



Results of First Round Examinations, 2011

Themed Examination Programme, 2011

Summary of Findings

Commission's response

Presenters:
Richard Hands & Tina Bryan-Bannister

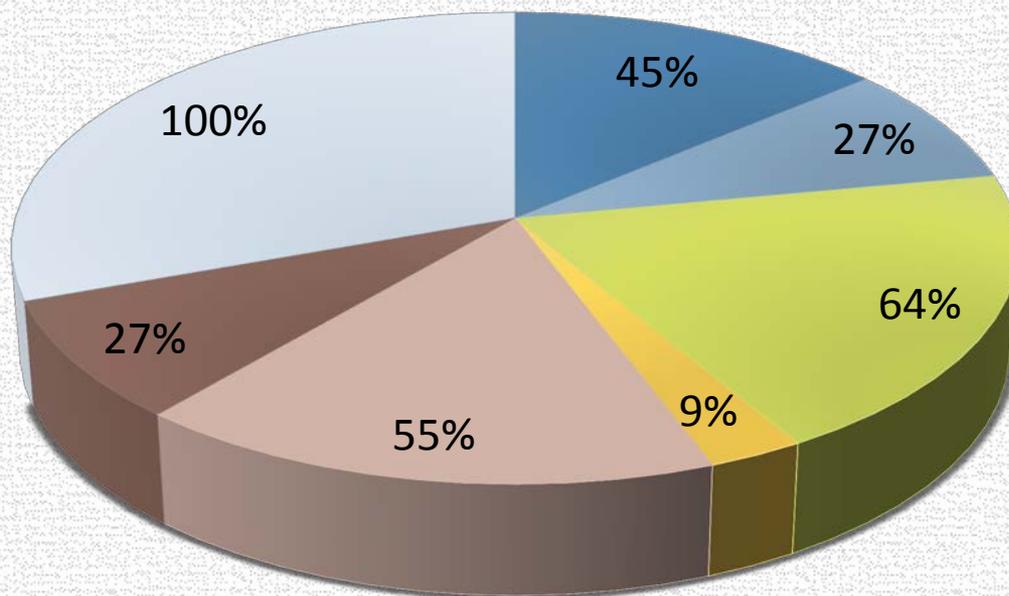
Overview

- Compliance with AML/CFT Legislation, 2011
- Major areas requiring improvement
- Risk Assessment
- Customer Due Diligence
- Placing Reliance on third parties
- Impact of the “objective test”
- Higher Risk jurisdictions
- Other vulnerabilities



