AML/CFT Guidance to Casinos

Department of Tourism

Ministry of Culture, Tourism and Civil Aviation

August, 2026

Abbreviations and Acronyms

ALPA	Asset (Money) Laundering Prevention Act, 2008
ALPR	Asset (Money) Laundering Prevention Rules, 2024
AML	Anti-money laundering
CDD	Customer Due Diligence
CFT	Combating Financing of Terrorism
DNFBP	Designated Non-Financial Business and Profession
DoT	Department of Tourism
DPMS	Dealers in Precious Metals and Stones
ECDD	Enhanced Customer Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ID	Identification
ML	Money Laundering
NRA	National Risk Assessment
PEP	Politically Exposed Person
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
TFS	Targeted Financial Sanctions
TTR	Threshold Transaction Reporting
UN	United Nations

I. INTRODUCTION

In addition to financial sectors, criminals often exploit non-financial sectors — such as Casinos, Real estate and Dealers in Precious Metals and Stones (DPMS) — to launder their illicit proceeds. These sectors are inherently higher-risk for money laundering due to the involvement of high volumes of cash transactions and the ability to obscure beneficial ownership. They allow criminals to make the initial placement of illegal proceeds while escaping the more rigorous detection and mitigation measures that the banking sector has put in place. Besides, they can also be used during the layering phase for concealing the illegal source of funds.

It is essential that casinos and other high-risk DNFBPs have sufficient understanding of ML/TF risks they face and that they apply measures to prevent being abused by the perpetrators of money laundering and terrorist financing. An effective system requires them to develop and apply risk-based AML/CFT policies, internal controls, and programs to adequately mitigate risks. However, they generally lack knowledge and awareness about their ML/TF risks and AML/CFT obligations. Hence, increased outreach and guidance are critical for improving the effectiveness of preventive measures in the sector.

Objective of the Guidance

- To enhance awareness among the casinos about their AML/CFT-related obligations.
- To provide guidance to the casinos to implement AML/CFT related measures.

Scope and limitations

The Guidance is applicable to all the casinos, including mini-casinos, operating throughout Nepal under the provision of Casino Regulations, 2025. All the casinos are subject to AML/CFT laws and regulations.

The Guidance is mainly intended to enhance awareness and compliance by these reporting entities. It doesn't include all the compliance requirements. Casinos should consult the ALPA, 2008, ALPR, 2024 and the AML/CFT directives issued by the DoT to ensure compliance.

II. MONEY LAUNDERING AND TERRORIST FINANCING RISKS

Casinos process very large volumes of cash, making it difficult to distinguish legitimate gambling from laundering attempts. The ability to convert cash into chips, play with minimal gambling activity, and redeem chips without meaningful gambling provides an attractive laundering mechanism. The involvement of foreign customers also provide venue for cross-border movement of laundered funds.

The casino sector is often associated with syndicated, organized, and cross-border laundering. Fraud is consistently the most prominent predicate offense associated with casino laundering. Proceeds from cyber-enabled fraud and investment fraud such as Ponzi or pyramiding scam are likely to use casino for layering purposes. Likewise, groups involved in virtual currency related fraud could use casino front-money accounts as a laundromart, interweaving the casino and crypto systems.

In Nepal, the National Risk Assessment (NRA) has found that the vulnerability in the casino sector is mainly driven by cash-intensive nature of casino operations and the open border with India. Moreover, the mini-casinos operating near the border with India could be at higher risk. Nepali citizens are prohibited from gambling in casinos. Hence, cross-border movement of illegal funds through foreign players is the main concern.

The NRA has also found that effectiveness of the implementation of AML/CFT preventive measures is low in the casino sector. Compared to the risk inherent in the sector, the number of suspicious transaction reporting is low. The insufficient monitoring, detection, and reporting of STR is of particular concern. The effectiveness of the compliance function has also found to be low. Furthermore, AML knowledge of business professionals and staff has been found limited.

III. INTERNATIONAL STANDARDS

FATF Recommendations pertaining to DNFBPs:

The FATF requires DNFBPs to implement preventive measures similar to those of traditional financial institutions. The FATF Recommendations 22 and 23 cover the customer due diligence and other measures that are applicable to the DNFBPs. As per these Recommendations, the customer due diligence and record keeping requirements set out in Recommendations 10, 11, 12, 15, and 17 (see footnote)[1] apply to the higher-risk DNFBPs in the following situations:

(i) **Casinos:** When customers engage in financial transactions equal to or above the applicable designated threshold.

