Asia/Pacific Group
on Money Laundering

Mutual Evaluation Workshop

For APG Assessors

And

Members of the APG Donors and Providers Group

Background Material and Exercises

Hosted by US Treasury

Washington DC

11-13 December 2013

WORKBOOK FOR PARTICIPANTS

Contents **Page**

AGENDA

APG Mutual Evaluation Workshop

Hosted by US Treasury

Washington DC

11-13 December 2013

WEDNESDAY 11 December 2013	
0800 – 0845	**Registration and Security** Those delegates who are joining the workshop on Wednesday 11 December for the first time are asked to attend from 8am to go through security processes
0845 – 0900	**Welcome, Introductions and Overview**
0900 – 0930	**Topic 1: Overview of the Evaluation Process and implications for DAP** Purpose and objectives of assessment/TC and effectiveness/overview of the major steps in the process/ broad timeline
0930 – 1030	**Topic 2: Risk and Context and implications for DAP** Risk is the starting point, and involved in all stages of the assessment – an assessed jurisdiction needs to set out its understanding of the risks to assessors – and to demonstrate how an understanding of risk and context underpins priority implementation of AML/CFT measures.
1030 – 1045	**Morning Tea**
1045 – 1230	**Topic 3 and Practical Exercise: Assessing Technical Compliance and implications for DAP** Exercise: Discussions of exercise outcomes on TC Presentation (30 minutes)- Explanation of the TC methodology using one FATF Recommendations and comment on TC exercise
1230 – 1330	**Lunch**
1330 – 1530	**Topic 4: Assessing Effectiveness and implications for DAP** Explanation of the effectiveness methodology using a number of immediate outcomes
1530 – 1545	**Afternoon Tea**
1545 – 1645	**Topic 5: Information – Data and Statistics**
1645 -1730	**Exercise 1: Discussing and Determining Team's Approach to Risk, TC and Effectiveness** - Including who will take the lead in asking questions in each mock interview, who will hold the pen for each immediate outcome
1730 Onwards	**Exercise 1:** ***Finalising above***

THURSDAY 12 December 2013		
08:45 – 9.30	**Topic 6: Preparing a country for Mutual Evaluations**	
9.30 – 10:45	**Topic 7: Finalising the MER and Mutual Evaluation**	
10:45 – 11:00	**Morning Tea**	
11:00 – 12:30	**Mock Evaluation:** Introduction of the Practical Scenario and mock assessor interview for practical exercise.	
12:30 – 13:30	**Lunch**	
13:30 – 15:00	**Mock Evaluation :** Mock assessor interview for practical exercise.	
15:00 – 15:30	**Afternoon Tea**	
15:30 onwards	**Mock Evaluation:** Team Discussion & drafting Determination of risk and context, analysis of criteria, core issues, considering of ratings and preparing prioritised recommendations	
FRIDAY 13 December 2013		
08.40 -10.30	**Mock Evaluation:** Team Discussion & finalising Determination of risk and context, analysis of criteria, core issues, considering of ratings and preparing prioritised recommendations	
10.30 – 11:00	**Morning Tea**	
11:00 – 12:00 pm.	**Mock Evaluation:** Finalising Reports	
12:00 – 13.30	**Lunch**	
13.30 – 15:00	**Mock Evaluation: Presenting findings and feedback from presenters** Each team makes a presentation of its key findings with questions, discussion and Presenters provide Observations for assessors and for DAP preparing a country for an ME	
15:00 – 15:30	**Afternoon Tea**	
15:30 – 16:45	**Clarification / expanding of any issues covered during the workshop**	
16:45 – 17.00	**Concluding Remarks**	

Questionnaire on Technical Compliance Update as provided to jurisdictions

Early in the Mutual evaluation process the country to be assessed is provided with the following Questionnaire on Technical Compliance to provide Updated information for the assessment team.

Background and Key documents

Countries should briefly note any significant changes to their AML/CFT system which have taken place since the last evaluation or since they exited the follow-up process. This includes:

- New AML/CFT laws, regulations and enforceable means.
- New competent authorities, or significant reallocation of responsibility between competent authorities.

Countries should list the principal laws and regulations in their AML/CFT system, and give a brief, high-level summary of their scope. The (translated) text of these laws should be provided to assessors. It is preferable to assign each document a unique number to ensure references are consistent. These numbers should be listed here.

Countries should list the main competent authorities responsible for AML/CFT policy and operations, and summarise their specific AML/CFT responsibilities.

1. [Example –"Since the last evaluation, Country X has passed the 'Law on Suspicious Transaction Reporting (2009)' and established an FIU. Responsibility for investigating suspicious transactions has been transferred from the Ministry of Interior to the FIU.

2. [Example –"The principal laws relevant to AML/CFT are:

- *Money Laundering Act (1963) (document L1) – establishes a criminal offence of money laundering*
- *Proceeds of Crime Act (2007) (document L2) – sets a legal framework for confiscation of the proceeds of crime*
- *National Security Act (2005) (document L3) – establishes a criminal offence of terrorist financing and a legal framework for implementing targeted financial sanctions*
- *Financial Sector Act (1999) (document L4) – provides the legal basis for financial sector regulation and supervision and sets out the basic AML/CFT obligations on firms. ...*

Risk and Context

Countries should provide assessors with available documents about the ML/TF risks in their country. They should list each document they provide, and briefly describe their scope. Countries should also note any important considerations about risk and context which they wish to bring to the attention of assessors. This should not duplicate information included in the documents provided. If countries wish to highlight specific contextual factors, they should provide documentation on these.

Countries should describe the size and structure of their financial and DNFBP sectors, using the tables in Annex I

Technical Compliance Information

Countries should provide information on their technical compliance with each of the Criteria used in the FATF Methodology.

For each criterion, countries should, as a minimum, set out the reference (name of instrument, article or section number) that applies.. Countries should refer to the *specific clauses* of their laws, enforceable means, or other mechanisms which are relevant to the criterion. *If necessary* countries should also *briefly* explain the elements of their laws, enforceable means, or other mechanisms which implement the criterion, (e.g. an outline of the procedures followed, or an explanation of the interaction between two laws). Countries should also note whether the law or enforceable means referred to has changed since the last MER or follow-up report.

The (translated) text of all relevant laws, enforceable means, and other documents should be provided separately (but as early as possible).

Countries should provide brief factual information only – there is no need for lengthy argument or interpretation. There is no need to set out each criterion in full. Information could be provided in the following form:

Recommendation 1

Criterion 1.1

1. [Example – "Country X has conducted separate risk assessments on Money Laundering (attached as document R1) and on Terrorist Financing (edited public version attached as document R2). These risk assessments are both used as the basis for the National Strategic Plan on AML/CFT (attached as document R3) which brings together both ML and TF risks."]

Criterion 1.2

2. [Example – "The Minister of Finance has overall responsibility for AML/CFT. The National Strategic Plan on AML/CFT (document R3) assigns responsibility for ML risk assessment to the National Police Authority (page 54), and for TF risk assessment to the Interior Ministry (page 55). Actions are coordinated through the National AML/CFT Coordinating Committee (terms of reference on page 52)."]

Criterion 1.3

3. [Example – "Both ML and TF risk assessments are required to be updated on an annual basis (document R3, pages 54, 55)"]

Criterion 1.4

4. *[Example – "The ML risk assessment is a public document (document R1). The TF risk assessment is confidential but available to selected staff of all relevant competent authorities. A public version of the TF assessment is prepared which sets out key findings for financial institutions, and DNFBPs (document R2)."]*

etc

Annex 1 to the questionnaire for technical compliance update: size and structure of the financial and DNFBP sectors

AML/CFT Preventive Measures for Financial Institutions and DNFBPs (R.10 to R.23)

Type of Entity*	No. Licensed / Regulated / Registered	AML/CFT Laws** / Enforceable Means for Preventive Measures	Date in Force or Last Updated (*where applicable*)	Other additional Information (*e.g.* highlights of substantive changes etc.)***
Banks				
Life Insurers				
Securities				
MVTS				
Casinos				
Lawyers				
Notaries				
Accountants				
Precious Metals & Stones Dealers				
Trust and Company Service Providers				
Others				

*Additional rows may be added for other type of financial institutions and DNFBPs. Countries may also choose to have more granular and specific classification of the types of financial institutions and DNFBPs.

** Countries should indicate the specific provisions in the AML/CFT laws that set out the CDD, record keeping and STR reporting obligations.

***Where there have been changes since its last update or where relevant, countries should also set out the specific provisions in the AML/CFT laws or enforceable means and key highlights of the obligations for other preventive measures (*e.g.* PEPs, wire transfers, internal controls and foreign branches and subsidiaries etc.).

Legal Persons and Arrangements (R.8, R.24 and R.25)

Type of Legal Persons / Arrangements*	No. Registered (where available)	Applicable Laws / Regulations / Requirements	Date in Force or Last Updated (*where applicable*)	Other additional Information (*e.g.* highlights of substantive changes etc.)**

*Additional rows may be added for other type of legal persons or arrangements. Countries may also choose to have more granular and specific classification of the types of legal persons or arrangements.

** Countries should indicate the specific provisions in the applicable laws / regulations / requirements and key highlights that set out the obligations to maintain the requisite information in R.24 (*e.g.* basic and beneficial ownership) and R.25 (*e.g.* settlors, trustees, protectors (if any), the (class of) beneficiaries, and any other natural person exercising control) respectively.

MOCK MUTUAL EVALUATION OF WESTEROS

INSTRUCTIONS TO PARTICIPANTS

1. You are the team assessing the Kingdom of Westeros. This is a limited assessment, focused on the criminal justice system and in particular, Westeros' effectiveness at investigating and prosecuting cases of money laundering.

2. Working in jurisdiction teams, you will assess ***Immediate Outcome IO.7 – ML Investigation and Prosecution.***

3. A draft of the Technical Compliance Annex is provided to consider in your assessment of IO.7 (see contents section for page number).

4. This booklet contains information and documents submitted by the Kingdom of Westeros as a basis for the assessment. Assessors should analyse this information as a basis for assessing effectiveness, and to prepare for on-site interviews with Westeros officials.

5. Three interviews have been scheduled with Westeros officials, lasting approximately 45 minutes each.

    - Chief Inspector, Financial Crimes Branch, National Police Agency; and
    - Deputy Head, General Prosecutions Section, Attorney General's Office
    - Head, Financial Intelligence Unit of Westeros;

6. The Assessment team should prepare a brief report using the attached MER Template, including ratings for the Immediate Outcome.

7. The Assessment team should prepare a brief 10 minute presentation for the final day of the workshop.

INFORMATION PROVIDED BY THE KINGDOM OF WESTEROS

General information on the country and its economy

1. Westeros is a small island nation located in the middle of the Pacific Ocean. Westeros covers an area of 30,000 square kilometres and is divided into four states. The capital of Westeros is King's Landing. As of 2008, the estimated population is 2 million people having a mean age of 45 and life expectancy averaging 77 years. Of these, about 30,000 are resident immigrant workers. The official languages are English and French and the literacy rate is 98% (as of 2008).

Economy

2. Westeros is a developed, industrial country with a free-market economy. The currency of Westeros is the Euro (EUR). In 2012, the gross domestic product (GDP) of Westeros was EUR 39 billion. The main industries are financial services (28%), logging (29%), mining (16%), fishing (21%) and agriculture (6%).

