UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

AUDIT

OF

ATLAS SYSTEM

Report No. 1163

Issue Date: 17 April 2014

(REDACTED)

Table of Contents

Report on the audit of the Atlas system
Executive Summary

The UNDP Office of Audit and Investigations (OAI), from 12 August to 27 September 2013, through KPMG, conducted an audit of the Atlas system (UNDP's Enterprise Resource Planning system). The audit aimed to assess the system's alignment to key areas of the UNDP internal control framework definition, business process controls, key reporting needs, and the IPSAS (International Public Sector Accounting Standards) Framework.

The review focused on: (a) application controls and security; (b) reporting and data reliability; (c) IPSAS and application configuration; (d) PeopleSoft interfaces; (e) database security; and (f) audit and monitoring tools. The last audit of the Atlas system was conducted by the United Nations Board of Auditors in 2012 and 2013 as part of the audit of financial statements of UNDP.

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**, which means "Internal controls, governance and risk management processes were generally established and functioning, but needed improvement. One or several issues were identified that may negatively affect the achievement of the objectives of the audited entity." This rating was mainly due to ███████████████████████████████████, granting of access to processing transactions to unauthorized users, and unauthorized users with add/update rights in the Atlas UNDP environment.

Key recommendations: Total =**11**, high priority = **3**

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:

Excessive access to transaction processing (Issue 2)

████████ had access rights for processing transactions within multiple modules of Atlas through application administration roles.

Recommendation: Lower risk relating to access to transaction processing by: (a) limiting general processing rights to business users and to a limited number of system administrators; and (b) restricting update/edit access of ████████ to security maintenance pages, specifically to pages required to modify user profiles, roles, and permission lists.

██████████ having access to UNDP environment (Issue 3)

Users with add/update access had the ability to make unauthorized changes to UNDP configurations and chartfields outside of UNDP's change management system (PHIRE), which could lead to processing delays and possible financial misstatements.

Recommendation: Manage the risk of potential unauthorized access by ██████████ by: (a) defining explicitly in the change management policy the configurations which can be made outside of the PHIRE (UNDP's change management tool) process (all chartfields, changes to business units, etc.); (b) developing a mechanism to monitor UNDP configuration and chartfields that can be updated outside of UNDP's change management system on a periodic basis for accuracy; and (c) until the implementation of Oracle's Configuration Controls Governor, considering taking quarterly extracts of key configuration tables, comparing results with prior periods, and then checking change tickets for any discrepancies to ensure no unauthorized changes occurred.

Management comments and action plan

The Directors of the Office of Information Systems and Technology, Office of Financial Resources Management, and Office of Human Resources accepted the recommendations addressed to their respective offices and are in the process of implementing them. Comments and/or additional information provided had 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.
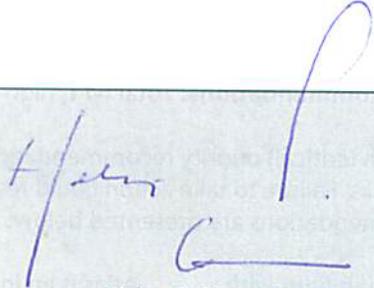
Helge S. Osttveiten
Director
Office of Audit and Investigations

I. About the Atlas system

UNDP uses as its Enterprise Resource Planning system an Oracle PeopleSoft system UNDP decided to call "Atlas". This was introduced in 2004, under the United Nations System Accounting Standards, the then prevailing accounting standards applicable to UNDP. Effective 1 January 2012, UNDP implemented IPSAS. This entailed a number of configuration changes in Atlas.

II. Audit results

As a result of the audit procedures performed, the audit team found that the internal controls, governance, and risk management processes over the Atlas system were largely established and functioning, but some improvements are needed.

Satisfactory performance was noted in the following areas:

(a) <u>PeopleSoft interfaces (links between the banking and treasury modules that facilitated the transfer of data)</u>. The management of data interfaces for transfer activities to and from third party banks was tightly controlled and proved to be a very stable environment. The interface process used gateway servers and security keys to manage the flow of data. Data was placed on the secure server and downstream processes accessing the data were required to use the secure key to access the data. Issues were rare, and if issues did occur, notifications were sent to the defined parties for awareness and timely resolution.

