



INTERNAL AUDIT DIVISION

REPORT 2018/102

Audit of Umoja implementation by the Department of Management

**Control improvements were required in
design documentation, system configuration,
master data management, system
functionality, system security and user
support**

23 October 2018

Assignment No. AT2017/519/02

Audit of Umoja implementation by the Department of Management

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of Umoja implementation by the Department of Management (DM). The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes to ensure effective implementation of Umoja. The audit covered the period from January 2015 to February 2018 and covered the risk areas in Umoja Integration (Foundation and Extension I), focusing on configuration and master data. The audit covered the system's data architecture, configuration, user authorization, access and security, control over master data, interface governance, system availability and performance, and user support. The audit included the business process areas of finance, human resources, payroll, time management, treasury, and procurement.

DM had made good progress on Umoja implementation since the earlier rollouts of the system. However, this audit showed that additional controls were required in the areas of design documentation, system configuration, master data management, system functionality, system security and user support.

OIOS made one critical and six important recommendations. To address issues identified in the audit, DM needed to:

- Update the Umoja business design documents and document a data dictionary for the system;
- Implement control enhancements: (i) over high-risk processes by factoring them into the continuous improvements change control process; and (ii) for the specific gaps identified in the present audit;
- Require the Umoja process owners to embed a review into the change control process so that an internal monitoring mechanism is factored into every change/improvement when it is considered and implemented;
- Review the assignment of high-risk roles and restrict them to authorized users; review and remove conflicts in the authorizations embedded in critical enterprise roles; and establish procedures to remove access to the Umoja system for separated/retired/reassigned staff in a timely manner (**critical**);
- Review and prioritize the implementation of continuous improvements for Umoja that include: (i) the outstanding functionalities; (ii) resolution of the issue concerning the automated investment portfolio reconciliation process; and (iii) functionality to support the new maternity leave policy;
- Define the performance benchmarks for the individual tasks of time-sensitive processes and include critical processes in periodic monitoring procedures, periodically collect performance feedback from users, and address the root causes of performance issues; and
- Ensure timely implementation of actions determined in the lessons learned report on the disaster recovery exercise and conduct a review of the disaster recovery plan following deployment of Umoja Extension II in 2019.

DM accepted five recommendations including the critical recommendation, and has initiated action to implement them. In addition, DM partially accepted one recommendation but did not accept the part relating to documentation of an Umoja data dictionary. OIOS is of the view that documenting the data dictionary is required to provide the basis for understanding the structure of the data maintained in Umoja and facilitate its ease of use by the user community. Therefore, the data dictionary should be documented sooner than later. DM also did not accept one recommendation relating to defining the performance

benchmarks for individual tasks of time sensitive processes and including critical processes in its periodic monitoring procedures. DM stated that OIOS should enhance its recommendation with specific examples, rather than having it as a global recommendation. OIOS has already provided examples in the report to describe the reported condition. These unaccepted recommendations have been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risks.

CONTENTS

	<i>Page</i>
I. BACKGROUND	1
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	2
III. AUDIT RESULTS	2-17
A. Data architecture	2-3
B. Risk management	3-11
C. ICT support system	11-17
IV. ACKNOWLEDGEMENT	17
 ANNEX I	
Status of audit recommendations	
 APPENDIX I	
Management response	

Audit of Umoja implementation by the Department of Management

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of Umoja implementation by the Department of Management (DM).
2. DM provides financial and administrative support services to more than 10 New York-based departments/offices of the United Nations Secretariat. DM is the owner of key administrative processes and has been leading the implementation of Umoja through the Umoja Office. DM sets the policies for Umoja business process design and system configuration to support such processes. Umoja is an application of SAP which supports management activities related to finance, budget, human resources (HR), supply chain, central support services, and other core business functions. This system was intended to replace numerous existing legacy information systems spread across the Secretariat. The approved budget for the Umoja project up to the end of 2019 was \$528.2 million and the total expenditure up to 31 December 2017 was \$439.4 million. Umoja supports the Organization at more than 400 locations with over 15,800 transactional and business intelligence users and over 103,000 roles provisioned cumulatively.
3. The deployment of Umoja is divided into phases (Foundation, Extension I, and Extension II), modules, and clusters. Clusters consisted of various offices and missions under the Secretariat. DM started the implementation with all peacekeeping missions in Cluster 1 and over the past five years, it has continued the rollout up to Cluster 4, namely, Headquarters, the Economic Commission for Latin America and the Caribbean, the Economic Commission for Africa, the Economic Commission for Europe, the Economic and Social Commission for Western Asia, the United Nations Offices at Geneva and Vienna, the United Nations Office on Drugs and Crime, the International Trade Centre, and the international tribunals.
4. Cluster 4 deployment was the largest and most complex and significantly expanded the Umoja user base. It involved rolling out harmonized business processes covering a vast range of functionalities including workforce management, time management, payroll, organizational management, travel management, finance, budget, procurement, logistics, project management and support services concurrently to a large number of Secretariat entities with divergent business models, systems and practices. Simultaneously, Extension I was rolled out at all field missions which were already operating with Umoja Foundation since the rollout of Clusters 1 and 2 in 2013 and 2014, respectively.
5. Extension II aims to build on the progress achieved with the deployment of Foundation and Extension 1 and will include additional processes such as programme management, conference and event management and service management, in addition to amplifying the existing Umoja processes. Umoja deployment included business design documents which contained configuration and master data specifications to be implemented to support the various United Nations business processes. Some aspects of Umoja were specifically customized in the area of HR to accommodate the complexity of various HR policies and procedures.
6. Comments provided by DM are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

7. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes to ensure the effective implementation of Umoja by DM.

8. This audit was included in the 2017 risk-based work plan of OIOS due to the risks associated with implementation of Umoja and its potential impact on the next deployment at other locations.

9. OIOS conducted this audit from July 2017 to February 2018. The audit covered the period from 1 January 2015 to February 2018. Based on an activity-level risk assessment, the audit covered risk areas in Umoja integration (Foundation and Extension I), focusing on configuration and master data.

10. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data; (d) review of Umoja configuration settings and controls over master data; (e) comparison of business design documents to Umoja configuration settings and master data; and (f) test of transactions and procedures.

11. The audit focused on the system's data architecture, configuration, user authorization, access and security, control over master data, interface governance, system availability and performance, and user support. The audit included business process areas of finance, HR, payroll, time management, treasury, and procurement. The travel module was not included in this audit as re-design of the module was ongoing. The grants management and logistics management modules were also not reviewed as they were expected to be fully functional as part of Umoja Extension II implementation. The Employee Self-Service module was not covered as it is planned to be covered in a separate audit.

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

III. AUDIT RESULTS

A. Data architecture

Need to update business design documents, document data dictionary and entity relationship diagrams

13. The professional standards defined in the Control Objectives for Information and Related Technology (COBIT) framework recommend the issuance of formal and clear documentation to ensure the transfer of adequate knowledge and skills for supporting ICT systems in an effective and efficient manner. Documentation should include business design documents (BDD), data dictionaries, technical diagrams of the relationship between data entities, data models and data flows, and these should align with the implemented configuration and master data in the system.

14. OIOS reviewed and compared medium and high-risk elements of BDD for the Umoja system to the Implementation Management Guide (IMG)¹ within the system. IMG contained the actual configuration implemented in Umoja. The review identified the following gaps:

(i) Several BDDs for HR, workforce management and time management were not up to date. In some other instances, differences were noted between the BDDs and the configuration implemented in the Umoja system (organization management, treasury, funds management, accounts payable, and payroll). For instance, for funds management, the BDDs had 8 configuration settings defined, however, there were 12 settings configured in the system. DM stated that update of BDDs depended on availability of staff relative to urgency of changes to be implemented. DM acknowledged that in some cases, there might be differences between the BDD and the system configuration and this usually points to delay in updating the BDDs.

¹ SAP IMG is the tool which adjusts the SAP system to the requirements of the company and contains information on the actual configuration implemented for the company.

(ii) Several custom tables, schema and fields were implemented in the Umoja system. However, no data dictionary was documented for the same, thus placing reliance on the knowledge of the project team.

