INTERNAL AUDIT DIVISION

REPORT 2016/164

Audit of Umoja change management

While some good change management procedures were in place, there were a few control weaknesses that needed to be addressed

15 December 2016
Assignment No. AT2015/519/04

Audit of Umoja change management

EXECUTIVE SUMMARY

The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over Umoja change management. The audit covered the period from November 2013 to March 2016 and included a review of governance mechanisms, monitoring procedures, change control processes, log management and access control.

The Umoja Office established some good change management procedures for managing the improvements of the Umoja system, including: (i) establishment of the change control and change advisory boards; (ii) use of a change control tracking system (Rapport); and (iii) development of change control guidelines. However, there were control weaknesses due to: (i) inadequate change management governance mechanisms; (ii) noncompliance with established access and change control procedures; (iii) lack of a systematic log management process; and (iv) undefined procedures for managing change and transport requests.

OIOS made four important recommendations. To address issues identified in this audit, the Umoja Office needed to:

- Define the criteria for determining significant and emergency change requests and ensure that these change requests are reviewed and approved by the Change Control Board and Change Advisory Board;

- Document and implement a log management policy and process, including the definition of retention requirements;

- Prevent the assignment of incompatible roles to any user in the Rapport and Umoja systems; and

- Ensure adequate tracking of change requests by defining the priority for all change requests, and configuring the Rapport application to capture all required fields defined in the change control strategy document.

The Umoja Office accepted the recommendations and initiated action to implement them.
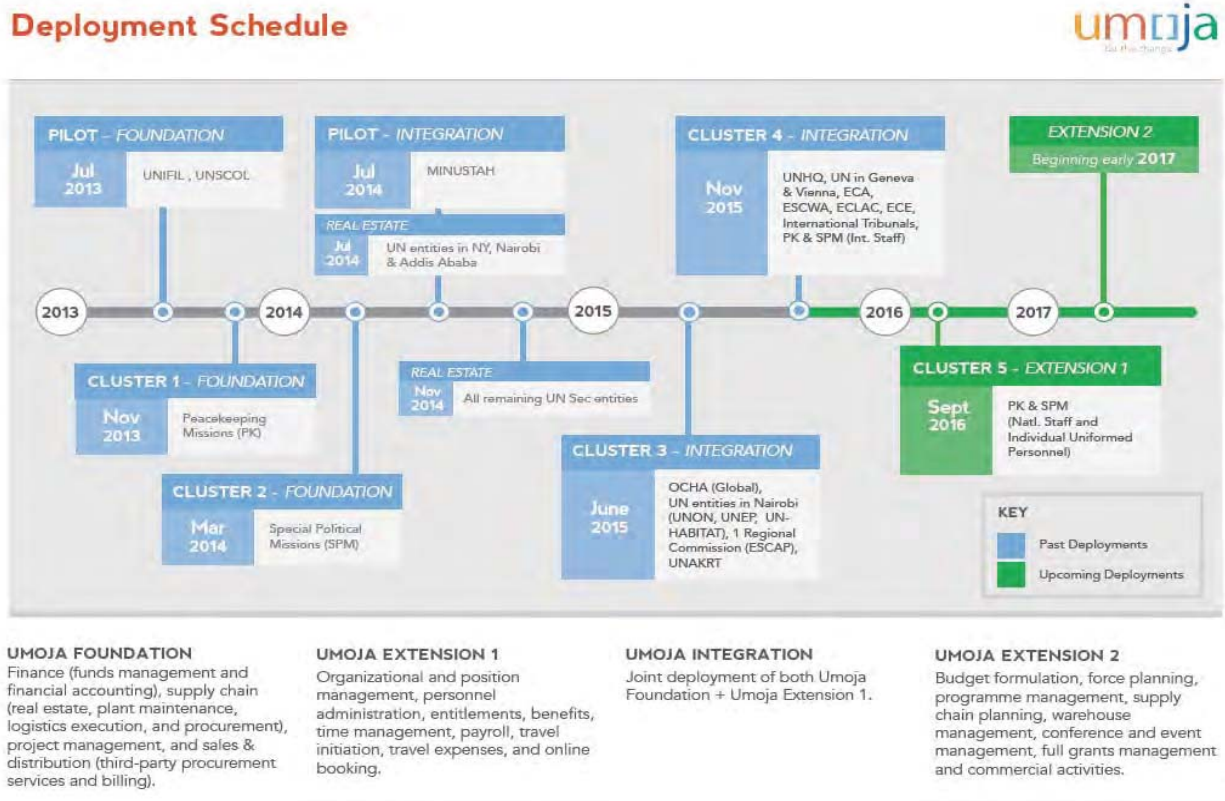
CONTENTS

Audit of Umoja change management

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of Umoja change management in the Umoja Office, Department of Management.

