UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

AUDIT

OF

DATA MANAGEMENT

IN

UNDP

Report No. 2277

Issue Date: 18 November 2020

Table of Contents

United Nations Development Programme
Office of Audit and Investigations

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

I. About data management

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.

Areas covered under the overarching term data management are data governance, data privacy/security, data classification/quality, and data warehousing/business intelligence, all of which can be described as follows:

- Data governance – planning, oversight, and control over management of data and the use of data and data-related resources.
- Data privacy/security – ensuring privacy, confidentiality, and appropriate access of data.
- Data classification/quality – defining, monitoring, maintaining data integrity, and improving data quality.
- Data warehousing/business intelligence – managing analytical data processing and enabling access to decision support data for reporting and analysis.

II. Audit results

OAI made two recommendations ranked high (critical) and six recommendations ranked medium (important) priority.

Low priority issues/recommendations were discussed directly and agreed with the Office and are not included in this report.

High priority recommendations, arranged according to significance:
(a) Develop a comprehensive data privacy policy and related procedures (Recommendation 3).
(b) Develop a framework (strategy) defining how metadata will be created, maintained, integrated, and accessed (Recommendation 7).

Medium priority recommendations, arranged according to significance:
(a) Adopt or develop a data management framework as a basis for the development of UNDP's data governance structure (Recommendation 1).
(b) Conduct a data readiness assessment (Recommendation 2).
(c) Define a timeline for the approach regarding the update of UNDP's 'Record Management Policies and Procedures' (Recommendation 4).
(d) Develop a business intelligence and data warehousing strategy and roadmap (Recommendation 8).
(e) Improve UNDP's data classification standards (Recommendation 5).
(f) Define, promote, and where possible, implement data quality standards (Recommendation 6).

The detailed assessment is presented below, per audit area:

A. Data governance

Issue 1 <u>Development of data governance structure not based on a data management framework</u>

UNDP management recognized that data could be considered a vital organizational asset and that it could help the organization to innovate and achieve its strategic goals. It was further recognized that UNDP should put a data governance structure in place to ensure optimal data usage, the development of which was tasked to the Chief Digital Officer, who was working on it.

Best practices suggest that a data governance structure best be developed using a data management framework, ensuring that the data governance structure addresses all facets of data management. Examples of existing data management frameworks that could be used are:

- Data Management Framework of the Data Management Association (DAMA).
- Data Management Capability Assessment Model (DCAM) of the Enterprise Data Management Council (EDM).
- Data Management Maturity of the Capability Maturity Model Integration (CMMI) Institute.

At the time of the audit, UNDP's data governance structure was still being developed. However, the development of the data governance structure was not based on a data management framework, which could provide guidance and assurance that the proposed data governance structure covered all relevant areas (e.g., data strategy, policies and standards, data architecture, data quality, etc.) as well as be helpful in measuring progress of the development process.

Developing a data governance structure without the use of a data management framework could increase the time needed to develop the governance structure as well as lead to a sub-optimal governance structure.

Priority Medium (Important)

Recommendation 1:

The Chief Digital Officer should adopt or develop a data management framework as a basis for the development of UNDP's data governance structure. It is recommended that the framework include methods to:

(a) understand and prioritize organizational needs;
(b) identify data critical to meeting organizational needs;
(c) establish a governing body(ies) responsible for the strategic guidance of the data governance program (e.g., a data governance council); and
(d) define metrics to measure the impact of the data governance program.

Management action plan:

The Chief Digital Officer and Office of Information Management and Technology are co-authoring a data strategy that intends to address the data governance recommendations made in this report. At this point in time, the CMMI Data Management Maturity (DMM)^{SM} Model has been identified as the basis for the governance structure and a reference model for state-of-the-practice process improvement. The DMM Model allows UNDP to evaluate against documented best practices, determine gaps, and improve management of data assets across functional, line of business, and geographic boundaries. The data strategy would use the DMM as a framework to ensure coverage of data management capabilities, baseline current state, and measure progress over time.

