GOVERNMENT OF BERMUDA

NAMLC CONSULTATION PAPER

Proposed Amendments to the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 to incorporate Proliferation Financing (PF) Risk Assessment and Mitigating Measures for AML/ATF Regulated Entities

JANUARY 28, 2026

THE NATIONAL ANTI-MONEY LAUNDERING COMMITTEE (NAMLC)
Ministry of Finance, 2nd Floor, Government Administration Building, 30 Parliament St., Hamilton, HM 12, BERMUDA

Table of Contents

I. INTRODUCTION AND BACKGROUND

Amendments to Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008

1. The National Anti-Money Laundering Committee (NAMLC) in accordance with its statutory mandate under section 49 (1) (a) of the Proceeds of Crime Act 1997 ("POCA"), is responsible for advising the Minister of Justice and the Minister of Finance on matters related to the detection and prevention of money laundering (ML), terrorist financing (TF), and the financing of proliferation (PF). In fulfilling this role, NAMLC continues to take steps to ensure Bermuda's framework remains effective and aligned with the Financial Action Task Force (FATF) 40 Recommendations and Eleven Immediate Outcomes, collectively referred to as "the Standards" to combat ML, TF and PF.

2. NAMLC has reviewed the recent amendments to Recommendation 1 (R.1) of the FATF Standards which now require countries and financial institutions (FIs), designated non-financial businesses and professions (DNFBPs), and virtual asset service providers (VASPs)[1] to identify, assess, understand and mitigate their proliferation financing (PF) risks. These obligations can be addressed within existing targeted financial sanctions (TFS) frameworks and/or compliance programmes, without the need to create separate processes for PF risk assessment or mitigation. Under R.1, PF risk refers strictly and only to the potential breach, non-implementation or evasion of the TFS obligations outlined in Recommendation 7.

3. In accordance with the updated FATF requirements, Bermuda has amended Section 49(1) of the Proceeds of Crime Act (POCA) 1997 to establish the legislative foundation for a national-level PF risk assessment. NAMLC has been designated as the coordinating body responsible for identifying, assessing and understanding Bermuda's PF risks as well as ensuring that these risk assessments remain current.[2]

4. Bermuda completed its first PF National Risk Assessment (NRA) in 2025. The assessment revealed that PF risk evaluation and mitigation measures for AML/ATF regulated entities are currently absent from the legislative framework. The findings were shared with stakeholders in both public and private sectors on October 22 and 23, 2025, respectively.

5. Within Bermuda, the AML/ATF regulated entities which fall within the FATF's definition of FIs and DNFBPs are set out in the suite of Proceeds of Crime legislation. They comprise:

    - AML/ATF Regulated Financial Institutions including Digital Asset Businesses (DABs);

[1] In Bermuda, Digital Asset Businesses (DABs) fall within the classification of Financial Institutions (FIs)
[2] The Proceeds of Crime (Miscellaneous) Act 2025 came into operation on the 20th of October 2025.

- independent professionals – that is, lawyers and accountants;
- casino operators;
- dealers in high value goods;
- real estate brokers and real estate professions.

6. The amendments to the Proceeds of Crime (Anti-Money Laundering/ Anti-Terrorist Financing) Regulations are aimed at ensuring full compliance with R.1.

7. The proposed legislative amendments are intended to ensure that obligations related to risk assessment and mitigation for FIs and DNFBPs are fully integrated into Bermuda's regulatory framework.

II. THE PROPOSED CHANGES

8. The following items have been identified as amendments that are required to ensure compliance with the revised FATF Standards:

A. Definitions of Proliferation Financing (PF) and Counter-Proliferation Financing (CPF):

9. The Proceeds of Crime Regulations do not contain a definition in respect of "proliferation" or "proliferation financing". Additionally, these terms are not defined in the suite of Proceeds of Crime legislation.

B. Requirement for AML/ATF Regulated Entities to Identify and Assess their PF risks:

10. The proposed amendments seek to establish legislative obligations requiring AML/ATF regulated entities to identify and assess their PF risks. In line with the **FATF criterion 1.15(a)** these obligations include requiring entities to:
    - 1.15(a)(i) document their PF risk assessments;
    - 1.15(a)(ii) keep these assessments up to date; and
    - 1.15(a)(iii) have appropriate mechanisms to provide PF risk assessment information to competent authorities and self-regulated bodies (SRBs.)

C. Requirement for AML/ATF Regulated Entities to Mitigate their PF risks:

11. The proposed amendments also aim to establish legislative obligations requiring AML/ATF regulated entities to mitigate their PF risk through measures consistent with the requirements of **FATF criterion 1.15(b – e).** These obligations include requiring entities to:
    - 1.15(b) have policies, controls and procedures, which are approved by senior management and consistent with national requirements and guidance from competent authorities and SRBs, to enable them to manage and mitigate the PF risks that have been identified (either by the country or by the financial institution or DNFBP);
    - 1.15(c) monitor the implementation of those controls and to enhance them if necessary;
    - 1.15(d) take proportionate measures to manage and mitigate the risks where higher PF risks are identified, (i.e. introducing enhanced

controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7); and

1.15(e) where the PF risks are lower, ensure that measures to manage and mitigate the risks are proportionate to the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

12. In addition to the risk mitigation measures required for AML/ATF regulated entities in Bermuda, **FATF criterion 1.11** requires countries, based on their understanding of their PF risks, to implement risk-based measures, proportionate to the risks identified and allocate resources efficiently, to mitigate PF risks. Regulatory amendments proposed to address criterion 1.15 (in respect of AML/ATF regulated entities) incorporate the development of risk-based mitigation measures for PF.

