
Update on the implementation of IFAD's Anti-Money Laundering and Countering the Financing of Terrorism Policy, and controllership

Document: EB 2022/137/R.23

Agenda: 13(a)

Date: 4 November 2022

Distribution: Public

Original: English

FOR: REVIEW

Useful references: IFAD Anti-Money Laundering and Countering the Financing of Terrorism Policy ([EB 2019/128/R.41/Rev.1](#)) and Internal Control Framework ([EB 2019/127/R.39](#)).

Action: The Executive Board is invited to review and take note of the update on the implementation of IFAD's Anti-Money Laundering and Countering the Financing of Terrorism Policy, and controllership.

Technical questions:

Advit Nath

Director and Controller
Financial Controller's Division
e-mail: a.nath@ifad.org

Update on the implementation of IFAD's Anti-Money Laundering and Countering the Financing of Terrorism Policy, and controllership

I. Background

A. Financial crime and controllership functions at IFAD

1. As IFAD's business model evolves to advance its mandate, the organization is further decentralizing, increasing delegation of authority (DoA) to the field, and engaging with the private sector. While these changes bring new opportunities, they are altering the risk profile and materiality of transactions. It is important to mitigate the related risks in order to protect IFAD's clean audit opinion and ensure continued donor and stakeholder confidence.
2. Two ways in which IFAD manages such risks is by compliance with the IFAD Anti-Money Laundering and Countering the Financing of Terrorism (AML-CFT) Policy supported by the financial crime function and compliance with the Internal Control Framework (ICF) supported by the controllership function.
3. Following approval of the AML-CFT and ICF policies at the end of 2019, the two functions were created by a President's bulletin in 2020 and set up in the Financial Operations Department within the Financial Controller's Division (FCD).
4. The FCD financial crime function, which is a compliance function, is responsible for: (i) performing daily screening and assessments (for sanctions, money laundering, terrorism financing, tax evasion, illicit fund flows and related areas) of entities and individuals IFAD conducts business with per the AML-CFT Policy ensuring that vendor/partner/staff master files are protected, as the custodian; and (ii) leading IFAD's personal data privacy and protection mechanisms, as the custodian.
5. The FCD controllership function, which is not an audit function but a support and review function between the first and third line functions, is responsible for: (i) setting and assessing optimal controls across IFAD per the ICF, which adheres to the principles established by the Committee of Sponsoring Organizations of the Treadway Commission and leading practice among international financial institutions (IFIs), multilateral development banks (MDBs) and United Nations agencies, ultimately aiming to support clean external audit opinions; (ii) providing digital tools and business process improvements that enable business efficiency; and (iii) enabling empowerment and monitoring of DoA, as the custodian.
6. Both functions are staffed, have established procedures and processes, and have implemented systems as well as communication and training to embed the functions into the organization.
7. Since October 2021, the financial crime function prevented IFAD from conducting business with 15 parties considered to have financial crime or related issues and deemed high risk or red (since inception in 2020: 34 parties). Enhanced monitoring or watch list parties since October 2021 totalled 43 parties (since inception in 2020: 71 parties).
8. Since October 2021, the controllership function has assessed and supported or is currently supporting 17 IFAD field offices, with an additional five offices planned for support by year-end 2022, bringing the total to 22 IFAD offices. To date, 35 recommendations for control enhancements have been provided. These digital tools (digital signatures, financial crime software, DoA e-forms, TeamMate+ Controls e-certifications, access rights reports, e-petty cash, e-forms for portfolio handover, and e-inventory) are new tools built, implemented and launched that were not available prior to inception of this function. Further, training has been provided to 1,077 personnel to date.

9. FCD works closely with other departments and divisions, particularly the Programme Management Department in IFAD offices globally, as well as the Office of the General Counsel, and shares relevant findings with the Office of Enterprise Risk Management, Office of Audit and Oversight and, as needed, the Ethics Office. FCD participates in IFI/MDB forums as a member to learn and share on leading practices. In 2022, FCD participated in the IFI/MDB Private Sector Integrity Meeting, where it presented IFAD's work on personal data privacy and protection, and participated in the sixth annual MDB Privacy Symposium led by the International Finance Corporation and the European Bank for Reconstruction and Development.
10. The purpose of this paper is to provide an overview of the progress made between 1 October 2021 and 30 September 2022 in the implementation of the ICF and AML-CFT policies approved by the Executive Board, and the related functions implementing the policies.