System of government

3. Westeros is a Monarchy. Its government is divided into executive, legislative and judicial branches. The executive branch is comprised of a King, the 'Hand of the King', and an appointed Cabinet. The federal legislative branch, known as the Parliament is bicameral and consists of a House of Representatives (containing 55 members) and a Senate (containing 16 members—four per state). The Government (National Party) has a majority in both houses, and has held power for the last 40 years. Westeros has a three-tiered court system that is comprised of four State District Courts (trial courts), four State Courts of Appeal and one Supreme Court (which is the country's highest court).

Legal system and hierarchy of laws

4. The legal system combines civil and common law principles. Laws are codified. State Courts are guided by (but not bound to follow) previous judgments of the Court of Appeal in their respective state. However, if a State Court judgment contradicts a previous judgment of its respective State Court of Appeal, both the defendant and prosecutor have an automatic right of appeal. State Courts of Appeal are not bound by each other's decisions. However, if a State Court of Appeal decides a point of law in a manner which contradicts a previous judgment of its own or another State Court of Appeal, the Department of Justice has an automatic right of appeal to the Supreme Court of Westeros. All courts are legally bound to follow decisions of the Supreme Court of Westeros (section 2 of the Supreme Court Act).

5. The Constitution of Westeros is the highest law in the land, and is the basis for enacting other laws. No other laws or regulations should conflict with the Constitution. From highest to lowest, the hierarchy of laws is the Constitution, federal laws, federal regulations, State laws, State regulations and municipal bylaws.

Transparency, good governance, ethics and measures against corruption

6. Historically, Westeros has suffered from widespread corruption at the highest levels of public office down through to the operational level. Over the years there have also been many allegations of electoral malpractice. However, since ratifying the 1997 Convention on Combating Bribery of Foreign Public Officials in International Transactions (the OECD Bribery Convention) in 2008, Westeros has worked to address the corruption problem.

7. The Anti-Corruption and Bribery Act (ACB Act), which came into force at the end of 2010, criminalises a broad range of corruption and bribery activities.

8. In 2010, the government formally established the Anti-Corruption Agency (ACA)—an independent agency that reports directly to the Parliament. The mandate of the ACA is to conduct full audits of each Ministry and government agency for the purpose of detecting corrupt activities and punishing those responsible. As part of the audit process, the ACA is authorised to apply a full range of sanctions, including taking disciplinary action against or dismissing employees, barring persons from working within the public sector and/or referring corruption and bribery cases to the National Police Authority (NPA) for criminal investigation where appropriate. The ACA began its work by targeting high-level politicians, judges and ministers. Following a large number of high-profile cases involving politicians, judges, ministers and two former Presidents, corruption at the political level has been largely eradicated. (The exception is the Ministry of Finance where a high level investigation is currently ongoing.) However, corruption continues to be a problem at the operational level in some agencies.

9. The ACA is now focusing on corruption at the operational level, on an agency-by-agency basis. In those agencies which have been audited to date, sanctions have been aggressively applied. In many agencies there were widespread dismissals of employees, disciplinary actions and, in some cases, subsequent criminal prosecutions. To date, the ACA has completed full audits of the Department of Justice (DOJ), NPA, the Ministry of Foreign Affairs (MFA) and the Financial Supervisory Authority (FSA). Corruption issues have now been largely addressed in these agencies. The ACA is scheduled to finalise its audit the Ministry of Finance next year.

General Situation of Money Laundering and Financing of Terrorism

10. Financial crime is a serious problem in Westeros. In 2009, as part of its anti-corruption campaign, the government commissioned an independent study of the country's money laundering (ML) and terrorist financing (FT) risk. Completed in 2010, the results of that study are summarised below.

Money laundering

11. In order of priority, criminal proceeds are most commonly generated in Westeros from the following predicates: corruption and bribery offences, drug trafficking and securities-related offences. Corruption and bribery continue to be major problems at the operational level in those agencies which have not yet undergone the ACA audit process and in the private sector.

12. Westeros is a major producer of marijuana and synthetic drugs such as methamphetamine and ecstasy. Three major organised crime groups with international ties, particularly in South America and Southeast Asia, control the drug production in Westeros. Most of the illicit drugs produced are destined for the North American market and generate approximately 950 million dollars worth of proceeds annually.

13. Securities offences also pose a serious problem that is wide-spread and increasing. The authorities have uncovered numerous cases of securities fraud, breaches of trust by investment managers, insider trading and market manipulation.

14. It should also be noted that Westeros is located in a region where many neighbouring countries also suffer from high levels of drug trafficking, corruption and bribery offences. As the most sophisticated financial centre in the region and the only one with a licensed stock exchange, the proceeds of these offences are often brought to Westeros to be laundered.

15. The money laundering risk is highest in the banking, securities and real estate sectors. Money laundering through the banking sector often involves customers who are legal persons with complicated ownership and control structures that may include shell companies.

16. In the securities sector, securities firms and brokers routinely accept large amounts of cash from their clients to be invested in Westeros's stock exchange. Investigations of securities offences often uncover

collusion between the customer (defendant) and a securities broker. Additionally, several major investigations of organised crime organisations have revealed strong links with several smaller securities firms.

17. In the real estate sector, property is often purchased using cash, frequently by intermediaries acting on behalf of foreign individuals, companies or trusts. Each year, Westeros receives a large number of mutual legal assistance requests in relation to enforcing foreign confiscation orders on real estate that was purchased in the country with the proceeds from foreign predicate offences. As well, the majority of domestic bribery investigations have revealed that at least some of the bribes received were invested in the local real estate market.

18. The money laundering risk is low in the insurance and foreign exchange sectors. The risk is low in the insurance sector because many of the insurance products and practices generally associated with high ML risk (single premium policies, ability to purchase insurance in cash, third party payment of premiums, policies with a short cancellation period allowing for refunds of premiums, issuing policies to customers who provide only a post office box as an address or to overseas clients) are prohibited. Furthermore, the possibility of obtaining early redemption of insurance policies is subject to strict conditions and is extremely limited. The insurance sector of Westeros is very small and no cases of ML through the sector have been detected.

19. The ML risk is low in the foreign exchange sector for the following reasons. The vast majority of foreign exchange business is conducted on behalf of customers who have established accounts with the foreign exchange dealer. Most of these are corporate customers which have international operations or are doing business abroad. Occasional transactions for tourists and other walk-in customers is relatively uncommon. There is little tourism in Westeros and citizens travelling abroad usually perform their foreign exchange transactions through their regular bank. Additionally, all foreign exchange transactions are subject to Westeros's strict exchange control regime, making it difficult to launder money through this sector.

20. The ML risk is moderate in the money remittance sector. Westeros's strict exchange controls make it difficult to launder money through cross-border wire transfers. The sector is very small since most people make wire transfers through their bank. There are, however, a few independent money remitters which are generally used by Westeros's immigrant worker population. Additionally, there is a small underground banking sector which is used primarily by a tiny refugee community from a country located in a conflict area where the formal financial system has been destroyed.

Terrorist financing

21. Westeros has not yet been the victim of a terrorist attack. However, there are a number of well-known terrorist organisations operating in neighbouring jurisdictions, and nearby countries have suffered terrorist attacks in the past decade. During the trials of the perpetrators, it came to light that the funds used to finance those attacks originated from bank accounts in Westeros. In one of these cases, a charity in Westeros was used to collect and transmit funds which were sent through its bank account to the charity's branch office and subsequently used to finance terrorist attacks in that country.

Overview of the Financial Sector and DNFBP

22. Westeros is the main financial centre in the region with a sophisticated, well-established banking, securities and insurance sectors, and an efficient payment system. The following chart shows the types of "financial institutions" (as defined by FATF) that operate in Westeros and indicates if they are subject to anti-money laundering (AML)/counter-terrorist financing (CFT) requirements and their AML/CFT regulator where one exists:

Financial Activity by Type of Financial Institution			
Type of financial institution activity (see the Glossary of the FATF 40 Recommendations)	**Type of Financial Institution that performs this activity**	**Subject to AML/CFT requirements**	**AML/CFT Supervisor/Regulator**
Acceptance of deposits and other repayable funds from the public	Banks Savings and loan institutions Credit unions	Yes	FSA
Lending	Banks Savings and loan institutions Credit unions	Yes	FSA
Financial leasing	Financial leasing companies	No	No
Transfer of money or value	Banks Money remitters	Yes Yes	FSA
Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	Banks	Yes	FSA
Financial guarantees and commitments	Banks	Yes	FSA
Trading in Money market instruments (cheques, bills, CDs, derivatives etc.)	Banks Securities brokers	Yes	FSA
Trading in Foreign exchange	Banks Foreign exchange dealers	Yes	FSA
Trading in Exchange, interest rate and index instruments	Banks Securities brokers	Yes Yes	FSA
Trading in Transferable securities	Securities brokers	Yes	FSA
Trading in Commodities	Banks Securities brokers	Yes Yes	FSA
Participation in securities issues and the provision of financial services related to such issues	Banks Securities brokers	Yes Yes	FSA
Individual and collective portfolio management	Securities brokers	Yes	FSA
Safekeeping and administration of cash or liquid securities on behalf of other persons	Banks	Yes	FSA
Otherwise investing, administering or managing funds or money on behalf of other persons	Securities brokers	Yes	FSA
Underwriting and placement of life insurance and other investment related insurance	Life insurance companies Independent insurance agents	Yes	FSA
Money and currency changing	Banks Foreign exchange dealers	Yes Yes	FSA

23. As at January 2009, there were 22 licensed banks (with 64 branches) operating in Westeros. Twelve are large global banks, four are large national banks with operations abroad, four are small savings and loan institutions and two are small credit unions. Neither savings and loan institutions, nor credit unions are authorised to have operations abroad. The combined assets of the banking sector are EUR 14 billion.

24. There are 14 securities firms (the combined assets of which are EUR 8 billion) employing 527 securities brokers. Two of these firms belong to large global financial groups and account for about 22% of the market share. Of the remaining 12 firms, 3 are mid-size operations and 9 are quite small with less than 30 employees each. There is one stock exchange in Westeros—Westeros Stock Exchange (WSE).

25. The insurance sector in Westeros is very small. There are three insurance companies employing 82 insurance brokers. All three companies offer life insurance, property damage/casualty insurance and health insurance. Premiums totalled EUR 2.1 million in 2011. The law prohibits offering single premium life insurance policies. Additionally, there 2 independent insurance agents doing business in the country.

26. The market for money remittance and foreign exchange is also very small. There are 3 companies providing money remittance services, all of which are very small operations, employing no more than two or three people. There are also 2 companies authorised to provide foreign exchange services.

27. Westeros has one casino in the country. Most of its business comes from local residents.

28. There are 250 chartered accountants and 316 lawyers (of which 175 are also notaries) who are licensed to do business in Westeros. Notaries do not exist in Westeros as a separate profession.

29. Trust and company service providers (TCSPs) do not exist as a separate sector. Only lawyers are authorised to provide trust services. Anyone can provide company services. In practice, lawyers and accountants often provide company services, but there are also about 42 private companies operating in Westeros which provide services relating to the creation, directorship and management of companies.

30. Westeros also has 550 licensed real estate agents, and 26 dealers in precious metals and stones (all of which are retail jewellery stores).

Scope and Coverage of Preventive Measures

31. AML/CFT preventative measures for the financial sector are set out in the AML/CFT Act, AML/CFT Regulations (issued by the Minister of Finance pursuant to section 28 of the AML/CFT Act), the Reporting Circular and the AML/CFT Guidelines. The AML/CFT Regulations are secondary legislation (see section 5 of the Interpretation Act).

32. Additionally, the FSA has issued AML/CFT Guidelines for accountable institution which sets out principles and "best practice standards". While no sanction can be applied for contravention of the AML/CFT Guidelines, accountable institutions are encouraged to observe the spirit of this guidance, and advised that the FSA will consider the degree of observance with the Guidelines when formulating its overall risk assessment and supervisory approach to that account institution.

