



INTERNAL AUDIT DIVISION

AUDIT REPORT

Audit of the talent management system (Inspira) at the United Nations Secretariat

Overall results relating to the effective implementation of Inspira, including system security, were initially assessed as partially satisfactory. Implementation of three important recommendations remains in progress

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

**27 November 2012
Assignment No. AT2012/512/1**

CONTENTS

	<i>Page</i>
I. BACKGROUND	1
II. OBJECTIVE AND SCOPE	1 - 2
III. AUDIT RESULTS	2 - 6
A. Information technology support system	3 - 6
C. Change management	5 - 6
IV. ACKNOWLEDGEMENT	6
ANNEX I Status of audit recommendations	
APPENDIX 1 Management response	

AUDIT REPORT

Audit of the talent management system (Inspira) at the United Nations Secretariat

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the talent management system (Inspira) at the United Nations Secretariat (the Secretariat).
2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations and rules.
3. With the implementation of Inspira, the Organization aims to integrate processes that in the past had been supported by different systems (i.e., Galaxy, Nucleus and the electronic performance appraisal system ePAS) into one platform. Inspira will be integrated with the enterprise resource planning system (Umoja). The following functionalities of Inspira have been deployed: (a) staffing at the United Nations Headquarters and Offices away from Headquarters; (b) ePerformance (Secretariat-wide); (c) enterprise Learning Management (ELM) as a pilot project at UNHQ; and (d) careers portal and business intelligence analytics. Inspira will also provide onboarding, consultant recruitment and position management capability.
4. Inspira is supported by the PeopleSoft software system, acquired by the Secretariat from the company Oracle through a service delivery model (Oracle on-demand). Through this service model, the software is physically hosted by the vendor (Oracle) and managed/supported on the basis of a tiered approach by the United Nations Inspira Team (Inspira Team) and Oracle staff. Oracle provides all infrastructure support related to servers and database, including critical and emergency issues.
5. Comments provided by OHRM are incorporated in *italics*.

II. OBJECTIVE AND SCOPE

6. The audit was conducted to assess the adequacy and effectiveness of the OHRM governance, risk management and control processes established to provide reasonable assurance regarding **the effective implementation of Inspira, including system security, in the United Nations Secretariat**.
7. The audit was conducted because the risk assessment performed by OIOS identified a number of risks with regard to the development of Inspira, including those pertaining to governance and change management.
8. The key controls tested for the audit were: (a) information technology (IT) support system; and (b) change management. For the purpose of this audit, OIOS defined these key controls as follows:
 - a. **Information technology support system** - controls that provide reasonable assurance that the system implemented is adequately supporting the talent management function and delivering the intended benefits to the Organization.

- b. **Change management** - controls that provide reasonable assurance that there is a systematic approach to dealing with this reform initiative from the conceptual stage until after the first few years of implementation.
9. The key controls were assessed for the control objectives shown in Table 1.
10. OIOS conducted the audit from March to July 2012. The audit covered the period from January 2011 to December 2011.
11. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to determine their effectiveness.
12. OIOS remotely conducted a series of technical tests to assess the operational effectiveness of Inspira configuration using standard best practices for auditing the reliability of the PeopleSoft controls. The audit scope included a review of the coordination between the Inspira and Umoja teams as well as with the Office of Information and Communications Technology (OICT), and training initiatives. This audit was carried out in New York and included a site visit to the Oracle data centre in Texas, USA.