The proposed amendments are hereto annexed for ease of reference.

Conclusion

D. NAMLC therefore seeks the cooperation of industry to review this Consultation Paper, and should you have any observations concerning the proposed amendments, you may provide written comments and feedback no later than **February 11, 2026,** to the email address below:

- Via e-mail: info-NAMLC@gov.bm

Annex I

Proposed Changes to the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations

Regulation No.	Current Regulation	Proposed Amendments in red
1	**Interpretation:** No definition of "proliferation", "proliferation financing" or "CPF"	**Interpretation:** "proliferation financing" means the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear (CBRN) weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and in contravention of international sanctions obligations that are in force in Bermuda. "CPF" means counter-proliferation financing
6	**Application of customer due diligence measures** 6 (1) Subject to regulations 7, 10, 11, 13(4) and 14, a relevant person must apply customer due diligence measures when he— (a) establishes a business relationship; (b) carries out an occasional transaction; (c) suspects money laundering, terrorist financing; or (d) doubts the veracity or adequacy of documents, data or information previously obtained for the purpose of identification or verification. (1A) Subject to paragraph (1), in the case of a trust or life insurance policy, a relevant person shall apply customer due diligence measures on a beneficiary as soon as the beneficiary is designated— (a) for a beneficiary that is identified as a specifically named natural person, legal entity or legal arrangement, taking the name of the person, entity or arrangement;	**Application of customer due diligence measures** 6 (1) Subject to regulations 7, 10, 11, 13(4) and 14, a relevant person must apply customer due diligence measures when he— (a) establishes a business relationship; (b) carries out an occasional transaction; (c) suspects money laundering, terrorist financing or proliferation financing; or (d) doubts the veracity or adequacy of documents, data or information previously obtained for the purpose of identification or verification. (1A) Subject to paragraph (1), in the case of a trust or life insurance policy, a relevant person shall apply customer due diligence measures on a beneficiary as soon as the beneficiary is designated— (a) for a beneficiary that is identified as a specifically named natural person, legal entity or legal arrangement, taking the name of the person, entity or arrangement;

	(b) for a beneficiary that is designated by characteristics or by class, obtaining sufficient information concerning the beneficiary to satisfy the relevant person that it will be able to establish the identity of the beneficiary at the time of payout.	(b) for a beneficiary that is designated by characteristics or by class, obtaining sufficient information concerning the beneficiary to satisfy the relevant person that it will be able to establish the identity of the beneficiary at the time of payout.
	1B) The customer due diligence legal requirements for legal persons or legal arrangements shall include— (a) full name and trade name; (b) date and place of incorporation, registration or establishment; (c) registered office address and, if different, mailing address; (d) address of the principal place of business; (e) whether and where listed on a stock exchange; (f) official identification number (where applicable); (g) name of regulator (where applicable); (h) legal form, nature and purpose (e.g. discretionary, testamentary, bare); (i) control and ownership; (j) nature of business; and (k) an obligation to collect information about the legal powers that regulate and bind a legal person or legal arrangement. (2) A relevant person must apply customer due diligence measures at appropriate times to existing customers on a risk-sensitive basis. (3) A relevant person must— (a) determine the extent of customer due diligence measures on a risk- sensitive basis depending on the type of customer, business relationship, geographic areas, services, delivery channels, product or transaction; and (b) be able to demonstrate to its supervisory authority that the extent of customer due diligence measures is appropriate in view of the risks of money laundering and terrorist financing. (3A) Where a relevant person is required to apply customer due diligence measures in the case of a trust or life insurance policy, the relevant person must include the beneficiary as a risk factor in determining the extent of customer due diligence measures required in accordance with paragraph (3).	(1B) The customer due diligence legal requirements for legal persons or legal arrangements shall include— (a) full name and trade name; (b) date and place of incorporation, registration or establishment; (c) registered office address and, if different, mailing address; (d) address of the principal place of business; (e) whether and where listed on a stock exchange; (f) official identification number (where applicable); (g) name of regulator (where applicable); (h) legal form, nature and purpose (e.g. discretionary, testamentary, bare); (i) control and ownership; (j) nature of business; and (k) an obligation to collect information about the legal powers that regulate and bind a legal person or legal arrangement. (2) A relevant person must apply customer due diligence measures at appropriate times to existing customers on a risk-sensitive basis. (3) A relevant person must— (a) determine the extent of customer due diligence measures on a risk- sensitive basis depending on the type of customer, business relationship, geographic areas, services, delivery channels, product or transaction; and (b) be able to demonstrate to its supervisory authority that the extent of customer due diligence measures is appropriate in view of the risks of money laundering, terrorist financing and proliferation financing. (3A) Where a relevant person is required to apply customer due diligence measures in the case of a trust or life insurance policy, the relevant person must include the beneficiary as a risk factor in determining the extent of customer due diligence measures required in accordance with paragraph (3).