33. CDD, record keeping and internal control requirements apply to banks, insurance companies and agents, securities firms and brokers, money remitters and foreign exchange dealers (collectively referred to as "accountable institutions"). The obligation to report STRs applies to accountable institutions and anyone carrying on business in Westeros (collectively referred to as "reporting entities").

Overview of commercial laws and mechanisms governing legal persons and arrangements

34. Constitutionally, company law falls within State (not federal) jurisdiction. Each State has its own company law, although these are relatively uniform.

35. There are five basic business forms available for enterprises doing business in Westeros: the sole proprietorship, the partnership, the public company, the private company and the limited liability company.

- A sole proprietorship is an unincorporated business that is owned by one individual and has no legal existence apart from its owner.

- A partnership is an unincorporated business that is owned by two or more individuals and has no legal existence apart from its owners.

- A public company is an incorporated business that has a legal existence apart from its owners and publicly lists its shares on a stock exchange.

- A private company is similar to a public company except that its shares are not listed on a stock exchange.

- A limited liability company has the characteristics of a private company in that its shares are not listed on a stock exchange and its owners enjoy limited liability. However, it has the characteristics of a partnership in that, for tax purposes, it has no legal existence apart from its owners.

36. All three types of company (public, private and limited liability) are formed by preparing articles of incorporation that set out the company's name, address, type of business, directors (including their names, dates of birth and addresses), senior management (including their names, dates of birth and addresses), the number and type of shares that the company is authorised to issue, the shareholders of the company (including their names, dates of birth and addresses) and a description of the company's control structure.

37. The articles of incorporation must be filed with the State Registry of Companies (SRC). The SRC reviews each filing to ensure that it contains all of the required information, but does not verify its accuracy. The information contained in the SRC is publicly available, upon payment of a subscription fee. Once a year, companies are required to update the information that is filed with the SRC by filing a "Confirmation of Information" form.

38. Trusts can be formed in Westeros. The services of a lawyer are required to prepare the trust deed. The trust deed must contain the names, dates of birth and addresses of the settlor, trustees and beneficiaries of the trust. The trust deed must also specify the purpose of the trust, its assets and any instructions relating to the management of those assets. The lawyer who prepared the trust deed is required to keep a copy of it. Trustees are obligated to update this information (if applicable) once per year by filing an "Addendum to a Deed of Trust" form with the lawyer who prepared the trust deed. Westeros also recognises foreign trusts.

Overview of strategy to prevent money laundering and terrorist financing

a. AML/CFT Strategies and Priorities

39. Westeros is a member of is a member of the FSAMLF (Fictional States' AML Forum - a regional body associated to FATF) and has endorsed the FATF Recommendations 2003. The government of Westeros has three key priorities in its AML/CFT strategy. First, the government is seeking to improve its legislative framework by extending AML/CFT requirements to the following sectors, none of which are currently subject to any AML/CFT obligations: accountants, casinos, dealers in precious metals and stones, lawyers and notaries, real estate agents, and TCSPs.

40. The second priority is to improve implementation of existing AML/CFT requirements in the securities sector.

b. The institutional framework for combating money laundering and terrorist financing

Department of Justice (DOJ)

41. The DOJ is the government ministry that handles criminal prosecutions. It is led by the Minister of Justice, and has the following departments which are directly involved in AML/CFT issues:

- ***Attorney General's Office (AGO):*** The AGO is responsible for prosecuting all criminal offences that are set out in the Penal Code or any other Act, including money laundering and terrorist financing offences. It is also responsible for drafting proposed amendments to the Penal Code and Terrorist Financing Act, and submitting them to the Parliament.

- ***Asset Control Unit (ACU):*** The ACU handles applications to freeze, seize and confiscate assets.

Ministry of Finance

42. The Ministry of Finance is the government entity that is responsible for administering the Anti-Money Laundering and Counter-Terrorist Financing Act (AML/CFT Act). The Ministry is led by the Minister of Finance, and has the following departments which are directly involved in AML/CFT issues:

- ***Financial Crimes Policy Development Unit (FCPDU):*** The FCPDU is responsible for developing and coordinating AML/CFT policy in Westeros. The FCPDU also coordinates the Ministry of Finance's administration of the AML/CFT Act, including drafting regulations to that Act.

- ***Financial Intelligence Unit of Westeros (FIUW):*** The FIUW is the financial intelligence unit (FIU) of Westeros and is responsible for receiving and analysing STRs, including preparing STR case files to be disseminated to law enforcement authorities.

Ministry of Foreign Affairs (MFA)

43. The MFA is the government entity that is responsible for handling requests for international cooperation. It is led by the Minister of Foreign Affairs, and has the following departments which are directly involved in AML/CFT issues:

- ***International Cooperation Department (ICD):*** The ICD handles incoming and outgoing requests for mutual legal assistance.

- ***Extradition Department (ED):*** The ED handles incoming and outgoing requests for extradition.

Law enforcement agencies

44. The following law enforcement agencies are directly involved in AML/CFT issues:

- ***National Police Authority (NPA):*** The NPA is the national police force of Westeros. It is responsible for investigating all offences pursuant to the Penal Code, including money laundering. It is also responsible for investigating criminal offences pursuant to the Anti-Corruption and Bribery Act, and the Securities Act.

- ***National Customs Authority (NCA):*** The NCA is the customs authority of Westeros, and responsible for controlling the cross-border movement of goods and currency.

Supervisory authorities with AML/CFT compliance responsibilities

45. The ***Financial Supervisory Authority (FSA)*** is responsible for licensing and supervising banks, insurance companies and agents, and securities firms and brokers. It is also responsible for registering and supervising money remitters and foreign exchange offices.

c. Approach concerning risk

46. Westeros has incorporated some aspects of a risk-based approach in the implementation of its AML/CFT regime. In late 2012, the National Police Authority and FIUW were commissioned to prepare a National Money Laundering Risk Assessment of Westeros.

47. Application of AML/CFT obligations to certain sectors: AML/CFT preventative measures apply to all financial institutions (as defined in the FATF Recommendations), with the minor exception of financial leasing companies. However, this exception is not based on a full ML/FT risk assessment.

48. Risk-based approach taken by financial institutions: The AML/CFT Regulations provide examples of low risk customers to whom financial institutions may apply simplified customer due diligence (CDD) measures, and high risk customers to whom financial institutions must apply enhanced CDD measures. This means that the financial institution must conduct a risk assessment to determine whether a customer is high or low risk.

49. Use of a Risk-Based Approach in Supervision: The FSA uses an impact and risk model to allocate supervisory resources among institutions, and to distinguish those institutions that may pose a higher threat to the achievement of supervisory objectives. Undertaking business activities deemed to be susceptible to ML/FT risks has a bearing on the institutions' overall risk assessment, and hence such institutions are subject to more intensive supervision and more frequent on-site inspections.

d. Progress since the last mutual evaluation or assessment

50. This is the second mutual evaluation of Westeros. Since last being assessed in 2001, Westeros has made significant legislative changes to its AML/CFT regime. Key changes include extending AML/CFT obligations to the securities, insurance, foreign exchange and money remittance sectors. Additionally, steps have been taken to address corruption at the political and operational levels.

INFORMATION PROVIDED BY WESTEROS:

SELF-ASSESSMENT AGAINST CRITERIA

Recommendation 3 – Money Laundering Offence

3.1 ML should be criminalised on the basis of the Vienna Convention and the Palermo Convention (see Article 3(1)(b)&(c) Vienna Convention and Article 6(1) Palermo Convention)

51. Money laundering (ML) was criminalised in September 2000 when section 555 of the Penal Code came into force. Money laundering has been criminalised on the basis of the Vienna and Palermo Conventions. Section 555 of the Penal Code states that:

> A person who knowingly:
>
> (a)converts or deals in any way with proceeds of a serious crime for the purpose of concealing the origin of those proceeds, or for the purpose of helping another person to avoid criminal prosecution or confiscation proceedings;
>
> (b)disguises or in any way obscures the source, location, movement, character or any other identifying aspect of proceeds of a serious crime, including any type of rights to those proceeds; or
>
> (c) acquires or possesses proceeds, knowing them to be the proceeds of a serious crime,
>
> knowing that such proceeds are the proceeds of a serious crime, commits an offence punishable by a maximum term of imprisonment of 5 years and/or a maximum fine of EUR 250 000.

3.2 The predicate offences for ML should cover all serious offences, with a view to including the widest range of predicate offences. At a minimum, predicate offences should include a range of offences in each of the designated categories of offence.

52. All serious offences (as that term is defined in section 10 of the Penal Code) are predicate offences for money laundering. Additionally, terrorist financing offences pursuant to the Terrorist Financing Act are predicate offences for money laundering.

3.3 Where countries apply a threshold approach or a combined approach that includes a threshold approach, predicate offences should, at a minimum, comprise all offences that:

(a) fall within the category of serious offences under their national law; or

(b) are punishable by a maximum penalty of more than one year's imprisonment; or

(c) are punished by a minimum penalty of more than six months' imprisonment (for countries that have a minimum threshold for offences in their legal system).

53. All serious crimes set out in the Penal Code are predicate offences for money laundering. Serious crimes are punishable by a maximum penalty of more than 1 year imprisonment (Penal Code, s.10).

Additionally, it should also be noted that insider trading and market manipulation are criminalised pursuant to the Securities Act and are subject to a maximum penalty of 4 years imprisonment.

3.4 The ML offence should extend to any type of property, regardless of its value, that directly or indirectly represents the proceeds of crime.

54. The ML offence applies to any property that directly or indirectly represents the proceeds of crime.

3.5 When proving that property is the proceeds of crime, it should not be necessary that a person be convicted of a predicate offence.

55. When proving that property is the proceeds of crime, it is not necessary that a person be convicted of the predicate offence although there is the need to specify the predicate offence, whether it occurs domestically or abroad.

3.6 Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically.

56. A person can be charged with laundering the proceeds of a predicate offence that was committed in a foreign country, provided that the conduct would have constituted a serious crime had it occurred in Westeros.

3.7 The ML offence should apply to persons who commit the predicate offence, unless this is contrary to fundamental principles of domestic law.

57. Self-laundering is criminalised.

3.8 It should be possible for the intent and knowledge required to prove the ML offence to be inferred from objective factual circumstances.

58. Section 555 of the Penal Code applies to any person who knowingly converts or deals in any way, disguises or in any way obscures, acquires or possesses proceeds. It is a well established principle of Westeros law that the intentional element of any offence can be inferred from objective factual circumstances (see Westeros v. Post (April 1988)).

3.9 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of ML.

59. A natural person convicted of laundering the proceeds of a serious crime or a terrorist financing offence is subject to a criminal penalty of up to 5 years in prison and/or a maximum EUR 250 000 fine (Penal Code, s.555; Terrorist Financing Act, s.6).

3.10 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures are without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

60. In general, it is contrary to the fundamental legal principles of Westeros's legal system to impose corporate criminal liability. However, very limited exceptions have been made in relation to offences of counterfeiting and piracy of goods, environmental crimes and terrorist financing offences.

61. Legal persons convicted of laundering the proceeds of terrorist financing, environmental crimes or offences relating to the counterfeiting or piracy of products are only subject to fines of up to EUR 500 000 (Terrorist Financing Act, s.6; Penal Code, ss.149(c) and 282(c)).

3.11 Unless it is not permitted by fundamental principles of domestic law, there should be appropriate ancillary offences to the ML offence, including: participation in; association with or conspiracy to commit; attempt; aiding and abetting; facilitating; and counselling the commission.