A set of data principles for UNDP are being drafted through a UNDP-wide consultation on the SparkBlue platform. These principles will lie at the heart of our data strategy providing guidance on ethical use of data and governance in UNDP. The process of drafting the strategy includes conducting over 40 strategic interviews with different business units, Regional Bureaux and Country Offices to understand and prioritize organization needs. A complete review of data architecture and identification of critical data use cases are also a part of the strategy.

Feedback from interviews and architecture reviews will support the establishment/designation of a data governance body to create and govern a broad set of data guardrails including usage, sharing, privacy, retention, acquisition, compliance, security, masking, privacy, quality, management, transparency, standardization, integrations, and technology. That body will define metrics to measure the impact of the data governance in UNDP.

Estimated completion date:
November 2020 – Data principles approved
December 2020 – Data strategy approved
December 2020 – Data Governance Group established

Issue 2 Data governance structure being developed without input from prior data readiness assessment

Best practices dictate that given the importance of data for an organization, it is critical to know what data there is, what data might be missing, how data is being used, and the quality of data before starting with the process to develop a data governance structure. The process to collect the aforementioned information is generally known as a data readiness assessment.

UNDP's data governance structure was being developed without first having conducted a data readiness assessment.

Not performing a data readiness assessment could potentially lead to a lack of awareness of organizational data, impacting the ability to properly govern data, ultimately impacting overall data quality within UNDP. Conducting a data readiness assessment could also help identify opportunities to eliminate bad data, ensure that clearly defined sources of data and business rules are in place, and define data stewardship.

Priority Medium (Important)

Recommendation 2:

The Chief Digital Officer should conduct a data readiness assessment, which, *inter alia,* can be done by analysing data and reports currently being used, identifying related issues and existing data gaps.

Management action plan:

The need for doing a data readiness assessment before recommending action is well acknowledged, and a data readiness assessment will be conducted through three key activities:

1. Over 40 strategic interviews and architecture reviews
2. Open consultation on SparkBlue platform
3. UNDP-wide data readiness survey

These activities will provide vital information into the data strategy to establish a data governance structure at UNDP. Our plan is to use this information as a baseline for a compressive review once the governance structure is established and metrics are defined.

Estimated completion date:
October 2020 – UNDP-wide survey completed and analysed

December 2020 – Results of interviews, consultations and survey responses published through the data strategy.
Quarter 1, 2021 – Data governance framework and metrics established.
Quarter 2, 2021 – A comprehensive review conducted with guidance from Data Governance Group.

B. Data privacy / security

Issue 3 Lack of an approved comprehensive data privacy policy

Strictly speaking, data privacy, or information privacy, refers to a specific kind of privacy linked to personal data. However, in a broader context data privacy can also refer all organizational data that is defined as sensitive or proprietary by the organization and that is to be shared with identified users only. Effective data privacy policies and procedures ensure that the right people can use and update data in the right way, by complying with the privacy, regulatory, and confidentiality needs of all stakeholders. Furthermore, transparency in how organizations request consent, abide by their privacy policies, and manage the data that they have collected is vital to building trust and accountability with the various stakeholders who expect privacy.

As more of UNDP's data becomes digitized and more information is shared online data privacy is taking on greater importance. UNDP acknowledged the importance of data privacy in general, as evidenced, for instance, in the 'Guidance to UNDP Country Offices on the privacy, data protection and broader human rights dimensions of using digital technologies to combat Covid-19'. It had also issued various policies relating to data or information, such as the 'Information Disclosure Policy' and the 'Information Security Policy'. However, UNDP did not have a comprehensive data privacy policy. The Office of Information Management and Technology was in the process of preparing a policy covering data privacy ('UNDP Data Protection Policy'), but that policy was at the time of the audit still in draft.

Additionally, while UNDP as one of the United Nations system organizations, did not have to comply with the various (supra)-national regulations covering data privacy (e.g., the European Union's GDPR [General Data Protection Regulation]) it would be beneficial for UNDP if it could provide assurance to its third parties (e.g., donors, host governments, vendors, etc.) that it takes data privacy seriously and that the policies and procedures in place provide a similar level of data protection as foreseen by the aforementioned (supra)-national regulations.