(ii) **Real estate agents:** when they are involved in transactions for their clients concerning the buying and selling of real estate

(c) **DPMS:** when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

IV. CUSTOMER DUE DILIGENCE (CDD)

CDD is a foundational process used by financial institutions and DNFBPs to verify the identity of their clients, understand their financial background, and prevent criminals from abusing the

[1] Recommendation 10, 11, 12, 15 and 17 dealt with customer due diligence, record keeping, politically exposed persons, new technologies and reliance on third parties respectively. For further details, please refer to: [FATF Recommendations]

financial system for ML or TF. The process involves identifying the customers and verifying their identity using reliable, independent source documents, data or information.

CDD involves looking for answers for the following questions:

Who are you?	Who really owns the money?	Is this normal?	How risky are you?
• Name and address • Occupation and source of income • This helps create a profile • This prevents transactions under false name or anonymously	• Determining the benefiial owner • Criminals often hide behind complex company structures. • CDD reveal layers to find the real person in charge.	• Is the buying or transaction behavior align with the usual pattern for the person with the similar profile? • Is the purpose and nature of transaction bonafide?	• Not all customers should be treated the same. • Politically Exposed Persons (PEPs) and other high-risk individuals should be subjected to enhanced due diligence.

CDD steps usually includes:

- Obtaining full legal name and address,
- Verifying identity using government-issued photo ID such as Citizenship certificate, National Identity Card, Passport or Driver's license,
- Recording the nature of transaction and items involved,
- Documenting the source of funds.

Blanket provision for all sectors: As notified through the Nepal Gazette (Effective date: 15 January 2026), no cash transaction is allowed above Rs.500,000 for the purchase of goods and services. This is applicable to all sectors, including casinos.

Specific provision for Casino: As per ALPA, 2008, and directive issued by DoT, CDD is mandatory for customers conducting transactions above Rs.200,000 per day.

Beneficial Ownership

Understanding who ultimately has control of a customer plays an important role in detecting, disrupting and preventing money laundering and terrorism financing. Casinos should identify the beneficial owners of their customers and assess the money laundering/terrorism financing risk they pose.

Beneficial Ownership refers to the natural person(s) who ultimately own, control, or benefit from a legal entity, such as a company or trust, even if their name does not appear in the official ownership documents. Beneficial owners often exert significant influence over the entity's operations, financial decisions, or assets. As per ALPA, 2008 "beneficial owner" means *"a natural person who, as the ultimate beneficiary or owner thereof, directly or indirectly, owns or controls or directs or influences a customer, transaction (account), property, legal person or legal arrangement."* Note that the casino's customer may have more than one beneficial owner.

CDD involves identification of beneficial owners (in addition to the customer) and verification of such identification.

Following measures may be taken to identify and verify beneficial ownership:

- ➢ Consider all types of ownership/ control interests.
- ➢ Obtain reliable, independent source documents, such as the record/registry of the Office of the Company Registrar
- ➢ Verify from publicly available information, if available
- ➢ Ensure the information is adequate and up-to-date

In case of accounts belonging to individuals:

- ➢ Confirm the account activities match with the customer profile
- ➢ In case of a personal account, ensure that it is not a mule account

Ongoing Monitoring

Casinos should conduct ongoing due diligence on the relationship and monitor transactions closely to ensure they align with the customer's risk profile, line of business, and source of funds where necessary.

Enhanced Customer Due Diligence (ECDD)

ECDD is a rigorous process applied to high-risk customers or transactions to mitigate risks of money laundering, terrorist financing, and other financial crimes. It involves gathering additional information, performing more detailed analysis, and conducting continuous monitoring to ensure compliance with regulatory requirements.

ECDD may involve:

- Verifying the purpose and background of the transaction of complex, large or unusual nature whose financial and legal objectives are not clear,
- Collecting further details regarding the customer, beneficial owner and related persons,
- Obtaining additional information on the customer and take self-declaration as and when required,

- Social media scan and publicly available information scan,
- Obtaining additional information on the intended nature of the business relationship,
- Obtaining information on the source of funds or source of wealth of the customer,
- Obtaining information on the reasons for intended or performed transactions,
- Obtaining the approval of senior management to commence or continue the business relationship.

Politically Exposed Persons (PEPs)

A PEP is an individual who holds or has held a prominent public position, either domestically or internationally, and is therefore considered to pose a higher risk of being involved in corruption, bribery, or other financial crimes due to their access to power and influence. ALPA, 2008 has defined both domestic and foreign PEPs.

Casinos should take specific measures for PEPs. The measures include having mechanisms to immediately identify PEPs, mechanism to identify family members and close associates of PEPs and mechanism to identify risk based on the official status and involvement of the PEP.

