at both entity and product level. ESG-related claims should be supported by appropriate policies, reliable data, and robust governance arrangements.

4. AML/CTF & MiFID II
Investment firms are expected to maintain robust AML/CTF and MiFID II frameworks covering customer due diligence, transaction monitoring, product governance, conduct of business, suitability and appropriateness assessments, and regulatory reporting. These measures support market integrity, investor protection, and compliance with regulatory requirements.

Key regulatory areas of focus *to be reviewed on an annual basis*

- **Anti-money laundering and countering the financing of terrorism** (as per Article 44 of the CSSF Regulation 12-02, as amended)
- **Remuneration policy** (as per point 2.17 of the CSSF Circular 10/437)
- **Market abuse** (as per Article 2(5)(b) of Commission Delegated Regulation (EU) 2016/957)
- **MiFID II** (as per Article 24(c) – MiFID II Delegated Regulation (EU) 2017/565)

Contacts

Jérôme Sosnowski
Partner
Internal Audit &
Controls Assurance Leader
IIA Luxembourg Board member
Tel: +352 45145 4353
jsosnowski@deloitte.lu

Cédric Lehmann
Manager
Internal Audit & Controls Assurance
Investment Firms
Tel: +352 45145 5857
clehmann@deloitte.lu

The Internal Audit and Controls Assurance team provides a broad range of services, including Internal Audits, ISAE reports, internal control framework assessments, and agreed-upon procedures. Leveraging Deloitte's extensive experience and multidisciplinary capabilities, we deliver high-quality, value-added solutions that help organizations strengthen governance, enhance controls, and navigate an evolving regulatory landscape.