62. There are general provisions in the Penal Code which set out a full range of ancillary offences, including attempt, conspiracy, aiding and abetting, etcetera. These ancillary offences apply to all Penal Code offences, including money laundering.

Recommendation 20 – Reporting of Suspicious Transactions

20.1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity , or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit.

63. The reporting obligations of the AML/CFT Act apply to any person who carries on, manages or is employed by a business.

64. A transaction must be reported where there is a founded suspicion that it may be related to a criminal offence pursuant to the Penal Code or any other Act (AML/CFT Act, s.22).

20.2 Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

65. All transactions must be reported, regardless of their amount. Persons are also required to report attempted transactions pursuant to section 2 of the Reporting Circular. The Reporting Circular is equivalent to a Regulation.

Recommendation 30 – Responsibilities of Law Enforcement and Investigative Authorities

30.1 There should be designated law enforcement authorities that have responsibility for ensuring that money laundering, associated predicate offences and terrorist financing offences are properly investigated, within the framework of national AML/CFT policies.

66. The National Police Authority (NPA) is designated with responsibility for investigating Penal Code offences and criminal offences pursuant to the Securities Act, the Anti-Corruption and Bribery Act and the Protection of Financial Information Act. The responsibilities of the NPA are set out in the Police and Intelligence Services Act (PIS Act).

30.2 Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related ML/TF offences during a parallel financial investigation , or be able to refer the case to another agency to follow up with such investigations, regardless of where the predicate offence occurred.

67. NPA officers investigating predicate offences are authorised to pursue the investigation of related money-laundering offences.

30.3 There should be one or more designated competent authorities to expeditiously identify, trace, and initiate freezing and seizing of property that is, or may become, subject to confiscation, or is suspected of being proceeds of crime.

68. The Asset Control Unit of the Ministry of Justice has authority to identify, trace, and initiate freezing and seizing of property suspected of being proceeds of crime.

30.4 Countries should ensure that Recommendation 30 also applies to those competent authorities, which are not law enforcement authorities, per se, but which have the responsibility for pursuing financial investigations of predicate offences, to the extent that these competent authorities are exercising functions covered under Recommendation 30.

69. The National Customs Authority has responsibility for pursuing financial investigations related to predicate offences for which it is the principal investigating authority, including the offences of smuggling and providing a false currency declaration.

30.5 If anti-corruption enforcement authorities are designated to investigate ML/TF offences arising from, or related to, corruption offences under Recommendation 30, they should also have sufficient powers to identify, trace, and initiate freezing and seizing of assets.

70. The Anti-Corruption Agency has the responsibility to conduct audits of government agencies for the purpose of detecting corrupt activities and punishing those responsible. The Anti-Corruption Authority does not yet have responsibility for investigating money laundering associated with corruption or initiating freezing of related assets.

Recommendation 31 – Powers of Law Enforcement and Investigative Authorities

31.1 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for:

(a) the production of records held by financial institutions, DNFBPs and other natural or legal persons;

(b) the search of persons and premises;

(c) taking witness statements; and

(d) seizing and obtaining evidence.

71. The powers of the National Police Authority are set out in the Police and Intelligence Services Act (1985). These include powers to search persons, vehicles, or premises; to obtain statements; and to seize property, including documents, in the course of an inquiry or investigation.

72. National Police Authority officers may obtain a judicial production order to compel the production of documents or other information held by any persons, including financial institutions or DNFBPs.

31.2 Competent authorities conducting investigations should be able to use a wide range of investigative techniques for the investigation of money laundering, associated predicate offences and terrorist financing, including:

(a) undercover operations;

(b) intercepting communications;

(c) accessing computer systems; and

(d) controlled delivery.

73. The NPA has the power to use controlled delivery or undercover techniques (section 6, Police and Intelligence Services Act). However, these powers can only be used if there are reasonable and probable grounds to believe that the investigation may involve an organised criminal group. These powers are most commonly used in drug investigations involving organised crime groups (which are involved in most of the drug trafficking and production that takes place in Westeros). Officers may also use wiretaps, provided the appropriate judicial order is obtained.

74. The National Police Authority can postpone or waive the arrest of any suspect, or the seizure of any funds or property, for the purpose of gathering additional evidence, identifying additional suspects or otherwise furthering an investigation (s.7 Police and Intelligence Services Act).

31.3 Countries should have mechanisms in place:

(a) to identify, in a timely manner, whether natural or legal persons hold or control accounts; and

(b) to ensure that competent authorities have a process to identify assets without prior notification to the owner.

75. The National Police Authority officers may obtain a judicial production order, compelling the production of all account information relating to a particular natural or legal person.A production order may be issued with general application to all financial institutions and DNFBPs, compelling such entities to identify whether they hold any account on behalf of the individual named, and if so, to provide information on such accounts.

31.4 Competent authorities conducting investigations of money laundering, associated predicate offences and terrorist financing should be able to ask for all relevant information held by the FIU.

76. The National Police Authority is authorised to seek information from the Financial Intelligence Unit of Westeros. Financial information is protected by the Protection of Financial Information Act and must not be disclosed other than in accordance with the law.

Recommendation 35 – Sanctions

35.1 Countries should ensure that there is a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with the AML/CFT requirements of Recommendations 6, and 8 to 23.1

77. Criminal sanctions and civil injunctive power are available for breaches of the AML/CFT requirements. For natural persons, criminal sanctions (imprisonment of up to 2 years and/or fines of up to EUR 100 000) may be applied by the courts following conviction (AML/CFT Act, s.31). For legal persons, the criminal sanction is a fine of up to EUR 200 000 (AML/CFT Act, ss.29-30). To date, no criminal sanctions have been imposed.

78. The FSA is also authorised to apply to a State Supreme Court for a civil injunction for the purpose of restraining conduct that may breach Part 3 or 4 of the AML/CFT Act (section 33). However, due to its severity, the sanction of a civil injunction is rarely applied in practice. To date, the civil injunction power has been used four times. All cases involved securities firms that had systemic and repeated breaches of the AML/CFT requirements relating to CDD, record keeping, internal controls and STR reporting.

79. Section 8 of the Reporting Circular sets out the following range of administrative sanctions for non-compliance with the STR reporting requirements: issuing a written warning or order to comply; ordering regular reports on measures being taken to address the breach; imposing administrative fines up to a maximum of EUR 100 000 (for natural persons) or EUR 200 000 (for legal persons); replacing managers, directors or controlling owners; barring persons from employment within the sector; and suspending, revoking or failing to renew an accountable institution's license. The FSA regularly applied administrative sanctions.

35.2 Sanctions should be applicable not only to financial institutions and DNFBPs but also to their directors and senior management.

80. Both criminal sanctions and the civil injunction power may be used in relation to natural persons who own, manage, direct or are employed by a reporting entity, and who are found to have knowingly breached the reporting obligation (AML/CFT Act, s.28). Administrative sanctions may also be applied against such persons for breaches of the reporting requirements (Reporting Circular, s.8).

[1] The sanctions should be directly or indirectly applicable for a failure to comply. They need not be in the same document that imposes or underpins the requirement, and can be in another document, provided there are clear links between the requirement and the available sanctions.

ANNEXES – DOCUMENTS PROVIDED BY WESTEROS

Anti-Money Laundering and Counter-Terrorist Financing Act (AML/CFT Act) (2002)

Part 1—Definitions

1. For the purposes of this Act, the following definitions apply:

(a) "accountable institution" means any of the entities, including their employees and agents, that are listed in section 2 of this Act;

(b) "customer" means the person who conducts a transaction or in whose name an account or business relationship is established;

(c) "monetary instrument" means a cheque, travellers cheque, promissory note or money order;

(d) "money remitter" means any person who engages in a business that accepts cash, monetary instruments or other stores of value from a customer in one location and pays out a corresponding sum to a person in another location through means of a message, transfer, clearing network or communication;

(e) "person" means a natural or legal person;

(f) "transaction" means establishing an account; making a deposit or withdrawal; making an exchange, transfer, placement or payment of cash or other assets; making a purchase or sale; or otherwise dealing in cash, monetary instruments or property.

Part 2—Scope of application

2. The following entities and their employees and agents are obligated to comply with the provisions contained in Parts 3 and 4 of this Act:

(a) banks;

(b) savings and loan institutions;

(c) credit unions;

(d) securities firms;

(e) securities brokers;

(f) insurance companies;

(g) insurance agents;

(h) money remitters; and

(i) foreign exchange dealers.

Part 3—Obligations on accountable institutions

Customer identification and verification procedures (Natural persons)

3. Accountable institutions shall collect and record the following information concerning customers who are natural persons:

(a) name;

(b) date of birth;

(c) address; and

(d) citizen identity number or passport number.

4. The information collected and recorded pursuant to section 3 shall be verified by reference to one of the following types of government-issued photo identification documents: a passport or citizen identity card. The identification document must be valid. Verification must include ensuring that the photograph and signature which appear in the identity document match the appearance and signature of the customer.

Customer identification and verification procedures (Legal persons and arrangements)

5. Accountable institutions shall collect and record the following information concerning customers who are legal persons:

(a) name;

(b) date of incorporation;

(c) address;

(d) type of business;

(e) names, dates of birth and addresses for all directors and senior management;

(f) names, dates of birth and addresses for all shareholders; and

(g) taxpayer identification number.

6. The information collected and recorded pursuant to section 5 shall be verified by reference to a certified copy of the articles of incorporation that has been issued, within the past six months, by the State Registry of Companies. A copy of the articles of incorporation shall be kept in the customer file.

7. In relation to the settlor, trustee and beneficiaries of a trust or other legal arrangement, the accountable institution shall collect, record and verify the information as specified in sections 3 and 4 of this Act (for natural persons) and sections 5 and 6 of this Act (for legal persons). The accountable institution shall also verify the legal status of the trust by reference to a certified copy of the trust deed that has been issued, within the past six months, by the lawyer who established the trust and is responsible for holding a copy of the trust deed. The accountable institution shall keep a copy of the trust deed in the customer file.

8. The accountable institution shall also: (i) collect and record the name, date of birth and address of the natural person(s) who is authorised to act on behalf of the legal person or arrangement; (ii) verify that person's identity; and (iii) verify that the person is authorised to act on behalf of the legal person or arrangement.

Timing of identification and verification

9. Accountable institutions must identify their customers in accordance with the procedures described in sections 3 to 8 in the following circumstances:

(a) when a business relationship is being established;

(b) when carrying out occasional transactions, including wire transfers, above EUR 10 000 on behalf of a person who is not an established customer;

(c) when there is a suspicion of money laundering or terrorist financing, and the transaction exceeds EUR 10 000 in value;

(d) when customer identification information being provided is not adequate to verify the identity of the customer; and

(e) when the accountable institution suspects that the identification documents being relied upon by the customer are invalid or false.

10. The customer's identity shall be verified at the time that the business relationship is established and before a transaction is carried out. In the case of an occasional customer, the customer's identity shall be verified before a transaction is carried out.

Identification of beneficial owners

11. If a customer indicates that he/she is establishing a business relationship or carrying out a transaction on behalf of another person, that person shall be identified in accordance with sections 3 to 8 of this Act.

Enhanced customer identification and due diligence

12. The Ministry of Finance may specify, in the regulations to this Act, high risk categories of customer, business relationship or transaction to which enhanced customer identification measures must be applied.

Simplified or reduced customer identification and due diligence

13. The Ministry of Finance may specify, in the regulations to this Act, low risk categories of customer, business relationship or transaction to which simplified customer identification measures may be applied.