The following measures may be taken to identify PEPs:

- Receive information from customer or self-declaration
- Check publicly available information
- Evaluate information available in social media
- Check commercially available database.
- Taking information from the related records kept in any agency according to the prevailing law.
- Prepare the list of PEPs internally list at least once in a year, by obtaining from organizations associated with Government of Nepal,
- PEPs should be listed as such until 5 years of retirement or being relieved from office

V. RECORD-KEEPING

Casinos must maintain all necessary records on transactions, as well as on CDD information, for at least five years. The records should be kept for at least five years even after the termination of the relationship or after the date of occasional transaction. However, if an account is closed but there is an ongoing investigation or litigation, all records must be retained until the case is officially closed. The record-keeping should be carried out in such a way that the Casinos are able to comply swiftly with information requests from the competent authorities.

Types of records kept

- ***Transaction Records:*** These must be detailed enough to permit the reconstruction of individual transactions (including the amounts and types of currency involved). This ensures the records can provide evidence for the prosecution of criminal activity if necessary.
- ***CDD and Account Records:*** Casinos should keep all records obtained through the CDD process. This includes official identification documents (such as passports, identity cards, or driving licenses), account files, business correspondence, and the results of any analysis undertaken (e.g., inquiries establishing the background and purpose of complex or unusually large transactions).

  Maintaining complete and updated records is essential for a casino to adequately monitor its relationship with its customers, wherever the relationship is established. Casinos must regularly review and update existing records to ensure they remain accurate and relevant. This not only enhances the entity's ability to effectively monitor for unusual or suspicious activities but also provides a vital audit trail in the event of disputes, legal actions, or regulatory inquiries.

  ALPA, 2008 has provisions that states that the reporting entity, including casinos, shall safely maintain all the records for a minimum period of five years and provide such records immediately as and when so demanded by the Financial Intelligence Unit, regulatory bodies, law enforcement agencies or other competent authorities.

VI. REPORTING

STR/ SAR Reporting

- As per ALPA 7, all reporting entities, including casinos, are required to file suspicious transaction report (STR) and suspicious activity report (SAR) to FIU immediately upon the assessment of such suspicion.
- FIU has issued STR Reporting Guidelines (Updated July 2025)[2] which includes red flags related to the Casino sector (See Annex-1). Once red flags are detected, the casino should analyze the transaction or activity to assess suspicion.
- Reports are to be filed to FIU through the goAML system. The casinos must be registered in the software first in order to be able to file suspicious transactions. The casinos are to

[2] www.nrb.org.np/contents/uploads/2025/10/STR.SAR-Guidelines-Updated-July-2025.pdf

contact FIU-Nepal in order to be registered into the system. (Registration link is provided in the *Links* section at the last page of this guidance document)

- The compliance officer and other relevant staff should keep the details on STRs/ SARs confidential. Tipping-off should be completely avoided, particularly to the concerned customer. The act of breach or any tipping-off is punishable under the section 44A of ALPA, 2008.

Other Reporting

- Casinos are required to file TTR within 15 days of such transaction. FIU-Nepal has issued Threshold Transaction Reporting Guidelines (Updated July 2025)[3]. The threshold transaction is Rs. 1 million conducted by a customer through single transaction or multiple transactions in a day.
- Casinos should submit institutional risk assessment reports, as per the provision of Section 35 of ALPA, 2008 to the DoT. Furthermore, they are required to submit regulatory reports as directed.

VII. TFS-RELATED

Casinos must screen customers against the UN consolidated sanctions list and Nepal's domestic designations before completing any transaction. Nepal's TFS Portal (established under the Implementation Procedures-TFS approved May 2025) provides real-time dissemination and must be used to check for new designations. Casinos should contact DoT for access to the Portal.

If a customer matches a designation:

- Verify that the customer is really the designated person,
- Freeze the assets promptly, within 24 hours from the time of designation published on the website of UN (For example: casino chips or any other assets in possession by the designated person during the transaction with casinos),
- Do not notify the customer before freezing the assets,
- Notify the DoT within three days from time of freezing of assets.

VIII. INTERNAL CONTROL

Risk Management

FATF Recommendation 1 requires financial institutions and DNFBPs to conduct ML/TF risk assessment of their business. Risk assessment is the first step that must be taken before developing AML/CFT program. It involves identifying and assessing the inherent ML/TF risks

[3] www.nrb.org.np/contents/uploads/2025/08/Threshold-Transaction-Reporting-Guidelines-Updated-July-2025.pdf

in the entity. Once risk assessment is completed, then only a program that minimizes or mitigates those risks can be implemented effectively. It is important that casinos review NRA and sectoral risk assessment (if available) while conducting their institutional risk assessment.

Risk assessments guide casinos in optimal allocation of the available resources towards the AML/CFT efforts and thereby implement risk-based approach to AML/CFT program effectively and efficiently. The nature and extent of the ML/TF risk assessment should be in commensurate with the nature and size of the business. On the basis of the risk assessment, casinos should formulate policies, procedures and control measures to mitigate and manage the identified risk in an effective manner.

