ESMA extends its operational-risk analysis

Developments such as the recent surges in cyber-attacks on financial firms, or technical glitches leading to flash crashes on trading venues, have heightened the sensitivity of market participants and regulators to potential disruptions in financial services providers' operations.

To identify operational risks in its remit and monitor their development and complexity, ESMA is widening its analytical framework. In its article "Operational risk assessment – the ESMA approach", published in ESMA's latest Trends, Risks, Vulnerabilities (TRV) Report No. 1, 2018, ESMA underlines the importance of operational resilience of market participants in its remit, such as Central Counterparties (CCPs), Central Securities Depositories (CSDs) or Trading Venues.

The article introduces ESMA's new systematic and comprehensive analytical approach to operational-risk monitoring in EU markets. ESMA will take a wide range of quantitative indicators into consideration, complemented by in-depth market intelligence. In doing so, ESMA focuses on three priority risk areas:

- **market misconduct**, such as market abuse, fraud, investor detriment and impairment of market data;
- **infrastructure disruptions**, such as system outages or unavailability of systems; and
- **cyber-attacks** which may lead to system outages, discontinuity in financial system operations and impaired integrity of client data.

On this basis, ESMA will cover its operational risk assessment in its semi-annual Trends, Risks, Vulnerabilities Reports, and further enhance the monitoring tools to inform our understanding of these risks and their salience.