Failure to complete customer identification and verification

14. When an accountable institution is unable to identify a new, established or occasional customer (subject to the provisions of section 15 below) in accordance with the procedures described in sections 3 to 8, no business relationship should be established or transaction carried out. Additionally, the accountable institution should consider whether it is appropriate to make a suspicious transaction report.

Identification measures applicable to existing customers

15. An accountable institution is not required to follow the procedures set out in sections 3 to 8 of this Act in relation to a person who became a customer of the accountable institution prior to this Act coming into force.

Ongoing due diligence

16. Accountable institutions are obligated to conduct ongoing due diligence on their customer relationships. This includes ensuring that the transactions being conducted are consistent with the accountable institution's knowledge of the customer and their business. Accountable institutions must keep records relating to any transactions that:

(a) appear to lack a legitimate purpose;

(b) are unusually large or complex or otherwise unusual in relation to the customer's usual pattern of transactions; or

(c) are suspicious.

Record keeping

17. Accountable institutions are required to maintain records on transactions, including information to identify customers and beneficiaries, the nature and date of the transaction, the type and amount of currency involved, and the type and identifying number of any account involved in the transactions, for a period of five years following completion of the transaction.

18. Accountable institutions are required to maintain customer identification records and account files for at least five years following the termination of the business relationship or closure of the account.

Internal controls

19. Accountable institutions are required to establish internal policies, procedures and controls for the collection of customer identification information, the retention of records, and the detection and reporting of suspicious transactions.

20. Accountable institutions are required to appoint a compliance officer to ensure compliance with the policies, procedures and controls referred to in paragraph 19.

Part 4—Obligations on all businesses and professions

Suspicious transaction reporting

21. There shall be a financial intelligence unit, the Financial Intelligence Unit of Westeros (FIUW), located within the Ministry of Finance. It shall be responsible for receiving and analysing all suspicious transaction reports (STRs) that are filed by reporting entities pursuant to section 22 of this Act. Where such analysis leads to a reasonable suspicion that the transaction is related to criminal activity, the FIUW shall, without delay, forward the STR and related analysis to the Minister of Finance for consideration. Within three business days of receiving an STR and related analysis, the Minister shall notify the FIUW of the outcome of such consideration and, if deemed appropriate, the FIUW shall immediately disseminate the STR and related analysis, to the appropriate law enforcement authorities.

22. An accountable institution or any other person who carries on, manages or is employed by a business and who knows or ought reasonably to have known or suspected, on the basis of a founded suspicion, that a transaction to which the business is a party or in any way involved is related to a criminal offence pursuant to the Penal Code or any other Act, shall advise the Financial Intelligence Unit of Westeros of the transaction without delay by filing an STR.

23. No person who must make or has made an STR may disclose that fact or any information regarding the contents of an STR to any other person, including the person in respect of whom the STR must be or has been made, otherwise than for the purpose of:

(a) carrying out the provisions of this Act;

(b) within the scope of the powers and duties of that person in terms of any legislation;

(c) legal proceedings, including any proceeding before a judge in chambers; or

(d) in terms of an order of a court.

Record keeping

24. Accountable institutions shall keep a copy of the document(s) that were used to verify the identity of the customer (as described in sections 3 to 8) for a period of six years after the transaction is carried out or following the termination of the customer relationship.

25. Accountable institutions entities shall also keep a copy of any records relating to transactions that were considered to be suspicious, regardless of whether an STR was ultimately filed with the FIUFR.

Part 5—Offences

26. An accountable institution that does not comply with the provisions of Part 3 of this Act is guilty of an offence.

27. A reporting entity that does not comply with the provisions of Part 4 of this Act is guilty of an offence.

28. A person who owns, manages or is employed by a reporting entity, including directors, who knowingly does or omits to do something for the purpose of preventing or obstructing the reporting entity from complying with the provisions of Part 4 of this Act, is guilty of an offence.

Part 6—Sanctions

29. An accountable institution that does not comply with the provisions of Part 3 this Act and is convicted of an offence pursuant to Part 5 of this Act is liable to a fine not exceeding EUR 200 000.

30. A reporting entity that does not comply with the provisions of Part 4 this Act and is convicted of an offence pursuant to Part 5 of this Act is liable to a fine not exceeding EUR 200 000.

31. A person that does not comply with the provisions of Part 4 of this Act and is convicted of an offence pursuant to Part 5 of the Act is liable to imprisonment for a period not exceeding two years or to a fine not exceeding EUR 100 000.

32. Where, on the application of the Financial Supervisory Authority, a State Supreme Court is satisfied that a person has engaged, or is proposing to engage, in conduct that constitutes or would constitute:

(a) an offence pursuant to Part 5 of this Act;

(b) attempting to commit such an offence;

(c) aiding, abetting, facilitating or counseling a person to commit such an offence;

(d) conspiring with another person or persons to commit such an offence,

the Court may grant an injunction in such terms as the court determines to be appropriate.

Part 7—General

33. The Minister of Finance is authorized to issue regulations and circulars for the purpose of preventing and detecting money laundering and terrorist financing activity, or to further elaborate the requirements of this Act.

34. The Financial Supervisory Authority and the Financial Intelligence Unit of Westeros are authorized to issue directions, circulars and guidance for the purposes of further elaborating the requirements of this Act.

35. The Financial Supervisory Authority shall be responsible for monitoring and supervising accountable institutions, including their directors and senior management, for compliance with the provisions of this Act, including any regulations, circulars or directions made pursuant to it, and for overseeing the application of applicable sanctions, where appropriate.

36. This Act shall come into force on 31 July 2002.

Anti-Money Laundering and Counter-Terrorist Financing Regulations (2002)

Introduction

1. These regulations apply to all accountable institutions as specified in the Anti-Money Laundering and Counter-Terrorist Financing Act (AML/CFT Act).

2. These regulations shall take effect on 1 September 2002.

Definitions

3. For the purpose of these Regulations the following terms are defined as follows:

   (a) "AML/CFT" means anti-money laundering and counter-terrorist financing;

   (b) "beneficial owner", in relation to a customer of an accountable institution, means the natural person who ultimately owns or controls the customer or the person on whose behalf a transaction is being conducted and includes the person who exercises ultimate effective control over a body corporate or unincorporate;

   (c) CDD measures" or "customer due diligence measures" means the process of identifying the customer and obtaining information required by Part 3 of the AML/CFT Act and sections 4 and 5 of these Regulations;

   (d) "customer" means a person in whose name an account is opened or intended to be opened, or for whom the accountable institution undertakes or intends to undertake any transaction without an account being opened;

   (e) "FIUW" means the Financial Intelligence Unit of Westeros.

Customer identification and verification procedures

4. For the purpose of implementing customer identification and verification procedures pursuant to provisions of Part 3 of the AML/CFT Act, the following categories of customer and business relationship shall be considered to be high risk:

   (a) customers who are not residents of Westeros;

   (b) legal persons that are authorized to issue shares in bearer form; and

   (c) private banking relationships.

5. For the purpose of implementing customer identification and verification procedures pursuant to provisions of Part 3 of the AML/CFT Act, the following categories of types of customers shall be considered to be low risk:

   (a) accountable institutions;

   (b) companies that are listed on a public stock exchange, including Westeros Stock Exchange (WSE);

   (c) pension funds; and

   (d) superannuation funds.

Record keeping

6. An accountable institution is required to maintain all business correspondence relating to customer accounts for a period of five years following the closure of the account.

7. Upon production of proper authority, an accountable institution shall make available all records which must be kept pursuant to the AML/CFT Act and any related regulations and circulars, and, if necessary, shall provide such records as evidence for prosecution of criminal activity.

8. An accountable institution shall retain documents as originals or copies, in paper or electronic form or on microfilm, provided that they are admissible as evidence in a court of law of Westeros.

9. An accountable institution is required to maintain all records which must be kept pursuant to the AML/CFT Act and any related regulations or circulars in a manner which will allow them to be retrieved within a period of five business days.

Suspicious transaction reporting

10. Reporting entities pursuant to section 22 of the AML/CFT Law are required to submit suspicious transaction reports to the FIUFR in the manner and form prescribed by the FIUFR.

Internal controls

11. In the development of internal policies, procedures and controls to prevent and detect money laundering and terrorist financing, an accountable institution shall take into consideration money laundering and terrorist financing threats that may arise from the use of new or developing technologies, especially those that favour anonymity.

12. An accountable institution shall appoint a management level officer to be responsible for compliance with AML/CFT obligations. Such compliance officer shall have timely access to all customer records and other relevant information required to ensure compliance with AML/CFT obligations.

13. An accountable institution shall maintain an independent audit function to regularly test the effectiveness of internal policies, procedures and controls, and its compliance with regulatory requirements.

14. An accountable institution that is incorporated in Westeros shall develop a group policy on AML/CFT and extend this to all of its branches and subsidiaries outside Westeros.

15. An accountable institutions shall implement screening procedures to ensure high standards when hiring employees.

16. An accountable institution shall implement training programs for staff on AML/CFT requirements and any related internal policies, procedures and controls. Such programs should also include information about current money laundering and terrorist financing methods, techniques and trends.

Reporting Circular (2003)

1. A person shall file a suspicious transaction report (STR) with the Financial Intelligence Unit of Westeros (FIUW) no later than 24 hours after forming a founded suspicion that the transaction to which the business is a party or in any way involved is related to a crime pursuant to the Penal Code or any other Act.
2. The obligation to report suspicious transactions applies to all transactions, included attempted transactions.
3. When a person is submitting an STR to the FIUFR, as required by law, the following information shall be included:
   (a) information to identify the customer including, where available, the name, address and date of birth;
   (b) a description of the transaction; and
   (c) the reasons why the person filing the STR considers the transaction to be suspicious.
4. For the purposes of section 3(a), the customer identification information shall usually include, at a minimum, the customer's name, address and date of birth. Where such information is not available or cannot be collected without alerting the customer to the fact that an STR may be filed, the information identifying the customer shall be descriptive nature, describing, to the extent possible, the customer's physical appearance.
5. For the purposes of section 3(b), the information describing the transaction shall include, at a minimum, the transaction date and amount.
6. For the purposes of section 3(c), the reasons why the person filing the STR considers the transaction to be suspicious should include both the subjective reasons for the suspicion and any objective facts or indicators that could reasonably support that suspicion.
7. A person who is obligated to file or has filed an STR is required to provide the FIUFR information directly as requested, within 5 working days of such request being received.
8. Where, in the course of exercising its powers of supervision and monitoring as set out in the Financial Sector Supervision Act, the Financial Supervisory Authority detects a breach of the obligations of this Circular, it may take any of the following actions, as considered appropriate given the circumstances and severity of the situation:
   (a) issue a written warning;
   (b) issue an order to comply with specified instructions;
   (c) ordering the accountable institution entity to provide regular reports on the measures that are being taken to address the violation;
   (d) imposing fines on a reporting entity for non-compliance up to a maximum of EUR 200 000;
   (e) imposing fines on an owner, manager or employee of a reporting entity for non-compliance up to a maximum of EUR 100 000;
   (f) replacing managers, directors or controlling owners;
   (g) barring persons from employment within the sector, either for a specified period or for life;
   (h) suspend the accountable institution's license; or

(i) fail to renew or revoke the accountable institution's license.

9. Where the Financial Supervisory Authority takes any of the actions described in section 8 of this Circular, the accountable institution involved may have the decision reviewed by the Financial Sector Appeals Tribunal (FSAT). The FSAT shall remain independent and shall be comprised of two lay members and a chairperson who shall be a State Supreme Court Judge. A decision of the FSAT may be appealed to the State Supreme Court on a point of law.