(iii) Entity relationship diagrams (ERD) describing the relationship among database tables for various Umoja modules (such as materials management, finance and HR) were not documented/available. As such, the process for determining the relationship between tables, fields and data structures was complex, time consuming and dependent on the knowledge of the project team. DM stated that: SAP standard delivered software has more than 70,000 tables; SAP does not provide ERDs for the relationships; the project team has no difficulty in supporting the system as the behaviour of standard SAP solutions is generally well known; and staff have the requisite training and skills to maintain the system. OIOS is of the view that DM needs to document the ERDs for custom tables and configuration to serve as a reference for anyone supporting the system. This would prevent overreliance on the knowledge of the project team.

(1) DM should: (i) update the Umoja business design documents as part of the change control process; and (ii) document an Umoja data dictionary.

DM accepted recommendation 1 (i) and stated that BDDs will be updated as part of the change control process. However, DM did not accept recommendation 1 (ii) stating that data dictionary is subject to the long-term nature of the rollout of Umoja and there are many dependencies. DM stated that OIOS may wish to consider this matter in its future audits of Umoja. OIOS is of the view that it is necessary to document the data dictionary because it provides the basis for understanding the enterprise data in Umoja and facilitates its ease of use by the user community. Therefore, it should be documented sooner than later. Recommendation 1 (i) remains open pending receipt of evidence that BDDs have been updated. Recommendation 1 (ii) has been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risk.

B. Risk management

Umoja configuration settings needed to be assessed to enable preventive controls for high risk processes

15. System configuration settings should enable application controls that prevent the possibility of unauthorized, fraudulent or invalid processing of transactions, and facilitate efficiency. A risk assessment should identify the applicable controls to minimize the need for intensive manual intervention and monitoring. Absence of preventive controls should be mitigated by adequate detective and monitoring controls.

16. OIOS review of configuration settings and controls over master data in Umoja showed that several validation controls were not enabled, implemented or configured. Manual interventions were required for many processes. DM explained that due to the high complexity of the system, implementation of such validations or controls may be very complex, time consuming and/or cost prohibitive. DM further stated that the project does not deem it necessary or feasible to undertake an across-the-board risk assessment of preventive controls. OIOS is of the view that DM needs to assess and implement validation controls over high-risk processes to minimize the risk of unauthorized, fraudulent or invalid transactions.

17. Process owners in DM had established policies, procedures and guidance materials to monitor compliance of processes in Umoja with organizational policies. For example, the Office of Human Resources Management (OHRM) documented several guidelines for its staff to monitor compliance with various types of entitlements and policies. However, the controls documented in these guidelines were not always enforced and oversight mechanisms in DM were not fully implemented to collate and analyze the

results of such monitoring to timely prevent, detect and correct errors, exceptions and non-compliance with internal policies.

18. OIOS noted the following lack of preventive controls with configuration and master data:

Human resources

(i) No validation controls were configured over critical master data fields such as date of birth, and date of entry on duty in the United Nations common system. OIOS detected 87 cases with date of birth showing an age of less than 10 years and 5 cases where the date of entry in the United Nations common system was later than the date of entry on duty in the United Nations Secretariat. OHRM stated that validation has now been added for the date of entry in the United Nations common system, but no validation is planned for the date of birth field as controls will be exercised through monitoring.

(ii) Staff with HR partner roles could change their own personal details such as name and date of birth in the Umoja system due to gaps in the Umoja security configuration. There was no monitoring process to detect such unusual changes to the HR master data. Similarly, cashiers and administrative officers could also change the personal information for staff members even though it was not required by their job functions. Any unauthorized change could impact the system's integrity. DM stated that it has commenced analysis in the case of cashiers and administrative officers who have access to change personal information.

(iii) The pension contribution start date in Umoja for all records migrated from the legacy system was shown as 01.11.2015 (not the actual contribution start date). DM stated that a solution to interface the system of the United Nations Joint Staff Pension Fund with Umoja is targeted for implementation by the first quarter of 2019.

(iv) Master data relating to education grant such as school names, school codes, school types (publicly funded or not), and cities was incomplete in Umoja. For example, 9,800 schools had a unique school identifier assigned to them in the system, whereas 27,000 others did not have any such unique identifier assigned to them. This required HR to manually validate the school information. A master data management procedure was required for maintaining this information in the system. DM stated that payments are not based on the school itself but on the type of school and documentation provided by the staff during settlement where a HR partner conducts full review of the claim. OIOS is of the view that master data should be completely populated in the system to reduce manual intervention and error as these master data references are used in determining education grant payments.

(v) Umoja allowed disbursement of education grant advance even if the claim for the previous year was not settled, which is contrary to applicable rules for receiving education grant. DM stated that the system was designed properly and that it is the responsibility of HR to ensure that settlements are processed before processing an advance as validations should not be hardcoded in the system because exceptions could be granted.

(vi) At the time of the audit, Umoja was not able to support automated calculation for special education grant cases where a special benefit had been granted, which could lead to error. DM stated that an automated solution was introduced in January 2018 as part of the new education grant schema, and that the automated calculation was confirmed during testing.

(vii) In certain situations, a staff member may not need to contribute towards education grant, in which case a manual workaround was required to document such cases. HR partners were required to input \$0.01 in the payment line in order to process the claim. This was prone to input error. For instance, if \$0 was

input instead of \$0.01, the staff member would be erroneously paid 75 per cent of the maximum admissible expenses, even though no payment was due. DM stated that this is the established process and there were no changes/enhancements to the solution contemplated as they are very unique situations which do not justify configuration from a cost/benefit perspective.

(viii) There was no validation link between education grant and education grant travel. A person who was not eligible for education grant could avail education grant travel. This process was manually controlled by the HR partners. DM stated that HR entitlement and travel are two independent modules and will remain as such, and that controls will continue to be manually performed by HR partners.

(ix) Staff Rule 4.5 (d) states that “A staff member who has changed his or her residential status in such a way that he or she may, in the opinion of the Secretary-General, be deemed to be a permanent resident of any country other than that of his or her nationality, may lose entitlement to home leave, education grant, repatriation grant and payment of travel expenses...”. The eligibility check to ensure compliance with this requirement was not configured in Umoja. HR partners were required to manually check the eligibility in each specific case, without appropriate guidelines. For instance, OIOS noted a case where a staff member acquired permanent residency in 2014 but availed home leave travel in 2016. DM stated that for home leave, the accrual eligibility was addressed and put into production in February 2018, and a data clean-up exercise was conducted for existing records. DM has provided the Umoja entities with reports to review, validate and correct home leave accrual eligibility.

(x) There were several cases where the amount of rental subsidy was computed manually because of the limitation in Umoja that required the maximum rent amount to be configured based on marital status and number of dependents. DM stated that there was a project underway to standardize the establishment of maximum rent amounts, which could help eliminate the manual cases, and that a change request was submitted for the entitlement monitoring functionality that initiates the exercise for rental subsidy monitoring. DM had also documented guidelines to conduct a random compliance check for rental subsidy applications and claims but this monitoring was not yet started. DM stated that enhancements to the entitlement monitoring functionality are in progress.

(xi) Umoja was not configured to check eligibility for rental deductions. Eligibility check was performed manually, and the deductions were processed manually in Umoja by the HR partner based on information received from mission management. DM stated that rental deduction is processed directly by the HR partner, based on local conditions, and it was not possible to automate it in the system.

(xii) Any change made to an existing dependent through Umoja employee self-service was not visible to the HR partner. Therefore, HR partners were required to compare the data submitted via employee self-service against what was already present in the system to validate the requested change. This led to additional manual effort. DM stated that a solution for this issue has been implemented.

Personnel management

(i) The Umoja system was not configured to prevent on-boarding or change of duty stations without evidence of the required medical clearance. OIOS detected 54 such cases in the system. DM stated that the system was properly configured, and this flexibility should be allowed in case of emergencies and other exceptional circumstances. To minimize the risk of invalid on-boarding or changes, OIOS is of the view that either a validation control should be configured in the system, or alternatively, a monitoring report should be used to periodically analyze and correct such instances. DM stated that a business intelligence report will be developed to analyse, monitor and correct these cases.

(ii) A temporary contract could be extended beyond 729 days without the required “cooling off” period as outlined in the ST/AI/2010/4/Rev.1 (Administration of temporary appointments). The system did not generate an error message requiring exception review by DM in such cases. DM stated that there was a warning message but no hard stop in the system, which was to allow exceptions to be granted by DM. To minimize the risk of unauthorized appointments, OIOS is of the view that either a validation control should be configured in the system, or alternatively, a monitoring report should be used to periodically analyze and correct such instances. DM stated that a business intelligence report will be developed to analyze, monitor and correct these cases.