	(4) Where— (a) a relevant person is required to apply customer due diligence measures in the case of a trust, legal entity (other than a body corporate) or a legal arrangement (other than a trust); and (b) the class of persons in whose main interest the trust, entity or arrangement is set up or operates is identified as a beneficial owner, the relevant person is not required to identify all the members of the class. (5) Where a relevant person suspects that a transaction relates to money laundering or terrorist financing and he believes that performing customer due diligence measures may tip-off the customer or potential customer to that suspicion, he shall not perform the customer due diligence measures. (6) Where a relevant person is unable to perform customer due diligence in accordance with paragraph (5) he shall, in lieu, file the necessary disclosure with the FIA. (7) For the purpose of paragraph (1A), "beneficiary" means the person named as beneficiary in a life insurance policy or a trust instrument.	(4) Where— (a) a relevant person is required to apply customer due diligence measures in the case of a trust, legal entity (other than a body corporate) or a legal arrangement (other than a trust); and (b) the class of persons in whose main interest the trust, entity or arrangement is set up or operates is identified as a beneficial owner, the relevant person is not required to identify all the members of the class. (5) Where a relevant person suspects that a transaction relates to money laundering, terrorist financing or proliferation financing and he believes that performing customer due diligence measures may tip-off the customer or potential customer to that suspicion, he shall not perform the customer due diligence measures. (6) Where a relevant person is unable to perform customer due diligence in accordance with paragraph (5) he shall, in lieu, file the necessary disclosure with the FIA. (7) For the purpose of paragraph (1A), "beneficiary" means the person named as beneficiary in a life insurance policy or a trust instrument.
8	**Timing of verification** 8 (1) This regulation applies in respect of the duty under regulations 6(1)(a) and (b) and regulation 6(1A) to apply the customer due diligence measures referred to in regulation 5. (2) Subject to paragraphs (3) to (5), a relevant person must verify the identity of the customer (and any beneficial owner) before the establishment of a business relationship or the carrying out of an occasional transaction. (3) Such verification may be completed during the establishment of a business relationship or after the establishment of a business	**Timing of verification** 8 (1) This regulation applies in respect of the duty under regulations 6(1)(a) and (b) and regulation 6(1A) to apply the customer due diligence measures referred to in regulation 5. (2) Subject to paragraphs (3) to (5), a relevant person must verify the identity of the customer (and any beneficial owner) before the establishment of a business relationship or the carrying out of an occasional transaction. (3) Such verification may be completed during the establishment of a business relationship or after the establishment of a business

	relationship or an account has been opened as provided under paragraphs (4) and (5) if— (a) this is necessary not to interrupt the normal conduct of business; and (b) there is little risk of money laundering or terrorist financing occurring, provided that the verification is completed as soon as practicable after contact is first established; and (c) any money laundering or terrorist financing risks that may arise are effectively managed. (4) The verification of the identity of the beneficiary under a life insurance policy or a trust may, subject to paragraph (3), take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy or trust. (5) The verification of the identity of an account holder may, subject to paragraph (3), take place after the account has been opened provided that there are adequate safeguards in place to ensure that— (a) the account is not closed; and (b) transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder), before verification has been completed.	relationship or an account has been opened as provided under paragraphs (4) and (5) if— (a) this is necessary not to interrupt the normal conduct of business; and (b) there is little risk of money laundering, terrorist financing or proliferation financing occurring, provided that the verification is completed as soon as practicable after contact is first established; and (c) any money laundering, terrorist financing or proliferation financing risks that may arise are effectively managed. (4) The verification of the identity of the beneficiary under a life insurance policy or a trust may, subject to paragraph (3), take place after the business relationship has been established provided that it takes place at or before the time of payout or at or before the time the beneficiary exercises a right vested under the policy or trust. (5) The verification of the identity of an account holder may, subject to paragraph (3), take place after the account has been opened provided that there are adequate safeguards in place to ensure that— (a) the account is not closed; and (b) transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder), before verification has been completed.
9	**Requirement to cease transactions, etc.** 9 (1) Where in relation to any customer, a relevant person is unable to apply customer due diligence measures in accordance with the provisions of these Regulations he— (a) shall not open an account or carry out a transaction for the customer;	**Requirement to cease transactions, etc.** 9 (1) Where in relation to any customer, a relevant person is unable to apply customer due diligence measures in accordance with the provisions of these Regulations he— (a) shall not open an account or carry out a transaction for the customer;