Without a comprehensive data privacy policy and related procedures, UNDP might be unable to adequately preserve and protect personal and other sensitive information from unauthorized accessed and from being shared. Furthermore, showing UNDP's adherence to the UN's personal data protection and privacy principles as adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018 might not be possible without UNDP having its own data privacy policy.

The inability of UNDP to provide assurance to its third parties (e.g., donors, host governments, vendors, etc.) that it takes data privacy seriously and that the policies and procedures in place provide a similar level of data protection as foreseen by the aforementioned (supra)-national regulations might negatively affect UNDP's relations with its stakeholders, potentially leading to financial and reputational risks for the organization.

Priority	High (Critical)
Recommendation 3: 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]).	
Management action plan: Due to the complexity and programmatic element of the recommendation, the Bureau for Management Services in collaboration with the Executive Office will develop and submit for approval a comprehensive data privacy policy that will align with the UN privacy policies. The Bureau for Management Services will be the focal point on operational data when developing the policy and the Executive Office will be the primary focal point on the programmatic side. **Estimated completion date:** December 2021	

C. Data classification / quality

Issue 4 Lack of a timeline regarding the update of UNDP's outdated records management policy

Records management, also known as records and information management, is an organizational function devoted to the management of information in an organization throughout its life cycle, from the time of creation or inscription to its eventual disposition. This includes identifying, classifying, storing, securing, retrieving, tracking, and destroying or permanently preserving records. The purpose of records management is part of an organization's broader function of governance, risk management, and compliance and is primarily concerned with managing the evidence of an organization's activities as well as the reduction or mitigation of risks associated with it.

UNDP's most current records management policy (Record Management) dated back to 2005 and no longer accurately reflected / related to current data usage and electronic storage options. In August 2020, a proposed approach regarding the update of UNDP's 'Records Management Policies and Procedures' prepared by the Bureau for Management Services was approved by the Acting Associate Administrator. However, the proposal did not include a timeline, making it impossible to assess whether the proposed approach was on track or not and when the proposed update was scheduled to be finished. Having a project without a defined timeline complicates project management and could cause unnecessary delays or result in not finishing the project at all.

Priority	Medium (Important)

Recommendation 4:

The Bureau for Management Services should define a timeline for its approach regarding the update of UNDP's 'Records Management Policies and Procedures'.

Management action plan:

The Bureau for Management Services will provide a timeline regarding the updates to UNDP's record management policies and procedures to ensure completion of the project.

Estimated completion date: November 2021

Issue 5 Unclear and unenforceable data classification standards

Data classification, in the context of information security, can be defined as the classification of data based on its level of sensitivity and confidentiality, and the impact to the organization should that data be disclosed, altered or destroyed without authorization. The classification of data is important because it helps determine what baseline security controls are appropriate for safeguarding that data.

UNDP's approach to data classification could be described as being based on the underlying presumption that any information concerning UNDP programmes and operations would be available to the public, in the absence of a compelling reason for confidentiality in line with the exceptions as described in Chapter IV (Exceptions) of UNDP's Information Disclosure Policy. To determine those exceptions to the Information Disclosure Policy (e.g., how to protect personal data that was not intended to be disclosed) the Office of Information Management and Technology issued a document titled 'Information Sensitivity Classification and Handling Guidelines'. However, these guidelines were not mandatory, not very well known within the organization, and could be considered difficult to implement.

The lack of clear and enforceable data classification and handling standards could increase the risk that information that needs to be kept confidential will be accessed by un-authorized people.

Priority	Medium (Important)

Recommendation 5:

The Bureau for Management Services should improve UNDP's data classification standards as follows:

(a) update and simplify the data classification guidelines (e.g., by limiting the number of sensitivity levels to three (limited internal use, internal use, public) and where possible grouping existing datasets into these levels);
(b) elevate these simplified guidelines to a policy to be included in the 'UNDP Programme and Operations Policies and Procedures'; and
(c) ensure consistency between provisions in the (to be developed) data privacy policy and the policy regarding data classification.

Management action plan:

The Bureau for Management Services will update and simplify the classification guidelines and make the policy refer to the UN classification standards, which will be included in the 'UNDP Programme and Operations Policies and Procedures'. The guidelines will also be consistent with the data privacy policy.