Time management

(i) Absence quota anomalies were found in many cases, which indicated that leave entitlement quota validation was not working correctly. For example, the maximum negative deduction allowed in Umoja for annual leave was 30 days, however, several staff members had negative annual leave quota of more than 120 days. DM acknowledged that leave entitlement quota functionalities may have issues and stated that it intends to conduct a full review of entitlement quota validation.

(ii) There was no link between the time management and travel management modules. The Umoja system would process home leave travel even if the required number of home leave points were not available and annual leave/home leave were not approved by the staff member’s supervisor. This check was required to be manually enforced by HR partners. DM stated that a business intelligence report will be developed to address such issues.

(iii) The Umoja system was not configured to check compliance with home leave policy requirements which required staff members to spend at least seven days in the country of home leave. OIOS detected cases with less than two days of home leave. DM stated that a business intelligence report will be developed to identify, monitor and address anomalies.

(iv) No validation was enforced on home leave points. Even though Umoja was configured to allow up to six negative home leave points, OIOS detected cases with negative leave points as high as 125. DM stated that for the few cases reviewed, this was due to staff recording home leave absence for workdays only, skipping weekends, for consecutive weeks of home leave; therefore, home leave points were deducted for each week taken. Training of staff on how to record home leave may be required.

(v) There was overuse of the exception time manager role, which was developed for the purpose of managing exceptional cases where a staff member in one organization unit has a time manager in another organization unit. HR partners assigned and maintained this role manually. Timely maintenance of this role was not always possible due to frequent movement of staff, which resulted in time managers receiving workflow notifications for staff no longer under their supervision. This occurred due to incomplete organizational structures in the system. DM stated that it has instructed entities to perform clean-up, and that a change request was submitted to limit the exception time manager relationship to a maximum duration of one year and prevent assignment of the role within the same organization unit.

Finance: General ledger

(i) The general ledger (GL) account creation data fields that controlled GL data entry (such as currency, tax category, reconciliation, and exchange rate difference) were set to “optional”. This gap could cause the recording of erroneous/missing financial data and should have therefore been assessed to determine whether the fields should be made mandatory. DM stated that the Accounts Division, in

consultation with the Umoja Office, will determine the cost/benefit of changing the configuration to make the currency field mandatory.

(ii) Monitoring over the open/close of accounting periods required further strengthening. For example, some users had enterprise roles assigned which allowed them to open/close periods, yet the roles were not defined in the enterprise role guide. Roles that allow opening and closing of accounting periods should be documented. DM stated that the opening and closing of accounting periods were treated very seriously and were closely monitored by the Accounts Division; a review of the list of users who have the role was conducted and only those necessary to perform the function were provisioned.

Finance: Accounts payable

(i) There was no tolerance setting enabled for document type KH which does not require a purchase order (PO) or funds commitment. The current setting was configured as 9,999,999,99.00. There should be limits set for non-PO invoices that would exceed the normal limit of United Nations Financial Rules. DM stated that operational controls are in place which require all such documents to be approved by finance officers with the necessary delegation of authority. However, the Accounts Division, in consultation with the Umoja Office, will review options for limiting the availability of the KH document type to a small group of users and potentially for a restricted group of balance sheet accounts.

(ii) 96 vendor records did not have duplicate invoice validation flag enabled in Umoja. In this scenario, payment processors would not be warned of any duplicate invoice submitted by the vendor before the payment is processed. DM stated that it will determine the reason for the missing validation flag.

Finance: Funds management

(i) There was a misalignment between the budget line structure and the actual expenditure and commitment line structure. DM stated that commitment items in Umoja are tied to specific GL accounts that ensure expenses are automatically classified accurately. Budgets are prepared outside the Umoja system since Umoja Extension II budget formulation functionality has not yet been implemented. Therefore, misalignment in Umoja was an unavoidable outcome that did not constitute an error. DM further stated that with the rollout of Umoja Extension II budget formulation, the budgeting and expenditure classification will be consistent.

Finance: Fixed assets

(i) There was misalignment between fixed assets depreciation keys and useful life in some cases (e.g., asset with useful life of 4 years was configured with depreciation key of Z000, which the system would translate to mean that the asset did not require depreciation). DM stated it will determine the cause of the misalignment and will mitigate future similar occurrences through training and monitoring. DM also stated that depreciation keys were entered in the asset master record based on the asset class (derived from the asset class) and should not be amended. To minimize the risks of incorrect accounting entries, OIOS is of the opinion that such exception cases should be clearly marked in the system.

(ii) The physical verification functionality for fixed assets and inventory was not deployed in Umoja. Therefore, the dates of physical verification were entered in the warranty date field. This resulted in unreliable management reports. DM stated that this practice has now been discontinued, and that this was a temporary/practical business decision taken in conjunction with Umoja to use the ‘warranty date’ field to reflect the date of the physical verification prior to the development of the Umoja based physical verification utility, which is now being implemented.

Procurement

(i) The process for periodic review and cleanup of vendor master was not established. OIOS review of the vendor master showed 271 duplicate vendors which required validation and de-duplication by the Procurement Division (PD). Further, some vendors had inconsistent information in their master records (such as numbers in the city name field). DM stated that the number of records requiring further validation represents a small fraction of the total number of more than 46,000 Z010 records. PD stated that a regular review exercise executed by an independent, external party would be beneficial.

(ii) The three-way match validation control (which allowed payments to vendors only upon the receipt of goods and invoices matched to the PO) could be bypassed in Umoja by the buyer. Several POs that bypassed the validation were noted in the Umoja system. PD explained that a fix for this deficiency was in progress. DM acknowledged that there is a feature whereby the buyer could disable the three-way match when creating the PO. PD proposed to resolve this issue by adding it to the list of enhancements to be worked on.

(iii) Sensitive data fields were not configured in Umoja for dual control over changes to vendor data, such as changes to vendor bank accounts. DM stated that process owners were accountable for managing the balance between risks and controls, and that an enhancement to activate dual control for vendor banking data has been developed and tested by Treasury and is expected to be rolled out in June 2018.

(iv) POs could be raised on vendors flagged for deletion by removing blocks on such vendors temporarily. For instance, OIOS noted an example (PO number 2200055049) where the PO was placed on a vendor (vendor number 1110010324) flagged for deletion, and no monitoring for such instances was in place. DM stated that this observation relates to operational exceptions whereby vendor blocks needed to be lifted temporarily, and that given the operational exceptions needed, it was not practical to enforce the control without acceptable definitions of exceptions. DM further stated that customization of the standard functionality is also not desirable unless unavoidable. OIOS is of the view that DM should institute an appropriate control to review such instances to minimize the risk of procuring goods from deleted vendors.

(v) The vendor registration level (which determined the contract award thresholds) was not recorded in the system. Umoja was not configured to prevent a procurement transaction above the threshold associated with the supplier's registration level. DM stated that automation of this within the Umoja system was reviewed and it was decided that implementing this change would require major developments to the interface between United Nations Global Marketplace and Umoja; instead, all procurement specialists were to manually validate the registration level. Further, it was proposed that a monitoring report to compare expenditure and registration level will be developed.

(vi) It was difficult to track the procurement of ICT assets due to the description of assets being captured in text fields in Umoja. DM stated that the review of material master records for all ICT contracts was underway, and the proper level of definition of ICT assets within the material master should be completed before the end of 2018.

Payroll

(i) Controls over danger pay were not optimal. Danger pay was not automatically suspended during leave or terminated upon departure of staff, resulting in the need for recoveries of overpayment. It was not linked to payroll and no reports were available to indicate staff who were outside the duty station to whom danger pay should not be paid. OHRM stated that there was a project underway to revisit the way danger

pay was administered and processed in Umoja. DM stated that the danger pay solution was planned for implementation in the second quarter of 2019.

Treasury and investment accounting

(i) Treasury business partner (broker/counterparty) information present in the Treasury's investment management system was manually recorded in Umoja. There was no link between the two systems, thus requiring treasury staff to manually reconcile information. DM stated that the Umoja process for managing treasury business partners was manually executed by the treasury administrator role, and that automating the creation of treasury business partners was not part of Umoja's scope. DM further stated that the cost-benefit of such automation had to be examined as the manual process poses no risk.