	(b) shall not establish a business relationship or carry out an occasional transaction with the customer. (c) shall terminate any existing business relationship with the customer; and (ca) in the case of a patron in a casino, shall not permit that patron to place any bet, or to undertake any further transactions of any nature, until such time as he has been able to apply the customer due diligence measures; (d) shall consider whether he is required to make a disclosure by section 46(2) of the Proceeds of Crime Act 1997 or paragraph 1 of Part I of Schedule I of the Anti-Terrorism (Financial and Other Measures) Act 2004. (2) Paragraph (1) does not apply where a professional legal adviser is in the course of ascertaining the legal position for his client or performing his task of defending or representing that client in, or concerning, legal proceedings, including advice on instituting or avoiding proceedings.	(b) shall not establish a business relationship or carry out an occasional transaction with the customer. (c) shall terminate any existing business relationship with the customer; and (ca) in the case of a patron in a casino, shall not permit that patron to place any bet, or to undertake any further transactions of any nature, until such time as he has been able to apply the customer due diligence measures; (d) shall consider whether he is required to make a disclosure by section 46(2) of the Proceeds of Crime Act 1997 or paragraph 1 of Part I of Schedule I of the Anti-Terrorism (Financial and Other Measures) Act 2004, or the pursuant to the International Sanctions Act 2003 and the regulations made thereunder. (2) Paragraph (1) does not apply where a professional legal adviser is in the course of ascertaining the legal position for his client or performing his task of defending or representing that client in, or concerning, legal proceedings, including advice on instituting or avoiding proceedings.
10	**Simplified due diligence** 10 (1) Subject to paragraph (1A), a relevant person is not required to apply the full customer due diligence measures referred to in regulation 5 in the circumstances mentioned in regulation 6(1)(a) or (b), or regulation 6(1A) where he has reasonable grounds for believing that the customer, product or transaction related to such product, falls within paragraph (2), (3), (4), (5), (6) or (7). (1A) Paragraph (1) applies only if— (a) after assessing the risk, the relevant person has reasonable grounds for believing that there is a low risk of money laundering and terrorist financing; and (b) the relevant person has no suspicion of money laundering or terrorist financing and the relevant person shall record its assessment.	**Simplified due diligence** 10 (1) Subject to paragraph (1A), a relevant person is not required to apply the full customer due diligence measures referred to in regulation 5 in the circumstances mentioned in regulation 6(1)(a) or (b), or regulation 6(1A) where he has reasonable grounds for believing that the customer, product or transaction related to such product, falls within paragraph (2), (3), (4), (5), (6) or (7). (1A) Paragraph (1) applies only if— (a) after assessing the risk, the relevant person has reasonable grounds for believing that there is a low risk of of money laundering, terrorist financing and proliferation financing; and (b) the relevant person has no suspicion of money laundering, terrorist financing or of proliferation financing and the relevant person shall record its assessment.

	(2) The customer is— (a) an AML/ATF regulated financial institution which is subject to the requirements of these Regulations; or (b) an AML/ATF regulated financial institution (or equivalent institution) which— (i) is situated in a country or territory other than Bermuda which imposes requirements equivalent to those laid down in these Regulations; (ii) has effectively implemented those requirements; and (iii) is supervised for compliance with those requirements. (3) The customer is a company whose securities are listed on an appointed stock exchange. (4) The customer is an independent professional (or similar professional) and the product is an account into which monies are pooled, provided that— (a) where the pooled account is held in a country or territory other than Bermuda— (i) that country or territory imposes requirements to combat money laundering and terrorist financing which are equivalent to those laid down in these Regulations; (ii) the independent professional has effectively implemented those requirements; and (iii) the independent professional is supervised in that country or territory for compliance with those requirements; and (b) information on the identity of the persons on whose behalf monies are held in the pooled account is available, on request, to the institution which acts as a custodian for the account.	(2) The customer is— (a) an AML/ATF regulated financial institution which is subject to the requirements of these Regulations; or (b) an AML/ATF regulated financial institution (or equivalent institution) which— (i) is situated in a country or territory other than Bermuda which imposes requirements equivalent to those laid down in these Regulations; (ii) has effectively implemented those requirements; and (iii) is supervised for compliance with those requirements. (3) The customer is a company whose securities are listed on an appointed stock exchange. (4) The customer is an independent professional (or similar professional) and the product is an account into which monies are pooled, provided that— (a) where the pooled account is held in a country or territory other than Bermuda— (i) that country or territory imposes requirements to combat money laundering, terrorist financing and proliferation financing which are equivalent to those laid down in these Regulations; (ii) the independent professional has effectively implemented those requirements; and (iii) the independent professional is supervised in that country or territory for compliance with those requirements; and (b) information on the identity of the persons on whose behalf monies are held in the pooled account is available, on request, to the institution which acts as a custodian for the account.
11	11 (1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures to business relationships with customers—	11 (1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures to business relationships with customers—