III. AUDIT RESULTS

13. The OHRM governance, risk management and control processes examined were **partially satisfactory** in providing reasonable assurance regarding **the effective implementation of Inspira, including system security, in the United Nations Secretariat**. OIOS made seven recommendations to address the issues identified in the audit. OHRM accepted the recommendations and took adequate actions for closing four of the seven recommendations. Controls were in place for establishing, confirming, approving and monitoring project tasks and for granting user permissions to make changes to schedule and batch jobs. However, there were control weaknesses relating to access control, segregation of duties, system configuration and security, change management and system support. OHRM started addressing the control weaknesses pertaining to the use of generic accounts and the untraceable access of Oracle staff to the system.
14. The initial overall rating was based on the assessment of key controls presented in Table 1. The final overall rating is **partially satisfactory** as implementation of three important recommendations remains in progress.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	Accurate financial and operational reporting	Safeguarding of assets	Compliance with mandates, rules and regulations
Effective implementation of Inspira, including system security	(a) IT support system	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(b) Change management	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Information technology support system

System configuration and security

15. OIOS performed a series of technical tests to assess whether the authority to schedule and release jobs in the system and modify and delete data was adequately segregated and assigned. The results of these tests showed three main categories of control weaknesses in the configuration of Inspira, as explained in the ensuing paragraphs.

(a) Use of generic accounts

16. Oracle staff used generic accounts to perform actions in Inspira. Hence, it was not possible to establish individual accountability and responsibility for the changes made to the data.

17. In addition, multiple generic accounts were active in the Inspira system with different levels of powerful permissions with the ability to modify data (i.e., ability to administer security, correction of access), to alter application data and configurations, etc. There were no mechanisms for determining to whom these accounts had been assigned. These generic accounts were not limited to the Oracle accounts, but also to accounts to which the Inspira support team had access. Where generic accounts are not limited, if not removed altogether, compensating controls are needed, whereby it is known “who” is using each account and “for what purpose”.

- (1) OHRM should disable all generic accounts, specifically removing the generic accounts assigned to Oracle staff, and should perform an end-user rationalization initiative for specifying the Oracle users that require access to PeopleSoft for support purposes.**
- (2) OHRM should establish detective controls whereby: (a) the Inspira Support Manager reviews periodically (at least quarterly) the activity of users, documents and signs off on the logs; and (b) similar reviews are conducted by Oracle at a minimum quarterly, documented, formally signed off and shared with the Inspira support team.**
- (3) OHRM should remove the access of the system development staff and Oracle staff to powerful account permissions (i.e., security, correction, mass change and workflow administrator).**

OHRM accepted recommendation 1 and stated that this recommendation had been implemented and that the generic PeopleSoft application accounts had been deleted. OHRM had changed its model so that the accounts that were previously maintained by Oracle would now be maintained by the Inspira database administrator, resolving the issue of the generic accounts. When needed, the account login credentials should be shared on an on-call basis and the passwords would be reset after the activity is over. OHRM has locked out all other generic accounts identified earlier. OIOS retested the system and confirmed the implementation of these changes. Based on the action taken by OHRM, recommendation 1 has been closed.

OHRM accepted recommendation 2 and stated that actions had been taken in line with the recommendation and a formal review process had been established. Recommendation 2 remains open pending receipt of documentation of the review process showing that the reviews are being conducted periodically.

OHRM accepted recommendation 3 and stated that this recommendation had been implemented and

that access rights were removed as recommended. Based on the action taken by OHRM and a satisfactory review by OIOS of the new test results, recommendation 3 has been closed.

(b) Segregation of duties

18. Inadequate segregation of duties existed among the staff members of the Inspira Support Centre (Human Resources Information Systems Section) in Bangkok. Staff assigned to the development function had access to powerful tools within the production environment through the App Designer and Data Mover tools using generic accounts. This access allowed the migration of changes to the production environment, including adding, updating and/or deleting user accounts as well as changing permissions and control settings within the PeopleSoft system. As stated in Secretary-General's report A/66/721 (29 February 2012), the Human Resources Information Systems Section is also providing Inspira application development, maintenance, production and user support through the Inspira Support Centre. In the opinion of OIOS, these responsibilities were not adequately segregated.

19. OHRM did not have in place a detective control, whereby the Inspira Team monitors, by way of logging reports, the changes into the production environment on a regular basis (e.g., weekly). OIOS could not determine who had used the Data Mover tool in Inspira, primarily due to the absence of adequate controls over the use of generic accounts. Notwithstanding that the PeopleSoft system allows for the tracking of changes to certain data and that Oracle has logging and review functions as part of its service, there was no evidence that these functionalities were being used by the Inspira Team for logging, monitoring and reviewing changes to data.

