नेपाल सरकार

राष्ट्रिय सहकारी नियमन प्राधिकरण
पुल्चोक, ललितपुर, नेपाल ।
(स्थापना-२०८१)

AML/CFT Guidance to Cooperatives

National Cooperative Regulatory Authority

September, 2026

(Amended and re-uploaded on: 11 September, 2026)

नेपाल सरकार

राष्ट्रिय सहकारी नियमन प्राधिकरण

पुल्चोक, ललितपुर, नेपाल ।

(स्थापना-२०८१)

Abbreviations and Acronyms

ALPA	Asset (Money) Laundering Prevention Act, 2008
ALPR	Asset (Money) Laundering Prevention Rules, 2024
AML	Anti-money laundering
MDD	Member Due Diligence
CFT	Combating Financing of Terrorism
DNFBP	Designated Non-Financial Business and Profession
DeoC	Department of Cooperatives
DPMS	Dealers in Precious Metals and Stones
EMDD	Enhanced Member Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
ID	Identification
ML	Money Laundering
NCRA	National Cooperative Regulatory Agency
NRA	National Risk Assessment
OCoR	Office of Cooperative Registrar
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

Money laundering and terrorist financing pose serious risks to the integrity and stability of the financial system. Financial cooperatives–like all financial institutions– can be exposed to these threats in the course of their business operations. Criminals seek financial products, including deposit and loan products, to conceal the origin and appearance of the illicit funds. Laundering can be attempted through structured cash deposit or layering through loan products. Likewise, cooperatives could be abused for raising fund for terrorist financing. Since banking sector generally has put in place more rigorous measures, criminals may divert their illicit proceeds to the usually less supervised financial cooperatives owing to displacement effect.

It is important that the cooperatives 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 cooperatives about their AML/CFT-related obligations.
- To provide guidance to the cooperatives to implement AML/CFT related measures.

Scope and limitations

This Guidance is applicable to all the registered cooperatives conducting saving and credit transactions. Furthermore, the Guidance is mainly intended to enhance awareness and compliance by these cooperatives. It doesn't include all the compliance requirements. Cooperatives should consult the ALPA, 2008, ALPR, 2024 and the directives issued by the NCRA and OCoR (previously DeoC).

II. MONEY LAUNDERING AND TERRORIST FINANCING RISKS IN COOPERATIVES SECTOR

Cooperatives could be abused for the laundering of the proceeds from a large number of predicate crimes. Its deposit accounts may be used for storage of funds derived from legitimate-looking sources by its members but could be proceeds from the corruption or bribery committed by the members' family members or relatives. Cooperative accounts may also be used as a mule account or stooge account and used for hiding the proceeds from various types of fraud, including cyber-enabled fraud. Besides, cooperatives can be used for self-laundering of proceeds from cooperative fraud.

Cooperatives may exhibit specific structural vulnerabilities. The proximity and trust-based relationships can be exploited, and smaller institutions may lack the capacity and expertise to identify complex illicit activity. Cooperatives often serve the members whose activity is cash-based, which increases the risk of placement. Furthermore, deficiencies of control measures, staff training, availability of technology and the ability to detect ML activity create critical vulnerabilities for criminals to exploit. Many cooperatives still grapple with understanding the ML/TF risks associated with legal persons and arrangements, which criminals and money launderers misuse for laundering the illegal proceeds.

In Nepal, the National Risk Assessment (NRA) finds that the overall ML vulnerability as medium-high, reflecting large size of the sector, extensive financial activity, involvement of PEPs, business persons, abuse of funds beyond cooperative laws and significant weakness in AML/CFT implementation and supervision. The NRA also finds that financial transparency in cooperatives is compromised by incomplete MDD, unverified know your member (KYM) profiles, as well as, inadequate PEP and beneficial ownership identification. Moreover, the high volume of cash transactions, inadequate transaction monitoring and limited suspicious transaction identification & reporting make the sector vulnerable to money laundering activities.

III. INTERNATIONAL STANDARDS

FATF Recommendations pertaining to Cooperatives:

The FATF requires cooperatives to implement preventive measures similar to those of traditional banks. All the provisions under the Recommendations 10, 11, 12, 15, 16, 17, 18, 20, and 21 (see footnote)[1] apply to cooperatives. As cooperatives rarely conduct cross-border transactions, the Recommendations 13 (Correspondent Banking), 14 (Money or Value Transfer Services) and 19 (Higher-risk countries) are not applicable to the cooperatives.

