# Financial Crimes Compliance Governance and Controls

All financial services companies or financial institutions (FIs) are required to have financial crime compliance ("FCC") governance and controls in place to manage financial crime risks. These typically include (dependent on local jurisdictional regulatory requirements): money laundering, terrorist financing, sanctions, bribery and corruption and fraud. These controls should be commensurate with the institution's risk profile and should take into account the institution's geographical footprint, customer base, regulatory requirements, products & services, size, capacity and structure.

This section covers the key elements of an FCC Governance and Control framework. Further information on designing and implementing controls around specific financial crime risks can be found in the Business Integrity section.

- What does financial crime compliance governance and controls cover:
  In this section and throughout the BII Toolkit for FIs financial crime compliance (FCC) governance and controls cover:
  - Anti-money laundering and counter-financing terrorism policies and procedures
  - Anti-bribery and corruption policies and procedures
  - Whistleblowing policies and procedures
  - Sanctions
  - Fraud & Tax Evasion
  - Market Abuse and Cyber Security

  The content developed, draws upon several resources that provide guidance on best practice in financial crime compliance. Please see the Resources Section.

The key elements of a robust financial crime compliance programme include the following:

- **Good governance and financial crime controls:** Robust management and oversight

of financial crime risks is directly linked to a strong tone from the top of an institution and robust governance structures to oversee an FCC programme. The board of directors and senior management have the responsibility to ensure that a firm's policies, controls and procedures are appropriately designed, implemented and communicated throughout the firm. An external statement on how the organisation is managing financial crime risks is also recommended e.g. in its Annual Report.

- **Roles, responsibilities and oversight:** The Board of Directors should also approve the appointment by senior management of an appropriately qualified Money Laundering Reporting Officer ("MLRO") or Compliance Officer to take responsibility for FCC matters. FIs should implement a three lines of defence model in their risk management organisational structure. The ownership of financial crime risks sits with the business as the first line of defence. The various risk and compliance functions established by management are the second line of defence – these are responsible for oversight of first line management of risks, undertaking controls testing and setting organisation-wide policies and assisting in the delivery of training. The third line of defence undertakes independent assurance of first and second line activities and is usually carried out by the internal audit function.

- **The Risk-based approach:** Management of financial crime risks should be proportionate and cost-effective, taking into account the risk profile and exposure for the institution to financial crime risks in its operations with most resources dedicated to the highest risks. FIs should perform a financial crime risk assessment to identify areas of heightened financial crime risks associated with their customers, operations and products/services, including money laundering, terrorist financing and bribery and corruption risks.

- **Policies & procedures:** The Board of Directors should oversee and approve all FCC risk assessment and management policies and procedures. The FI should formulate robust and fit-for-purpose policies and procedures based on financial crime risk assessments to ensure that these are proportionate and in-line with the institution's identified risks. To ensure continuous improvement, a process should be implemented to ensure regular (e.g.) annual review and updates to policies with senior level approval of changes.

- **Review and assurance:** As part of the three lines of defence model, an FI should appoint an independent audit function to oversee the review and assurance of the FCC compliance programme. This function should conduct timely review and testing of

various FCC policies and procedures to assess applicability and test for compliance. It is also recommended that an FI conducts periodic reviews by an external agency to provide an independent view on the effectiveness of the FCC programme and continues to improve controls.

- **Training:** All staff should be regularly trained (e.g. annually) on key financial crime risks, for example AML/CFT, KYC, bribery & corruption and sanctions. Targeted and more in-depth financial crime training should be given to staff involved in financial crime risk management across all 3 lines of defence. Consideration should be given to how detailed the training needs to be for different teams and how it should be delivered. The use of case studies to demonstrate how financial crime risks are managed is recommended. Records should be maintained on financial crime training delivered including completion rates. Where training is mandatory it should be clear that failing to complete the training may result in disciplinary action.