(4) OHRM should ensure that access to the App Designer tool is: (a) limited to the Management of the Inspira Team in Bangkok; and (b) enabled for Oracle support staff only when required for performing changes in PeopleSoft.

(5) OHRM should control the use of the Data Mover tool of PeopleSoft by: (a) revoking the access of all system development staff to the Data Mover tool in the production environment; and by (b) allowing updates to the production data to no more than two users with the implementation of corresponding firewall control rules.

OHRM accepted recommendations 4 and 5, and stated that these recommendations had been implemented. Based on actions taken by OHRM and a satisfactory review by OIOS of the new test results, recommendations 4 and 5 have been closed.

Physical inspection of the Oracle data centre

20. OIOS inspected the Oracle data centre in Austin, Texas, where Inspira is hosted. For the security of this site, Oracle referenced the security industry standard (i.e., Uptime Institute). The inspection of the data centre covered physical and technical security. The facility is fully redundant, with disaster recovery services provided by an external third party service provider (Iron Mountain).

21. Oracle had put in place the following control mechanisms:

- a. Security at the data centre was governed by database requirements of the Federal Aviation Administration regulations, the national aviation authority of the United States of America. Access to the building and computer rooms was controlled with metal detectors, single entry/exit points, double man-trapped doors, 24/7 armed guard security watch, perimeter fencing, vehicle pop-up barriers and biometrics (eyes, hand and body

weight). Oracle claimed to be a Tier IV embassy-level security facility, though it had not fully met the requirements relating to dual power input and number of engine-generators;

- b. Processes and procedures were in place to govern the data centre and provide training on-the-job; and
- c. Proper ventilation and continuous cooling/chilling system was in place. The data centre floor was raised and water was used as the preferred fire prevention system.

22. In OIOS' opinion, the controls implemented at the Oracle data centre were adequate for ensuring the physical security and maintenance of the Inspira operation.

B. Change management

Change management, testing and quality assurance

23. The sample cases reviewed by OIOS confirmed that PeopleSoft changes had gone through a formal, documented procedure for integration and user acceptance testing (UAT) with appropriate sign-off by business owners. Since January 2011, a controlled process and related procedures for testing, approving and logging was put in place for all change requests deployed to Inspira.

24. Although the Inspira team did not have documentation of peer review of PeopleSoft changes, OHRM confirmed that the development team would decide if a peer review is required based on the effort estimated for the change request.

Coordination with OICT

25. While a programme charter had been established, there was no formal arrangement or service level agreement between the Inspira Team and OICT and no dedicated OICT staff representation on the Inspira project management team. Additionally, OICT had not assessed the security arrangements of the Oracle system in accordance with its Application Security Framework and Information Security Advisory Services role to ensure compliance with OICT standards.

(6) OHRM should formalize the role of the Office of Information and Communications Technology (OICT) in accordance with the Organization's ICT strategy and responsibility, and request OICT to assess the security of Inspira.

OHRM accepted recommendation 6 and stated that it agreed with OICT that its role would be documented and formalized in the programme charter. The programme charter was under internal review and would be circulated for sign-off in the fourth quarter of 2012. OHRM would initiate discussions regarding a security assessment of Inspira by OICT in the fourth quarter of 2012, to be completed in the first quarter of 2013. Recommendation 6 remains open pending receipt of the revised programme charter and outcome of the security assessment of Inspira by OICT.