IV. MEMBER DUE DILIGENCE (MDD)

MDD is a foundational process used by Cooperatives to verify the identity of their members, understand their financial background, and prevent criminals from abusing the cooperatives' financial system for ML or TF. The process involves identifying the members and verifying their identity using reliable, independent source documents, data or information.

MDD involves looking for answers for the following questions:

[1] Recommendation 10, 11, 12, 15, 16, 17, 18, 20 and 21 deals with customer due diligence, record keeping, politically exposed persons, new technologies, payment transparency, reliance on third parties, internal controls, reporting of suspicious transactions, and tipping-off & confidentiality respectively. For further details, please refer to: FATF Recommendations

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 organizational structures. • MDD 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 members should be treated the same. • Politically Exposed Persons (PEPs) and other high-risk individuals should be subjected to enhanced due diligence.

MDD 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,
- Understanding the intended purpose of the relationship
- Documenting the source of funds.

When should a cooperative conduct MDD?

A cooperative should conduct MDD when opening an account for a new member. MDD should also be conducted when previously obtained information is insufficient, outdated, or requires verification. Likewise, MDD should be conducted when there are suspicions or concerns regarding money laundering or terrorist financing (ML/FT), as well as when conducting high-risk transactions or dealing with high-risk members, including Politically Exposed Persons (PEPs).

In case of all financial institutions, including cooperatives, there is a cash withdrawal limit of NPR 500,000 on a single transaction (Nepal Gazette Notice effective 15 January 2026). However, withdrawal above the threshold amount may be allowed if application citing specific reason is received for such withdrawal and the request is found reasonable.

Beneficial Ownership

Understanding who ultimately has control of a member plays an important role in detecting, disrupting and preventing money laundering and terrorism financing. Cooperatives should identify the beneficial owners of their members 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 member, transaction (account), property, legal person or legal arrangement."* Note that a cooperative's member may have more than one beneficial owner.

MDD involves identification of beneficial owners (in addition to the member) 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 member profile
- In case of a personal account, ensure that it is not a mule account

Ongoing Monitoring

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

Enhanced Member Due Diligence (EMDD)

EMDD is a rigorous process applied to high-risk members 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.

EMDD 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 member, beneficial owner and related persons,
- Obtaining additional information on the member 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 member,
- 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.

Cooperatives 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 member 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 at least once in a year, by obtaining data 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

Cooperatives must maintain all necessary records on transactions, as well as on MDD 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 cooperatives 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.
- ***MDD and Account Records:*** Cooperatives should keep all records obtained through the MDD 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 cooperative to adequately monitor its relationship with its members, wherever the relationship is established. Cooperatives 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 cooperatives, 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 cooperatives, 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 cooperatives (See Annex-1). Once red flags are detected, the cooperatives should analyze the transaction or activity to assess suspicion.
- Reports are to be filed to FIU through the goAML system. The cooperatives must be registered in the software first in order to be able to file suspicious transactions. The cooperatives are to 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 member. The act of breach or any tipping-off is punishable under the section 44A of ALPA, 2008.

Other Reporting

- Cooperatives are required to file TTR within 15 days of such transaction. FIU-Nepal has issued Threshold Transaction Reporting Guidelines (Updated July 2025). The threshold transaction is Rs.1 million or more of cash deposit made through single transaction or multiple transactions by a member in a day.[3] *
- Cooperatives should submit institutional risk assessment reports as per the provision of section 35 of ALPA, 2008 to the OCoR/DeoC or NCRA. Furthermore, they are required to submit regulatory reports as directed.

VII. TFS-RELATED

Cooperatives must screen members 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. Cooperatives should contact the NCRA or OCoR/DeoC for access to the Portal.

If a member matches a designation:

- Verify that the member 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: deposit in a cooperative account or any other assets in possession with designated person during the transaction with Cooperatives),
- Do not notify the member before freezing the assets,
- Notify the NCRA/OCoR within three days from time of freezing of assets.

---

[2] www.nrb.org.np/contents/uploads/2025/10/STR.SAR-Guidelines-Updated-July-2025.pdf
[3] www.nrb.org.np/contents/uploads/2025/08/Threshold-Transaction-Reporting-Guidelines-Updated-July-2025.pdf
* Amended on 11 September 2026 as per the TTR Guidelines of NRB and the Directive issued by NCRA.