II. Implementation and results

A. Financial crime function

11. The IFAD AML-CFT Policy aims are to prevent IFAD from conducting business with parties that are on the sanctions lists adopted by IFAD or have been involved in money laundering, terrorism financing or related risks – and thereby reduce the organization's exposure to reputational damage, financial loss or legal liability.
12. The financial crime function implements the AML-CFT Policy and leads on all AML, CFT, sanctions, tax and related areas. In 2022, a Data Protection Officer post was created to lead data privacy and protection matters in IFAD to comply with IFAD's personal data protection guidelines.
13. Financial crime procedures, aligned to the AML-CFT Policy, were developed which detail the scope of screening and assessments, approach to integrity due diligence (IDD) and enhanced due diligence monitoring including know-your-customer requirements, methodology for ratings, escalation, recommendations and reporting as well as training and support.
14. An industry-standard automated software solution by LexisNexis has been implemented at IFAD and currently has more than 2 billion entries containing enforcement records, adverse media and adopted sanctions lists, among other relevant data. The LexisNexis financial crime software performs automatic daily screening on about 23,000 parties in IFAD's vendor/partner/staff master files, and any exceptions are flagged for follow-up by a financial crime specialist. The tool also captures downstream partners IFAD conducts business with. The software is available to all IFAD staff globally, who also use the software to confirm if there are any integrity concerns on prospective partners/vendors/consultants. Figure 1 illustrates a dashboard used by the team for analysis.

Figure 1
Dashboard used by the FCD financial crime team



15. IFAD has incorporated key clauses on AML-CFT and sanctions in negotiated borrowing and financing agreements, including supplementary funds agreements. AML-CFT processes have also been incorporated in IFAD documents such as the Framework for IFAD non-Sovereign Private Sector Operations, strategy for supplementary resources, environmental, social and corporate governance due diligence procedures, Green Climate Fund guidelines, the Integrated Borrowing Framework, letter to the borrower, Treasury Guidelines and IFAD's Investment Policy Statement.
16. Deep-dive enhanced due diligence (EDD) assessments are conducted for high-risk activities/transactions/parties and may include detailed know-your-customer and money laundering, terrorism financing and related risk questionnaires and reviews, deeper-dive verification of ultimate beneficial ownership, regular scheduled assessments at shorter intervals, potential use of investigative firms hired locally, and detailed reporting and audit trails.
17. Following an IDD and/or EDD assessment, each party IFAD is conducting business with or planning to do so is provided a rating and recommendation based on the risk assessment according to the standard IFAD four-point risk scale – high (red), substantial (orange), moderate (yellow) and low (green) aligned to IFI/MDB industry standards. Any high or substantial risk parties are immediately deactivated in IFAD's master files, thus no payment can be made to these parties until reactivated if and when risks are mitigated. There is a key control and monitoring of activation and reactivation of items in master files within FCD.
18. As at September 2022, of the around 23,000 parties screened on a daily basis, cumulatively the vast majority (99.1 per cent) were green (low risk), a small percentage (0.8) were orange or yellow (substantial or moderate risk) where there are certain less significant concerns that do not warrant curtailing a business relationship, and a smaller percentage (0.1 per cent) were red (high risk) where IFAD would normally curtail or not enter into a business relationship. The procedures require escalation of substantial and high-risk items to the IFAD Controller who is actively involved in these items, and escalation of high-risk items to the Chief Financial Officer for awareness and review. In addition, regular reporting to the relevant risk committee is established.

19. IFAD launched personal data privacy guidelines in 2021 aligned to leading practices on personal data privacy and protection globally. These provide the eight principles for data protection (legitimate, fair and transparent use of data, purpose limitation, data minimization, accuracy, storage limitation, security, transfer of personal data protocols and accountability), roles for staff, types of personal data and special category data, rules for reporting data breaches, rights of data subjects and mechanisms to exercise these rights, requirements for data protection impact assessments, rules for sharing personal data, and governance and reporting processes. IFAD successfully passed the European Union assessment for this new pillar.