2. Umoja is an implementation of the SAP enterprise resource planning software, an application that supports management activities related to finance, budget, human resources, supply chain, central support services, and other core business functions. This integrated transactional system replaced numerous existing legacy information systems previously used across the Secretariat.

3. The Umoja project team is responsible for coordinating and leading the project in collaboration with the Assistant Secretaries-General responsible for the four main functional areas of human resources, finance and budget, supply chain, and central support services. A full-time project team was dedicated to the Umoja project, following the adoption of resolution 63/262 by the General Assembly in March 2009.

4. The two governing bodies that oversaw the Umoja change control process were the Change Control Board (CCB) and the Change Advisory Board (CAB). The CCB met frequently to address and mitigate risks. Change requests with significant impact on scope, schedule, budget, and deliverables of Umoja were escalated to the CAB for review, and to the Umoja Steering Committee for approval.

5. The deployment schedule of Umoja is shown in Figure 1 below.

Figure 1: Umoja deployment schedule

1

6. The Secretary-General's sixth progress report (A/69/385) on the Umoja project identified key achievements, including the design, build and test of high-priority change requests resulting from lessons learned during the Umoja Integration pilot in the United Nations Stabilization Mission in Haiti (MINUSTAH), and the strengthening of the enterprise support model implemented throughout the Organization.

7. Projected direct resource requirements for the Umoja project until 31 December 2015 remained unchanged at $385 million. The resource requirements for the biennium 2016-2017 were $54.2 million.

8. Comments provided by the Umoja Office are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

9. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over Umoja change management.

10. This audit was included in the 2015 risk-based work plan of OIOS due to the risks associated with change control in implementing the Umoja project and its impact on the deployment schedule and available resources.

11. OIOS conducted this audit from August 2015 to March 2016. The audit covered the period from November 2013 to March 2016 and included a review of governance mechanisms, monitoring procedures, change control processes, log management and access control. Based on an activity-level risk assessment, the audit covered higher and medium risks in the Umoja Office in the areas of project management and information and communications technology (ICT) support system.

12. The audit methodology included: (i) interviews of key personnel; (ii) review of relevant documentation; (iii) analytical reviews of data; and (iv) walkthroughs of processes and procedures.

III. OVERALL CONCLUSION

13. The Umoja Office had established some good practices for managing change controls and improvements of the Umoja system, including: (i) establishment of the change control and change advisory boards; (ii) use of a change control tracking system (Rapport); and (iii) development of change control guidelines. However, there were control weaknesses due to: (i) inadequate change management governance mechanisms; (ii) noncompliance with established access and change control procedures; (iii) lack of a systematic log management process; and (iv) undefined procedures for managing change and transport requests.

IV. AUDIT RESULTS

A. Project management

Need to define significant and emergency change requests and ensure their approval

14. The Umoja change control strategy defined: (i) governance mechanisms; (ii) roles and responsibilities; and (iii) standard operating procedures for managing changes relating to the system. In particular, the strategy defined the criteria for requesting, evaluating, deciding and tracking changes to the

project scope and related activities and deliverables, requiring that all change requests with a significant impact on scope, schedule, budget, and deliverables that were not resolved by the CCB should be escalated to the CAB for approval.

15.   The following control weaknesses were noted in this area:

(i)   The criteria for determining the "significant impact" of a change were not defined.

(ii)   The Umoja SAP production support approach procedures provided some guidance on emergency changes. However, the document did not adequately define what constituted an emergency change, nor the corresponding procedures to record (in the change request tracking system Rapport) the actions taken by the Umoja Office to address them.

(iii)   Whereas change requests with a significant impact on scope, schedule, budget and deliverables required a review by the CAB and approval by the Umoja Steering Committee, and any change requests that could not be resolved by the CCB required escalation to the CAB, there was no evidence that the CAB had met to review and approve change requests with a significant impact on the project. These included:

(a)   Additions to scope which entailed significant effort in design, build and test, estimated in the amount of $16.1 million, as described in the Secretary-General's sixth progress report;

(b)   Enhancements and modifications to meet the requirements of field operations, identified during pilot implementation of Umoja in MINUSTAH, as described in the seventh progress report of the Secretary-General;

(c)   A change that pertained to installation of a link to an external third party tool which should have been implemented in Umoja only after obtaining CCB approval; and

(d)   A change request for the Onapsis tool, which required submission to the CCB for review, was not submitted. In addition, the SAP change and transport strategy document stated that the release of a transport should be restricted to the Solutions Architect Team, and that before releasing transports, the reviewer should ensure that they were all reviewed and released. These criteria were not met with the release of Onapsis into the Umoja environment.