Hosting arrangement for business continuity and disaster recovery planning

26. Inspira is included as a critical application in the business continuity plan of OHRM, which had not yet been finalized at the time of the audit fieldwork. A review of the documentation provided showed that the Inspira disaster recovery plan included the technical process, policies and procedures related to the recovery of Inspira after a disaster to the primary infrastructure site. The Inspira team tested the

disaster recovery arrangements in late 2010 and found them to be fully operational. The team was working with OICT to move the Inspira disaster recovery over to OICT once its general hosting programme is in place. OIOS is of the view that the move of the Inspira disaster recovery over to OICT should be further considered in the context of the hosting arrangements of the application with Oracle, including an analysis of costs and the capacity of OICT.

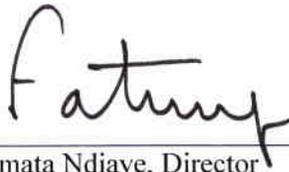
27. As the programme management delivery phase of Inspira nears its planned completion date of 2013, the role of OICT needs to be clearly documented and a service level agreement established for maintenance and support. Additionally, now that the Valencia data centre has been completed, there is a need for OHRM to reassess the requirements for hosting the Inspira application and its disaster recovery procedure. The outsourcing arrangement with Oracle for hosting the application (per the GA Resolution) was intended to be temporary and was executed through an amendment to the system integration contract, with several add-ons including disaster recovery. If the determination is made to continue to outsource the hosting of the application with Oracle, then the contractual arrangement needs to be formally subject to competitive bidding. OHRM advised that discussions with OICT are ongoing regarding the hosting of Inspira, and that OICT was not in a position to host the services for disaster recovery. Therefore, a yearly extension of the disaster recovery services with Oracle was approved until December 2012, and the Oracle contract for hosting was extended until July 2013.

(7) OHRM should, in collaboration with the Office of Information and Communications Technology, address the relocation of the hosting services for disaster recovery, including establishing timelines, support and maintenance requirements.

OHRM accepted recommendation 7 and stated that it sought the concurrence of OICT on the disaster recovery strategy, and that OICT had agreed that Oracle Corporation would continue to provide disaster recovery hosting until 2014. Recommendation 7 remains open pending receipt of documentation on the outcome of deliberations between OICT and OHRM on disaster recovery strategy for Inspira.

IV. ACKNOWLEDGEMENT

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



Ms. Fatoumata Ndiaye, Director
Internal Audit Division, OIOS

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

AT2012/512/1 – Audit of the talent management system (Inspira) at the United Nations Secretariat

Recom. no.	Recommendation	Critical/ ¹ Important ²	C/ ³ O ³	Actions needed to close recommendation	Implementation date ⁴
1.	The Office of Human Resources Management should disable all generic accounts, specifically removing the generic accounts assigned to Oracle staff, and perform an end-user rationalization initiative for specifying the Oracle users that require access to PeopleSoft for support purposes.	Important	C		9 November 2012
2.	The Office of Human Resources Management should establish a detective control whereby: (a) the Inspira Support Manager reviews periodically (at least quarterly), the activity of users, documents and signs off on the logs; and (b) similar reviews are conducted by Oracle conducted at a minimum quarterly, documented, formally signed-off and shared with the Inspira support team.	Important	O	Receipt of documentation on the review process, and showing that the reviews are being conducted periodically and are effective.	
3.	The Office of Human Resources Management should remove the access of the system development staff and Oracle staff to powerful account permissions (i.e. security, correction, mass change and workflow administrator).	Important	C		9 November 2012
4.	The Office of Human Resources Management should ensure that access to the App Designer tool is: (a)	Important	C		9 November 2012

¹ Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.

² Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

³ C = closed, O = open

⁴ Date provided by [client] in response to recommendations. [Insert “Implemented” where recommendation is closed; (implementation date) given by the client.]