(ii) The 'payment term' field could be changed by cashiers when processing the payment in Umoja, which was not an optimal internal control. DM stated that cashiers were instructed not to modify any field in the payment document that should only be executed by the accounts payable user.

(iii) SAP provided a document sequence control feature over financial documents to ensure completeness and proper audit trail. Any gaps in this document sequence could indicate error or fraud. OIOS noted that there was no review process instituted by DM to review such gaps. For example, there were gaps in the document sequence for finance and treasury documents. DM confirmed that the process needed to be reviewed and that a process is planned to be implemented once resources are available to tackle the issue. DM further stated that number range gaps generally result from a known process in SAP where document numbers are lost in the buffer. The Umoja Office has raised this issue with SAP to understand and address the eventual technical issues that cause such number range gaps.

(iv) Centralized cash management should be limited to Treasury staff. However, this limitation was not enforced as the automated payment programme (F110) could be run by several individuals other than Treasury staff across duty stations. Payment approvers (signatories) could also change the payment date. Furthermore, the assignment payment lists were not acted upon in a timely manner, which resulted in funds/cash being blocked for use. DM stated that cash management is already centralized, i.e., all the operation cash requirements are calculated at Headquarters. DM also stated that Treasury was in the process of reviewing the Umoja cashier enterprise role in the context of the Secretary-General's reform initiatives and other efficiency reviews. It is expected that these reviews will result in modification to provisioning of access to F110 and potentially other transaction codes that impact cash calculations.

(v) The responsibility, roles and timelines for closing the United Nations' bank accounts in Umoja were not defined, once the account was physically closed. Keeping the bank account open in Umoja could lead to notional entries being passed and the associated relationship management agreements with the banks would remain open pending closure in Umoja, which could result in outgoing payment instructions to the physically closed bank account. DM stated that from a technical point of view the responsibilities have been defined between Umoja and the Office of Programme Planning, Budget and Accounts and this process was currently under implementation through iNeed.

(vi) Dual control over bank accounts had not been evaluated for possible preventive control configuration for bank signatories, which was currently manually monitored by Treasury. DM stated that the need for such a preventive control needs to be evaluated before proposing the automation; Treasury and the Umoja Office must prioritize more pressing needs and control risks.

(2) DM should implement control enhancements: (i) over high-risk processes by factoring them into the continuous improvements change control process; and (ii) for the specific gaps identified in the present audit.

DM accepted recommendation 2 and stated that recommendation 2 (i) has been implemented and recommendation 2 (ii) will be implemented by 31 December 2020. Recommendation 2 remains open pending receipt of evidence that: control enhancements over high-risk processes have been implemented through the continuous improvements change control process; and that specific gaps identified in the present audit have been addressed.

Monitoring mechanisms needed to be strengthened

19. Master data and transactions should be monitored in the system to minimize the possibility of unauthorized or invalid processing of transactions. This detective control is especially important in the absence of configuration of appropriate preventive controls. OIOS review of controls over master data in Umoja showed that there was no monitoring of important master data and transactions to compensate for the absence of preventive controls configured in the system. For instance:

(i) Reports on unposted assets were available in Umoja but not periodically reviewed. DM stated that the fixed assets management officer periodically checks unposted assets and there were some that could not be removed for various reasons. DM further stated that a change request was in the process of being tested to allow display access to the Supplier Relationship Management (SRM) module by non-transactional SRM users, which will assist in addressing the issue.

(ii) OIOS review of payroll transactions noted that 135 records for 2017 had not been posted to the general ledger, some as far back as March, May, September and October 2017. This would indicate that there was no timely review of payroll exceptions. DM stated that it may be the result of timing as to when the report was run and that currently, it was working on resolving 13 payroll transactions not posted in 2017 that needed a data fix.

(3) DM should: (i) require the Umoja process owners to embed a review into the change control process so that an internal monitoring mechanism is factored into every change/improvement when it is considered and implemented; (ii) implement the enhancement to display access to Supplier Relationship Management to non-transactional users; and (iii) fix and post the 135 payroll records outstanding from 2017.

DM accepted recommendation 3 and stated that recommendation 3 (i) has been implemented and a review by process owners is embedded into the change control process for every improvement/change when it is considered and implemented. DM further stated that an enhancement is in progress to address recommendation 3 (ii) while recommendation 3 (iii) is expected to be implemented by first quarter of 2019. Recommendation 3 remains open pending receipt of evidence demonstrating that it has been fully implemented.

C. ICT support system

User authorization, access management and system security parameters require strengthening

20. Access to Umoja should be restricted in accordance with users' functional roles and responsibilities and in alignment with the "Access Control for the United Nations Secretariat ICT Technical Procedure" published by the Office of Information and Communications Technology (OICT) in November 2013. In

addition, the Umoja Office developed guidance materials such as enterprise role guide and Security Liaison Officer (SLO) workbook detailing the process and requirements for assignment of the type and level of access for Umoja users.

21. The following gaps were noted with the user authorization and access management procedures in Umoja:

(i) The powerful SAP query transaction code SUIM (SAP User Information System code for viewing user IDs, roles, profiles, and authorizations) was not restricted in the Umoja system, which could give users access to view a wide range of information which they may not be authorized to read. The SUIM transaction code was granted to an exceptionally large number of users. The risk of granting such access had not been evaluated.

(ii) The type and level of access to the functions and information in Umoja was controlled through various enterprise roles assigned to users. The enterprise roles were built by combining various complex and micro level authorizations in Umoja. Any unwarranted/unauthorized switching 'on' and 'off' of these authorizations would have a significant impact on the integrity of data and transactions in the system. DM stated that they do not recognize this as a gap and that it is a necessary feature of any system. DM further stated that it is not aware of any other way of building the security roles. OIOS is of the view that DM needs to address this issue as it exposed the system to the risk of unauthorized access.

(iii) The Umoja Office used manual processes to design enterprise roles and to check the appropriateness of various authorizations embedded in these roles, which was inadequate given the level of complexity and number of enterprise roles. For example, there were about 3,500 enterprise roles combined with more than 20 workflows. Any change in staff assignment or functions required extensive manual update of workflow tables for the user by the Umoja security team. OIOS found instances where gaps in authorization resulted in grant of access to HR partners, administrative officers and cashiers such that they were allowed to change some aspects of their own personal information (name and date of birth). DM stated that even though enterprise role composition was done manually, extensive testing was/is done to limit unintended access. DM further stated that the Governance, Risk and Compliance Tool will be implemented in future after Umoja Extension II rollout is completed, but may not obviate all of the risks implied in the audit observation.

(iv) Inconsistencies were noted between the Umoja enterprise role guide and actual role assignments in the system. Some enterprise roles marked as conflicting in the enterprise role guide were assigned to users, e.g., enterprise roles for payroll PY.01 and PY.04 marked as conflicting in the enterprise role guide were assigned to the same user. DM stated that SLOs and Financial Approvers were responsible for ensuring that conflicting roles were not assigned. DM further stated that Umoja has since implemented a segregation of duty feature in the user access provisioning application which indicated instances when a SLO attempts to assign roles with segregation conflict(s). So, these conflicts will be significantly reduced going forward.

(v) The enterprise role guide needed to be updated for some enterprise roles. For example, it did not restrict assignment of conflicting treasury roles, e.g., TR.05: Front office user and TR.01: Back office user.

(vi) There were inadequate operational procedures and timelines to remove access of retired or separated staff in Umoja. OIOS noted instances where separated staff still retained access to critical information and functions in Umoja (such as HR). This was because users were granted access to Umoja through the Unite identity solution, which also provided access to various other ICT applications of the United Nations. OIOS was informed that immediate removal of access to Unite identity was not desirable as retired/separated staff might still need access to ICT applications other than Umoja. DM stated that

Umoja and all process owners are preparing criteria for bulk deprovisioning of Umoja users who are not active staff members.

(vii) Similarly, there was no process in place to seek periodic confirmation from the responsible managers on validity and roles of the staff mapped to them in the Umoja system. Thus, staff who had changed functions sometimes retained access to enterprise roles and workflows related to their previous job role. DM stated that SLOs were informed and expected to undertake a periodic check of access validity of user identities and roles that have been provisioned.

