

ESMA Brief - 2012

Regulatory Standards and Governance Arrangements in Organisations (Emphasis on ESMA and EMIR) (governance)

ESMA, under Article of EMIR, is obligated to form detailed standards about several organisational factors, among them being governance arrangements, compliance policy, information technology systems, remuneration policy, and disclosure of rules. It was suggested that these standards should not be too precise, especially about individual roles, and that stakeholders' input on governance is necessary. The appointment of a chief officer was seen as a good solution for proper governance. Accountability processes towards stakeholders should also be put in place. Concerns about conflicts of interest were addressed, and specific suggestions for the resolution of these conflicts were analyzed. It was found that current rules were generally satisfactory, and no changes were required. Certain potentially sensitive or unnecessary information, such as commercially sensitive topics, security compromises, or already-public information, could be excluded from obligatory disclosure. Other subjects discussed include the potential need for making changes in some governance models, the idea of following certain principles for data reporting and aggregation, and requirement for a detailed organizational chart. The organization's active awareness and response to significant changes in its structure or operations is also emphasized. The details of all the aspects should be outlined within the regulatory technical standards, which are to be developed by ESMA in collaboration with the ESCB. The governance arrangements proposed are intended to ensure prudent management, thus promoting stability and efficiency.

Information Technology Systems and Security Frameworks in CCP Operations (technology)

The information stipulates the need for robust information technology systems and information security frameworks in Central Counterparties (CCPs). This includes guidelines for systems development, investment strategies, and outsourcing arrangements for IT resources. There's emphasis on thorough documentation of roles, qualifications, and training of IT staff. It also highlights the need for internal controls, compliance, risk assessment, and internal audits. Additionally, robust procedures need to be in place for new technology introduction and an annual review of IT systems. The IT architecture must be well-documented, reliable, and secure. The document enforces that the CCP must appoint heads of risk, technology, compliance, and any other critical function under certain regulations. Proposals for organizational structure, remuneration policy, compliance policy and IT security are outlined too. Lastly, it mentions stakeholders' feedback offering suggestions on officer appointments and the utilization of straight through processing (STP) technology.

Balancing Confidentiality and Transparency in Reporting Back Testing Results (confidentiality)

The key concern revolves around the potential conflicts of interest and issues of confidentiality in sharing back testing results and analysis with the risk committee. There is a necessity to report these findings while also maintaining confidentiality. Thus, mechanisms need to be put in place to reconcile data effectively without violating confidentiality requirements. There is

also a suggestion for a universal trade identifier to facilitate data comparison with no breach of confidentiality. While there are concerns over data sensitivity and complexity in interpreting results, a pragmatic approach towards disclosure restrictions is being proposed to uphold commercial confidentiality. However, implementing this may be costly and complex. Such issues need to be addressed to avoid confidentiality breaches and to make data access easier for competent authorities, giving counterparties and trade repositories (TRs) additional certainty. Record-keeping that ensures data security and confidentiality and has measures for error correction and timely recovery in case of system failure is also vital. ESMA's stance is that while honoring confidentiality, a certain level of transparency is necessary, hence the decision to share aggregated data in a non-confidentiality breaching manner.

Business Model Strategy and Compliance Costs (business model)

The text discusses the implications associated with implementing new standards into existing and upcoming Central Counterparties (CCPs). The existing CCPs may face high compliance costs, needing to modify their business model and risk management framework to align with these new standards. This change may also require regulatory authorities to closely monitor the CCPs, leading to additional costs. The restrictive investment standards prescribed may limit the flexibility of CCPs in investing in financial instruments matching their liabilities, potentially leading to losses. There's also a risk that CCPs could become complacent, investing in permissible instruments under the current policy rules without assessing their suitability. Furthermore, modifying business models to comply with the standards may limit the diversity of investment portfolios and the ability to match investment durations with CCP liabilities. On the other hand, new CCPs are envisaged to face lesser costs as there would be no need to amend existing models.

Overview of ESMA's Framework and Market Conditions (environment)

The report focuses on the importance of Central Counterparties (CCPs) establishing a framework to identify market conditions that challenge their financial capabilities. Stress testing is essential in this process and should be accomplished through monthly detailed analyses. However, the review frequency may vary due to the continuously changing market environment. CCPs are warned against reducing their safety margins due to a highly competitive environment. Various commodities and their codes are listed highlighting the range of economic sectors involved.

The European Securities and Markets Authority's (ESMA) annual report discusses their objectives, the economic environment, and the achievements they've made. The report also outlines the volatility of the economic environment in relation to the securities market and the continued difficulties in the banking sector. Primary issuances by corporate firms and banks saw a strong rebound on European exchanges. However, the hedge fund and private equity industries faced a tough year due to tightened funding conditions. The report concludes with the emphasis on stringent guidelines for automated trading platforms and investment firms. The guidelines aim to prevent potential market abuse and manipulation. First-time regulation of ESMA's Credit Rating Agencies is also indicated as a highlight.