10. This Circular is issued by the FIUFR pursuant to section 33 of the AML/CFT Act.

Guidance Note on Suspicious Transaction Reporting (2005)

Introduction

1. This Guidance Note is issued by the Financial Supervisory Authority (FSA) to provide guidance on how to comply with the obligation to report suspicious transactions set out in the Anti-Money Laundering and Counter-Terrorist Financing Act (AML/CFT Act), and the regulations and circulars issued thereunder.

2. Accountable institutions and other persons who carry on, manage or are employed by a business in Westeros (collectively referred to as reporting entities) are reminded of the importance of reporting suspicious transactions with a view to mitigating the risk of the financial system of Westeros being used for money laundering or terrorist financing.

Key concepts

3. Money laundering is a process intended to mask the benefits derived from criminal conduct (proceeds of crime) so that they appear to have originated from a legitimate source. Generally, there are three stages to the money laundering process, during which there may be numerous transactions that could alert a person to the money laundering activity:

(a) Placement - The proceeds are physically disposed of;

(b) Layering - The proceeds are separated from their source by creating layers of financial transactions designed to disguise the audit trail; and

(c) Integration - The proceeds are apparently legitimised. If the layering process succeeds, the integration schemes place the laundered funds back into the economy so that they re-enter the financial system appearing to be legitimate business funds.

4. Terrorism seeks to influence or compel governments into a particular course of action or seeks to intimidate the public or a section of the public through the use or threat of violence, damage to property, danger to life, serious risks to health or safety of the population or disruption of key public services or infrastructure. Terrorists require funds to carry out acts of terrorism and terrorist financing provides the funds needed. Sources of terrorist financing may be legitimate or illegitimate. It may be derived from criminal activities such as kidnapping, extortion, fraud or drug trafficking. It may also be derived from legitimate income such as membership dues, sale of publications, donations from persons or entities sympathetic to their cause, and sometimes income from legitimate business operations belonging to terrorist organisations. Terrorist financing involves amounts that are not always large and the associated transactions may not necessarily be complex given that some sources of terrorist funds may be legitimate. However, the methods used by terrorist organisations to move, collect, hide or make available funds for their activities remain similar to those used by criminal organisations to launder their funds. This is especially so when the funds are derived from illegitimate sources, in which case, the terrorist organisation would have similar concerns to a typical criminal organisation in laundering the funds.

Obligation to report

5. All accountable institutions under the AML/CFT Act and any other person who carries on, manages or is employed by a business in Westeros must comply with the obligation to report suspicious transactions pursuant to Part 4 of the AML/CFT Act.

6. The obligation to report suspicious transactions applies to all transactions and attempted transactions, regardless of their amount, and regardless of whether they may be related to tax matters.

7. The obligation to report is triggered when such a person knows or ought reasonably to have known or suspected, on the basis of a founded suspicion, that a transaction to which the business is a party or in any way involved is related to a crime pursuant to the Penal Code or any other Act.

8. A “founded suspicion” is a subjective suspicion that is “founded” (i.e. based) on at least one objective fact or indicator which could reasonably lead to the conclusion that the transaction is related to a serious crime. This is a very low level of proof, but means that there must be at least some justification for the suspicion based on at least one objective fact.

Internal controls to implement the reporting obligation

9. Accountable institutions are required to establish internal procedures for reporting suspicious transactions. This includes having adequate processes and systems in place for detecting, identifying, handling and reporting suspicious transactions. Other reporting entities are encouraged to establish similar types of processes.

Identification of suspicious transactions

10. Reporting entities should consider the terrorist lists published by the Ministry of Foreign Affairs when determining whether a particular transaction is suspicious. Reporting entities should consider filing an STR even though there is no positive match against any name if the surrounding circumstances raise sufficient suspicions.

11. Reporting entities are encouraged to familiarize themselves with the studies of money laundering and terrorist financing trends, methods and techniques (typologies) which are published periodically by the FIUFR and by the typologies studies published on the public website of the Financial Action Task Force (FATF). Examples of suspicious transactions set out in these studies are not intended to be exhaustive and are only examples of ways money laundering and terrorist financing may take place.

12. If any transactions or patterns of transactions matching such typologies, or transactions that are otherwise suspicious, are identified, this should prompt further enquiries by the reporting entity. However, such enquiries should be conducted in a discrete manner, so as not to alert the customer to the fact that a suspicion has been aroused or an STR may be filed.

Reporting suspicious transactions

13. Reporting entities should have effective and efficient procedures in place for reporting suspicious transactions. This includes having an internal process for evaluating, without delay, whether a matter should be referred to the FIUFR. Where a suspicion is founded, there should be mechanisms in place to ensure that the FIUFR receives the STR within 24 hours.

14. Reporting entities must file STRs electronically. The public website of the FIUFR contains electronic forms for this purpose. In urgent cases, reporting entities are also encouraged to contact the FIUFR by telephone and the emergency number posted on its website.

Record keeping

15. Reporting entities should maintain a complete file of all transactions that have been considered as suspicious, including transactions that are not ultimately reported to the FIUFR because further inquiries demonstrate that the initial suspicion is unjustified.

Financial Sector Supervision Act

1. The Financial Supervisory Authority (FSA) is responsible for monitoring and supervising the following entities (which shall be collectively referred to as "supervised entities") for compliance with all applicable laws:
   (a) banks;
   (b) savings and loan institutions;
   (c) credit unions;
   (d) securities firms;
   (e) securities brokers;
   (f) insurance companies;
   (g) insurance agents;
   (h) money remitters; and
   (i) foreign exchange dealers.
2. In the course of fulfilling its responsibilities, the FSA shall have the authority to compel production of any information that relates to the organisation, functioning, situation, customer relationships, transactions and management of a supervised entity.
3. In the course of fulfilling its responsibilities, the FSA shall have the authority to gain access to any records, documents, information, premises, director, manager or employee of a supervised entity. It shall also have the authority to take examine and take copies of any records, document or information and to take statements from any director, manager or employee of a supervised entity.
4. If a supervised entity knowingly and intentionally denies the FSA access to its records or premises, or knowingly supplies inaccurate or incomplete information, it shall be liable to pay a fine of up to EUR 50 000.
5. If an employee of a supervised entity intentionally provides a false statement or false information to the FSA, the employee shall be liable to pay a fine of up to EUR 20 000.

Protection of Financial Information Act (excerpts)

Introduction

1. The purpose of this Act is to ensure that financial information is appropriately safeguarded and only used in accordance with the law.

Definitions

2. For the purpose of this Act, the term "financial information" means customer identification information, account information and transaction details.

3. For the purpose of this Act, the term "financial institution" means a:

   (a) bank;

   (b) savings and loan institution;

   (c) credit union;

   (d) securities firm;

   (e) securities broker;

   (f) insurance company;

   (g) insurance agent;

   (h) money remitter;

   (i) foreign exchange dealer; and

   (j) other reporting entities as defined in the AML/CFT Act.

Duty of confidentiality

4. A financial institution is required to maintain all financial information in a secure manner, such that it cannot be accessed by unauthorized personnel.

5. A financial institution and its owners, directors, managers and employees are prohibited from disclosing financial information, other than as specifically provided in the law.

6. No financial institutions or its owners, directors, managers or employees shall be subject to civil or criminal liability for disclosing financial information, provided that such disclosure is specifically required by any legislative, regulatory or other administrative provision, and is made in good faith.

7. No government ministry, agency, department or unit that collects and maintains financial information shall disclose such information other than as specifically provided in the law.

Offences

8. A natural person who breaches a provision of this Act commits an offence punishable by a maximum term of imprisonment of 2 years and/or a fine up to EUR 100 000.

9. A legal person who breaches a provision of this Act commits an offence punishable by a fine of up to EUR 200 000.

Interpretation Act (excerpts)

1. When interpreting the provision of a written law, an interpretation that promotes the purpose or object underlying the written law (whether that purpose or object is expressly stated in the written law or not) shall be preferred to an interpretation that would not promote that purpose or object.

2. When interpreting the provision of any written law, the language should be given as broad an interpretation as is reasonably possible on a plain reading of the legislation.

3. Every Act and Code issued by the Parliament of Westeros is primary legislation which shall come into force, upon or following publication in the Gazette of Westeros, as follows:

   (a) where a particular day for its coming into operation is specified by the Act or Code, on the expiration of the previous day; or

   (b) where the day of its coming into operation is the date of its publication in the Gazette, on the expiration of the previous day.

4. Where any Act or Code, or any part thereof, is repealed, subsidiary legislation issued under it shall remain in force so far as it is not inconsistent with the repealing Act or Code and unless the contrary intention appears until it has been revoked or replaced by subsidiary legislation issued or made under the provisions of the repealing Act or Code.

5. An Act or Code may authorise a Minister to issue subsidiary legislation, meaning any order in council, proclamation, rule or regulation which imposes mandatory requirements, the non-compliance with which are punishable by sanctions. Where a duly authorized Minister exercises the power to issue subsidiary legislation, such legislation shall come into force, upon or following publication in the Gazette of Westeros, as follows:

   (a) where a particular day for its coming into operation is specified by the order in council, proclamation, rule or regulation, on the expiration of the previous day; or

   (b) where the day of its coming into operation is the date of its publication in the Gazette, on the expiration of the previous day.

6. An Act or Code may authorise a Minister or government authority to issue directions or circulars, the non-compliance with which are punishable by sanctions. Where a duly authorized Minister or government authority exercises the power to issue a direction or circular, such direction or circular shall come into force, upon or following its issuance, as follows:

   (a) where a particular day for its coming into operation is specified by the direction or circular, on the expiration of the previous day; or

   (b) where the day of its coming into operation is the date of its issuance, on the expiration of the previous day.

Penal Code (excerpts)

Section 2:

A person who is convicted of an offence pursuant to this Code may, additionally, be subject to civil or administrative proceedings arising from the same conduct.

Section 10:

A "serious crime" is any offence that is set out in this Code and is subject to a maximum penalty of more than one year imprisonment.

Section 313:

It is an offence to attempt to commit any of the offences set out in this Code.

Section 32:

It is an offence to conspire to commit any of the offences set out in this Code.

Section 33:

It is an offence to counsel someone in the commission of any of the offences set out in this Code.

Section 34:

It is an offence to facilitate the commission of any of the offences set out in this Code.

Section 35:

It is an offence to aid and abet the commission of any of the offences set out in this Code.

Section 40:

Anyone who has been convicted of charges involving theft, fraud, embezzlement, money laundering, terrorist financing, corruption, bribery or abuse of public office is permanently disqualified from being on the board of directors of any company, unless the conviction has been overturned on appeal.

Section 1409:

(a) A natural person who knowingly creates, manufactures, produces, distributes, pirates, copies, buys, possesses or otherwise deals in counterfeit products of any form, including any type of audio or visual recording, commits an offence punishable by a maximum term of imprisonment 5 years and/or a maximum fine of EUR 250 000.

(b) A legal person that knowingly creates, manufactures, produces, distributes, pirates, copies, buys, possesses or otherwise deals in counterfeit products of any form, including any type of audio or visual recording, is punishable by a maximum fine of EUR 500 000 and any directors or senior managers who knowingly participated in such activities are punishable by a maximum term of imprisonment 5 years and/or a maximum fine of EUR 250 000.

(c) A legal person who launders the proceeds of the offences described in this section commits an offence pursuant to section 555 of this Code and is punishable by a maximum fine of EUR 500 000. Any directors or senior managers who knowingly participated in such activities commit an offence and are punishable pursuant to section 555 of this Code.