(viii) Gaps were noted in the configuration of the Umoja security module. High risk items were analyzed and corrected by the Umoja security team during the audit.

(4) DM should: (i) review the assignment of high-risk roles and restrict them to authorized users; (ii) review and remove conflicts in the authorizations embedded in critical enterprise roles; and (iii) establish procedures to remove access to the Umoja system for separated/retired/reassigned staff in a timely manner.

DM accepted recommendation 4 and stated that recommendation 4 (i) and 4 (ii) have been implemented. Recommendation 4 remains open pending receipt of evidence demonstrating that it has been fully implemented.

Need to consolidate and assess functionalities and interfaces yet to be implemented

22. A system implementation should include all functionalities and interfaces required by management to perform the necessary business transactions and functions, and to achieve maximum benefit from the system. COBIT recommends documenting interface requirements of information systems, including expected deliverables, constraints to its design, specifications about the data to be exchanged, timing and sequencing dependencies, and monitoring mechanisms to check that interface transmissions are accurate and complete.

23. Several functionalities in Umoja and interfaces with other systems were planned to be implemented. However due to changing priorities, many of them have not yet been implemented. A consolidated list of such pending functionalities and interfaces was not kept and assessed for implementation. Some of these functionalities/interfaces identified during the audit are listed below:

Treasury

(i) Investment management systems used by Treasury for actual trading were not integrated with Umoja. Counter party information, settlement instructions and trades executed in the investment systems were manually entered and settled in Umoja. Due to manual intervention, this was prone to error. DM stated that development of the related interfaces is on the list of continuous improvements of Umoja functionality.

(ii) The automated investment portfolio reconciliation process in Umoja was not working. The investment accounts unit manually performed the reconciliation using Excel by comparing information downloaded from the bank with Umoja. DM stated that they have verified the process and concluded that the automated reconciliation process is working without technical issues for the United Nations Headquarters portfolio, however there were intermittent issues causing the reconciliation of one of the other portfolios to fail on specific days. DM also stated that Umoja is currently investigating these issues.

(iii) The average daily balance functionality for distribution of interest income on the investment cash pool bank account in Umoja was not working. As a result, investment income was distributed manually in Umoja by the Accounts Division on a six-months basis using journal entries. This was a manual process prone to error, as it was performed using a business intelligence (BI) report that was not periodically tested or verified. DM stated that the average daily balance interest distribution functionality has not been given priority over other more urgent items requested by the business. DM also stated that the BI report currently used to calculate the interest distribution has been fully tested with business involvement and the business typically performs a reconciliation of the calculated amounts when executing the report to validate the result.

(iv) Treasury used spreadsheets for cash projection requirements as the Umoja cash forecast reports were not considered reliable. DM stated that Treasury has gradually changed the operational approach to cash management over the past months and the reports initially requested and designed for this purpose no longer meet these new requirements. DM further stated that Umoja has been supporting this change process by first addressing issues detected with standard SAP transactions, and that Treasury will open a change request to implement reports to support the new process as soon as the requirements are stable.

Human Resources

(i) The new maternity leave policy allowed maternity leave to be combined with other types of leave, but this policy was yet to be implemented in the Umoja system. DM stated that this is currently under review.

(5) DM should review and prioritize the implementation of continuous improvements for Umoja that include: (i) the outstanding functionalities; (ii) resolution of the issue concerning the automated investment portfolio reconciliation process; and (iii) functionality to support the new maternity leave policy.

DM accepted recommendation 5 and stated that it will review and prioritize the implementation of continuous improvement functionality based on business priorities and the General Assembly's guiding principle on customization. Recommendation 5 remains open pending receipt of evidence that: (i) the outstanding functionalities been reviewed and prioritized for implementation; (ii) the issue with the automated investment portfolio reconciliation process has been resolved; and (iii) functionality to support the new maternity leave policy has been implemented.

Gaps in tracking Umoja process performance

24. System testing requires: (i) measuring product performance under different 'traffic' conditions and comparing them against metrics identified as part of a system test plan, system performance metrics, and key performance indicators which should measure values as part of system testing.

25. The Umoja team received daily and weekly performance monitoring reports on the Umoja infrastructure (i.e., hardware, software, and network) from the external vendor who was responsible for monitoring the infrastructure. These reports included performance measures of processor and memory usage, as well as some tasks such as transaction codes, reports, batches and dialogs. However, several other time sensitive processes were not included in the performance monitoring procedures (e.g., the critical daily processes of the cashiers 'FTE_BSM' (read bank statement), 'BNK_APP' (used to approve payment prior to releasing) which were not listed in the performance monitoring reports. DM stated that Umoja provides a monthly performance report containing various indicators that were monitored to gauge the system's health from certain perspectives, and that if specific processes become problematic, these were typically

reported by users and then reviewed. DM also stated that the continuous improvement monitoring programme already includes tools for detailed analysis of process inefficiencies, including potential user-related problems, which have been brought to the attention of the process owners.

26. OIOS also noted that process performance reports were not shared with the respective process owners to notify them of any discrepancies or performance issue for which they were responsible. For example, the cashiers reported performance issues whilst using several transaction codes (i.e., FAGLL03, FPRL_LIST and BNK_MONI). In addition, a transaction had to be processed manually which caused \$70,000 in overdrawn accounts. DM stated that the Umoja team engaged SAP MaxAttention services to review and assess in greater detail the performance issue of transactions FAGLL03, FPRL_LIST and BNK_MONI, and that the Umoja Functional Team and SAP are also investigating solutions to improve the overall performance of these transactions.

27. OIOS also noted various performance issues in the SRM module, for which the Umoja team hired SAP to analyze. Several actions to improve the performance of SRM processes were recommended but were yet to be implemented at the time of the audit. DM stated that these changes are part of the SRM upgrade under way as a holistic package, which is more efficient to test.

(6) DM should: (i) define the performance benchmarks for the individual tasks (transaction codes, batches, reports, dialogs) of time-sensitive processes; and (ii) include critical processes in its periodic monitoring procedures, periodically collect performance feedback from users, and address the root causes of performance issues.

DM did not accept recommendation 6 stating that it was its understanding that OIOS would enhance this recommendation with specific examples, rather than having it as a global recommendation. OIOS has already provided examples in the report to support the described condition. This unaccepted recommendation has been closed without implementation and may be reported to the General Assembly indicating management's acceptance of residual risk.

Governance and change management of Umoja interfaces was adequate

28. The Application Interface Profile Registry Governance group (AIP Governance group) managed the AIP registry which was established as a centrally deployed and managed service by OICT. One of the purposes of this registry was to align the AIP registry with the OICT Enterprise Architecture. In addition, the "Umoja Data Interfaces United Nations Secretariat ICT Technical Procedures" established procedures to address data interfacing requirements around the Umoja solution. Standard templates should be used for documenting functional and technical requirements of these interfaces listed in the AIP registry.

29. OIOS reviewed the Umoja interfaces and noted that there were 62 existing interfaces as of 25 August 2017 which were not part of the AIP registry. The documentation of interface specifications was not standard and version control was not optimal since change requests tickets were managed by separate tickets that were not adequately versioned in sequential order to facilitate implementation. Also, there was no central repository for the final approved technical and functional interface specifications. DM stated that the AIP was not established to be the main governing body for the data exchange with Umoja and the AIP's scope was to provide a master data feed from Umoja to legacy stand-alone applications only. DM further stated that the Umoja change control board was the governing body and therefore the Umoja interfaces that are part of an end-to-end Umoja process will not appear in the registry.

30. There were no service level agreements (SLA) between Umoja and the interfaced application owners that regulated the maximum response times for addressing the issues encountered in the Umoja

interfaces. DM stated that Umoja did not establish an SLA for each interface as they were subordinate to the overall Umoja SLA and the interfaces were part of the solution discussed and agreed upon between the business process owner and Umoja team. DM further stated that a standard protocol and alert mechanism exists and is in place to monitor the timely execution of each interface, and that critical interfaces are specifically monitored.