Compliance with AML/CFT Legislation, 2011

Pie Chart showing Compliance with AML/CFT Legislation

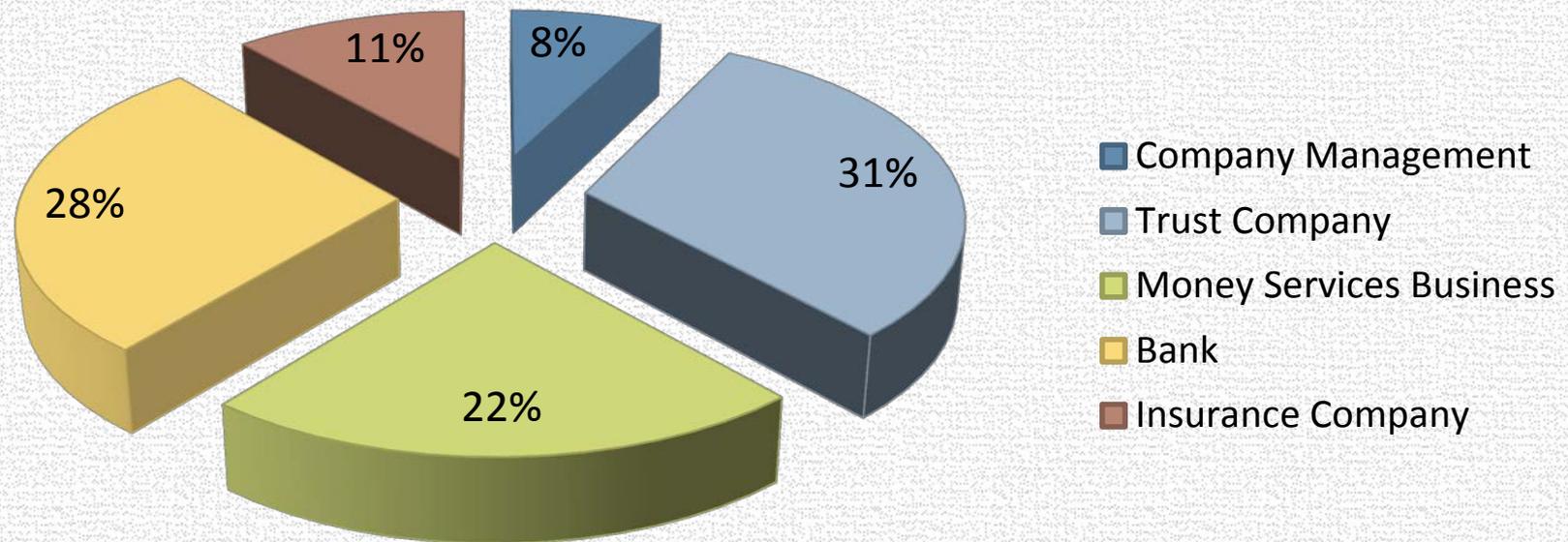


- General AML/CFT Policies and Procedures
- Risk Assessment Profile and Risk Based Approach
- Customer Due Diligence / Know Your Customer
- MLRO / MLCO (approved)
- Training and Staff Awareness
- Suspicious Activity Reports (SARs)
- Record Keeping



Compliance with AML/CFT Legislation, 2011

Pie Chart showing Average Compliance with AML/CFT Legislation per Sector



Major areas requiring improvement

- Some service providers failed to document AML/CFT policies and procedures.
- A minority of service providers had completed a risk assessment and implemented a risk based approach in relation to customers, products and services and geographical location.
- Although AML/CFT training may have been provided, a number of relevant staff did not have adequate knowledge of the AML/CFT framework.
- Low level of suspicious activity reporting.



Risk Assessment

Section 3(1) of the AML/CFT Code, 2009

A service provider shall carry out and document a risk assessment for the purpose of:

- a. Assessing the money laundering and terrorist financing risks that it faces;
- b. Determining how to best manage those risks; and
- c. Designing, establishing, maintaining and implementing AML/CFT policies, systems and controls that comply with the requirements of the AML/CFT Regulations and Code.



Risk Assessment

Section 3(2) of the AML/CFT Code, 2009

The risk assessment carried out should take account of –

- a. The service provider's organisational structure;
- b. Customers;
- c. Countries with which its customers are connected;
- d. Products and services; and
- e. How those products and services are delivered.



Risk Assessment

The assessment should consider –

- The risk appetite of the financial services business itself;
- The need for clear distinction between the assessment of risk level and the impact of mitigation measures; and
- The potential features of financial services business in Anguilla that should properly be assessed as “higher” risk: for example, non “face to face” business, reliance on third party introducers, private banking, international business companies, customer insistence on excessive secrecy, overly complex ownership structures.



Customer Due Diligence

- Two phases to customer due diligence are to gather the facts and to make a commonsense assessment to determine the risk.
- Enhanced due diligence should be conducted on higher risk customers including Politically Exposed Person (“PEPs”), and those using higher risk products and services.
- The source of funds and source of wealth information should be obtained.



Placing Reliance on third parties

- The legislative framework allows service providers to place reliance on third parties for elements of due diligence.
- Where a service provider relies on an introducer or intermediary to apply customer due diligence measures, the service provider remains liable for failure to apply those measures.



Impact of the “objective test”

- Sections 128 and 129 of the POCA require a person to disclose knowledge or suspicion of money laundering to the authorities where he or she “*knows or suspects, or **has reasonable grounds for suspecting**, that another person is engaged in money laundering.*”
- A person can be guilty of an offence by not disclosing information where an ordinary person (with relevant experience in financial services) would consider sufficient grounds for disclosure existed.
- Limited opportunities are offered to employees in financial services to have a “reasonable excuse” for not disclosing.



Higher Risk jurisdictions

- Complex use of complex structures to conceal true ownership;
- Informal corporate control structures;
- Importance of political patronage links in securing corporate ownership or valuable franchises;
- Endemic corruption, evidenced for example in Transparency International's Corruption Perception Index and other publically available resources;
- Emphasis on form over substance in the legal, accounting and regulatory environments;
- Limited depth of the financial system; and
- Significant physical risk in the business conflict resolution.



Other vulnerabilities

- Anguilla may be targeted by unregulated investment and forex broking and dealing.
- The activities may be linked to insider dealing in securities, “penny share” schemes such as “pump and dump” and boiler room scams.
- Asset protection may conceal attempts to protect the proceeds of crime, especially fraud, or assist in fraudulent preference.



Final Assessment of the 2011 Onsite Examination

- Level of compliance with the POCA, the Regulations and the Code was disappointing and worrying.
- The Code specifies minimum standards with which all service providers must comply.
- Anguilla, as a jurisdiction, and its service providers have been given a commitment to meet accepted standards in the international efforts to combat money laundering and the financing of terrorism.



Reputation of Jurisdiction

“Do you think that Anguilla has a good reputation?”