16.   This condition was due to the lack of criteria to define significant and emergency change requests for approval by the established governing boards, which may result in additional costs, system failures, and unauthorized changes.

(1) The Umoja Office should: (i) define the criteria for determining significant and emergency change requests; and (ii) ensure that such change requests are reviewed and approved by the Change Control Board and the Change Advisory Board in accordance with the terms established in the change control strategy.

The Umoja Office accepted recommendation 1 and stated that it will update the "Production Break/Fix: Logging Service Requests in INTTRK" guidelines to reflect the criteria for emergency change requests. In consultation with the process owners and the project owner, it will include clear tolerance limits to define the boundaries of the CCB and guide escalation to the CAB. Recommendation 1 remains open pending receipt of evidence demonstrating the: (i) update and

> definition of criteria for emergency change requests; and (ii) update of the procedure for review and approval of all change requests by the CCB and CAB in accordance with their established terms of reference.

B.   ICT support system

<u>Action was taken to strengthen compliance with production change control processes</u>

17.   The Umoja Office documented two change management procedures (Umoja production change control procedure and Umoja SAP change and transport strategy) to manage the various systems used for processing SAP transport requests.[1] Furthermore SAP best practices suggest moving transport requests in a timely manner between the various computing environments (i.e., development, quality assurance, pre-production, and production).

18.   The following control weaknesses were noted in this area:

(a) The Umoja production change control and transport strategy document defined a naming convention for describing change requests and ensuring consistency and ownership of the issues. Also, the document stated that transports should not be approved if they did not conform to the defined convention. OIOS review of the change requests released into the Umoja production environment showed inconsistencies in their naming; and

(b)   The Umoja Office did not define a frequency for applying updates to the SAP software.

19.   This condition was due to non-compliance with change control procedures, which may lead to errors, unauthorized changes, and security breaches.

20.   The Umoja Office took additional actions and provided evidence showing that SAP does not allow the implementation of automated validations controls of naming conventions. The exceptions identified were caused by staff who had disregarded the standard. The supervisor of the concerned staff member had taken follow-up measures and issued written reminders on the need to abide by the naming convention standard. With regard to the frequency of updates of the SAP software, the Umoja Office provided copy of the Umoja eighth progress report (A/71/390), which explained the detailed approach for the upgrade. OIOS therefore concluded that appropriate action had been taken to strengthen compliance with production change control processes.

<u>Need to design and implement a log management policy and process</u>

21.   A production client is a self-contained environment in the SAP system with its own set of master data and database tables. SAP best practices require that the security settings of a production client should prevent any direct changes and updates to them. Best practices also require that any change made in the security settings should be systematically logged.

22.   The Umoja Office configured the security settings of the production client in line with the SAP best practices, preventing any direct changes and updates to it. However, the security settings of the Umoja production client were amended in November 2015 to facilitate the processing of some activities

---

[1] Change requests were implemented in the Umoja production system using "transport requests".

related to Umoja Cluster 4 deployments. As a result, changes made in the security settings prior to 1 December 2015 could no longer be verified.

23.   This condition was due to the absence of a log management policy and process, which may prevent the identification and potential investigation of any unauthorized changes and updates to the Umoja system.

> **(2) The Umoja Office should document and implement a log management policy and process, including the definition of retention requirements.**
>
> *The Umoja Office accepted recommendation 2 and stated that the log retention policy will be reviewed and documented in consultation with OICT.* Recommendation 2 remains open pending receipt of evidence of the implementation of a log management policy and process, including the definition of retention requirements.

Need to comply with the access control procedure

24.   The ICT technical procedure of the Secretariat on access control defined rules for user account management (such as expiration of user accounts and removal of access rights). Therefore, the same rules should govern the expiration of user accounts and removal of access rights in Umoja.