	(a) in accordance with paragraphs (2) to (4); (aa) in instances where a person or a transaction is from or in a country that has been identified as having a higher risk by the Financial Action Task Force or the Caribbean Financial Action Task Force; (ab) in instances where a person or a transaction is from or in a country which represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions; (b) in any other situation which by its nature may present a higher risk of money laundering or terrorist financing (2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures— (a) ensuring that the customer's identity is established by additional documents, data or information; (b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by an AML/ATF regulated financial institution (or equivalent institution) which is subject to equivalent Regulations; (c) ensuring that the first payment is carried out through an account opened in the customer's name with a banking institution. (3) A banking institution (the "correspondent") which has or proposes to have a correspondent banking relationship institution ("the respondent") must - (a) gather sufficient information about the respondent to understand fully the nature of its business; (b) determine from publicly-available information the reputation of the respondent and the quality of its supervision;	(a) in accordance with paragraphs (2) to (4); (aa) in instances where a person or a transaction is from or in a country that has been identified as having a higher risk by the Financial Action Task Force or the Caribbean Financial Action Task Force; (ab) in instances where a person or a transaction is from or in a country which represents a higher risk of money laundering, corruption, terrorist financing or being subject to international sanctions; (b) in any other situation which by its nature may present a higher risk of money laundering, terrorist financing or proliferation financing. (2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures— (a) ensuring that the customer's identity is established by additional documents, data or information; (b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by an AML/ATF regulated financial institution (or equivalent institution) which is subject to equivalent Regulations; (c) ensuring that the first payment is carried out through an account opened in the customer's name with a banking institution. (3) A banking institution (the "correspondent") which has or proposes to have a correspondent banking relationship institution ("the respondent") must - (a) gather sufficient information about the respondent to understand fully the nature of its business; (b) determine from publicly-available information the reputation of the respondent and the quality of its supervision;

	(c) assess the respondent's controls relating to anti-money laundering control and anti-terrorism financing controls; (d) obtain approval from senior management before establishing a new correspondent banking relationship; (e) document the respective responsibilities of the respondent and correspondent; (f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent— (i) has verified the identity of, and performs ongoing due diligence on, such customers; and (ii) is able upon request to provide relevant customer due diligence data to the correspondent. (3A) Where a casino operator knows or has reason to suspect that the patron— (a) has fiduciary obligations that may create a risk of the misappropriation of funds; (b) is associated with individuals or entities known to be connected to the illicit generation of funds or the laundering of such funds; (c) has sources of wealth or income incommensurate with his gaming activity; (d) has been bankrupt; or (e) has a prior history of criminal or dishonest conduct, the casino operator must apply on a risk-sensitive basis enhanced customer due diligence measures as set out in paragraph (3B). (3B) Enhanced customer due diligence required under paragraph (3A) must compensate for the higher risk posed on a case by case basis, and such measures may include, but not be limited to, one or more of the following— (a) assessing whether the patron is the beneficial owner of all funds proposed for use in gaming; (b) establishing the source of funds proposed for use in gaming;	(c) assess the respondent's controls relating to anti-money laundering controls, anti-terrorism financing controls and counter-proliferation financing controls; (d) obtain approval from senior management before establishing a new correspondent banking relationship; (e) document the respective responsibilities of the respondent and correspondent; (f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent— (i) has verified the identity of, and performs ongoing due diligence on, such customers; and (ii) is able upon request to provide relevant customer due diligence data to the correspondent. (3A) Where a casino operator knows or has reason to suspect that the patron— (a) has fiduciary obligations that may create a risk of the misappropriation of funds; (b) is associated with individuals or entities known to be connected to the illicit generation of funds or the laundering of such funds; (c) has sources of wealth or income incommensurate with his gaming activity; (d) has been bankrupt; or (e) has a prior history of criminal or dishonest conduct, the casino operator must apply on a risk-sensitive basis enhanced customer due diligence measures as set out in paragraph (3B). (3B) Enhanced customer due diligence required under paragraph (3A) must compensate for the higher risk posed on a case by case basis, and such measures may include, but not be limited to, one or more of the following— (a) assessing whether the patron is the beneficial owner of all funds proposed for use in gaming; (b) establishing the source of funds proposed for use in gaming;

	(c) ensuring that the patron has no prior history associated with AML/ATF offences or; (d) increasing the frequency of the monitoring of the patron's gaming activity.	(c) ensuring that the patron has no prior history associated with AML/ATF offences or breaches of international sanctions obligations; (d) increasing the frequency of the monitoring of the patron's gaming activity.
12	**Branches and subsidiaries** 12 (1) A relevant person must require its branches and subsidiary undertakings which are located in a country or territory other than Bermuda— (a) to adopt group-wide policies and procedures that— (i) facilitate the sharing of customer due diligence and transaction information; and (ii) ensure adequate safeguards on the confidentiality and use of information exchanged, in order to manage the risk of money laundering and terrorist financing through the application of AML/ATF compliance functions; and (b) to apply, to the extent permitted by the law of that country or territory, measures at least equivalent to those set out in these Regulations with regard to customer due diligence measures, ongoing monitoring and record-keeping. (2) Where the law of such a country or territory does not permit the application of such equivalent measures by the branch or subsidiary undertaking located in that country or territory, the relevant person shall— (a) inform the Bermuda Monetary Authority accordingly; and take additional measures to handle effectively the risk of money laundering and terrorist financing. (3) In this regulation "subsidiary undertaking" except in relation to an incorporated friendly society, has the meaning	**Branches and subsidiaries** 12 (1) A relevant person must require its branches and subsidiary undertakings which are located in a country or territory other than Bermuda— (a) to adopt group-wide policies and procedures that— (i) facilitate the sharing of customer due diligence and transaction information; and (ii) ensure adequate safeguards on the confidentiality and use of information exchanged, in order to manage the risk of money laundering and terrorist financing through the application of AML/ATF/CPF compliance functions; and (b) to apply, to the extent permitted by the law of that country or territory, measures at least equivalent to those set out in these Regulations with regard to customer due diligence measures, ongoing monitoring and record-keeping. (2) Where the law of such a country or territory does not permit the application of such equivalent measures by the branch or subsidiary undertaking located in that country or territory, the relevant person shall— (a) inform the Bermuda Monetary Authority accordingly; and take additional measures to handle effectively the risk of money laundering, terrorist financing and proliferation financing. (3) In this regulation "subsidiary undertaking" except in relation to an incorporated friendly society, has the meaning