Estimated completion date: November 2021

Issue 6 Lack of operational data quality standards

Data quality refers to the overall utility of a dataset and its ability to be easily processed and analysed, leading to insights that help the organization make better decisions. To be of high quality, data must be consistent and unambiguous. High-quality data is essential to cloud analytics, Artificial Intelligence initiatives, business intelligence efforts, and other types of data analytics.

Existing UNDP policies did not provide clear definitions and quality standards for operational data, nor did data-related policies and guidelines (e.g., Information Sensitivity Classification and Handling Guidelines) include information regarding data monitoring to ensure quality and auditability of data.

Lack of high-quality data standards could negatively affect UNDP's decision-making abilities using business intelligence, leading to less than optimal decisions.

Priority	Medium (Important)
Recommendation 6: The Bureau for Management Services should define, promote, and where possible, implement data quality standards.	
Management action plan: The Bureau for Management Services will define operational data quality standards. The vast majority of the data quality standards for operational data will be implemented as part of the new ERP cloud platform planned to be released in January 2022. **Estimated completion date:** December 2021	

D. Data warehousing / business intelligence

Issue 7 Lack of metadata management procedures

Metadata, as the description of data such as what describes a vender name or what describes an address, has a vital role in data management. It helps the organization to understand its data, systems, and workflows. Metadata is also used to identify private or sensitive data and minimize the risk of its exposure.

At the time of the audit 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. Poorly managed metadata could lead to redundant data, inconsistent data definitions, data misuse, and conflicting/competing data sources.

Priority High (Critical)

Recommendation 7:

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 action plan:

The Chief Digital Officer in collaboration with the Bureau for Management Services will develop a framework as part of the data strategy defining how metadata will be maintained, integrated and accessed.

Estimated completion date: November 2021

Issue 8 Lack of a defined strategy to develop business intelligence and data warehousing

Generally, business intelligence covers the processes and methods of collecting, storing, and analysing data from business operations or activities to optimize performance and to create a comprehensive view of an organization to help it make better, actionable decisions. A data warehouse is an integral part of business intelligence and can be described as a central repository of integrated data from one or more disparate sources, storing current and historical data in one single place that can be used for the creation of analytical reports for users throughout the organization.

As evidenced in the approved 2020–2023 UNDP IT Strategy, UNDP understood and acknowledged the importance of data warehousing and business intelligence services for the organization. However, at the time of the audit the organization had not translated this understanding into a concrete strategy to develop business intelligence and data warehousing.

The lack of a defined strategy to develop business intelligence and data warehousing could negatively affect UNDP's ability to make informed, data-based decisions.

Priority Medium (Important)

Recommendation 8:

The Bureau for Management Services, in collaboration with the Chief Digital Officer, should prepare a strategy to develop a business intelligence and data warehousing if need be as part of the data strategy currently being developed by the Chief Digital Officer.

Management action plan:

The Bureau for Management Services in collaboration with the Chief Digital Officer will ensure the data warehousing strategy and roadmap is included as part of the data strategy.

Estimated completion date: June 2021

Definitions of audit terms - ratings and priorities

A. AUDIT RATINGS

- **Satisfactory** The assessed governance arrangements, risk management practices and controls were adequately established and functioning well. Issues identified by the audit, if any, are unlikely to affect the achievement of the objectives of the audited entity/area.

- **Partially Satisfactory / Some Improvement Needed** 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.

- **Partially Satisfactory / Major Improvement Needed** The assessed governance arrangements, risk management practices and controls were established and functioning, but need major improvement. Issues identified by the audit could significantly affect the achievement of the objectives of the audited entity/area.

- **Unsatisfactory** The assessed governance arrangements, risk management practices and controls were either not adequately established or not functioning well. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area.

B. PRIORITIES OF AUDIT RECOMMENDATIONS

- **High (Critical)** 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.

- **Medium (Important)** Action is required to ensure that UNDP is not exposed to risks. Failure to take action could result in negative consequences for UNDP.

- **Low** Action is desirable and should result in enhanced control or better value for money. Low priority recommendations, if any, are dealt with by the audit team directly with the Office management, either during the exit meeting or through a separate memo subsequent to the fieldwork. Therefore, low priority recommendations are not included in this report.