Enhancing Corporate Governance through Ensuring Accountability (accountability)

The need for establishing processes to ensure accountability to stakeholders is crucial for maintaining good corporate governance. The respondents favor the approach that includes

minimizing risk and promoting accountability. In their view, the accountability of senior management is necessary for the registration of any supervised entity. Additionally, the governance is responsible for defining the mission, independence, objectivity, scope, authority, and accountability standards of the internal audit function. Key elements of the governance include defining composition, roles, responsibilities, management structure, procedures for appointment, risk management, compliance, internal control functions, and processes for stakeholder accountability. It's suggested that the final responsibility and accountability for risk management should be taken by the board of a Central Counterparty (CCP). Furthermore, the accountability should also extend to shareholders, owners, employees, clearing members, customers, and relevant stakeholders. This accountability is expected to reflect in ESMA's annual report, demonstrating their deliverables against objectives and showcasing transparency to EU institutions and the public. Moreover, for a CCP, it is proposed to have dedicated chief risk officer, chief technology officer, chief compliance officer and heads for any other function it deems relevant for reinforcing compliance with relevant regulations and ensuring accountability.

CCPS Compliance with International Standards and Impact on Trade Repository Services (international standards)

The central concern is with the conformity of Central Counterparties (CCPs) to international standards as noted in specific regulations and directives. CCPS are expected to maintain financial and business info records in line with international standards with annual audits conducted by recognized firms. A complete set of annually prepared financial statements is also required as part of an application.

Concerns have been raised regarding divergence from international standards, inconsistency with bilateral margining, the potential for limited mutualized resources and the impact on end-users. However, most respondents prefer a minimum fixed at 95%, in conformity with international standards.

For OTC derivatives, some suggest a longer liquidation period considering the complexity of default management. Compliance with international standards is important and should also lead to international convergence and improved supervisory cooperation and information exchange.

CCPs financial statements should be made publicly available in compliance with EU legislation on auditing, helping ensure the consistency EU requirements with International standards and enabling Trade Repository Services to operate globally.

Organizational Structure, Governance, and Compliance in Financial Institutions (internal controls)

The summary details the importance of a defined organizational structure, robust accounting, safekeeping procedures, and internal controls within financial organizations like a Central Counterparties (CCP) and trade repositories. It emphasizes the requirement for these entities to operate under low credit risk, based on stable and objective internal or external risk assessments. Essentially, the security and ease of access to held assets, particularly gold and other financial instruments, are a pivotal concern. The document further expounds on adhering to local and international regulatory guidelines, particularly for entities operating in different countries.

A section is dedicated to the provisions needed when applying for the registration of a trade repository. It highlights the necessity of providing comprehensive details about the staff employed – their roles, qualifications, and specific training related to the trade repository

business they handle. The internal structure of controls, independence of its governing bodies, and the aptitude of the staff is deemed crucial in the application process. Moreover, the obligations associated with the segregation and safekeeping of assets are highlighted, and necessary arrangements for safeguarding member's or client's ownership rights are detailed.

Establishment and Role of ESMA's Financial Innovation Standing Committee (innovation)

Despite the potential risks that standardization might impede innovation, a key development has emerged with the creation of the ESMA's Financial Innovation Standing Committee (FISC) headed by Anneli Tuominen. The FISC's primary task is to identify risks to investor protection and financial stability in the realm of financial innovation and to devise risk mitigation strategies. Through data analysis, they respond and adapt to issues as they arise. The committee is part of the Joint Committee of European Supervisory Authorities, contributing to work on financial activities and consumer/investor-related issues. Other subcommittees handle issues relating to cross sector developments, anti money laundering, and consumer protection specifically at a cross sector level and in the sphere of financial literacy and education. The aim of these committees is coordinated regulation and supervision of novel financial activities, and to identify and tackle potential market risks and vulnerabilities.

Governance, Risk Management, and Regulatory Compliance in Financial Sector (fraud)

The material explores key requirements for the competent authority within the group of a Central Counterparty (CCP). It outlines various reporting obligations, including significant changes in structure, ownership, and capital level, alterations in organizational routes that could impact risk management, details about regulatory authorities, threats to compliance, possible spill-over effects, and potential risk of contagion. Performance issues, member default events, sanctions, and potential changes about stress testing, risk models, and new commercial proposals are also included. In terms of senior management and board members, information required includes curriculum vitae for assessing their capability and any criminal convictions. A declaration stating any disciplinary or criminal history, involvement in insolvencies, compliance issues, regulatory investigations, disqualifications for misconduct or malpractice are necessary. The outcome also delves into the implication of criminal sanctions for violations related to insider dealing and market manipulation, particularly those involving fraudulent activities with the intent of illicit profit, affecting market integrity.

Disclaimer: The content herein was sourced from the European Securities and Market Authority (ESMA) at <https://www.esma.europa.eu> and summarized by ChatGPT. ChatGPT is known to generate inaccurate information. Always refer to ESMA's original documents for complete and accurate information.