	given by section 86 of the Companies Act ('parent and subsidiary undertakings') and, in relation to a body corporate in or formed under the law of a country or territory other than Bermuda, includes an undertaking which is a subsidiary undertaking within the meaning of any rule of law in force in that country or territory. (4) For the avoidance of doubt, the provisions of this regulation apply to branches and subsidiaries located inside and outside of Bermuda.	given by section 86 of the Companies Act ('parent and subsidiary undertakings') and, in relation to a body corporate in or formed under the law of a country or territory other than Bermuda, includes an undertaking which is a subsidiary undertaking within the meaning of any rule of law in force in that country or territory. (4) For the avoidance of doubt, the provisions of this regulation apply to branches and subsidiaries located inside and outside of Bermuda.
12A	**Financial groups** 12A A financial group shall implement group-wide policies and procedures against money laundering and terrorist financing which are applicable and appropriate to all members of the financial group, and these policies and procedures shall include— (a) procedures and requirements set out in Part 2 (Customer Due Diligence), Part 3 (Record-keeping, Systems, Training etc.) and Part 4 (Transfer of Funds), as applicable, of these Regulations; (b) policies and procedures for sharing information required for the purposes of customer due diligence and money laundering and terrorist financing risk management, including information on transactions which appear unusual and have generated a suspicious transaction report; (c) the provision at group level of compliance, audit and anti-money laundering and anti-terrorist financing functions, of customer, transaction and account information from branches and subsidiaries when necessary for anti-money laundering or anti-terrorist financing purposes; and (d) adequate safeguards on the confidentiality and use of information exchanged.	**Financial groups** 12A A financial group shall implement group-wide policies and procedures against money laundering, terrorist financing and proliferation financing which are applicable and appropriate to all members of the financial group, and these policies and procedures shall include— (a) procedures and requirements set out in Part 2 (Customer Due Diligence), Part 3 (Record-keeping, Systems, Training etc.) and Part 4 (Transfer of Funds), as applicable, of these Regulations; (b) policies and procedures for sharing information required for the purposes of customer due diligence money laundering terrorist financing and proliferation financing risk management, including information on transactions which appear unusual and have generated a suspicious transaction report; (c) the provision at group level of compliance, audit and anti-money laundering, anti-terrorist financing and proliferation financing functions, of customer, transaction and account information from branches and subsidiaries when necessary for anti-money laundering, anti-terrorist financing or proliferation financing; and (d) adequate safeguards on the confidentiality and use of information exchanged.

14	**Outsourcing** 14A (1) Where a relevant person delegates its AML/ATF compliance function to another entity (outsourcing), the relevant person shall retain ultimate responsibility for the AML/ ATF compliance function. (2) In this regulation, ultimate responsibility includes the obligation to— (a) ensure that the provider of the outsourced AML/ATF compliance function has in place— (i) AML/ATF systems; (ii) AML/ATF controls; and (iii) AML/ATF procedures, that are in compliance with the Bermuda AML/ATF requirements; (b) consider the effect that outsourcing compliance functions has on the money laundering and terrorist financing risk; (c) assess the money laundering and terrorist financing risk associated with outsourced functions and record its assessment; and (d) monitor any perceived risk on an ongoing basis and, where the compliance functions (Compliance Officer or Reporting Officer) are involved to— (i) ensure that the roles, responsibilities and respective duties are clearly defined and documented; and (ii) ensure that the Compliance Officer or Reporting Officer and all employees understand the roles, responsibilities and the respective duties of all parties. (3) Where a relevant person delegates its compliance function to another entity (outsourcing), the relevant person shall adopt policies and procedures to monitor and manage the service provider carrying out those compliance functions.	**Outsourcing** 14A (1) Where a relevant person delegates its AML/ATF/CPF compliance function to another entity (outsourcing), the relevant person shall retain ultimate responsibility for the AML/ATF/CPF compliance function. (2) In this regulation, ultimate responsibility includes the obligation to— (a) ensure that the provider of the outsourced AML/ATF/CPF compliance function has in place— (i) AML/ATF/CPF systems; (ii) AML/ATF/CPF controls; and (iii) AML/ATF/CPF procedures, that are in compliance with the Bermuda AML/ATF/CPF requirements; (b) consider the effect that outsourcing compliance functions has on the money laundering, terrorist financing and proliferation financing risk; (c) assess the money laundering, terrorist financing and proliferation financing risk associated with outsourced functions and record its assessment; and (d) monitor any perceived risk on an ongoing basis and, where the compliance functions (Compliance Officer or Reporting Officer) are involved to— (i) ensure that the roles, responsibilities and respective duties are clearly defined and documented; and (ii) ensure that the Compliance Officer or Reporting Officer and all employees understand the roles, responsibilities and the respective duties of all parties. (3) Where a relevant person delegates its compliance function to another entity (outsourcing), the relevant person shall adopt policies and procedures to monitor and manage the service provider carrying out those compliance functions.