B. Controllership function

20. The FCD controllership function and ICF aims are to ensure robust internal controls at each decentralized field office and headquarters office, roll-out of digital tools to enhance automated controls rather than rely on manual controls susceptible to error and fraud, and to enhance DoA particularly to the field offices in order to empower and enable the IFAD front-line functions.
21. Through a combination of physical and virtual missions, the function provides dedicated review and support to IFAD field and headquarters offices, which was not provided at IFAD before. The goal is for IFAD to be fully comfortable with the internal controls at all its global offices, which are certified by heads of offices, and that these offices are equipped with the latest digital tools and empowerment through DoA in order to operate effectively to achieve IFAD goals.
22. On its first objective of ensuring robust internal controls, assessment of optimal internal controls is performed per the annual risk-based workplan, on six dimensions: (i) access rights and duties segregation; (ii) delegation or sub-delegation of authority; (iii) bank accounts and cash; (iv) project procurement fraud risk; (v) financial closures; and (vi) fraud risk in business processes. It coordinates with relevant headquarters divisions that may have responsibilities in the six dimensions.
23. The six dimensions are assessed through control testing, which includes, but is not limited to, a review of: (i) results of a control questionnaire completed by the offices; (ii) discussions with IFAD office personnel; (iii) mapping of business processes, internal audit and external reports; (iv) internal dashboards; (v) access rights of personnel; (vi) data from procurement and other systems on potential fraud; (vii) hosting agency relationship and reconciliations; (viii) bank account and petty cash register and reconciliations; (ix) financial crime results and risks, fraud indicators and results; (x) consultant data and other material expense line items; and (xi) other relevant information to corroborate and support findings.
24. The outcome of the missions is a mission report that includes a controller's scorecard (table 1), which is a financial health card on the six dimensions reviewed for the IFAD office. Where control weaknesses are noted, recommendations are written in the report and an action plan is prepared by the office with a timeline for implementation and follow-up. The mission report also includes an annex (table 3) summarizing the digital tools and training status for follow-up.

Table 1

Controller's scorecard

	Internal control dimensions	Rating
Field office or division: internal controls in place	1. Access rights and duties segregation	
	2. Delegation and sub-delegation	
	3. Bank accounts, cash and assets safeguarding	
	4. Project procurement fraud risk	
	5. Financial closures	
	6. Fraud risk in business processes	
Overall internal controls score for office or division		

	No major control weakness or efficiency issues – no action required
	Some control weakness or efficiency issues requiring an action plan to remedy (up to 12 months)
	Significant control weaknesses or efficiency issues requiring an action plan to remedy (two to six months)

25. Once the mission report is agreed and issued, the head of office is required to complete a certification of adequate internal controls, which is signed digitally and used as a basis for the overall corporate certification of internal controls issued annually and signed by the President, Chief Financial Officer and Controller.
26. The function uses an industry-standard software solution TeamMate+ Controls for all of the above activities, ensuring an end-to-end digital approach to missions, documentation, reporting and certifications.
27. Since inception two years ago, the function has conducted 14 review and support missions with another three under way and five are planned by year-end 2022 (table 2). Of the 14 missions concluded, 11 were rated as green (no major control weaknesses), three were rated as yellow (some control weaknesses requiring action) and none were rated red (significant control weaknesses). In the same period, 35 recommendations were given, 18 were implemented and the remaining are on track for implementation by due dates.

Table 2

Controllership function list of IFAD field offices with review and support missions and recommendations

Regional division	List of countries with completed assessment	Number of recommendations issued	Number of recommendations in progress	Number of recommendations implemented
APR	Bangladesh	3	3	0
APR	China	2	1	1
APR	India	2	1	1
APR	Indonesia	3	3	0
APR	Philippines	1	1	0
APR	Viet Nam	3	0	3
ESA	Kenya	2	1	1
ESA	South Africa	3	2	1
LAC	Peru	3	0	3
NEN	Egypt	3	3	0
NEN	Sudan	3	0	3
NEN	Türkiye	3	0	3
WCA	Cameroon	3	2	1
WCA	Côte d'Ivoire	4	3	1

ESA	United Republic of Tanzania	Underway		
ESA	Rwanda	Underway		
LAC	Brazil	Underway		
ESA	Ethiopia	To be launched by end 2022		
LAC	Panama	To be launched by end 2022		
WCA	Senegal	To be launched by end 2022		
WCA	Nigeria	To be launched by end 2022		
WCA	Ghana	To be launched by end 2022		
	Total		38	20
				18