(b) <u>PeopleSoft workflow configurations (system configurations for transaction approval in line with segregation of duty requirements)</u>. Multiple business transaction approval workflows used within Atlas were in line with leading practices. These workflows helped mitigate the possibility of segregation of duty conflicts when users were granted access to two or more business processing pages.

(c) <u>IPSAS training programs</u>. Strong IPSAS training programs were in place to ensure that staff were informed of the IPSAS accounting and process impacts on Atlas.

(d) <u>Data migration</u>. There was a detailed plan in place to migrate the pre-2012 Development Project Assets into Atlas as at 31 December 2014. Initial steps were already being taken.

OAI proposes 11 recommendations that are ranked high (critical) and medium (important) priority. Low priority recommendations were discussed directly and agreed with the concerned offices and are not included in this report.

High priority recommendations, arranged according to significance:

(b) Lower risk relating to access to transaction processing (Recommendation 2).
(c) Manage the risk of potential unauthorized access by ▮▮▮▮▮▮▮▮ (Recommendation 3).

Medium priority recommendations, arranged according to significance:
(a) Address risk relating to access to unpost (i.e. cancel/reverse) journal entries for transactions (Recommendation 4).
(b) Develop a mechanism to monitor whether heads of offices are performing their full user access reviews (Recommendation 5).

(c) Review regularly lists of open status Customer Relationship Management and resolve them in a timely manner (Recommendation 6).
(d) Perform a periodic review of the database monitoring tools (Recommendation 7).
(e) Automate the interface of the third party mark-to-market valuation process to the Atlas system (Recommendation 8).
(f) Prioritize the effort of logging all open project change requests into a central location (Recommendation 9).
(g) Finalize the ongoing project by automating the existing manual components of the financial reporting package (Recommendation 10).
(h) Keep a single version of the status report of the Automated Financial Statement Project and keep this as a consistent standard for reporting (Recommendation 11).

The detailed assessment is presented below, per audit area:

A.   Application controls and security

[**NOTE**: This section has been redacted as it is deemed to contain sensitive information.]

███████████████

██

██████████████████████████ ██████

Issue 2   <u>Excessive access to transaction processing</u>

The audit noted that ██ within the UNDP directory had access to process transactions within multiple modules of Atlas through application administration roles. ████

████████
█ ███████████
█ ██████████
█ ███████████
█ █████████

Providing non-business users with access to transaction pages may present the risk that those users will process unauthorized business transactions outside of their regular functions, leading to data errors, even incorrect financial statements or fraud. There are mitigating controls in place for voucher and vendors. In addition, ██████████████████████████████ do not have access to vendor route control roles.

Priority	High (Critical)
Recommendation 2: Lower risk relating to access to transaction processing by: (a) limiting general processing rights to business users and to a limited number of system administrators; and (b) restricting update/edit access of ███████████ to security maintenance pages, specifically to pages required to modify user profiles, roles, and permission lists. **Responsible HQ bureau/Office:** Office of Information Systems and Technology	
Management action plan: The Office of Information Systems and Technology will review developers/application support and ███████ access rights in conjunction with the ████████ controls currently in place. **Estimated completion date:** By third quarter, 2014.	

Issue 3 ▮▮▮▮▮▮▮▮▮▮▮▮▮ having access to UNDP environment

The audit noted ▮▮ had add/update access to the UNDP configuration (i.e., business units and public queries) and chartfield pages (i.e., departments, accounts, donor codes).

Users with add/update access have the ability to make unauthorized changes to UNDP configurations and chartfields outside of UNDP's change management system (PHIRE), which could lead to processing delays and possible financial misstatements.

Management indicated the possibility of using Oracle's Configuration Controls Governor to track configuration changes; however, this tracking system had not been implemented at the time of the audit.

Priority	High (Critical)
Recommendation 3: Manage the risk of potential unauthorized access by ▮▮▮▮▮▮▮▮▮▮▮▮▮▮ : (a) defining explicitly in the change management policy the configurations which can be made outside of the PHIRE (UNDP's change management tool) process (all chartfields, changes to business units, etc.); (b) developing a mechanism to monitor UNDP configuration and chartfields that can be updated outside of UNDP's change management system on a periodic basis for accuracy; and (c) until the implementation of Oracle's Configuration Controls Governor, considering taking quarterly extracts of key configuration tables, comparing results with prior periods, and then checking change tickets for any discrepancies to ensure no unauthorized changes occurred. **Responsible HQ bureau/Office:** Office of Information Systems and Technology	
Management action plan: ▪ The Office of Information Systems and Technology will review and update the change management policies and procedures to better identify changes made ▮▮▮▮▮▮▮▮▮▮▮▮▮ . ▪ In addition, the Office of Information Systems and Technology will review page access settings to impose the appropriate technical controls on changes that support the change management policies and procedures. ▪ The proposal for implementation of the Configuration Controls Governor to track configuration changes will be presented to the ICT Governance group for prioritization and implementation including budget allocation. **Estimated completion date:** By third quarter, 2014.	