25.   OIOS reviewed critical user authorizations in Umoja and identified several control weaknesses, which were referred to the Umoja Office for resolution. These included:

(i) The Umoja Office did not conduct periodic monitoring of user access in accordance with the ICT technical procedure. Issues were found with the integrity of user access controls, including users who had left the Organization but retained a valid access in Umoja, and instances of "Super-User" accounts (i.e., HCL_DASHBY; and HCL_AHLAWAT) with indefinite expiration dates in Umoja. Given that the Umoja Office has taken action on this condition, no additional recommendation has been issued in this area; and

(ii) Unsegregated roles: The production change control procedure developed by the Umoja Office defined various roles and responsibilities for performing various steps in the change control management process. The procedure also identified some incompatible roles (i.e., "Assignee" and "Tester"; "Tester" and "Reporter") that should not have been assigned to the same user. However, there were several instances where incompatible roles had been assigned to the same user (i.e., "Assignee" same as "Tester"; "Tester" same as "Reporter"). Also, some users had incompatible roles in Umoja (i.e., "Release Transport Request" and "Import Transport Request").

26.   This condition was due to non-compliance with the established access control procedure, which may result in unauthorized access to the Umoja system and may compromise its integrity and availability.

> **(3) The Umoja Office should prevent the assignment of incompatible roles to any user in Rapport and Umoja.**
>
> *The Umoja Office partially accepted recommendation 3 and stated that it does not accept the statement "all users" as control of end user access is the responsibility of the process owners, following established procedures in the Umoja user role guides and that this part of the recommendation should not be addressed to Umoja Office but rather to each process owner. Umoja will implement regular monitoring mechanisms for SAP Basis access. The Umoja Office accepted the part of the recommendation related to "Rapport" and the guidelines will be updated*

accordingly. OIOS clarifies that the reference to the assignment of incompatible user roles in Umoja pertained to unsegregated roles and non-compliance with the Umoja production change control procedures and user roles defined in Umoja. Recommendation 3 remains open pending receipt of evidence of the actions taken to prevent the assignment of incompatible roles in "Rapport" and Umoja.

Need to strengthen the tracking of change requests data

27. The Umoja change control strategy document defined the mechanisms for tracking changes, including their costs, priority status, deferred dates, review dates, CCB decisions, and identification numbers.

28. The Umoja Office used the change control tracking system called Rapport to record the data associated with change requests that have been processed. The following control weaknesses were noted:

(i) Undefined priority of change requests: 3,444 of a total 4,152 change requests did not have assigned priority; and

(ii) Inadequate configuration of the change tracking system: Rapport was not configured to capture all required fields related to the details of change requests (i.e., "CCB Tab" fields).

29. This weakness was due to the inadequate tracking of change request data, which may prevent the CCB from making correct decisions about changes.

(4) The Umoja Office should ensure adequate tracking of change requests by: (i) defining the priority for all change requests; and (ii) configuring the Rapport application to capture all required fields defined in the change control strategy document.

The Umoja Office accepted recommendation 4 and stated that it will review the change control strategy document and align Rapport and the document. Recommendation 4 remains open pending receipt of evidence that the Umoja Office has: (i) defined the priority for all change requests; and (ii) configured the application "Rapport" to capture all required fields defined in the change control strategy document.

IV.   ACKNOWLEDGEMENT

30. OIOS wishes to express its appreciation to the management and staff of the Department of Management and the Umoja Office 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

Audit of Umoja change management

Rec. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	The Umoja Office should: (i) define the criteria for determining significant and emergency change requests; and (ii) ensure that such change requests are reviewed and approved by the Change Control Board and the Change Advisory Board in accordance with the terms established in the change control strategy.	Important	O	Evidence demonstrating the (i) update and define criteria for emergency change requests; and (ii) update of the procedure for the review and approval of all change requests by the CCB and CAB in accordance with their established terms of reference.	31 March 2017
2	The Umoja Office should document and implement a log management policy and process, including the definition of retention requirements.	Important	O	Evidence of implementation of a log management policy and process, including the definition of retention requirements.	31 March 2017
3	The Umoja Office should prevent the assignment of incompatible roles to any user in Rapport and Umoja.	Important	O	Evidence of the actions taken to prevent the assignment of incompatible roles in Rapport and Umoja.	31 March 2017
4	The Umoja Office should ensure adequate tracking of change requests by: (i) defining the priority for all change requests; and (ii) configuring the Rapport application to capture all required fields defined in the change control strategy document.	Important	O	Evidence that the Umoja Office has (i) defined the priority for all change requests; and (ii) configured the application "Rapport" to capture all required fields defined in the change control strategy document.	31 March 2017

---

[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 the Umoja Office in response to recommendations.