Employee Screening and Integrity

Casinos should implement adequate screening procedures to ensure high ethical and professional standards when hiring new employees. This ensures that individuals joining the institution do not pose an internal risk to the integrity of the financial system. Fit and proper test criteria to be adopted by casinos during selection and appointing the employee including senior management and board members.

Ongoing Employee Training

Casinos should maintain an ongoing employee training program. The training should be tailored to the specific responsibilities and risk exposures of different staff members. It aims to ensure that employees fully understand their AML/CFT obligations, can identify suspicious transactions/activities , and are kept up to date on evolving regulations and illicit financing typologies

Compliance Officer

The role of a compliance officer (or chief AML/CFT officer)[4] involves acting as the central figure in an entity's AML/CFT regime. Their key responsibilities and characteristics include:

- **Ongoing Monitoring (Second line of defense):** They are responsible for continuously monitoring the fulfillment of all AML/CFT duties. This involves conducting sample testing of compliance and reviewing exception reports to ensure procedures are properly implemented.
- **Reporting and Escalation:** They hold the specific responsibility of reporting suspicious transactions to the appropriate authorities. Additionally, they must alert senior management or the board of directors if the institution is failing to address AML/CFT procedures responsibly.

[4] As per Section 7P of ALPA, 2008

- **Primary Point of Contact:** The official serves as the main liaison regarding all AML/CFT issues for both internal departments and external authorities, including supervisory bodies and FIU.
- **Independence and Authority:** To guarantee impartial advice and unbiased judgments, the official should be at a management level and should not have business line responsibilities to avoid potential conflicts of interest. They must have a direct reporting line to senior management or the board, and possess enough stature and authority to ensure compliance issues are taken seriously.
- **Expertise and Proactive Management:** The official should be fully conversant with the institution's AML/CFT regime, regulatory requirements, and ML/FT risks. They must be provided with sufficient resources to effectively execute their duties and play a proactive role in risk management.

IX. SUPERVISION & ENFORCEMENT

Casinos are required to cooperate with the DoT during onsite inspection and avail transaction and account records when requested. They should also provide data and reports when requested on offsite basis.

The DoT, as the designated supervisor, has the power to:

- Issue formal warnings and financial penalties.
- Revoke or suspend business license.
- Escalate issues to FIU and law enforcement agencies.
- Other sanctions under Section 7V of ALPA, 2008

Various administrative penalties and other sanctions may be taken against the casinos that do not comply with AML/CFT measures. The amount of administrative fines depend on the type and seriousness of non-compliance. These administrative measures are covered along with the directives issued by the DoT.

Annex 1: STR and SAR-related red flags for Casinos, included in FIU's STR Reporting Guidelines[5]

1. If activities are inconsistent with the customer's profile.

2. If false identity is used to open and operate casino accounts.

3. If the client provides inconsistent identity information or refuses to provide required identification.

4. If client is known to have used multiple names.

5. If there is a dramatic or rapid increase in size and frequency of transactions.

6. If the client requests that a winning cheque be issued in the name of a third party.

7. If noticeable changes are observed in spending/betting pattern.

8. If clients request cheques not related to gaming winnings, often purchasing chips with large amounts of cash and then exchanging them for cheques at the end.

9. If a client purchases a large volume of chips with cash, participates in limited gambling activity to create the appearance of significant gambling, and then cashes the chips for a casino cheque.

10. If the client purchases and cashes out casino chips with little or no gaming activity.

11. If the client shows no concern for winning or losing, but displays unusual interest in casino policies on payouts.

12. If client exchanges small denomination bank notes for large denomination bank notes.

13. If any deviation in transactions or suspicious activities is identified by casino business.

14. If funds are withdrawn from account shortly after being deposited.

15. If there is lack of proper sources of deposited amount.

16. If transactions involve PEPs and high net worth individuals who are linked to each other.

17. If players are from high-risk countries.

[5] These guidelines are minimum, the casino may develop and determin additional red flags to detect and ensure suspicious transaction and activity.

Related Links:

goAML Registration Portal: *https://goaml.fiu.nrb.org.np/PRD/Home*

FIU Website: *https://www.nrb.org.np/departments/fiu/*

DoT Website: *https://tourismdepartment.gov.np/*

TFS Portal: *https://moha.gov.np/en/post/tfs-login*

FATF Website: *https://www.fatf-gafi.org/en/home.html*

TTR Guidelines: *https://www.nrb.org.np/contents/uploads/2025/08/Threshold-Transaction-Reporting-Guidelines-Updated-July-2025.pdf*

STR Guidelines: *https://www.nrb.org.np/contents/uploads/2025/10/STR.SAR-Guidelines-Updated-July-2025.pdf*

***