Recom. no.	Recommendation	Critical/ ¹ / Important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
5.	<p>limited to the Management of the Inspira Team in Bangkok; and (b) enabled for Oracle support staff only when required for performing changes in PeopleSoft.</p> <p>The Office of Human Resources Management should control the use of the Data Mover tool of PeopleSoft by: (a) revoking access of all system development staff to the “Data Mover” tool in the production environment; and (b) allowing updates to the production data to no more than two users with the implementation of corresponding firewall control rules.</p>	Important	C		9 November 2012
6.	<p>The Office of Human Resources Management should formalize the role of the Office of Information and Communications Technology (OICT) in accordance with the Organization’s ICT strategy and responsibility, and request OICT to assess the security of Inspira.</p>	Important	O	Receipt of the revised Charter, and outcome of the security assessment of Inspira by OICT.	31 March 2013
7.	<p>The Office of Human Resources Management should, in collaboration with the Office of Information and Communications Technology, address the relocation of the hosting services for disaster recovery, including establishing timelines, support and maintenance requirements.</p>	Important	O	Receipt of documentation on the outcome of deliberations between OICT and OHRM on disaster recovery strategy for Inspira.	

APPENDIX I

MANAGEMENT RESPONSE

AT2012/512/1 – Audit of the talent management system (Inspira) at the United Nations Secretariat

Rec. no.	Recommendation	Critical/ ¹ /important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1.	The Office of Human Resources Management should disable all generic accounts, specifically removing the generic accounts assigned to Oracle staff, and perform an end-user rationalization initiative for specifying the Oracle users that require access to PeopleSoft for support purposes.	Important	Yes	Chief, Inspira Support Center - Bangkok	Implemented	This has been completed.
2.	The Office of Human Resources Management should establish a detective control whereby: (i) the Inspira Support Manager reviews periodically (at least quarterly), the activity of users, documents and signs-off on the logs; and (ii) similar reviews are conducted by Oracle conducted at a minimum quarterly, documented, formally signed-off and shared with the Inspira support team.	Important	Yes	Chief, Inspira Support Center - Bangkok	Implemented	Actions have been taken in line with the recommendation and a formal review process has been established.
3.	The Office of Human Resources Management should remove the access of the System Development staff and Oracle staff to powerful account permissions (i.e. security, correction, mass change, and workflow administrator).	Important	Yes	Chief, Inspira Support Center - Bangkok	Implemented	This has been completed.
4.	The Office of Human Resources Management should ensure that access to the App Designer tool is: (i) limited to the Management of the Inspira Team in Bangkok; and (ii) enabled for Oracle support staff only when required for performing changes in PeopleSoft.	Important	Yes	Chief, Inspira Support Center - Bangkok	Implemented	This has been completed.

¹ Critical recommendations address significant and/or pervasive deficiency or weakness in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.

² Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Rec. no.	Recommendation	Critical/ ¹ / important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
5.	The Office of Human Resources Management should control the use of the Data Mover tool of PeopleSoft by: (i) revoking access to the "Data Mover" tool in the production environment for all system development staff; (ii) preventing generic accounts from having permanent access to the Data Mover tool; and (iii) allowing updates to the production data to no more than two users with the implementation of corresponding firewall control rules.	Important	Yes	Chief, Inspira Support Center - Bangkok	Implemented	This has been completed.
6.	The Office of Human Resources Management should formalize the role of the Office of Information and Communications Technology (OICT) in accordance with the Organization's ICT strategy and responsibility, and request OICT to assess the security of Inspira.	Important	Yes	INSPIRA Programme Coordinator, Human Resources Information Systems Section (HRISS)	31 March 2013	OHRM met with OICT on 21 August and agreed that the role of OICT will be documented in the Programme Charter and will be formalized accordingly. The Programme Charter is under internal review and will be circulated for sign off in the fourth quarter of 2012. OHRM will initiate discussions regarding a security assessment of INSPIRA by OICT in the fourth quarter of 2012. Target will be to complete this assessment in the first quarter of 2013.
7.	The Office of Human Resources Management should, in collaboration with the Office of Information and Communications Technology, address the relocation of the hosting services for disaster recovery, including establishing timelines, support and maintenance requirements.	Important	Yes	Chief, Planning, Monitoring and Reporting Service & HRISS	Implemented	This has been completed. OICT has agreed that Oracle Corporation will continue to provide DR hosting until 2014.