

Once an FI has conducted a risk assessment, the entity should establish risk-based proportionate policies, processes & controls and identify resources to assess and manage financial crime risks in line with local, national and applicable regulations and best practice. The firm's risk assessment must be documented and kept up to date. The policies should also be updated regularly (e.g. annually) to take into account any changes in regulation, local law or changes in the firm's risk profile, owing to changes in customer base, product or jurisdiction.

As best practice, all policies should be subject to review and control testing including regular risk & control assessments (e.g. annually) to determine whether they have identified all the inherent risks to be managed, there are relevant processes and controls in place to manage and mitigate the identified risks and residual risks are manageable in line with the FIs risk appetite. Such risk reviews should be recorded. Peer benchmarking can also be used to assess whether an FIs policies are fit-for-purpose.

See BI section for further detail policies and procedures relating to AML/CFT risks, bribery and corruption, fraud, tax evasion and sanctions.