ARCTIC INTELLIGENCE

Compliance. The smart way.

Fraud Risk Domain

Fact Sheet

WHAT IS FRAUD?

Fraud is a deliberate act of deception, typically carried out for financial gain or to secure some unfair or unlawful advantage. It involves intentionally misrepresenting facts, information, or intentions to deceive others. Fraud can take various forms and occur in different contexts, including financial transactions, business operations, personal interactions, and more.

CONDUCTING A FRAUD RISK ASSESSMENT IN

12 STEPS

STEP 01

Establish Objectives: Define the goals of the assessment, such as identifying potential fraud risks, evaluating their impact, and implementing preventive measures.

STEP 02

Assemble a Team: Form a multidisciplinary team that includes representatives from various departments, such as finance, operations, legal, and compliance.

STEP 03

Identify Assets and Processes: List all the assets, processes, and areas of your organisation that could be susceptible to fraud, including financial transactions, data handling, and employee activities.

STEP 04

Identify Potential Risks: Brainstorm potential fraud risks associated with each asset or process. Consider scenarios where fraud could occur, such as unauthorised access to financial systems or manipulation of records.

STEP 05

Assess Impact and Likelihood: Evaluate the impact and likelihood of each identified fraud risk. This helps prioritise risks and focus efforts on the most significant threats.

STEP 06

Implement Controls: Develop and implement controls to mitigate identified risks. These controls could include segregation of duties, access controls, monitoring systems, and whistleblower mechanisms.

STEP 07

Document Policies and Procedures: Create clear policies and procedures that outline how to prevent and respond to fraud. Ensure employees are aware of these policies and understand their roles.

STEP 08

Training and Awareness: Provide training to employees about fraud risks, prevention measures, and how to report suspicious activities. Raise awareness about the importance of ethical behaviour.

STEP 09

Monitor and Review: Continuously monitor the effectiveness of the implemented controls. Regularly review and update the assessment to account for changes in processes, technologies, or external factors.

STEP 10

Response Plan: Develop a response plan that outlines the steps to take if fraud is detected. This includes conducting investigations, involving legal authorities if necessary, and communicating with stakeholders.

STEP 11

Engage Internal and External Auditors: Involve internal and external auditors to review the assessment process and provide an objective evaluation of your organisation's fraud risk management.

STEP 12

Ongoing Improvement: Use the insights gained from the assessment to refine your fraud prevention strategies over time. Adapt to new risks and challenges that may emerge.

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
New Zealand +64 (0) 9889 9825
Singapore +65 6817 8650

EMEA

United Kingdom +44 20 8157 0122

AMERICAS

USA +1 917 730 4484
Canada +1 613 518 8002

GLOBAL

support@arctic-intelligence.com

ARCTIC INTELLIGENCE

Compliance. The smart way.