	(4) In this regulation, "outsourcing" and "outsourced" means— (a) AML/ATF systems; (b) AML/ATF controls and (c) AML/ATF procedures, obtained outside of a relevant person.	(4) In this regulation, "outsourcing" and "outsourced" means— (a) AML/ATF/CPF systems; (b) AML/ATF/CPF controls and (c) AML/ATF/CPF procedures, obtained outside of a relevant person.
16	**Systems** 16 (1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures, approved by its governing body, relating to— (a) customer due diligence measures and ongoing monitoring; (b) reporting; (c) record-keeping; (d) internal control; (e) the performance and documentation of any products or services (prior to launch) and the continual documentation of risk assessment and management of such products and services, in a form available to share with the supervisory authority; (ea) risk mitigation mechanisms which include— (i) consideration of the national or of the relevant person's risk assessment results or conclusions; (ii) the ability to effectively supply information to the supervisory authority; and (iii) the application of enhanced measures where the relevant person's risk assessments identify a higher risk; (f) the monitoring and management of compliance with and the internal communication of such policies and procedures in order to prevent activities related to money laundering and terrorist financing. (1A) Where a relevant person intends to introduce a new product, practice or technology, the relevant person must perform and document a risk assessment prior to the launch of such product, practice or technology.	**Systems** 16 (1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures, approved by its governing body, relating to— (f) customer due diligence measures and ongoing monitoring; (g) reporting; (h) record-keeping; (i) internal control; (j) the performance and documentation of any products or services (prior to launch) and the continual documentation of risk assessment and management of such products and services, in a form available to share with the supervisory authority; (ea) risk mitigation mechanisms which include— (iv) consideration of the national or of the relevant person's risk assessment results or conclusions; (v) the ability to effectively supply information to the supervisory authority; and (vi) the application of enhanced measures where the relevant person's risk assessments identify a higher risk; (f) the monitoring and management of compliance with and the internal communication of such policies and procedures in order to prevent activities related to money laundering, terrorist financing and proliferation financing. (1A) Where a relevant person intends to introduce a new product, practice or technology, the relevant person must perform and document a risk assessment prior to the launch of such product, practice or technology.

	(2) The policies and procedures referred to in paragraph (1) include policies and procedures— (a) which provide for the identification and scrutiny of— (i) complex or unusually large transactions; (ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and (iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering, o r terrorist financing; (b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity; (c) to determine whether a new or existing customer is a politically exposed person; (d) under which— (i) anyone in the organisation to whom information or other matter comes in the course of the business as a result of which he knows or suspects or has reasonable grounds to suspect that a person is engaged in money laundering or terrorist financing is required to comply with sections comply with sections 46(5) of the Proceeds of Crime Act 1997 or, as the case may be, section 9 or paragraph 1 of Part 1 of Schedule 1 to the Anti-Terrorism (Financial and Other Measures) Act 2004; and (ii) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion that a person is engaged in money laundering or terrorist financing. (3) A relevant person must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiaries which are located outside Bermuda.	(2) The policies and procedures referred to in paragraph (1) include policies and procedures— (a) which provide for the identification and scrutiny of— (i) complex or unusually large transactions; (ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and (iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering, terrorist financing or proliferation financing; (b) which specify the taking of additional measures, where appropriate, to prevent the use money laundering, terrorist financing or proliferation financing of products and transactions which might favour anonymity; (c) to determine whether a new or existing customer is a politically exposed person; (d) under which— (i) anyone in the organisation to whom information or other matter comes in the course of the business as a result of which he knows or suspects or has reasonable grounds to suspect that a person is engaged in in money laundering, terrorist financing or proliferation financing is required to comply with sections comply with sections 46(5) of the Proceeds of Crime Act 1997 or, as the case may be, section 9 or paragraph 1 of Part 1 of Schedule 1 to the Anti-Terrorism (Financial and Other Measures) Act 2004; and (ii) where a disclosure is made to the nominated officer, he must consider it in the light of any relevant information which is available to the relevant person and determine whether it gives rise to knowledge or suspicion that a person is engaged in in money laundering, terrorist financing or proliferation financing (3) A relevant person must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiaries which are located outside Bermuda.