Note: APR = Asia and the Pacific Division; ESA = East and Southern Africa Division; LAC = Latin America and the Caribbean Division; NEN = Near East, North Africa and Europe Division; WCA = West and Central Africa Division

28. On its second objective of providing digital tools to enhance controls across IFAD, the function coordinates several key technology projects: (i) digital signatures; (ii) TRACE Blockchain by IFAD; (iii) roll-out of the LexisNexis financial crime software solution; (iv) Teammate+ Controls; (v) e-forms for DoA; (vi) e-forms for personal data privacy protection; (vii) e-access rights reports; (viii) e-petty-cash reconciliation reports; and (ix) e-form for the handover process for country directors.
29. Digital signatures have been implemented at IFAD, and in eight months of use over 4,000 pages were securely digitally signed with over 150 persons globally trained and further roll-out continuing. The TRACE Blockchain project traces funds from donor to farmer, has completed the pilot phase 1 and is now in phase 2 of implementation. The financial crime software is available to 700 staff globally who can query the system in advance of hiring vendors/consultants/partners. TeamMate+ Controls is used by 17 offices who have completed or are undergoing controllership review and support missions also used to digitally sign certifications on adequate internal control and appropriate use of DoA. Over 40 e-forms have been completed over the past year by staff globally to suggest new or modified DoAs. An e-access rights report has been prepared listing 1,716 access rights in IFAD Offices to ensure appropriate access rights by authorized persons only to key financial and core systems. E-petty cash reconciliations have been provided to two offices; e-forms for personal data breaches and data subjects to request information have been made available; and an e-form was created for handover by country directors who move offices to provide digital easy-to-find records when the portfolio handovers occur.

Table 3

Controllership function mission report annex on digital tools provided and training status

<i>Digital tool</i>	<i>Number of personnel provided with training</i>	<i>HQ / IFAD Country Office (Field)</i>
Digital signatures	151	HQ / Field
Financial crime software	704	HQ / Field
DoA e-forms	72	HQ / Field
Teammate+ Controls	52	Field
Access rights report	54	Field
E-petty cash	27	Field
E-forms for portfolio handover	5	Field
E-inventory	12	Field
Total	1 077	

30. On its third objective of DoA, the function is the custodian of IFAD’s Accountability Framework and the IFAD Delegation of Authority Framework, which aim to empower staff particularly in the field while ensuring a high level of accountability. A corporate DoA working group including FCD controllership revised over 40 DoAs

issued in President's Bulletin PB/2021/03 in five areas: (i) procurement; (ii) human resources; (iii) field operations; (iv) governance and protocol; and (v) budget and finance, thus increasing DoA across IFAD. Since then, 52 additional changes were made based on requests for changes to delegations through e-forms from staff globally, illustrating that DoA is a "living document" that adapts to changes to further empower staff.

31. In 2022, the most significant DoA of budget delegation to country directors was successfully implemented for two regional divisions – ESA and WCA – as phase 1 of the project. Since the launch, all country directors in Africa (ESA and WCA) totalling 50 persons have the ability to raise or make budget commitments and payments directly without having to route the requests through regional or headquarters offices, adding significant empowerment to field staff in support of IFAD's decentralization initiative.

III. Training, awareness and culture

32. Training, awareness and constant communication are fundamental to embedding these two new functions (financial crime and controllership) into IFAD's corporate culture.
33. Face-to-face training through a partnership with the UK-based Chartered Institute of Public Finance and Accountancy (with some sessions temporarily held virtually due to the COVID-19 pandemic) for 180 personnel has been completed since inception for both functions. Dedicated training was also provided to the 50 budget holders and assistants in the field who received new delegated budget authority.
34. E-learning modules have been built for data privacy and protection (completed by 35 staff including all data stewards) and a new e-learning module for DoA is close to finalization and will be rolled out by year-end 2022.
35. Blogs have been issued for each of the two new functions. In addition, intranet messages, permanent links in intranet corners and numerous presentations at divisional staff meetings about DoA, data privacy and protection aim to embed the new functions into IFAD culture.