Gaps in Umoja production support structure need to be addressed

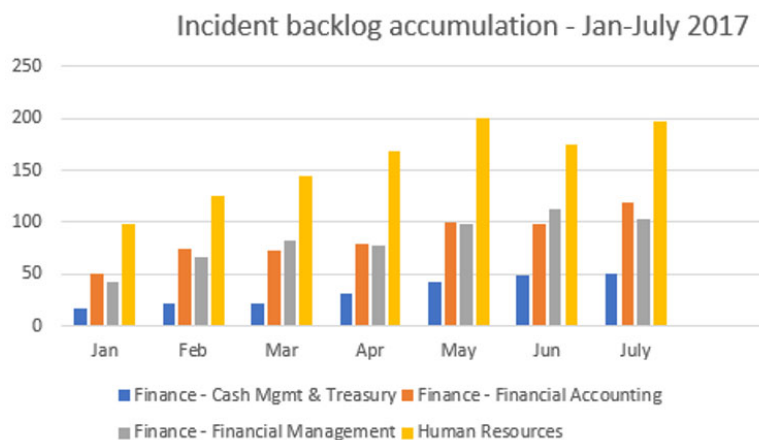
31. An ICT service management framework should define the level of support required for the continuous and reliable functioning of ICT operations. The framework should detail the criteria and processes to document the requirements of SLAs. The framework should also specify the roles, tasks, and responsibilities of internal and external service providers.

32. OIOS assessed the effectiveness of the production support process including: (i) registration of Umoja user inquiries (incidents and requests); (ii) escalation process; (iii) resolution; and (iv) closure.

33. Until January 2018, tier-1 Umoja production support for Headquarters (i.e., initial receipt point for incidents and requests) was coordinated through two entities: (i) the Unite Service Desk of OICT; and (ii) Headquarters Deployment Group (HDG) which consisted of assigned staff from various departments. A separate (Lotus Notes) ticketing system was used for tracking and reporting the cases handled by the HDG. User inquiries relating to business process issues were handled by the HDG and the ones that HDG could not resolve were transferred to the Unite Service Desk for escalation to the relevant escalation groups.

34. The Unite Service Desk served as the escalation hub and documented guidelines for Umoja iNeed production support for resolving the incidents and requests that were technical in nature. Issues that required system changes were escalated to tier-2 and tier-3 when the Umoja change control process took over the workflow. Between 1 January 2017 and 18 July 2017, the service desk received 12,890 cases (incidents, problems, service requests).

35. Analysis of the Unite Service Desk tickets showed that there was increasing backlog of unresolved issues for certain business processes (see chart below).



36. Time taken for the work orders related to resolution of reported issues or service requests was not controlled through operational agreements or SLAs between groups. OIOS analysis of the Umoja change request tickets (tier-3) showed that various issues had been open for several months. The Umoja Office

explained that timely implementation of project deliverables took precedence over system improvements or issue resolution; finding a solution for several issues was not easily resolved.

37. HDG was disbanded in January 2018. As of February 2018, the Unite Service Desk did not update its production support procedures after HDG was disbanded, which may result in unclear escalation points and longer resolution times. In addition, within the context of the Global Service Delivery Model (GSDM), a “Shared Catalog of Administrative Services” was planned to be deployed within iNeed in the future and was expected to resolve the lack of clarity and improve the efficiency of the escalation process by avoiding unnecessary escalation points. DM stated that OICT has been assisting the business in the shared catalog of administrative services in iNeed, and once the business has signed off on this change, OICT would implement it. However, the deployment is likely to be impacted by the General Assembly decisions on the GSDM proposals. DM also stated that the HDG was disbanded as directed by the General Assembly; a solution will be sought through newer arrangements that are evolving in the context of GSDM.

38. Since this issue would be covered by recommendation 5 concerning the review and prioritization of tasks under the continuous improvement programme, OIOS did not make any additional recommendation in this area.

Disaster recovery planning needs to be improved

39. An ICT disaster recovery plan should be developed in conjunction with a business continuity plan and provide recovery strategies to meet the objectives of the plan. Disaster recovery failover and failback exercises (testing) should be conducted on a regular basis to ensure the availability of the system and critical transaction processing, in the case of unforeseen events impacting the system.

40. The Umoja technical team, in coordination with OICT, Department of Field Support and service providers, performed a planned failover and failback exercise on 6 and 13 May 2017. During the tests, Umoja was unavailable for significantly longer than was originally planned. A lessons learned report was documented for all phases of this recovery exercise which included issues, causes, recommended actions as well as responsible teams to ensure quicker recovery. Timely implementation of the actions listed in the lessons learned report was necessary to minimize the risk of unavailability during an event that impacts the availability of the production systems.

41. Additionally, disaster recovery invocation criteria were not clear to address the scenarios of the unavailability of critical processes (certain transactions, reports, and transaction codes) when the Umoja servers were up and running. There were reported instances of some transactions that timed-out due to conflicting processes accessing the same data. This type of process unavailability was not categorized as unavailability of Umoja. For example, in January 2018, cashiers experienced several hours of unavailability of certain processes which caused missed targets and financial obligations. The disaster recovery team was not aware of the unavailability incident. DM stated that when there is significant non-availability of critical processes, the user community impacted will bring the issue to the notice of the appropriate teams, and that besides the monitoring by the infrastructure teams, Umoja duty managers are available 24/7 to respond to outages and problems. DM further stated that in the event of a peculiar combination of processes being impacted, the initial reaction is to determine the root cause and try to resolve, rather than invoke a disaster recovery plan that has many ramifications.

42. The continuity of business processes depends on Umoja process availability (not only server availability). Therefore, interactions of conflicting processes (such as payroll and cashiers) should be assessed and optimized for continuity. OIOS noted that the coordination and collaboration across process owners and their representatives is well established and functioning smoothly.

(7) DM should: (i) ensure the timely implementation of actions determined in the lessons learned report on the disaster recovery exercise; and (ii) conduct a review of the disaster recovery plan following the deployment of Umoja Extension II in 2019.

DM accepted recommendation 7 and stated that the infrastructure is currently being replaced and once this is completed, the outstanding lessons learned actions will be addressed. Further review of disaster recovery plan will be conducted following deployment of Umoja Extension II. Recommendation 7 remains open pending receipt of evidence that: (i) actions determined necessary in the lessons learned report on the disaster recovery exercise have been implemented; and (ii) a review of the disaster recovery plan has been conducted following the deployment of Umoja Extension II in 2019.

IV. ACKNOWLEDGEMENT

43. OIOS wishes to express its appreciation to the management and staff of DM for the assistance and cooperation extended to the auditors during this assignment.

(Signed) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

ANNEX I

Audit of Umoja implementation by the Department of Management

Rec. no.	Recommendation	Critical ² / Important ³	C/ O ⁴	Actions needed to close recommendation	Implementation date ⁵
1	DM should: (i) update the Umoja business design documents as part of the change control process; and (ii) document an Umoja data dictionary.	Important	O	Recommendation 1 (i): Receipt of evidence that business design documents have been updated. Recommendation 1 (ii): Closed without implementation based on management's acceptance of residual risk.	30 June 2019
2	DM should implement control enhancements: (i) over high-risk processes by factoring them into the continuous improvements change control process; and (ii) for the specific gaps identified in the present audit.	Important	O	Receipt of evidence that: control enhancements over high-risk processes have been implemented through the continuous improvements change control process; and that specific gaps identified in the present audit have been addressed.	31 December 2020
3	DM should: (i) require the Umoja process owners to embed a review into the change control process so that an internal monitoring mechanism is factored into every change/improvement when it is considered and implemented; (ii) implement the enhancement to display access to Supplier Relationship Management to non-transactional users; and (iii) fix and post the 135 payroll records outstanding from 2017.	Important	O	Receipt of evidence demonstrating that it has been fully implemented.	31 March 2019
4	DM should: (i) review the assignment of high-risk roles and restrict them to authorized users; (ii) review and remove conflicts in the authorizations embedded in critical enterprise roles; and (iii) establish procedures to remove access to the Umoja system for separated/retired/reassigned staff in a timely manner.	Critical	O	Receipt of evidence demonstrating that it has been fully implemented.	31 March 2019

² Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

³ Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

⁴ C = closed, O = open

⁵ Date provided by DM in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

ANNEX I

Audit of Umoja implementation by the Department of Management

Rec. no.	Recommendation	Critical²/ Important³	C/ O⁴	Actions needed to close recommendation	Implementation date⁵
5	DM should review and prioritize the implementation of continuous improvements for Umoja that include: (i) the outstanding functionalities; (ii) resolution of the issue concerning the automated investment portfolio reconciliation process; and (iii) functionality to support the new maternity leave policy.	Important	O	Receipt of evidence that: (i) the outstanding functionalities been reviewed and prioritized for implementation; (ii) the issue with the automated investment portfolio reconciliation process has been resolved; and (iii) functionality to support the new maternity leave policy has been implemented.	31 December 2020
6	DM should: (i) define the performance benchmarks for the individual tasks (transaction codes, batches, reports, dialogs) of time-sensitive processes; and (ii) include critical processes in its periodic monitoring procedures, periodically collect performance feedback from users, and address the root causes of performance issues.	Important	C	Closed without implementation based on management's acceptance of residual risk.	Not applicable
7	DM should: (i) ensure the timely implementation of actions determined in the lessons learned report on the disaster recovery exercise; and (ii) conduct a review of the disaster recovery plan following the deployment of Umoja Extension II in 2019.	Important	O	Receipt of evidence that: (i) actions determined necessary in the lessons learned report on the disaster recovery exercise have been implemented; and (ii) a review of the disaster recovery plan has been conducted following the deployment of Umoja Extension II in 2019.	(i) 31 March 2019 (ii) 30 June 2020

APPENDIX I

Management Response



United Nations **Nations Unies**
 INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar, Deputy Director
 A: Internal Audit Division, Office of Internal Oversight Services

DATE: 19 September 2018

THROUGH: Olga de la Piedra, Director
 S/C DE: Office of the Under-Secretary-General for Management

FROM: Mario Baez, Chief, Policy and Oversight Coordination Service
 DE: Office of the Under-Secretary-General for Management

SUBJECT: **Draft report on an audit of Umoja implementation by the Department of Management**
 OBJET: **(Assignment No. AT2017/519/02)**

1. We refer to your memorandum dated 28 August 2018 regarding the above-subject draft report and provide you with comments from the Department of Management (DM) below and in the attached Appendix I.

A. Human Resources

Paragraph 18 (ii)

Staff with HR partner roles could change their own personal details such as name and date of birth in the Umoja system due to gaps in the Umoja security configuration. There was no monitoring process to detect such unusual changes to the HR master data. Similarly, cashiers and administrative officers could also change the personal information for the staff members even though it was not required for their job functions. Any unauthorized change could impact the integrity of the system. DM stated that the case of cashiers and administrative officers having access to change personal information will be further analyzed and addressed, and that OHRM will monitor HR partner access to modifying their own records and will look at restricting Umoja HR partner roles.

2. DM has commenced analysis in the case of cashiers and administrative offices who have access to change personal information.

Paragraph 18 (iii)

The pension fund contribution start date in Umoja for all records migrated from the legacy system was shown as 01.11.2015 (not the actual contribution start date). DM stated that currently, payroll manually checks the legacy system for the correct participation date, and that efforts are in progress to address this issue.

3. A Umoja change request has been submitted by OHRM for analysis and future development of changes whereby the pension fund dates will be loaded from the pension fund into Umoja. The solution to interface UNJSPF's system with Umoja is targeted for implementation by the first quarter of 2019.

*DM-2017-07574
 21-Sept-2018*

Paragraph 18 (iv)

Master data relating to education grant such as school names, school codes, school types (publicly funded or not), and cities was incomplete in the Umoja system. For example, 9,800 schools had a unique school identifier assigned to them in the system, whereas 27,000 others did not have any such unique identifier assigned to them. This required HR to manually validate the school information. A master data management procedure was required for maintaining this information in the system. DM stated that this is a very low risk item. As these master data references are used in determining education grant payments, OIOS is of the opinion that master data should be completely populated in the system to reduce manual intervention and error.

4. It should be noted that payments are not based on the school itself but on the type of school and documentation provided by staff during settlement where a Human Resources Partner conducts a full review for each claim.

Paragraph 18 (v)

The education grant module was not enabled for entitlement validity check. The eligibility check was performed by HR manually for each application. Although DM stated that Umoja performs a number of eligibility checks such as nationality versus duty station, child age, contract type and duration, and type of duty station (family versus non-family), OIOS found that this did not prevent the HR partner from processing education grant for ineligible staff as the application was entered and validated manually.

5. DM requests OIOS to provide the details of the cases identified where the Human Resources Partner processed an education grant for ineligible staff and details on the specific eligibility checks it referred to.

Paragraph 18 (x)

Staff Rule 4.5 (d) states that “A staff member who has changed his or her residential status in such a way that he or she may, in the opinion of the Secretary-General, be deemed to be a permanent resident of any country other than that of his or her nationality, may lose entitlement to home leave, education grant, repatriation grant and payment of travel expenses...”. The eligibility check to ensure compliance with this requirement was not configured in Umoja. HR partners were required to manually check the eligibility in each specific case, without appropriate guidelines. For instance, OIOS noted a case where a staff member acquired permanent residency in 2014 but availed home leave travel in 2016. DM stated that for home leave, the accrual eligibility was addressed and put into production in February 2018, and a data clean-up exercise was conducted for existing records.

6. On 5 March 2018, OHRM provided Umoja entities with reports to review, validate and correct Home Leave Accrual eligibility. The solution is implemented (Ref: INTTRK-15002).

Paragraph 18 (xi)

There were several cases where the amount of rental subsidy was computed manually because of the limitation in Umoja that required the maximum rent amount to be configured based on marital status and number of dependents. DM stated that there was a project underway to standardize the establishment of maximum rent amounts, which could help eliminate the manual cases, and that a change request was submitted for the entitlement monitoring functionality that initiates the exercise for rental subsidy monitoring. DM had also documented guidelines to conduct a random compliance check for rental subsidy applications and claims but this monitoring was not yet started.

7. Enhancements to the Entitlement Monitoring functionality are in progress (Ref: INTTRK-16294).

Paragraph 18 (xiii)

Any change made to an existing dependent through Umoja employee self-service was not visible to the HR partner. Therefore, HR partners were required to compare the data submitted via employee self-service against what was already present in the system to validate the requested change. This led to additional manual effort. DM stated that a solution for this issue was in progress.

8. The solution provided by SAP was tested and it is now in production (Ref: INTTRK-14072).

B. Personnel Management

Paragraph 18 (i)

The Umoja system was not configured to prevent on-boarding or change of duty stations without evidence of the required medical clearance. OIOS detected 54 such cases in the system. DM stated that the system was properly configured, and this flexibility should be allowed in case of emergencies and other exceptional circumstances. To minimize the risk of invalid on-boarding or changes, OIOS is of the opinion that either a validation control should be configured in the system, or alternatively, a monitoring report should be used to periodically analyze and correct such instances.

9. A Business Intelligence report will be developed to analyze, monitor and correct these cases.

Paragraph 18 (ii)

A temporary contract could be extended beyond 729 days without the required cooling off period as outlined in the ST/AI/2010/4/Rev.1 (Administration of temporary appointments). The system did not generate an error message requiring exception review by OHRM in such cases. DM stated that there was a warning message but no hard stop in the system, which was to allow exceptions to be granted by OHRM. To minimize the risk of unauthorized appointments, OIOS is of the opinion that either a validation control should be configured in the system,

or alternatively, a monitoring report should be used to periodically analyze and correct such instances.

10. A Business Intelligence report will be developed to analyze, monitor and correct these cases.

C. Time Management

Paragraph 18 (i)

Absence quota anomalies were found in many cases, which indicated that leave entitlement quota validation was not working correctly. For example, the maximum negative deduction allowed in Umoja for annual leave was 30 days, however, several staff members had negative annual leave quota of more than 120 days. DM stated that it was in the process of determining cases where the configured limit of negative 30 was not being enforced. DM further stated that there was no specific validation in the entitlement other than the carry forward every year being capped at 60 days (sometimes waived); explanations of high entitlements exist, and in general while looking at entitlements, consideration should always be given to the initial transfer balance and the existence of any waiver to the 60-day rule.

11. DM acknowledges that leave entitlement quota functionalities may have issues and intends to conduct a full review of entitlement quota validation.

Paragraph 18 (ii)

There was no link between the time management and travel management modules. The Umoja system would process home leave travel even if the required number of home leave points were not available and annual leave/home leave were not approved by the staff member s supervisor. This check was required to be manually enforced by HR partners. DM stated that time management and travel would remain as two independent modules and that control should be performed through monitoring and training of HR partners.

