UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

Empowered lives.
Resilient nations.

AUDIT

OF

ATLAS SYSTEM

Report No. 1759

Issue Date: 21 June 2017

(REDACTED)

Table of Contents

United Nations Development Programme
Office of Audit and Investigations

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] <u>Recommendation</u>: 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.

Helge S. Osttveiten
Director
Office of Audit and Investigations

I. About the Atlas system

UNDP uses as its enterprise resource planning system Oracle PeopleSoft applications, which UNDP elected to label "Atlas."

II. Audit results

Satisfactory performance was noted in the following areas:

(a) Application controls. As an organization that has commitment control enabled, the budget override policy was appropriately established and documented. Also, based on the testing performed around budget checks, UNDP was tracking any budget overrides through a custom-built dashboard and transactions were reviewed for any exceptions.

(b) Reporting and data reliability. No issues were noted regarding reporting and data reliability.

(c) Change management. The change management procedure was appropriately established for non-emergency and emergency releases. The change management tool used for the migration of configuration changes contained appropriate approval, and test procedures were integrated and followed.

(d) PeopleSoft interfaces. The management of data interfaces for transfer activities was well controlled.

(e) Audit and monitoring tools. Audit and monitoring tools were found to be working well.

OAI made four recommendations ranked high (critical) and three 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) Improve the use of [redacted] (Recommendation 1).
(b) Implement a formal process by which access [redacted] is provided on an as needed basis (Recommendation 2).
(c) Segregate [redacted] duties [redacted] (Recommendation 3).
(d) Identify and document key configurations (Recommendation 4).

Medium priority recommendations, arranged according to significance:

(a) Request the United Nations International Computer Centre to assign [redacted] (Recommendation 5).
(b) Conduct a formal periodic user profile review/recertification process of all active user profiles that have access [redacted] (Recommendation 6).
(c) Where possible, [redacted] personal information data used [redacted] (Recommendation 7).

The detailed assessment is presented below, per audit area:

A. Access controls and security

1. Access to [redacted]

Issue 1 Disproportionate access to [redacted]

User profiles that contain rights to [redacted] should be clearly assigned, used and monitored to ensure limited and careful use. The [redacted] is the primary [redacted] in Atlas. User profiles granted access to [redacted] can create and make changes to [redacted] within the Atlas [redacted]

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

This level of access in [redacted] presents a risk [redacted] within [redacted], which can lead to [redacted]

Priority High (Critical)

Recommendation 1:

The Office of Information Management and Technology should improve the use of [redacted] tools by:

(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.

Management action plan:

The Office of Information Management and Technology will address the recommendation and will further review the list, taking into consideration the need to [redacted]

Estimated completion date: April 2018

Issue 2 Ability to add and/or modify data [redacted]

User profiles that contain rights to transfer and/or modify large amounts of data elements [redacted] should be clearly assigned, used and monitored, to ensure limited and careful use. provides the ability to: transfer [redacted]

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

The level of access granted to the [redacted] enables changes to [redacted] within the existing change management process, thus leading to [redacted]

Priority	High (Critical)

Recommendation 2:

The Office of Information Management and Technology should implement a formal process by which access to the [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.

Management action plan:

The Office of Information Management and Technology will address the recommendation and will further review the list.

Estimated completion date: April 2018

Issue 3 Excessive system access by [redacted]

User profiles of support staff [redacted] may potentially bypass established approvals and modify [redacted], while at the same time [redacted]

The audit noted that [redacted] user profiles, [redacted], had a broad level of access within [redacted] The level of access includes the ability to [redacted]

The lack of proper segregation of duties regarding [redacted] presents a risk that could result in unauthorized [redacted]

Priority	High (Critical)

Recommendation 3:

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

Management action plan:

The Office of Information Management and Technology will review [redacted] In addition, the Office of Information Management and Technology will implement the review of selected user account activity through its quarterly risk review meetings.

Estimated completion date: April 2018

Issue 4 User profiles with the potential of [redacted]

Configuration management allows for critical changes to the configuration and as such should be controlled through a restricted change management process.

The audit noted that [redacted] maintained application user profiles that allowed [redacted]

Bypassing the [redacted] may result in [redacted] and may lead to [redacted]

Priority High (Critical)

Recommendation 4:

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 action plan:

The Office of Information Management and Technology will review the [redacted] profiles that have access to [redacted] and where possible [redacted] aligning them with business needs. Furthermore, the Office of Information Management and Technology will further assess [redacted] to determine whether any [redacted]

Estimated completion date: July 2018

Issue 5 Inadequate database [redacted]

[redacted] configuration settings should [redacted]

[redacted] accounts to [redacted] databases is done by [redacted] The audit noted that the [redacted] databases [redacted] which did not [redacted] as follows:

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Inadequate [redacted] settings can lead to [redacted] access to [redacted] and may [redacted]

Priority Medium (Important)

Recommendation 5:

The Office of Information Management and Technology should request [redacted] to [redacted] the database [redacted] that is in accordance with leading practices.

Management action plan:

The Office of Information Management and Technology will submit [redacted] in accordance with leading practices.

Estimated completion date: December 2018

Issue 6 Limited user access review process

User profile access rights should be regularly monitored and periodically reviewed in order to ensure that they reflect the continuous needs of authorized users.

The audit noted that the existing user access review process [redacted] The review process was [redacted]

The [redacted] review of user profile access may result in [redacted] conflicts may arise [redacted]

Priority	Medium (Important)
Recommendation 6: The Office of Information Management and Technology should conduct a formal periodic user profile review/recertification process [redacted] This process should be [redacted]	
Management action plan: The Office of Information Management and Technology [redacted] **Estimated completion date:** December 2018	

Issue 7 <u>Weak protection of</u> [redacted]

[redacted] use strong controls to ensure [redacted] In most cases, [redacted] used to [redacted] To provide the same level [redacted] the data used to [redacted] The audit noted that [redacted] were [redacted] without [redacted]

The lack of [redacted] may result in [redacted]

Priority	Medium (Important)
Recommendation 7: The Office of Information Management and Technology, where possible, should [redacted]	
Management action plan: The Office of Information Management and Technology will assess [redacted] and present [redacted] to assess the possibility [redacted] **Estimated completion date:** December 2018	

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 <u>not included in this report</u>.