▮ ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮

Issue 4 Excessive access to unpost (i.e. cancel/reverse) journal entries for transactions

The audit noted that users from other agencies had the ability to modify UNDP transactions. For example, the audit team found that 11 individual roles and 133 users across different agencies outside of UNDP had access to unpost journal entries (i.e., cancel/reverse transactions entered into the system) within the Atlas General Ledger.

This access, coupled with the lack of business unit security or chartfield security, increases the possibility that journals may be unposted without proper authorization from the concerned business unit and may cause a disruption in the closing process, and may even lead to incorrect financial statements.

Priority	Medium (Important)

Recommendation 4:
 	
 Address the risk relating to access to unpost journal entries by:
 	
    (a) assessing the extent to which security features in PeopleSoft 9.1 can be used to restrict users from other agencies from modifying UNDP transactions; and
 	
    (b) planning for the implementation of the new security features upon transition to PeopleSoft 9.2 as a way to provide additional assurance to UNDP management that users are not processing transactions for General Ledger accounts outside of their respective agencies or business units.
 	
 Responsible HQ bureau/Office: Office of Information Systems and Technology and Office of Financial Resources Management	

Management action plan: The Office of Information Systems and Technology will assess the degree of fit of the new business unit and chartfield security (currently available in PeopleSoft version 9.1) when it migrates to PeopleSoft version 9.2 in 2015. The Office of Information Systems and Technology will present its findings and recommendations of its assessment to the ICT Governance Group for project and budget prioritization as required. Pending the upgrade to PeopleSoft 9.2, the Office of Information Systems and Technology will assess the feasibility of developing a monitoring mechanism for unposted activity. **Estimated completion date:** By second quarter, 2015.	

B. Audit and monitoring tools

Issue 5 Finance user access review not documented

The audit noted a complete Atlas finance user access review was not signed-off by the Office of Financial Resources Management or respective data owners (i.e., Procurement) in 2012. While this is not required by UNDP policy, it is leading practice to have data owners review user access on a periodic basis (i.e., annually) to ensure access is appropriate. This audit observation related to two user reviews: (a) the Office of Financial Resources Management is to sign-off on Internal Control Framework Atlas profile deviations, and (b) heads of office are

required to perform a monthly Atlas review of all their respective users. The audit noted that a corporate system to monitor compliance with the requirement that heads of office perform the monthly Atlas review did not exist.

At the time of the audit, there was a policy in place for the heads of office to perform a monthly review of user access. However, evidence of compliance with this policy did not exist. Therefore, management did not have assurance that the access provided to all users was appropriate. Users may change job responsibilities during the year or may leave UNDP while not having their Atlas profiles updated in a timely manner, which could lead to excessive and unauthorized access.

Priority	Medium (Important)
Recommendation 5: Develop a mechanism to monitor whether heads of offices are performing their full user access reviews in accordance with the UNDP Internal Control Framework. If a mechanism cannot be developed to enforce the Internal Control Framework user review policy at the current documented frequency, updating the policy is recommended. **Responsible HQ bureau/Office:** Office of Information Systems and Technology	
Management action plan: The Office of Information Systems and Technology will work with the Office of Financial Resources Management, the Office of Human Resources and Procurement Support Office to develop mechanism to enhance monitoring of reviews carried out by heads of UNDP offices. **Estimated completion date:** By fourth quarter, 2014.	

Issue 6   Delayed completion and closure of production requests

The audit noted, through a review of the Customer Relationship Management (CRM) production ticket activity for the year 2013, that some tickets were open for more than a month. These open tickets represented 3 percent of the tickets in the list (330/10,919); the majority of these were related to Copenhagen's Office of Human Resources.