	(4) A relevant person must have systems in place enabling it to respond promptly to enquiries from a supervisory authority (in respect of a relevant person under the authority's supervision), the Financial Intelligence Agency or a police officer— (a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and (b) the nature of that relationship. 16(5) A relevant person shall take appropriate steps (including the use of risk mitigation mechanisms referred to in paragraph (1)(ea)) to identify, assess and understand its money laundering, terrorist financing risks (depending on the type of customers, business relationships, countries or geographic areas, services, delivery channels, products or transactions), and shall document the risk assessments and keep them updated.	(4) A relevant person must have systems in place enabling it to respond promptly to enquiries from a supervisory authority (in respect of a relevant person under the authority's supervision), the Financial Intelligence Agency or a police officer— (a) whether it maintains, or has maintained during the previous five years, a business relationship with any person; and (b) the nature of that relationship. 16(5) A relevant person shall take appropriate steps (including the use of risk mitigation mechanisms referred to in paragraph (1)(ea)) to identify, assess and understand its money laundering, terrorist financing risks (depending on the type of customers, business relationships, countries or geographic areas, services, delivery channels, products or transactions) and proliferation financing risks, and shall document the risk assessments and keep them updated.
17	**Internal reporting procedures** 17 (1) A relevant person must appoint a Reporting Officer and maintain internal reporting procedures which require that— (a) a report is to be made to the Reporting Officer of any information or other matter which comes to the attention of an employee and which in the opinion of that employee gives rise to a knowledge or suspicion that another person is engaged in money laundering or terrorist financing. (b) any such report be considered by the Reporting Officer in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report does give rise to such a knowledge or suspicion; (c) the Reporting Officer be given access to any other information which may be of assistance to him in considering the report; and	**Internal reporting procedures** 17 (1) A relevant person must appoint a Reporting Officer and maintain internal reporting procedures which require that— (a) a report is to be made to the Reporting Officer of any information or other matter which comes to the attention of an employee and which in the opinion of that employee gives rise to a knowledge or suspicion that another person is engaged in money laundering, terrorist financing or proliferation financing; (b) any such report be considered by the Reporting Officer in the light of all other relevant information for the purpose of determining whether or not the information or other matter contained in the report does give rise to such a knowledge or suspicion; (c) the Reporting Officer be given access to any other information which may be of assistance to him in considering the report; and

	(d) the Reporting Officer disclose to the Financial Intelligence Agency the information or other matter contained in a report, where the reporting officer knows or suspects or has reasonable grounds to suspect that a person is engaged in money laundering or terrorist financing. (2) Paragraph (1) does not apply where the relevant person is an individual who neither employs nor acts in association with any other person. (3) The relevant person shall be responsible for ensuring its Reporting Officer is adequately trained to carry out the role.	(d) the Reporting Officer disclose to the Financial Intelligence Agency the information or other matter contained in a report, where the reporting officer knows or suspects or has reasonable grounds to suspect that a person is engaged in money laundering, terrorist financing or proliferation financing. (2) Paragraph (1) does not apply where the relevant person is an individual who neither employs nor acts in association with any other person. (3) The relevant person shall be responsible for ensuring its Reporting Officer is adequately trained to carry out the role.
17A	**Independent audit function** 17A (1) A relevant person must maintain an independent audit function to be conducted by a qualified independent third party or internally by persons independent of any other function, the lines of business over which the function has audit responsibilities, and financial operations. (2) An independent audit function must provide and document an independent and objective evaluation of the robustness of the AML/ATF framework, and the reliability, integrity and completeness of the design and effectiveness of the AML/ATF risk management function and AML/ATF internal controls framework, and the AML/ATF compliance.	**Independent audit function** 17A (1) A relevant person must maintain an independent audit function to be conducted by a qualified independent third party or internally by persons independent of any other function, the lines of business over which the function has audit responsibilities, and financial operations. (2) An independent audit function must provide and document an independent and objective evaluation of the robustness of the AML/ATF/CPF framework, and the reliability, integrity and completeness of the design and effectiveness of the AML/ATF/CPF risk management function and AML/ATF/CPF internal controls framework, and the AML/ATF/CPF compliance.
18	**Training etc.** 18 (1) A relevant person must take appropriate measures so that all relevant employees of his are— (a) made aware of the law relating to money laundering and terrorist financing;	**Training etc.** 18 (1) A relevant person must take appropriate measures so that all relevant employees of his are— (a) made aware of the law relating to money laundering, terrorist financing and proliferation financing;

	(b) regularly given training in how to recognise and deal with transactions which may be related to money laundering or terrorist financing; and (c) screened prior to hiring to ensure high standards. (2) For the purposes of this paragraph, an employee is a relevant employee if— (a) at any time in the course of his duties, he has, or may have, access to any information which may be relevant in determining whether any person is engaged in money laundering or terrorist financing; (b) at any time plays a role in implementing and monitoring compliance with anti-money laundering or anti-terrorist financing requirements.	(b) regularly given training in how to recognise and deal with transactions which may be related to money laundering, terrorist financing or proliferation financing; and (c) screened prior to hiring to ensure high standards. (2) For the purposes of this paragraph, an employee is a relevant employee if— (a) at any time in the course of his duties, he has, or may have, access to any information which may be relevant in determining whether any person is engaged in money laundering, terrorist financing or proliferation financing; (b) at any time plays a role in implementing and monitoring compliance with anti-money laundering, anti-terrorist financing or counter-proliferation financing requirements.