- Governance structures
  FIs should implement a governance structure that is commensurate to the size and nature of their business. An effective governance structure should include the following:
    - Allocate responsibilities for financial crime risks management across the 3 lines of defence ensuring accountability at a senior level and sufficient resourcing commensurate to managing the identified risks.
    - Establish financial crime and/or reputational risk committees to approve risk appetite and policies, discuss high-risk / challenging cases and review effectiveness of compliance controls and management information. Clear reporting lines and escalation channels for financial crime risks to be discussed/approved should also be established.
    - Identify and manage conflicts of interest, in particular where staff hold several functions cumulatively, and
    - Assess and record key decisions and observations relating to the management of money laundering, terrorist financing, bribery & corruption and sanctions risks.

- Three Lines of Defence

  The three lines of defence model refers to a comprehensive framework designed for the overall management of risks within an organisation. The model includes the following features:

    - Governing bodies and senior management: The board and senior management ultimately hold collective responsibility for establishing the necessary risk governance and control framework for the FI. They direct the management and three lines of defence in managing and reporting adherence to risk management principles.
    - First line (business): The primary responsibility for owning and managing organisational risks (including FCC risks) is the business who directly interact with customers. They are responsible for designing and implementing appropriate mitigating controls including assessment, escalation, approval and

reporting of risks, alongside employee training.

- Second line (Risk functions): Risk management and compliance functions are responsible for setting institution-wide policies and risk appetite, staff-wide training and oversight of first line activity and compliance with regulations and internal policies & risk appetite. Second line functions may also approve high risk customers, products and transactions.

- Third line (Internal Audit): Providing risk assurance on the effectiveness of the governance, risk management and internal controls; including first- and second-line controls.

- Tone from the top & effective risk management culture
  Implementation of FCC controls are only effective in an organisation where senior management set and enforce a clear level of risk appetite and embed a culture of compliance where identification and management of financial crime risks is critical and breaches of regulations and internal policy is not tolerated. Examples of good practice include the following:
  - Senior management, including the board, take leadership on financial crime issues ensuring clear accountabilities, communication and effective oversight of FCC risks;

  - Establishing a public statement on the institution's website outlining how FCC risks are managed including relevant FCC policies e.g. AML/CFT and AB&C policies/Code of Conduct.

  - Clearly articulating and enforcing the FI's FCC risk appetite aligned to relevant financial crime laws and international guidance, including not entering into business relationships where the institution is unable to manage the risk effectively;

  - Allocating sufficient resource to mitigate financial crime risks across the three lines of defence;

  - Ensuring that a strong risk culture is embedded to promote effective identification, challenge, escalation and reporting of financial crime issues to

enable it to comply with all relevant regulatory requirements and its own risk appetite and standards.

- Risk appetite
  Risk appetite is the level of risk that an organisation is prepared to accept in pursuit of its objectives. Following a financial crime risk assessment, an FI should establish risk-based principles or guardrails to assist in assessing whether financial crime risks associated with its operations (customers, transactions, products & services) are inside or outside risk appetite or require escalation for further determination. The risk appetite should always take account of local and international financial crime regulations and good practice guidance. See the Business Integrity section for further information on financial crime risk assessments.

- Management information (MI) and reporting
  Good MI provides senior management and the board with the information to determine if the FI is effectively managing financial crime risks to which it is exposed including meeting its regulatory obligations. Reporting to both senior management and the board on financial crime risks should be provided regularly e.g. quarterly. Examples of useful MI for decision making around financial crime risks include the following:
  - An overview of the financial crime risks to which the entity is exposed, including information about emerging threats or changes in an entity's risk appetite;
  - An overview of systems and controls to mitigate risks, including information about the effectiveness of controls in place and any relevant changes to risk management principles;
  - Legal and regulatory developments and the impact these have on the FIs approach;
  - Relevant information about business relationships; including information around high -risk customers and transactions, relationships that have been exited as a result of financial crime-related issues, findings of any regulatory visits and number of law enforcement enquiries, financial crime training delivered and the number of alerts for suspicious activity reports (SARs) and suspicious transaction

reports (STRs) that have been filed or investigated.

Reporting to the board on financial crime-related information should be provided at a suitable committee; for example, a Group/Board Risk and Audit committee. It is also important that the chair or members of this committee (at least one member) has relevant financial crime risk management experience to advise on the information reported and provide relevant action/guidance.