

Market Abuse Risk Domain

Fact Sheet

WHAT IS MARKET ABUSE?

Market abuse refers to a range of unethical and illegal activities that can undermine the integrity of financial markets. These activities typically involve manipulative or deceptive practices intended to distort market prices, mislead other market participants, or unfairly exploit non-public information for personal or financial gain. Market abuse undermines the fairness and efficiency of financial markets, and it is targeted by regulatory authorities through a combination of surveillance, enforcement, and penalties to maintain market integrity.

What are the key components of a Market Abuse Risk Assessment?

Environmental Risks

Evaluate the vulnerability to market abuse based on the organisations external and internal operating environment.

Customer Risks

Evaluating the profiles and behaviours of customers to identify those who may pose higher risks of engaging in market abuse, such as high-frequency traders, insider employees, or customers with histories of regulatory issues.

Product and Service Risks

Analyzing the financial products and services offered by the institution to identify those that may be more susceptible to market abuse, such as complex derivatives, low-liquidity stocks, or high-leverage instruments.

Channel Risks

Reviewing the trading platforms and communication channels used by the institution to identify potential vulnerabilities, such as dark pools, electronic trading systems, or unmonitored messaging apps.

Transaction Risks

Identifying specific trading behaviours or patterns that could indicate market abuse, such as large, unusual trades, large trades executed before significant market announcements, or repeated patterns of order cancellations.

Country Risks

Evaluating risks associated with operating in different regulatory environments, especially in jurisdictions with weak regulatory oversight or lack of enforcement or transparency.

Evaluation of Controls

Policies and Procedures

Assessing the effectiveness of existing policies, procedures, and systems designed to prevent and detect market abuse. This includes surveillance systems, trade monitoring, and compliance programs.

Training and Awareness

Evaluating the adequacy of training programs that educate employees, traders, and other relevant parties on the risks and indicators of market abuse, as well as the consequences of engaging in such activities.

Surveillance Systems

Implementing or enhancing monitoring systems to detect suspicious trading activities in real-time.

Reporting Mechanisms

Reviewing the channels available for employees and stakeholders to report suspicious activities, such as whistleblower programs or internal reporting systems.

Risk Scoring and Prioritisation

Regulatory Compliance

Ensuring that the institution is fully compliant with relevant laws and regulations designed to prevent market abuse, and that there are processes in place to monitor regulatory changes.

Risk Scoring

Assigning risk scores to identified risk factors based on their likelihood of occurrence and potential impact. This helps prioritise the risks that need more immediate attention.

Gap Analysis

Identifying gaps in current controls or processes that may leave the institution vulnerable to market abuse and determining the urgency of addressing these gaps.

Mitigation Strategies

Enhanced Surveillance

Implementing or upgrading surveillance systems to monitor trading activities more effectively, including real-time analysis of trades and automated alerts for suspicious patterns.

Policy and Procedure Updates

Revising or introducing new policies and procedures to address identified risks, such as stricter controls over high-risk products or enhanced due diligence on certain customer segments.

Strengthening Reporting and Communication

Enhancing internal and external communication channels to ensure timely and effective reporting of suspicious activities.

Regular Audits and Reviews

Conducting regular audits and risk assessments to ensure ongoing compliance and effectiveness of controls, and to adapt to new or emerging risks.

Ongoing Monitoring and Review

Continuous Monitoring

Establishing processes for continuous monitoring of trading activities and updating risk assessments as new risks emerge or as the regulatory environment evolves.

Periodic Reviews of Incidents

Analysing incidents of suspected or actual market abuse to learn from them and improve controls.

Feedback Loops

Creating mechanisms for regular feedback and updates on the risk assessment process to ensure it remains current and effective.

What are the steps to conducting a Market Abuse Risk Assessment?

Step 1 - Develop an understanding of the Regulatory Framework

Organisations must ensure a thorough understanding of applicable laws, regulations, and guidelines related to market abuse in the jurisdictions where the organisation operates. This includes knowing the specific types of market abuse (e.g., insider trading, market manipulation) prohibited by law and aligning the market abuse risk assessment process with the expectations of the relevant regulatory bodies.

Step 2 - Establish Governance and Accountability

Organisations must ensure that senior management is actively involved in the market abuse risk assessment process, providing oversight and support. It is also important to have clearly defined roles and responsibilities of individuals or teams involved in conducting the market abuse risk assessment, including the compliance, risk management, and internal audit functions etc..

Step 3 - Define the Scope and Objectives

Organisations must clearly define the scope of the market abuse risk assessment, including which markets, products, services, and business units will be covered, as well as, set specific objectives for the market abuse risk assessment, such as identifying potential market abuse risks, evaluating the effectiveness of existing controls, and determining areas for improvement.

Step 4 - Identify and Assess Risks

Organisations must identify potential risk factors for market abuse across various risk groups, including environmental, customer, product and service, channels, transactions, and jurisdictional factors. Once the risk factors have been identified, organisations must assess their likelihood and potential impact on the institution or market, which may involve examining historical data, market trends, and known incidents of market abuse.

Step 5 - Implement Operating Controls to Mitigate and Manage Risks

Organisations must implement operating controls including (but not limited to), implementing surveillance and continuous monitoring systems, employee training and awareness programs, developing internal and external reporting mechanisms, ongoing reviews and updates, as well as, independent audits to validate the effectiveness of the market abuse risk assessment process.

Step 6 - Evaluate the Design and Operational Effectiveness of the Control Environment

Organisations must evaluate the design and operational effectiveness of controls such as systems, policies and procedures to detect and prevent market abuse; identify any gaps or areas for improvement and develop an action plan to enhance controls.

Step 7 - Assess the alignment of Residual Risks to the Risk Appetite and Risk

Organisations must assess the residual risks after the implementation of mitigating controls to determine whether this aligns to the Risk Appetite Statement defined by the Board or whether the residual risk falls outside of the risk tolerance levels, and if so document the recommended actions to bring back into alignment.

Step 8 - Escalation and reporting of identified market abuse risks and incidents to relevant stakeholders

Organisations must define clear processes for escalating market abuse risks and incidents to the Board and ensure timely and accurate reporting of these to regulatory authorities, as required by law.

About Arctic Intelligence


Arctic Intelligence (www.arctic-intelligence.com) is a multi-award winning, RegTech firm that specialises in audit, risk and compliance software related to financial crime compliance and risk management. Arctic Intelligence has helped hundreds of large and small clients across over 20 industry sectors and 20 countries and has also developed strong industry partnerships around the world.

Arctic has developed two leading cloud-based software solutions that leverage technology to re-engineer the way in which major financial institutions and other regulated businesses manage their enterprise-wide financial crime and non-financial crime risks.

[VISIT OUR WEBSITE](#)

[BOOK A DEMO TODAY](#)

APAC

 Arctic Intelligence Head Office
Level 4, 11-17 York Street,
Sydney, NSW 2000, Australia

 **Call us on your local number:**
Australia +61 (0) 2 8001 6433
Hong Kong +852 (0) 8197 4022
New Zealand +64 (0) 9889 3324
Singapore +65 6817 8650

EMEA

 United Kingdom +44 20 8157 0122

AMERICAS

 USA +1 646 475 3718
Canada +1 613 5188002

 support@arctic-intelligence.com



Compliance. The smart way.