The goal of a helpdesk operation is to facilitate the timely resolution of an issue or deferring to an individual who can resolve the issue. To reach this goal, the management of a helpdesk must monitor their respective issues and ensure they are resolved. To accomplish this, the following steps must be taken: (a) helpdesk management must meet with the Office of Information Systems and Technology and the Office of Human Resources to reach an agreement on which group owns the "Type" category that is assigned to each ticket in CRM; and (b) helpdesk management must provide guidelines, with consideration for the service level agreement guidelines that require the timely resolution of open tickets. Considerations for closing a ticket may include contacting business process owners who initiate tickets after a specified number of days, asking if the issue still exists and if no response is received within a specified date, the ticket should be closed.

In response to the draft report, management provided the following statements regarding reasons and scenarios for the unresolved Customer Relationship Management cases.

(a) In 64 percent of cases, there was no dedicated Human Resource support within the helpdesk. While the issues had been mainly addressed outside of CRM, there was no mechanism in place for following up on helpdesk cases and therefore they remained open.

(b) In 14 percent of the cases, the issues related to the change control processes that were managed by the Office of Information Systems and Technology. Management indicated that these cases had now been closed, and that the Technical Support Group in Copenhagen would modify its procedures going forward so that this can be avoided.

(c) In 22 percent of the cases, the issues related to eServices. As noted in (a), there was a need for helpdesk support to ensure that the expansion of eServices was fully supported and that issues were resolved.

Production issues that are not resolved and closed in a timely manner may lead to delays in day-to-day processing and a dissatisfied user community.

Priority	Medium (Important)
Recommendation 6: Review lists of open status Customer Relationship Management helpdesk tickets regularly and resolve them in a timely manner. **Responsible HQ bureau/Office:** Office of Human Resources	
Management action plan: As part of the Office of Human Resources structural review, the Chief of Human Resources Infrastructure Support will review the existing issues and make needed recommendations to strengthen the Customer Relationship Management support arrangements for human resources related matters, including long-outstanding cases. **Estimated completion date:** By third quarter, 2014.	
OAI Response: OAI acknowledges the comments provided by management and will validate them as part of the follow-up process at a later stage.	

C. Database security

Issue 7   Staff with access to production database and front-end application development and production

The audit noted two user IDs with access to the front-end Atlas production environment had production database access as well.

1. Staff A (Server and Database Access)
2. Staff B (Database Access)

Users with access to both production database and the front-end application have the ability to bypass change controls, which may lead to fraudulent processing and potential misstatements.

While separating access to production database and the front-end application is recommended to be in line with leading practices, the audit team understands this is not always a viable option in order to keep the system running and continue daily processing. UNDP currently has database monitoring tools (Oracle Enterprise Manager - OEM) to provide detection controls to track changes within the database. While these tools are reviewed on an ad-hoc basis, there is a need to perform a periodic review of these tools to ensure that all changes are in line with defect/issue requests.

Priority	Medium (Important)
Recommendation 7:	
Perform periodic review of the database monitoring tools in place to ensure that all changes made by users with access to both production database and the front-end application are in line with defect/issue requests. **Responsible HQ bureau/Office:** Office of Information Systems and Technology	
Management action plan:	
The Office of Information Systems and Technology will perform this periodic review. **Estimated completion date:** By fourth quarter, 2014.	

D.   IPSAS and application configuration

Issue 8   Calculation of mark-to-market valuations manually done

The audit noted approximately 10 percent of the $5 billion of investments held by UNDP were required to be marked to market. Page 38 of the Business Requirements Document sets out the steps required to perform the mark-to-market (or fair value) valuation in Atlas. Treasury management advised that the prices are fed from Bloomberg into Atlas, however, the treasury module has limited capability in performing mark-to-market valuations and as a result adjusting gains/losses in the Atlas General Ledger is required. The valuations of mark-to-market are performed outside of Atlas and the gains and losses are manually posted in the system.

The manual calculation and posting of gains and losses from market valuations of investments increases the risk of human error and consequently increases the risk of incorrect valuation of financial instruments in the financial statements.

