

Background

The UN Security Council resolutions 1267 (1999) and 1333 (2000) established a list of terrorist suspects and a sanctions committee, which have expanded over the years to encompass a range of lists and committees. UN member states and UN Agencies, funds, and bodies are obligated to comply with these resolutions as relevant, recognizing the humanitarian carve outs that exist to ensure that operations can remain principled. One of the methods by which the Agency ensures compliance and neutrality is by conducting bi-annual screening in January and July, as well as integrating screening into normal business processes led by the respective department. The bi-annual screening process is designed to align with Security Council resolutions and uphold their provisions.

Bi-annual screening analyzes datasets of around 6 million registered Palestine refugees, personnel, private individuals, and entities. It covers funds received from or paid to suppliers, loan recipients, donors, implementing partners, and third parties. The process is overseen by Protection division and performed in collaboration with relevant departments.

The process involves checking for potential name matches against the UN Security Council Consolidated List using technical algorithms. It is noteworthy that there have been no confirmed matches reported thus far.

In late 2022, a major update of screening process was initiated, including integrating the LexisNexis risk solution (“Bridger Insight™ XG” and world compliance dataset) to facilitate the screening process. “Bridger Insight™ XG” replaces internally developed technical algorithms by providing the platform for configuration of the required business rules while “World Compliance” is expected to facilitate screening against the most up-to-date UN sanction list.

Objective and Purpose of Audit

The audit aimed to assess whether governance, risk management and internal control processes over the bi-annual screening process were adequate, effective and in line with the relevant procedures. The period of review focused on 3 cycles between July 2021 to January 2023.

What DIOS concluded

The bi-annual screening process was assessed as “Partially Satisfactory – Major Improvement Needed,” which means that “The assessed governance arrangements, risk management practices and controls were generally established and functioning but need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved.”

The rating was due to the need to enhance standard operating procedures (SOPs), conduct a risk assessment to validate adequacy of coverage for screened datasets, and review the effectiveness of algorithms used in the screening process. Although there are areas for improvement, DIOS acknowledges that the screening of relevant data was carried out as expected during the audited periods. Management's efforts to address some of the identified issues are highlighted in the good practices section.

DIOS observations on the different components of the screening process reviewed are summarized below:

Governance: Roles, responsibilities, and general screening practices have been defined, with draft SOPs in place. However, further enhancements are needed to align the SOPs with the actual screening process, planned automation efforts, and process redesigns. It is also important to include provisions for data privacy and protection during screening.

Data collection: The SOPs define the relevant datasets for the screening process, but their coverage is affected by the cut-off period and exclusion of certain data subgroups. Additional datasets that could be valuable for screening have been identified

Screening algorithm: Independent testing highlighted the need for improved robustness in the SQL-based algorithms used for screening. These algorithms also involve manual interventions and have limited audit trail capabilities.

Oversight and monitoring: The assessment, validation, and clearance of potential matches lack standardization, with identified gaps in the process. During the audit, different practices were observed, and evidence of screening completion was not available for all datasets.

Reporting and Knowledge management: Document management lacks a clear and systematic approach. Additionally, there is a need to establish a specific internal reporting process upon completion of each screening cycle.

Good Practices

At the time of reporting, efforts were ongoing to update existing SOPs and finalize the implementation of the LexisNexis solution to provide more robust outcomes. Rollout of these is scheduled for the July 2023 screening cycle.

What DIOS recommended

DIOS made key recommendations across 4 categories aimed to effectively strengthen the operating effectiveness of the screening process as summarised below. Protection Division should:

1. Accelerate **policy and SOP enhancements** for a consolidated and systematic approach to Agencywide screening, including training and communication efforts for stakeholders and in particular addressing:

- a. Management of privacy and data protection risks and implementation of access controls for screening data on local user machines
- b. establishing procedures for checking minimum quality requirements before conducting screening
- c. Clarifying requirements for cut-off periods and dataset subgroups to ensure complete and accurate data extraction.
- d. Formalize procedures for assessment, validation, communication, and clearance of

potential matches, defining threshold requirements and roles/responsibilities.

- e. Strengthen supervisory and oversight procedures, consider automated exception reporting and pre-built workflows.
- f. Establishing a process for reporting screening results to demonstrate compliance with screening policy obligations.

2. Incorporate regular **risk assessments** in relevant departments as part of the screening process to evaluate coverage adequacy and ensure consistency in implementation.

3. Configure the proposed **automated solution** (LexisNexis) to address technical gaps before implementation, such as matching capabilities and reporting.

4. Implement **continuity measures** for screening data availability, including migrating records to a centralized location to mitigate keyman risk.

What management is doing to address DIOS recommendations.

Management accepted the recommendations and are in the process of implementing them. Specifically, management is prioritizing the development of new SOPs, including on supervisory oversight and strengthening of controls on data collection, is intended to safeguard the overall effectiveness of the screening process.

Further, the planned implementation of "LexisNexis" by end of June 2023 for the July screening process may address areas highlighted for management attention in this report. Recommendations #1c and #1f are also partially addressed through implementation of the new solution, by having capability to flag datasets with low quality and generation of consolidated reports for completed screening cycles.

In addition, recommendation #1d, #1e and #4, could be partially addressed by the new solution, as system controls configured as part of the business rules are expected to standardize thresholds for identification of potential matches, provide better controls over access management, auditability, and continuity in

alignment with the Agency's Information security policies.

On the other hand, risk assessments by relevant departments to regularly evaluate the adequacy of

the scope of coverage remain a high priority to safeguard the overall effectiveness of the screening process.

Methodology, Approach and Disclosure

DIOS conducted an audit of the bi-annual Screening process to assess the adequacy and effectiveness of governance, risk management and internal control processes over UNRWA's screening against the UN consolidated sanction list. The audit focused on the design and operating effectiveness with respect to, governance, completeness of data collected and its management, technical algorithms, to better support management decision making for the overall enhancement in policy, internal controls, and implementation of the new automated screening process.

The audit considered the ongoing major upgrade to its bi-annual screening process, updating its SOP and transitioning the technical SQL algorithms towards "LexisNexis" risk solution, a new, automated, bi-annual screening process.

The audit covered three screening cycles i.e., December 2021, June, and December 2022 across the screening sub processes that included governance, collection of data, technical screening algorithms, oversight & monitoring, and knowledge management (record keeping).

The audit approach included enquiries and discussions with relevant staff, review of control processes and documents, analysis and examination of selected samples and other procedures deemed necessary including re-performance by building test cases for review of the technical algorithms. The fieldwork was conducted in two sprints i.e., November 2022 and between February and March 2023.

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing. It was completed in conformity with the approved work plan and took into consideration the risk assessment exercise conducted prior to the audit.

Pursuant to OD14, this summary of findings and recommendations including management action taken to address recommendations is made publicly available on the DIOS internet page upon issuance of the report on 26 July 2023.