Cybersecurity – Central Bank of Ireland Expectations

On 10 March 2020, the Central Bank of Ireland ("**Central Bank**") published its findings following a thematic inspection into the cybersecurity risk management practices in investment firms and fund service providers (referred to in the letter as asset management firms). The purpose of the inspection was to determine the adequacy of cybersecurity controls and cybersecurity risk management practices of the inspected firms and to identify good practices.

According to the industry letter, the key findings of the inspection are:

- While some firms have made good progress in certain areas, many of the weaknesses highlighted in the Central Bank's 2016 Cross Industry Guidance on IT and Cybersecurity Risks were still prevalent at the time of the inspection and the Central Bank has concerns regarding the arrangements that are in place to adequately oversee all cybersecurity risks.
- Boards and senior management are not prioritising the need to embed a strong culture of cybersecurity throughout the organisation to a sufficient extent. There should be a sufficient skill set on the board to challenge and oversee the strategy. This skill set should be built upon and refreshed regularly to enable the board to understand the evolving nature of the threat and the implications for the business.
- Cybersecurity incident response and recovery plans did not meet the Central Bank's expectations, with many being in draft form, incomplete or not tested with an appropriate frequency.
- Deficiencies in information technology ("**IT**") asset inventories were identified, where the inventories did not capture the complete IT estate and / or classify assets by their business criticality.
- While all firms reported on cybersecurity risks, the quality and frequency of the reporting was variable. In general, risk indicators used were overly focused on qualitative indicators with insufficient utilisation of quantitative indicators.

The letter notes that cybersecurity is a practice that remains underdeveloped in the asset management industry and firms must give more consideration and support to identifying and managing the different threats to which they are exposed, whilst recognising that the inherent risks of IT are increasing continuously. The letter also notes that firms must focus on increasing the maturity of their cybersecurity model by driving a process of continuous improvement.

The annex to the letter sets out the key findings and the Central Bank's expectations.

- **Cybersecurity Risk Governance:** Firms should have a comprehensive, documented and board-approved IT and cybersecurity strategy, supported by sufficient resources and aligned with the overall business strategy. Firms' senior management should ensure that a well-defined and comprehensive IT and cybersecurity risk management framework is in place that provides effective oversight of IT-related risks and gives assurance to the board regarding the management of these risks within the firm.
- **Cybersecurity Risk Management:** Firms should implement, maintain and communicate an appropriate cybersecurity risk management framework that includes risk identification, assessment and monitoring, the design and implementation of risk mitigation and recovery strategies, and testing for effectiveness. Cybersecurity risk assessments should be conducted at regular intervals, at least annually, and should be comprehensive, considering internal and external sources of risk. Assessments should have appropriate parameters for evaluating and prioritising risk, such as risk likelihood and potential impact on the business operations of the firm.
- **IT Asset Inventories:** A thorough inventory of IT assets, classified by business criticality, should be established and maintained to support an effective IT Risk Management framework. A process (for example, a business impact analysis) should also be in place to regularly assess the business criticality of IT assets and assess the associated risks in a holistic manner. Configuration baselines for IT assets should be established, with divergence from the baselines identified and managed appropriately.
- **Vulnerability Management:** Exposure to vulnerabilities should be assessed on a continuous basis, on the entirety of the IT estate and include identification of external and internal vulnerabilities. Robust safeguards should be in place, including a proactive patch management process and a comprehensive configuration hardening activity, to protect against cybersecurity threats.
- **Security Event Monitoring:** Cybersecurity management activities should address the timely detection of security events and incidents, ensure comprehensive monitoring of all assets containing or processing critical data, and assess the potential impact to the business. Additionally, regular reviews should take place to assess the effectiveness of detection processes and procedures.
- **Security Incident Management:** Firms should have documented cybersecurity incident response and recovery plans in place that provide a roadmap for the actions the firm will take during and after a security incident. Incident response plans should address, inter-alia, roles and responsibilities of staff, incident detection and assessment, reporting and escalation, as well as response and recovery strategies to be deployed. Communication with relevant external stakeholders, including customers and the Central Bank, should also form a part of the response plan.

The letter should be brought to the attention of all board members and senior management before **30 April 2020**.