VIII. INTERNAL CONTROL

Risk Management

FATF Recommendation 1 requires financial institutions 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 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 cooperatives review NRA and sectoral risk assessment (if available) while conducting their institutional risk assessment.

Risk assessments guide cooperatives 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, cooperatives should formulate policies, procedures and control measures to mitigate and manage the identified risk in an effective manner.

Employee Screening and Integrity

Cooperatives 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 cooperatives during selection and appointing the employee including senior management and board members.

Ongoing Employee Training

Cooperatives 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.

---

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

- **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.
- **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

Cooperatives are required to cooperate with the NCRA and OCoR/DeoC during onsite inspection and avail transaction and account records when requested. They should also provide data and reports when requested on offsite basis.

The NCRA and OCoR/DeoC, as the designated supervisor, has the power to:

- Issue formal warnings and financial penalties.
- Suspend operating license and deregistration.
- 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 cooperatives 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 NCRA/ OCoR.

Annex 1: STR and SAR-related red flags related to cooperative sector included in FIU's STR Reporting Guidelines[5]

1. *If a member attempts to open or operate accounts under a false name.*
2. *If a member is reluctant to provide standard information when opening an account, provides minimal or fictitious information, or submits details that are difficult or costly to verify.*
3. *If an account is opened with an address or employment location outside the local service area without a reasonable explanation.*
4. *If there is a sudden change in the member's financial profile, transaction pattern, or account activity.*
5. *If a member uses instruments, products, or services that are unusual for their known profile.*
6. *If a transaction appears suspicious and the member is blacklisted by the Credit Information Bureau or categorized as high-risk by the reporting institution.*
7. *If member is suspected for using personal account for business or other purposes, or vice-versa.*
8. *If member conducts series of complicated transfers of funds that seems to be an attempt to hide the source and intended use of the funds.*
9. *In case of an account opened in the name of an entity, an organization or association, which is found to be linked or involved with a suspected terrorist organization.*
10. *If a member frequently deposits funds identified as proceeds from asset sales, but the existence or ownership of such assets cannot be substantiated.*
11. *If there are large cash withdrawals from a previously dormant or inactive account.*
12. *If an account is closely connected to other business accounts without any clear or legitimate reason for the relationship.*
13. *If deposits to or withdrawals from a corporate account are primarily in cash.*
14. *If member requests movement of funds that are uneconomical or irrational without valid justification.*
15. *If cheques are regularly returned due to insufficient funds.*
16. *If a member is found to have used, made, or been involved with counterfeit coins or currency.*
17. *If there is a large volume or high frequency of transactions in an individual savings account that significantly differs from the member's initial declaration.*

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

18. *If a member repeatedly withdraws funds from their own individual account and deposits them into multiple other accounts without valid reasons.*

19. *If funds are transferred from a cooperative society to the personal bank accounts of its board members.*

20. *If dividend payments appear unusual or disproportionate to the actual shareholding.*

21. *If cooperative staff or employee accounts are used to route funds on behalf of non-members in order to artificially inflate fund balances, conceal true ownership, or bypass cooperative membership restrictions.*

22. *If digital or mobile payment platforms linked to cooperative accounts are used without clear operational justification or are inconsistent with typical cooperative transaction patterns.*

23. *If third parties unrelated to the cooperative's members or leadership frequently manage or authorize transactions on cooperative accounts.*

24. *If documentation related to membership verification, capital contributions, or loan disbursements is inconsistent, incomplete, or missing.*

25. *If the cooperative conducts cross-border fund transfers or remittances from its account maintained at commercial banks on behalf of a member.*

26. *If cooperative accounts are used to repeatedly route funds among related accounts without a clear business purpose, indicating potential layering or circular transactions.*

27. *If cooperative accounts are used for cash-based fundraising campaigns with unclear beneficiaries or unverifiable project outcomes.*

28. *If loan repayments show unusual patterns, such as early full settlement or installment schedules inconsistent with normal cooperative lending practices.*

29. *If cooperative accounts are used for real estate or asset purchases without proper valuation, supporting documentation, or official registration.*

Related Links:

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

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

DeoC Website: *https://deoc.gov.np/*

NCRA Website: *https://ncra.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*

***