Priority	Medium (Important)

Recommendation 8:
Automate the mark-to-market valuation process to Atlas while taking into consideration the results from a cost and benefit analysis of its implementation.
Responsible HQ bureau/Office: Office of Financial Resources Management/Treasury Division

Management action plan:
Mark-to-market classification is limited only to the After Service Health Insurance portfolio. At the time of IPSAS implementation, UNDP was considering outsourcing the management of this portfolio to an external fund manager. Therefore, it wasn't considered cost effective to automate the process in Atlas until the outsourcing decision was made. UNDP expects the outsourcing to be completed by the end of Q2 2014. When the transfer to the external managers is completed, UNDP expects to automate the mark-to-market process with data interface into Atlas to post the required entries, including mark-to-market adjustments.
The implementation plan will take this current risk into account when designing the new process.
Estimated completion date: By second quarter, 2014.

E.   Reporting and data reliability

Issue 9   No centralized tracking of project change requests

The audit noted the lack of a centrally logged list of open projects and tasks that are requested by the user community. In addition, project change requests on the list of open requests had expired due dates. This is an overall observation related to the lifecycle of report and project requests from receipt to closure of requests. This does not relate to the issue of ticket tracking referred to in Issue 6.

Subsequent to the audit field work, management of the Office of Information Systems and Technology and the Office of Financial Resources Management indicated that they were in the process of identifying all open requests and categorizing, prioritizing and logging them into a central location that is by these offices.

Priority	Medium (Important)

Recommendation 9:
Prioritize the effort of logging all open requests into a central location. Attainable dates should be maintained on projects and tracked for completion. If a project requires changes in delivery timeline, the original due date should be reflected.
Responsible HQ bureau/Office: Office of Information Systems and Technology

Management action plan:
All new requests are currently tracked in Customer Relationship Management.
Estimated completion date: Implemented.
OAI Response
OAI will validate the management feedback and confirm implementation of this recommendation as part of the standard desk follow-up after issuance of this audit report.

Issue 10 Financial reporting process not fully automated

The audit noted that the existing financial reporting process involved manual and automated components. There was a project in place to automate the entire financial reporting package. While most of the reports had been completed, the project had missed deadlines over the past year, impacting the ability to reduce risks related to the periodic reporting of financial results through the use of spreadsheets as opposed to system-automated reports.

Integrity of reported financial data can be negatively impacted by the manual process of creating periodic financial statements, as this could lead to miscalculations or user error. Completely automating this process would be more effective and would decrease the risk of errors occurring during the financial statement creation process.

Priority	Medium (Important)
Recommendation 10:	
Finalize without delay the ongoing project by automating the existing manual components of the financial reporting package.	
Responsible HQ bureau/Office: Office of Financial Resources Management	
Management action plan:	
UNDP management agreed to finalize the project for the automation of the financial statements, and is proceeding with an alternative software platform (Hyperion).	
Estimated completion date: By end fourth quarter, 2014 for implementation of Hyperion	

Issue 11 Inconsistent project reporting

The audit noted that no consistent standard of reporting was followed on the status of the items being tracked on the Automated Financial Statement Project. The Office of Financial Resources Management and the Office of Information Systems and Technology were maintaining and managing separate lists of development objectives related to this project and the lists were not consistent with each other. Furthermore, the separate lists portrayed two versions of the status of the reports.

Subsequent to the audit field work, the audit team was informed that the draft audit recommendation had been implemented and the issue had been resolved.

Priority	Medium (Important)
Recommendation 11: Keep a single version of the status report on the Automated Financial Statement Project. A consistent standard should be followed for the information being reported by both groups. **Responsible HQ bureau/Office:** Office of Information Systems and Technology and Office of Financial Resources Management	
Management action plan: All project status reports for the implementation of the alternative software platform (Hyperion) will be captured through the Office of Information Systems and Technology project management tools (PHIRE/CRM) to ensure consistent standards. **Estimated completion date:** Implemented	
OAI Response OAI will validate the management feedback and confirm implementation of this recommendation as part of the standard desk follow-up after issuance of this audit report.	

Definitions of audit terms - ratings and priorities

A.   AUDIT RATINGS

- **Satisfactory**   Internal controls, governance and risk management processes were adequately established and functioning well. No issues were identified that would significantly affect the achievement of the objectives of the audited entity.

- **Partially Satisfactory** Internal controls, governance and risk management processes were generally established and functioning, but needed improvement. One or several issues were identified that may negatively affect the achievement of the objectives of the audited entity.

- **Unsatisfactory**   Internal controls, governance and risk management processes were either not established or not functioning well. The issues were such that the achievement of the overall objectives of the audited entity could be seriously compromised.

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 that are considered moderate. Failure to take action could contribute to 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>.