12. A Business Intelligence report will be developed to address such issues.

Paragraph 18 (iii)

The Umoja system was not configured to check compliance with home leave policy requirements which required staff members to spend at least seven days in the country of home leave. OIOS detected cases with less than two days of home leave. DM stated that absences were not recorded for weekends, whilst the seven-day requirement was based on calendar days, and that manual checks are performed by the certifying officer at the time of review of the expense report.

13. A Business Intelligence report will be developed to identify, monitor and address anomalies.

D. Payroll

Controls over danger pay were not optimal. Danger pay was not automatically suspended during leave or terminated upon departure of staff, resulting in the need for recoveries of overpayment. It was not linked to payroll and no reports were available to indicate staff who were outside the duty station to whom danger pay should not be paid. OHRM stated that there was a project underway to revisit the way danger pay was administered and processed in Umoja. DM stated that the danger pay solution was currently under review/redesign and will align the danger pay entitlement with the processing of other entitlements.

14. The Danger Pay solution is under development. Testing is planned for November/December 2018 and implementation is scheduled for the second quarter of 2019.

E. User authorization, access management and system security parameters require strengthening

Paragraph 22 (vi)

There were inadequate operational procedures and timelines to remove access of retired or separated staff in Umoja. OIOS noted instances where separated staff still retained access to critical information and functions in Umoja (such as HR). This was because users were granted access to Umoja through the Unite identity solution, which also provided access to various other ICT applications of the United Nations. OIOS was informed that immediate removal of access to Unite identity was not desirable as retired/separated staff might still need access to ICT applications other than Umoja. DM stated that automated revocation of access poses business risks due to the pervasive nature of transactions covered in Umoja and privileges managed through the Unite identity solution. DM further stated that OICT was leading a working group to propose a set of parameters that could be promulgated into an initial policy for the revocation of access to the retired/separated staff.

15. Umoja and all Process Owners are preparing criteria for bulk deprovisioning of Umoja users who are not active staff members.

F. Human resources

Paragraph 24 (i)

The new maternity leave policy allowed maternity leave to be combined with other types of leave, but this policy has yet to be implemented in the Umoja system. DM stated that this is a new policy and DM is currently reviewing its impact on system design and requirements.

16. This is currently under review.

Recommendation 2

DM should implement control enhancements: (i) over high-risk processes by factoring them into the continuous improvements change control process programme; and (ii) for the specific gaps identified in the present audit.

17. DM requests that the text of recommendation 2 to be amended as shown above in order to avoid any confusion with the Continuous Improvements Monitoring Programme as described in paragraphs 134-138 of the ninth progress report on Umoja (A/72/397).

Recommendation 5

DM should review and prioritize the implementation of ~~the~~ continuous improvements functionality programme for Umoja that includes: (i) the outstanding functionalities; (ii) resolution of the issue concerning the automated investment portfolio reconciliation process; and (iii) functionality to support the new maternity leave policy.

18. DM requests that the text of recommendation 5 to be amended as shown above in order to avoid any confusion with the Continuous Improvements Monitoring Programme as described in paragraphs 134-138 of the ninth progress report on Umoja (A/72/397).

19. Thank you for giving us the opportunity to provide comments on the draft report.

Management Response

Audit of Umoja implementation by the Department of Management

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	DM should: (i) update the Umoja business design documents as part of the change control process; and (ii) document an Umoja data dictionary.	Important	(i) Yes (ii) No	Umoja Project Director	(i) 30 June 2019 (ii) Not applicable	(i) Business Design Documents (BDDs) are updated as part of the change control process. BDDs identified in the context of the audit are being updated subject to Umoja Extension 2 priorities and availability of staff. (ii) In respect of the request by OIOS to reconsider this aspect of the recommendation which DM did not previously accept, a data dictionary is appropriately developed after the rollout of full functionality. DM therefore does not accept this part of the recommendation as it is subject to the long-term nature of the rollout of the Umoja solution and there are many dependencies. OIOS may wish to consider this matter in its future audits of Umoja.
2	DM should implement control enhancements: (i) over high-risk processes by factoring them into the continuous improvements change control process programme; and (ii) for the specific gaps identified in the present audit.	Important	Yes	Process Owners and Umoja Project Director	(i) Implemented (ii) 31 December 2020	(i) Based on experience of the system control enhancements over high-risk processes, they are considered and factored into the continuous improvements' formal change control process, subject to business priorities and the General Assembly's guiding principle on customization. (ii) DM has provided comments in the body of the memorandum above regarding enhancements

¹ Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

² Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Management Response

Audit of Umoja implementation by the Department of Management

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						for the specific gaps that were identified by OIOS.
3	DM should: (i) require the Umoja process owners to embed a review into the change control process so that an internal monitoring mechanism is factored into every change / improvement when it is considered and implemented; (ii) implement the enhancement to display access to Supplier Relationship Management to non-transactional users; and (iii) fix and post the 13 payroll records outstanding from 2017.	Important	Yes	(i) Process Owners and Umoja Project Director (ii) Umoja Project Director (iii) Assistant Secretary-General and Controller, OPPBA	(i) Implemented (ii) 31 March 2019 (iii) 31 March 2019	i) A review by Process Owners is embedded into the change control process for every improvement/change when it is considered and implemented. ii) The enhancement is currently in Pre-Production. iii) A number of items have been fixed and posted and the remaining ones are expected to be completed by the first quarter of 2019.
4	DM should: (i) review the assignment of high-risk roles and restrict them to authorized users; (ii) review and remove conflicts in the authorizations embedded in critical enterprise roles; and (iii) establish procedures to remove access to the Umoja system for separated/retired/reassigned staff in a timely manner.	Critical	Yes	(i) Umoja Security Team Lead (ii) Umoja Project Director and Process Owners (iii) Umoja Project Director and Process Owners	(i) Implemented (ii) Implemented (iii) 31 March 2019	i) High-risk items were analyzed and corrected by the Umoja Security Team during the audit. ii) The Segregation of Duties Matrix was released in production in April 2018 and populated by the delegated Roles Owners. iii) The Umoja team and all Process Owners are preparing criteria for bulk deprovisioning of Umoja users that are not Active staff members.

Management Response

Audit of Umoja implementation by the Department of Management

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
5	DM should review and prioritize the implementation of the continuous improvements programme for Umoja that includes: (i) the outstanding functionalities; (ii) resolution of the issue concerning the automated investment portfolio reconciliation process; and (iii) functionality to support the new maternity leave policy.	Important	Yes	(i) Process Owners and Umoja Project Director (ii) Umoja Project Director and Assistant Secretary-General and Controller, OPPBA (iii) Assistant Secretary-General, OHRM and Umoja Project Director	31 December 2020	DM will review and prioritize the implementation of continuous improvement functionality based on business priorities and the General Assembly's guiding principle on customization. (i) OHRM has reviewed Umoja pending functionalities and has established priorities. A number of functionalities such as the on-boarding form and separation process, are now out of scope given the low value added or the use of different technology. Other functionalities, such as Employee Self-Service for Education Grant and Manager Self-Service for contract extension, are still in scope, but are subject to availability of resources and priorities. (ii) An update on the automated investment portfolio reconciliation process will be provided by the end of 2018 (iii) The functionality to support the new maternity leave policy is still under review.
6	DM should: (i) define the performance benchmarks for the individual tasks (transaction codes, batches, reports, dialogs) of time-sensitive processes; and (ii) include critical processes in its periodic monitoring procedures, periodically collect performance feedback from users, and address the root causes of performance issues.	Important	No	Not applicable	Not applicable	It was DM's understanding that OIOS would enhance this recommendation with specific examples; rather than having it as a global recommendation (paragraph 21 of DM's Interoffice Memorandum to OIOS of 26 June 2018 refers).

Management Response

Audit of Umoja implementation by the Department of Management

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
7	DM should: (i) ensure the timely implementation of actions determined in the lessons learned report on the disaster recovery exercise; and (ii) conduct a review of the disaster recovery plan following the deployment of Umoja Extension II in 2019.	Important	Yes	Umoja Project Director and Assistant Secretary-General, OICT	(i) 31 March 2019 (ii) 30 June 2020	(i) Infrastructure is currently being replaced and once this is completed, the outstanding lessons learned actions will be addressed. (ii) A review will be conducted following the deployment of Umoja Extension II.