UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

AUDIT

OF

DATA MANAGEMENT

IN

UNDP

Report No. 2277

Issue Date: 18 November 2020

Report on the Audit of Data Management in UNDP
Executive Summary

The UNDP Office of Audit and Investigations (OAI) conducted an audit of data management in UNDP from 6 July to 14 August 2020. Data management is an overarching term that describes the processes used to plan, specify, enable, create, acquire, maintain, use, archive, retrieve, control, protect and purge data. Given that data is an asset, which when managed well can increase an organization's effectiveness and contribute to its success, proper data management is important. The audit aimed to assess the adequacy and effectiveness of the governance, risk management and control processes relating to the following areas and sub-areas:

  (a) Data governance
  (b) Data privacy / security
  (c) Data classification / quality
  (d) Data warehousing / business intelligence

The audit covered the activities regarding data management from 1 January 2019 to 30 June 2020. This was the first audit regarding data management in UNDP.

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*. Due to the COVID-19 pandemic, the audit was conducted remotely. Scope limitations due to the nature of the remote audit related to the following activities:

  (a) Meetings with all parties involved in the audit were done virtually, limiting the audit team's observation of auditees' interaction and dynamics.

Overall audit rating

OAI assessed the Office's performance as **partially satisfactory/some improvement needed**, which means "the assessed governance arrangements, risk management practices and controls were generally established and functioning, but need some improvement. Issues identified by the audit do not significantly affect the achievement of the objectives of the audited entity/area." This rating was mainly due to the lack of an approved comprehensive data privacy policy, and lack of metadata management procedures.

Key recommendations: Total = **8**, high priority = **2**

The eight recommendations aim to ensure the following:

Objectives	Recommendation No.	Priority Rating
Achievement of the organization's strategic objectives	1, 2, 8	Medium
Effectiveness and efficiency of operations	4, 5, 6	Medium
	7	High
Compliance with legislative mandates, regulations and rules, policies and procedures	3	High

For high (critical) priority recommendations, prompt action is required to ensure that UNDP is not exposed to high risks. Failure to take action could result in major negative consequences for UNDP. All high (critical) priority recommendations are presented below:

Lack of an approved comprehensive data privacy policy (Issue 3)	Although UNDP acknowledged the importance of data privacy, the organization did not have a comprehensive data privacy policy.

Recommendation: The Bureau for Management Services should develop and submit for approval a comprehensive data privacy policy and related procedures with the purpose to:

(a) protect sensitive information from misuse or unauthorized exposure;
(b) foster adherence to the UN's personal data protection and privacy principles; and
(c) provide assurance that UNDP's data privacy is in line with UN privacy policies and where applicable harmonized with main (supra)-national regulations covering data privacy (e.g., the EU's GDPR [General Data Protection Regulation]).

Lack of metadata management procedures (Issue 7)	UNDP did not have centralized metadata management, which could be considered a necessity as the capacity of the organization to collect and store data was constantly increasing.

Recommendation: The Chief Digital Officer, in collaboration with the Bureau for Management Services, should develop a framework (strategy) defining how metadata will be created, maintained, integrated, and accessed.

Management comments and action plan

The Assistant Administrator and Director of the Bureau for Management Services and the Chief Digital Officer accepted all the recommendations and are in the process of implementing them. Comments and/or additional information provided have been incorporated in the report, where appropriate.

Low risk issues (not included in this report) have been discussed directly with management and actions have been initiated to address them.

Helge
Osttveiten
2020.11.18
15:26:23 -05'00'

Helge S. Osttveiten
Director
Office of Audit and Investigations