Section 282:

(a) A natural person who knowingly commits any of the following environmental crimes is punishable by a maximum term of imprisonment 5 years and/or a maximum fine of EUR 250 000:

(i) an unauthorised disposal of material, chemical or nuclear waste in violation of section 89 of the Environmental Protection Act;

(ii) an act which seriously endangers a protected animal or plant species as defined in sections 34 to 46 of the Endangered Species Act;

(iii) an act which seriously endangers fishing stocks located within the territorial waters of Westeros as defined in sections 22 to 26 of the Maritime Fisheries Act; or

(iv) an act which seriously endangers protected habitats and forested areas within the territory of Westeros as defined in sections 21 to 23 of the National Parks and Forests Act.

(b) A legal person that knowingly commits any of the environmental crimes described in subsection (a) is punishable by a maximum fine of EUR 500 000 and any directors or senior managers who knowingly participated in such activities are punishable by a maximum term of imprisonment 5 years and/or a maximum fine of EUR 250 000.

(c) A legal person who launders the proceeds of the offences described in this section commits an offence pursuant to section 555 of this Code and is punishable by a maximum fine of EUR 500 000. Any directors or senior managers who knowingly participated in such activities commit an offence and are punishable pursuant to section 555 of this Code.

Section 333:

Any person who unlawfully and intentionally delivers, places, discharges or detonates an explosive or other lethal device in, into or against a place of public use, a State or government facility, a public transportation system or an infrastructure facility with the intent to cause death or serious bodily injury, or to cause extensive destruction of such a place, or to attempt or threaten to commit such an act, commits an offence punishable by a maximum of 30 years imprisonment.

Section 334:

Any person who, on board an aircraft in flight, unlawfully, by force or threat thereof, or by any other form of intimidation, seizes, or exercises control of, that aircraft, or attempts or threatens to perform any such act., commits an offence punishable by a maximum of 30 years imprisonment.

Section 335:

Any person who unlawfully and intentionally:

(a) performs an act of violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that aircraft;

(b) destroys an aircraft in service or cause damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight;

(c) places or causes to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or cause it damage thereby rendering it incapable of flight or which may endanger its safety in flight;

(d) destroys or damages air navigation facilities or interfere with their operation, if any such act is likely to endanger the safety of an aircraft in flight;

(e) knowingly communicate any false information which endangers the safety of an aircraft in flight.;

(f) uses any device, substance or weapon to perform an act of violence against a person at an airport serving international civil aviation which causes or is likely to cause serious injury or death;

(g) uses any device, substance or weapon to destroy or seriously damage the facilities of an airport serving international civil aviation or aircraft not in service located thereon or disrupt the services of the airport, if such an act endangers or is likely to endanger safety at that airport; or

(h) attempts or threatens to commit any of the acts set out in paragraphs (a) to (g).

commits an offence punishable by a maximum of 30 years imprisonment.

Section 336:

Any person who intentionally commits, attempts to commit or threatens to commit:

(a) a murder, kidnapping or other attack upon the person or liberty of an internationally protected person; or

(b) a violent attack upon the official premises, the private accommodation or the means of transport of an internationally protected person likely to endanger his person or liberty,

commits an offence punishable by a maximum of 30 years imprisonment.

Section 337:

Any person commits an offence of hostage-taking, punishable by a maximum of 20 years imprisonment, who seizes or detains and threatens to kill, to injure or to continue to detain another person as a hostage in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or abstain from doing any act as an explicit or implicit condition for the release of the hostage. It is also an offence to attempt or threaten to commit such an act.

Section 3308:

Any person who unlawfully and intentionally:

(a) seizes or exercises control over a ship by force or threat thereof or any other form of intimidation;

(b) performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship;

(c) destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship;

(d) places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship;

(e) destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship;

(f) communicates information which he knows to be false, thereby endangering the safe navigation of a ship;

(g) injures or kills any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (f);

(h) uses against or on a fixed platform or discharges from a fixed platform any explosive, radioactive material or BCN weapon in a manner that causes or is likely to cause death or serious injury or damage; or discharges, from a fixed platform, oil, liquefied natural gas, or other hazardous or noxious substance in such quantity or concentration that causes or is likely to cause death or serious injury or damage; or threatens to commit such an offence; or

(i) attempts or threatens to commit any of the acts set out in paragraphs (a) to (h).

commits an offence punishable by a maximum of 30 years imprisonment.

Section 3309:

It is an offence, punishable by a maximum of 30 years imprisonment, to intentionally and without lawful authority do any act which constitutes:

(a) the receipt, possession, use, transfer, alteration, disposal or dispersal of nuclear material and which causes or is likely to cause death or serious injury to any person or substantial damage to property;

(b) a theft or robbery of nuclear material;

(c) an embezzlement or fraudulent obtaining of nuclear material;

(d) an act constituting a demand for nuclear material by threat or use of force or by any other form of intimidation; or

(e) an attempt or threat to use nuclear material to cause death or serious injury to any person or substantial property damage, or

(f) the commission of any offence described in this section for the purpose of compelling a natural or legal person, international organization or State to do or to refrain from doing any act.

Section 555:

A person who:

(a) converts or deals in any way with proceeds of a serious crime for the purpose of concealing the origin of those proceeds, or for the purpose of helping another person to avoid criminal prosecution or confiscation proceedings;

(b) disguises or in any way obscures the source, location, movement, character or any other identifying aspect of proceeds of a serious crime, including any type of rights to those proceeds; or

(c) acquires or possesses proceeds,

knowing that such proceeds are the proceeds of a serious crime, commits an offence punishable by a maximum term of imprisonment of 5 years and/or a maximum fine of EUR 250 000.

Section 556:

For the purposes of section 555 of this Code, the term “proceeds” means any type of cash, cheques, monetary instruments (including, but not limited to bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts or letters of credit, and any interest, dividends or other income on or value accruing from or generated by them), goods and moveable assets of every kind, including any legal documents or instruments evidencing title to, or interest in such assets, where such proceeds are derived from or obtained through the commission of any serious crime as that term is defined in section 10 of this Code.

Supreme Court Act (1965) (excerpts)

Section 2: Decisions of the Supreme Court of Westeros are binding on all State Courts and State Courts of Appeal, regardless of whether the case relates to a criminal or civil matter.

Public Prosecutions Act (2006)

1. The purpose of this Act is to ensure that offences are prosecuted in a fair and just manner by:
   (a) establishing the position of the Attorney General;
   (b) establishing the Attorney General's Office (AGO); and
   (c) ensuring the independence of the Attorney General and the AGO.
2. In this Act, the term "prosecution" includes the decision whether or not to prosecute, the prosecution proceeding itself and any other matters arising from that prosecution, including interlocutory applications, appeals, and applications to freeze, seize or confiscate property.
3. There shall be an Attorney General who shall be the head of the AGO and who:
   (a) shall be appointed by the Minister of Justice, in consultation with the Chief Justice of the Supreme Court of Westeros and the Director of the Bar Association of Westeros;
   (b) is a lawyer of good standing with at least 15 years' experience, who has graduated from an accredited law school of Westeros and who has never been convicted of a criminal offence or declared bankrupt;
   (c) shall ensure that the AGO conducts all prosecutions independently, impartially and fairly in accordance with the provisions of this Act; and
   (d) shall ensure that the AGO is staffed by lawyers of good standing who have graduated from an accredited law school of Westeros and who have never been convicted of a criminal offence or declared bankrupt.
4. There shall be an AGO that is headed by the Attorney General and which:
   (a) is an independent agency located within the Ministry of Justice;
   (b) is responsible for conducting all criminal prosecutions that are within the jurisdiction of the Ministry of Justice, including prosecutions of Penal Code offences and criminal offences pursuant to any other Act;
   (c) shall carry out its functions independently, impartially and fairly; and
   (d) has the sole discretion to determine whether a prosecution should proceed.
5. The AGO shall proceed with a prosecution if:
   (a) there is sufficient evidence, which is likely to be admissible, on each element of the offence, such that there is a prima facie case to present to the court; and
   (b) the prosecution is not being brought for an improper purpose that would bring the administration of justice into disrepute.
6. All AGO staff, including the Attorney General, must pass a security clearance procedure (which includes a criminal records check) and sign a confidentiality agreement at the start of their employment. Any AGO staff member who is found to be in breach of the confidentiality agreement shall be dismissed.

Police and Intelligence Services Act (1985)

Part 1—Structure and jurisdiction of the National Policy Authority (NPA)

1. The National Police Authority (NPA) is the national police force of Westeros and shall be headed by the National Police Commissioner. It shall have full operational independence and shall maintain at least one office in each of the states of Westeros.

2. The NPA has jurisdiction to investigate any offence under the Penal Code, Anti-Corruption and Bribery Act, Securities Act, and the Protection of Financial Information Act.

Part 2—Powers

3. In the course of inquiring into or investigating a matter within the NPA's jurisdiction, or participating in related proceedings (including proceedings undertaken for the purpose of freezing, seizing or confiscating property), an officer of the NPA may:

    1. enter any place or vehicle and remain for a reasonable time, subject to the provisions section 4 below;

    2. search any place or person, subject to the provisions section 4 below;

    3. seize any property, including documents or electronically-held information;

    4. stop and detain any person for a reasonable period of time, or carry out an arrest; and

    5. obtain a statement from any person.

4. If the place is a dwelling, an officer of the NPA may enter without the consent of the occupier:

    to arrest or detain a person, only if the officer has reasonable grounds to suspect that the person to be arrested or detained is located within the dwelling; or

    6. to search, only if the officer has obtained from a judge a warrant that authorises a search of the dwelling. The application for a search warrant shall be based on reasonable and probable grounds to believe that evidence of a matter within the NPA's jurisdiction may be located in the dwelling.

5. An officer of the NPA may obtain from a judge an order compelling any natural or legal person to produce any property, including documents or electronically-held information. The application for a production order shall be based on reasonable and probable grounds to believe that evidence of a matter within the NPA's jurisdiction may be produced.

6. If there are reasonable and probable grounds to believe that an investigation may involve an organised criminal group, an officer of the NPA may:

    (a) may obtain from a judge an order authorising the use of a wiretap;

    (b) conduct a controlled delivery of an illegal drug; or

    (c) carry out an undercover operation.

7. An officer of the NPA may postpone or waive the exercise of any powers set out in this Act for the purpose of doing any lawful act which could further an investigation, including gathering additional evidence, identifying suspects and witnesses, or freezing and seizing property.

OFFCUTS

RESOURCES AND ORGANISATION OF COMPETENT AUTHORITIES

Attorney General's Office

81. The AGO is a fully independent agency that is located within the Ministry of Justice. It has its headquarters in King's Landing and a regional office in each of Westeros's four States. The AGO is headed by the Attorney General who is responsible for ensuring that all AGO prosecutions are conducted independently, impartially and fairly (PP Act, s.3(c)).

82. The AGO has two specialised units that are relevant to AML/CFT—the Financial Crimes Unit (AGO/FCU) which is responsible for prosecuting money laundering and terrorist financing and the Asset Confiscation Unit (AGO/ACU) which is responsible for handling applications relating to the freezing, seizing and confiscation of assets. The AGO/FCU prosecutes all financial crimes (including terrorist financing) and associated money laundering.

83. The AGO is responsible for providing the public prosecution service and conducting all prosecutions within the jurisdiction of the Department of Justice, including prosecutions pursuant to the Penal Code (such as money laundering) and any other Act (including terrorist financing offences pursuant to the Terrorist Financing Act) (PP Act, s.4(b)). It has full operational independence and autonomy (Public Prosecutions Act (PP Act), s.4).