APPENDIX I

Management Response

Management Response

AUDIT OF UMOJA CHANGE MANAGEMENT

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	The Umoja Office should: (i) define the criteria for determining significant and emergency change requests; and (ii) ensure that such change requests are reviewed and approved by the Change Control Board and the Change Advisory Board in accordance with the terms established in the change control strategy.	Important	Yes	Deputy Director, Umoja	31 March 2017	1) Umoja will update the "Prod Break/Fix: Logging Service Requests in INTTRK" guidelines to reflect the criteria for Emergency Change Requests. Please note that emergency change requests are only used in exceptionally critical cases where there is an operational time-based criticality. Emergency change requests are documented in the transition summary in an INTTRK record, through the workflow details. 2) In consultation with the Process Owners and the Project Owner, Umoja will include clear tolerance limits that will define the boundaries of the Umoja Change Control Board (CCB) and will guide escalation to the Umoja Change Advisory Board (CAB). The guideline document will be updated accordingly. The following tolerance areas and thresholds will be proposed: a. Scope - "any change in the scope of functionality which impacts the timeline for a Steering Committee or General Assembly endorsed milestone related to the deployment of an Umoja solution release".

[1] "Critical" denotes a recommendation which, if not implemented, would most likely lead to the occurrence or recurrence of an identified high risk event with a serious impact on the Organization's mandate, operations or reputation.
[2] "Important" denotes a recommendation which, if not implemented, may lead to the occurrence or recurrence of an identified risk event with an unfavorable or adverse impact on the Organization's mandate, operations or reputation.

Management Response

AUDIT OF UMOJA CHANGE MANAGEMENT

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						b. Schedule - "any change in the timeline which impacts a Steering Committee or General Assembly endorsed milestone related to the deployment of an Umoja solution release". c. Budget - "any change which has a potential impact on the planned costs for the period, which are based on the GA approved appropriation for the period". d. Deliverables - "any change in a single deliverable or a set of deliverables which impacts the timeline for a Steering Committee or General Assembly endorsed milestone related to the deployment of an Umoja solution release".
2	The Umoja Office should document and implement a log management policy and process, including the definition of retention requirements.	Important	Yes	Deputy Director, Umoja	31 March 2017	The log retention policy will be reviewed and documented in consultation with OICT. The Umoja Office configured the security settings of the production client in line with the SAP best practices, preventing any direct changes and updates to it. However, the security settings of the Umoja production client were amended in November 2015 to facilitate the processing of some activities related to Umoja Cluster 4 deployments. As a result, changes made in the security settings prior to 1 December 2015 could no longer be verified.

Management Response

AUDIT OF UMOJA CHANGE MANAGEMENT

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						Changes and warnings/errors in any SAP solution are logged and recorded in a number of ways. Supplementary information was provided to OIOS.
3	The Umoja Office should prevent the assignment of incompatible roles to any user in Rapport and Umoja.	Important	Partially	Deputy Director, Umoja	31 March 2017	Umoja does not accept the statement "all users" as control of end user access is the responsibility of the Process Owners, following established procedures in the Umoja User Role Guides. This part of the recommendation should not be addressed to Umoja but rather to each Process Owner.

With regards to SAP Basis (system administration) access, Umoja will implement regular monitoring mechanisms for SAP Basis access.

The SAP Basis Administration team needs to the ability to create transport requests and to apply Basis-related OSS notes, as well as the ability to release and import transports to other systems in Umoja landscape. The latter is a service which is provided by Basis resources for SAP implementations. The client settings are enabled to only allow transport creation in client 100 of the D (development) systems only.

Transport management is handled through the Umoja Change Management tool (the INTTRK process) for transports created by all Umoja resources, including those created by Basis team members for application of Basis- |

Management Response

AUDIT OF UMOJA CHANGE MANAGEMENT

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						related OSS notes. Umoja accepts the part of the recommendation related to Rapport. The guidelines will be updated accordingly. Specifically, Umoja will update the "Prod Break/Fix: Logging Service Requests in INTTRK" guidelines to reflect that two roles in an INTTRK can potentially be exercised by the same individual. This is particularly necessary in areas where there is only limited expertise available in the Secretariat. Oversight is provided by issue managers and approvers which mitigates any related risk.
4	The Umoja Office should ensure adequate tracking of change requests by: (i) defining the priority for all change requests; and (ii) configuring the Rapport application to capture all required fields defined in the change control strategy document.	Important	Yes	Deputy Director, Umoja	31 March 2017	Umoja will review the change control strategy document and align Rapport and the document.