



**AUDIT**

**OF**

**ATLAS SYSTEM**

**Report No. 1759**  
**Issue Date: 21 June 2017**

**(REDACTED)**

## Report on the Audit of the Atlas System Executive Summary

The UNDP Office of Audit and Investigations (OAI) conducted an audit of the Atlas system (UNDP's enterprise resource planning system) from 20 December 2016 to 17 March 2017 through KPMG. The audit aimed to assess the system's data alignment to the established UNDP Internal Control Framework; the system's alignment to key reporting requirements; and data lineage and key interface efficiency and controls.

The audit focused on: (a) access controls and security; (b) application controls; (c) reporting and data reliability; (d) change management; (e) PeopleSoft interfaces; and (f) audit and monitoring tools relevant to UNDP and the United Nations Capital Development Fund (UNCDF). All other users/participating agencies were excluded from this audit. The last audit of the system was conducted by OAI through KPMG in 2013.

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

### Overall audit rating

OAI assessed the Atlas system 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 vulnerabilities with the level of access to development and data administration tools and the level of access to transactional and configuration data in the Atlas UNDP environment.

### Key recommendations: Total = 7, high priority = 4

For high (critical priority recommendations, prompt action is required to ensure 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.

Disproportionate access to system components  
(Issue 1)

Seven application user profiles within the [redacted] had the ability to [redacted] within the [redacted] utilizing [redacted]

Recommendation: The Office of Information Management and Technology should improve the use [redacted] (a) limiting access to the [redacted] to the authorized personnel (typically two or less) to perform [redacted]; and (b) implementing a formal process to gain temporary access [redacted], including a review process to assess that access was used to perform the prescribed duties and/or correct a problem.

Ability to add and/or modify data using the Data Mover Utility  
(Issue 2)

The audit noted that, within the [redacted] user profiles had the ability to [redacted]

Recommendation: The Office of Information Management and Technology should implement a formal process by which access [REDACTED] is provided on an as needed basis and/or in the event of a critical error, or by allowing [REDACTED]. When this access is granted, there should be a review process to ensure that the access was used properly, to perform the prescribed duties, and/or correct a problem.

Excessive system access by support personnel (Issue 3)

The audit noted that [REDACTED] had a broad level of access within the [REDACTED]. The level of access includes the ability to [REDACTED].

Recommendation: The Office of Information Management and Technology should segregate [REDACTED]. In instances where there is a business need [REDACTED], appropriate and formally documented reviews of selected user profile account activity should be performed to ensure the activity is appropriate and authorized.

User profiles with the potential of bypassing the formal change management process (Issue 4)

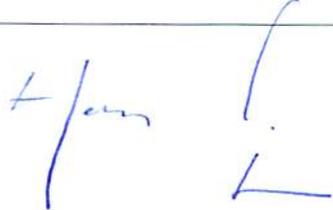
The audit noted that [REDACTED] maintained application user profiles that allowed [REDACTED].

Recommendation: The Office of Information Management should identify and document key configurations. Where changes to the identified configurations settings is minimal, access should be [REDACTED]. A formal process should be established to review [REDACTED] to ensure that changes are accurate and authorized.

### Management comments and action plan

The Officer-in-Charge of the Office of Information Management and Technology accepted all of the recommendations and is in the process of implementing them. Comments and/or additional information provided have been incorporated in the report, where appropriate.

Issues with less significance (not included in this report) have been discussed directly with management and actions have been initiated to address them.

A handwritten signature in blue ink, appearing to read 'H. Ostveiten', enclosed in a rectangular box.

Helge S. Ostveiten  
Director  
Office of Audit and Investigations