84. The AGO's annual budget is about EUR 32 million.

85. The AGO employs up to 190 prosecutors and 50 administrative support staff. The AGO/FCU and AGO/ACU are staffed with 15 and 12 prosecutors respectively. The AGO has sufficient technical resources to perform its functions, including electronic legal research and case management tools.

86. The Prosecutor General and other prosecutors who work for the AGO are must be lawyers of good standing who graduated from an accredited Westeros law school and who have never been convicted of a criminal offence or declared bankrupt (PP Act, s.3(d)). The Prosecutor General and all staff of the AGO must sign a confidentiality agreement at the start of their term of employment (PP Act, s.6). Additionally, all staff receive periodic training (every 2 years) on ethical issues, including the duty to maintain confidentiality.

87. At the start of their employment, prosecutors receive extensive and relevant training on general issues such as how to conduct a prosecution, draft legal briefs, handle evidentiary issues, interview witnesses, conduct cross-examination, research legal issues and comply with the rules of criminal procedure. Refresher courses on these and more advanced issues are provided annually.

88. Prosecutors in the AGO/FCU and AGO/ACU receive a special 6-month training concerning how to prosecute financial crimes. This training is also refreshed annually.

National Police Authority

89. The structure and responsibilities of the NPA are set out in the Police and Intelligence Services Act (PIS Act). The NPA is a fully independent agency that is located within the Ministry of Justice, and has its headquarters in King's Landing and a regional office in each of Westeros's four states. It was established pursuant to section 1 of the PIS Act.

90. The NPA is headed by the National Police Commissioner and is comprised of a general Investigations Division and five specialised investigative units: the Anti-Corruption Unit (which handles corruption and bribery investigations, including referrals from the ACA), the Drug Squad

(which involves investigations involving illicit drugs), the Fraud Squad (which handles fraud-related investigations), the Major Crimes Unit (which handles investigations involving murder, robbery and serious assaults), and the Organised Crime Squad (which handles major investigations involving organised crime groups).

91. The NPA's annual budget is currently about EUR 14 million. The NPA employs 1,375 police officers and 500 administrative/support staff.

92. All employees undergo rigorous background and security checks. Persons with a criminal record are not eligible for employment. All employees undergo follow-up background checks every 2 years, and periodic random drug checks throughout their careers. Persons found to be using illegal drugs face disciplinary action and, in the case of recidivism, dismissal. All NPA employees are required to sign confidentiality agreements.

93. New NPA officers must successfully complete an intensive 18-month training program at Westeros Police Academy which teaches ethics (with practical law enforcement applications), general investigative techniques (including surveillance and undercover techniques), methods of evidence gathering (including search and seizure), physical fitness and defensive tactics, use of firearms, interviewing techniques, and criminal procedure (including how to apply for a search warrant and a subpoena for the production of documents). Each year, officers must undergo 4 additional weeks of more specialized training which includes courses on the investigation of offences related to national security threats, such as terrorism offences. Members of the Fraud Squad must pass a 6-week course on investigating financial crimes, and are also required to attend at least 30 hours of additional training on financial investigations during each year that they are with the Squad.

STATISTICS

STATISTIC PROVIDED BY THE AGO NPA

ML investigations, prosecutions and convictions:

Year	Number of investigations for ML	Number of prosecutions for ML	Number of convictions for ML in State Courts
2000	0	0	0
2001	0	0	0
2002	0	0	0
2003	2	0	0
2004	4	1	0
2005	6	4	3
2006	18	10	8
2007	29	12	10
2008	33	10	9
2009	15	5	2
2010	16	6	3
2011	14	7	2
2012	14	5	3
TOTALS	**151**	**60**	**40**

Breakdown of NPA units that conducted money laundering investigations							
YEAR	**Anti-Corruption Unit**	**Drug Squad**	**Fraud Squad**	**Major Crimes Unit**	**Organised Crime Squad**	**General Investigative Division**	**TOTAL**
2003	0	0	2	0	0	0	**2**
2004	0	1	3	0	0	0	**4**
2005	0	2	2	1	1	0	**6**
2006	0	3	3	1	2	1	**10**
2007	0	3	5	2	2	1	**13**
2008	0	3	3	2	2	2	**12**
TOTAL	**0**	**12**	**18**	**6**	**7**	**4**	**47**

Police Officers assigned to NPA units, as of 1/1/2013	
General Investigations Division	720
Anti-corruption Unit	60
Drug Squad	195
Fraud Squad	80
Major Crimes Unit	200
Organised Crimes Unit	120

STATISTIC PROVIDED BY THE AGO

Convictions in State Courts for other Serious offences

	2008	2009	2010	2011	2012
Participation in organised crime groups	15	21	23	26	24
Illicit trafficking in narcotic drugs	47	25	30	28	28
Corruption and bribery	14	11	12	16	15
Fraud	28	39	35	34	29
Insider trading	8	7	5	7	6

Statistics – Breakdown of the types of predicate offences underlying ML convictions

Underlying predicate offence	Number
Drug trafficking	7
Unlawful production of illicit drugs	2
Participation in an organised crime organisation	6
Securities-related fraud	4
Fraud (other)	3
Counterfeiting currency	2
Theft	2
Murder	1
TOTALS	**27**

Sanctions applied to persons convicted of ML offences*:

Year	Imprisonment sanctions		
	Up to 1 year	1-3 years	3-5 years
2005	3	-	-
2006	7	1	-
2007	7	2	1
2008	8	-	1
2009	1	-	1
2010	2	1	-
2011	1	1	-

* Most of these ML investigations were conducted by the Fraud Squad.

STATISTIC PROVIDED BY THE FIU

NUMBER OF ENTITIES REPORTING ANNUALLY TO THE FIU –BY SECTOR						
Type of reporting entity	**Number of entities in the sector**	**2005**	**2006**	**2007**	**2008**	**Average percentage of institutions reporting in the sector annually**
Banks	**16**	16	16	15	16	**98%**
Savings and loan institutions	**4**	3	3	4	3	**81%**
Credit unions	**2**	1	2	2	2	**88%**
Securities firms	**14**	1	2	1	2	**11%**
Insurance companies	**3**	1	3	2	2	**67%**
Independent insurance agents	**2**	1	2	2	1	**75%**
Money remitters	**67**	45	64	62	60	**86%**
Foreign exchange dealers	**42**	31	33	38	37	**83%**

STR FILINGS IN THE SECURITIES SECTOR – BREAKDOWN BY SECURITIES FIRM					
Securities firms	**2005**	**2006**	**2007**	**2008**	**TOTALS**
Firm 1	0	0	0	0	**0**
Firm 2	0	0	0	0	**0**
Firm 3	7	6	6	7	**26**
Firm 4	0	0	0	0	**0**
Firm 5	0	0	0	0	**0**
Firm 6	0	0	0	0	**0**
Firm 7	0	0	0	0	**0**
Firm 8	0	3	0	3	**6**
Firm 9	0	0	0	0	**0**
Firm 10	0	0	0	0	**0**
Firm 11	0	0	0	0	**0**
Firm 12	0	0	0	0	**0**
Firm 13	0	0	0	0	**0**
Firm 14	0	0	0	0	**0**
TOTALS	**7**	**9**	**6**	**10**	**32**

STR Receipt and Dissemination

Year	STRs Received	STRs Disseminated to law enforcement
2007	492	93
2008	512	65
2009	550	48
2010	536	26
2011	483	30
2012	601	18

DRAFT TECHNICAL COMPLIANCE ANNEX

The following is the Team's summary analysis of technical compliance with the recommendations relevant to IO.7 prepared ahead of the onsite visit to Westeros based on the materials provided. A number of information gaps with TC compliance remain to be addressed during the onsite visit.

3.2 Technical Compliance (R.3, R.20, R.30, R.31)

Recommendation 3 – Money laundering offence

- Scope of coverage of predicate offences – (clarification of the gaps needed)
- The definition of property does not cover immovable assets (case law or other means to clarify coverage of direct & indirect property is covered)
- Recognition of foreign predicates is not clearly established in statute (case law or other means to clarify)
- Available sanctions are not proportionate or dissuasive for natural persons (case law or other means to clarify scope of coverage legal persons)
- Risk & context facts include the sources of proceeds of crime and channels of laundering

Rating:

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

- No agency designated to investigate TF
- Deficiencies in R.3

Rating:

Recommendation 31 – Powers of law enforcement and investigative authorities

.

- No powers or special investigative techniques to investigate TF
- Special investigative techniques limited to organised criminal group and not available for accessing computer systems remotely

Rating:

MER TEMPLATE

3. LEGAL SYSTEM, OPERATIONAL ISSUES, REPORTING, AND SANCTIONS

***Key Findings** [less than half a page]*

Assessors should briefly summarise their conclusions for this chapter, highlighting the most significant findings on risk and context, as well as technical compliance and effectiveness.

3.2 Technical Compliance (R.3, R.30, R.31) [under one page in total]

Briefly summarise the overall level of compliance with each of Recommendations 3, 30 and 31 – this should be built on the draft technical compliance annex. The summary points should include any deficiencies that are particularly significant (more minor/technical deficiencies are dealt with in the technical annex). NB analysis of all the criteria should not be included here, but will be set out separately in the technical annex. Assessors may also note any new, unusual or otherwise good technical requirements or practises.

Noting the characteristics of an effective system for IO7, assessors may wish to include summary points on any elements of Recommendations 1,2,37,39 or 40 that are particularly significant to Immediate Outcome 7.

Provide a rating for each of recommendations 3, 30 and 31.

Recommendation 3 – Money laundering offence

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Recommendation 31 – Powers of law enforcement and investigative authorities

Other Recommendations relevant to IO7 – TC compliance issues

3.4 Effectiveness: Immediate Outcome 7 (ML investigation and prosecution) [under one page]

This section should set out assessors' analysis of Immediate Outcome 7***.***

The first paragraph(s) should note any general considerations regarding the country's risks and context which affect the assessment.

This section should also summarise assessors' general impression of whether the country appears to exhibit the *characteristics of an effective system*.

Assessors should set out their analysis on each of the Core Issues with two or three dot points on each. It may be appropriate to consider each of the core issues in turn or to set out the analysis sector-by-sector; or to proceed step-by-step with the analysis of each element of the process covered by the Outcome. Assessors ***should highlight any general conclusions they reach on them***.

Assessors should note the main sources of information and evidence used (*e.g.* sections (a) and (b) of each Immediate Outcome). Assessors are not required to use all the information noted in the methodology – but should set out here the information and evidence which has a material influence on their conclusion and note any technical compliance issues which influence the level of effectiveness.

Finally, set out overall conclusions on the Immediate Outcome: the extent to which the country is achieving the outcome, and the main reasons for the conclusion. The overall level of effectiveness should take into account: (a) the core issues, (b) any relevant technical compliance issues/deficiencies; (c) risks and contextual factors; and (d) the level of effectiveness in other Immediate Outcomes that are relevant. In cases where there seems to be a significant inconsistency between the level of effectiveness and the level of technical compliance with the relevant Recommendations, assessors should explain in detail the basis and the specific reasons for their conclusions. Assessors' conclusions should be primarily descriptive, and should make clear the main reasons why the outcome is or is not achieved.

3.5 Rating for Effectiveness

Conclude with the rating for effectiveness.

3.6 Recommendations [4-6 prioritised recommendations]

This section should set out four to six prioritised recommendations on how the country should improve its level of effectiveness and its level of compliance with the FATF Recommendations. The section should include assessors' recommendations regarding the Immediate Outcomes and Recommendations covered in this chapter of the MER. Assessors will therefore need to consider a range of Outcomes and Recommendations, and actions aimed at addressing both technical deficiencies and practical issues of implementation or effectiveness, and decide which actions should be prioritised.