Bank of South Sudan

BoSS On-site- Oversight Procedure

March 2026

Contents Page

GLOSSARY

BSD	Banking Supervision Department
BSS	Bank of South Sudan
FMI	Financial Market Infrastructure
IRP	Institutional Risk Profile
OD	Oversight Division
OPF	Oversight Policy Framework
OP	Oversight Plan
PFMI	Principles for Financial Market Infrastructures
PSD	Payment System Department
PSO	Payment System Operator
PSP	Payment Services Provider
RMA	Risk Management Assessment

1. Purpose

1.1 This procedure has the purpose of describing relevant processes for conducting the on-site oversight at Payment System Operators (PSOs) and Payment Services Providers (PSPs).

1.2 On-site oversight activities of the PSPs that are banks will be organized in coordination with Banking Supervision Department (BSD) of the BoSS. Joint on-site inspections will be organized in this regard between BSD and Payment System Department (PSD) of the BSS. PSD will delegate its staff members, when the BSD will plan and organize an on-site inspection at the banking PSP.Strong cooperation and coordination should be ensured between the BoSS functions responsible for payment system oversight (PSD) and for banking supervision (BSD). The need for cooperation and coordination rests on different reasons.

1.3 On-site oversight activities of non-bank PSPs will be planned and organized by the PSD.

1.4 On-site oversight of the PSOs will be carried out by the PSD only for the systems which are not operated by the BoSS, and which are subject to oversight according to the Oversight Policy Framework (OPF) of the BoSS. Financial Market Infrastructures (FMIs) and prominent systems which are operated by the BoSS will be overseen only according to the Procedure for conducting off-site oversight and OPF of the BoSS.

2. Reference documents

- The Bank of South Sudan Act, 2011 (Amendment),2023
- E-money regulation, 2017(Amendment),2025
- Oversight Policy Framework, 2026

3. Responsibility

The Oversight Division (OD) of the Payment System Department (PSD) will ensure compliance with this procedure.

4. Preparatory activities

4.1 Developing an institutional risk profile

The OD shall develop institutional risk profiles (IRP) for all entities subject to on-site oversight. The IRP presents a summary of all information on the entity that is relevant to an understanding of its risk profile. The IRP is a dynamic document and is constantly updated to ensure that it presents current and accurate information about the PSP or PSO. The IRP includes the risk management assessment (RMA) which is carried out based on the information collected by the OD during both off-site and on-site oversight. The RMA seeks to identify the major areas of risk which the institution faces, assesses the quality of the institution's management of such risks and determines prospects for the institution's risk profile. For more details on how the RMA is carried out please see the *Procedure for conducting off-site oversight.*

4.2 Developing an Oversight Plan

On the basis of the information contained in the IRP, including the outcome of the analysis presented in the risk matrix (please see the *Procedure for conducting off-site oversight*), the OD develops an oversight plan (OP) for all institutions subject to oversight. The OP sets out the oversight actions that are deemed to be appropriate in light of the information held on the institution and the related oversight concerns, including issues that have arisen as a result of the off-site oversight activities. The plan indicates the proposed period of the oversight inspections; it clarifies oversight objectives, and relevant oversight activities that should be undertaken during on-site inspections.

4.3 Submission of the Oversight Plan for approval

After that the OD has prepared the OP, and upon the endorsement of the plan by the PSD Director, the plan is submitted to the Governor/ Deputy Governor for the approval.

4.4 Submission of the Oversight Letter

Prior to the start of an on-site oversight, the Management of the entity subject to Oversight should be advised, by way of a letter, on the dates, objectives, and scope of the oversight inspection, and information requirements in respect to the upcoming oversight.

5. Conducting of the on-site oversight

The on-site oversight is of two types. These are *full scope* and *limited scope* oversight on-site activities.

5.1 In conducting the full scope oversight, the oversight team should carry out verification of the adequacy of risk management framework and of regulatory compliance of the overseen entity, and find out whether any infringements of the legal and regulatory framework has been admitted by the overseen entity, and whether risk management framework is robust and adequate.
The oversight team will examine and assess the following checklist of relevant elements during the on-site inspection:

- legal charter of the overseen entity,
- a description of the overseen institution's organizational structure which should be well-defined, transparent and with a consistent distribution of responsibilities;
- the structure of executive bodies of the overseen entity and the line of responsibility;
- a description on the use of agents and branches;
- a description of the outsourcing conditions and arrangements;
- documents attesting that the overseen entity holds capital required by the legal and regulatory framework;
- a list of shareholders /associates and shares /holdings held in the overseen entity's capital, data and documents relating to them, which contain information according to identity /registration documents
- a detailed description of the activity of the overseen entity and financial reports confirmed by an external auditor;
- internal procedures to identify, manage, monitor and report the risks to which the overseen entity is or might be exposed (governance risk, financial risk, operational risk, etc,);

- internal control mechanisms, including administrative and accounting procedures;
- internal control arrangements for measures required to comply with obligations in relation to anti-money laundering and anti-terrorist financing;
- business continuity and security measures for payment system administration/ payment services provision, including clear identification of critical operations, continuity plans and a procedure for testing and periodic review of adequacy and effectiveness of the plans concerned;
- the organization and management of information systems, including the method of protecting information and personal data of payment system participants/payment services users, and a description of the process for recording, monitoring, supervising and restricting access to sensitive data regarding payments;
- procedures in place to monitor, handle and follow up a security incident and security related customer complaints, including an incidents reporting mechanism;
- an IT security policy document, including a detailed risk assessment in relation to its payment services provision/payment system operation and a description of security control and mitigation measures taken to adequately protect payment service users/payment system participants against the risks identified, including fraud and illegal use of sensitive and personal data;
- regulations, internal policies and other relevant documents that will prove that the overseen entity has adequate and safe measures for protecting the funds of payment system participants/payment service users and of payment instruments used
- reports and the internal documents prepared as a result of executed operations,
- internal and external acts of business (contracts, certificates, minutes, applications, informative notes, etc.), including on the shareholders / associates, beneficial owners, customers, counter-agents of the person subject to control,
- other relevant documents and data, based on the requirements stipulated in relevant legal and regulatory framework and off-site oversight carried out by the BSS.

5.2 Limited scope (targeted) oversight covers issues that exist at a particular institution or may relate to an industry-wide issue in which case limited scope oversight would be undertaken at all relevant institutions

6. Exit meeting

After the conclusion of every on-site oversight activity, the oversight team will hold an exit meeting with the management of the overseen institution to discuss oversight activity findings, conclusions, and recommendations. The exit meeting aims at pointing out and having common observation on the findings of the oversight.

7. Oversight Report

After that the Oversight Division ensures that the report is refined; it will submit it to the BSS Management accompanied with a letter to be addressed to the overseen institution outlining the key recommendations.

The Oversight Report will contain the following elements:

- the date and place it was drawn up;
- the date and number of the decision (oversight letter) of the BSS, based on which the oversight inspection was carried out;
- the name and address of the inspected entity;

- period of inspection;
- information on the oversight inspection results, including the infringements and risk management weaknesses identified and their nature;
- the name, surname and signatures of the inspectors who carried out the oversight inspection.

From the findings, the institution risk profile will be updated and the oversight team will continue to monitor the implementation of recommendations by the overseen institution.

Johnny Ohisa Damian

Governor

Bank of South Sudan