



INTERNAL AUDIT DIVISION

AUDIT REPORT

PENSYS and document imaging system

Additional controls are needed to increase efficiency and security of the pension administration system

31 December 2008

Assignment No. AT2008/800/01

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES - BUREAU DES SERVICES DE CONTRÔLE INTERNE
INTERNAL AUDIT DIVISION - DIVISION DE L'AUDIT INTERNE

TO Mr. Bernard Cochemé, Chief Executive Officer
A United Nations Joint Staff Pension Fund

DATE 31 December 2008

REFERENCE IAD: 08- 02074

FROM Dagfinn Knutsen, Director
DE Internal Audit Division, OIOS



SUBJECT **Assignment No. AT2008/800/01 - Audit of PENSYS and document imaging system**
OBJET

1. I am pleased to present the report on the above-mentioned audit.
2. In order for us to close the recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
3. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 1, 2, 8, 9, 12, 13, 14, 15 and 17) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Ms. Jaana Sareva, Secretary to the UNJSPF Audit Committee
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Maria Gomez Troncoso, Officer-in-Charge, Joint Inspection Unit Secretariat
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Programme Officer, OIOS
Mr. William Petersen, New York Audit Service, OIOS

INTERNAL AUDIT DIVISION

SECRET/CONFIDENTIAL

FUNCTION

“The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization” (General Assembly Resolution 48/218 B).

CONTACT INFORMATION

DIRECTOR:

Dagfinn Knutsen, Tel: +1.212.963.5650, Fax: +1.212.963.2185,
e-mail: knutsen2@un.org

DEPUTY DIRECTOR:

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,
e-mail: ndiaye@un.org

CHIEF, NEW YORK AUDIT SERVICE:

William Petersen: Tel: +212.963.3705, Fax: +1.212.963.3388
e-mail: petersenw@un.org

EXECUTIVE SUMMARY

Audit of PENSYS and document imaging system

OIOS conducted an audit of the PENSYS system at the United Nations Joint Staff Pension Fund (UNJSPF or the Fund). The overall objective of the audit was to determine whether adequate controls are in place to ensure accuracy of the benefit calculation process, and data confidentiality and integrity in the PENSYS system. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

OIOS performed the first audit of the PENSYS system in 2004 (audit assignment AS2004/800/04). In light of the findings detailed in this audit report, OIOS reconfirms its conclusion that the functionalities of the PENSYS system could be significantly improved with the adoption of an integrated system based on an open client/server technology and web based platform. The UNJSPF has taken significant steps towards this technological direction.

A long-term strategic plan for the PENSYS system was prepared in 2005, and a study is being conducted on the best options available for replacing PENSYS with a new pension administration system. UNJSPF is aiming to have the new pension administration system operational by 2014.

The results of this audit indicated that the current status of controls in the PENSYS system, together with the manual processing of benefits, are effective to ensure adequate pension calculations. However, the PENSYS system presents control weaknesses that, if not adequately addressed, would expose UNJSPF to risks of inefficiencies and data insecurity. These control weaknesses include:

- (a) Unsegregated information technology functions;
- (b) Manual processing: The current benefit calculation process relies on several manual controls and calculations;
- (c) Undefined ownership of data and applications;
- (d) Informal change management procedures; and
- (e) Inconsistencies in logical access control.

OIOS verified and confirmed that all eight recommendations relating to the PENSYS system, as reported in the previous audit report (AS2004/800/04), have been implemented.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-5
II. AUDIT OBJECTIVES	6
III. AUDIT SCOPE AND METHODOLOGY	7-9
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Application environment	10-14
B. Processing and interfaces	15-27
C. Data and application ownership	28-35
D. Change management	36-39
E. Logical access control	40-44
F. Status of previous OIOS audit recommendations on PENSYS	45
V. ACKNOWLEDGEMENT	46
ANNEX 1 – Status of Audit Recommendations	

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of PENSYS. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The PENSYS system is a mission critical system that supports the operational processing of pensions. In the early 1990s, the first modules were developed in-house, and more functionality has been added ever since. PENSYS supports the following operational processes:

- (a) Participant processing;
- (b) Payments processing;
- (c) Benefits processing;
- (d) Payroll processing; and
- (e) Operations control.

3. OIOS performed the first audit of PENSYS in 2004 (audit assignment AS2004/800/04) and concluded that the functionalities of the PENSYS system could be significantly improved with the adoption of an integrated system based on a client/server technology and web based platform. The UNJSPF has taken significant steps towards this technological direction. A long term strategic plan for PENSYS had been prepared in 2005 and a study is being conducted on the available options for replacing PENSYS with a new pension administration system. Currently, UNJSPF is preparing a budget estimate to replace PENSYS and to have the new pension administration system operational by 2014.

4. In addition, a document imaging system (Content Manager) supports the PENSYS operational processes (workflows) and contains all supporting documentation and correspondence.

5. Comments made by UNJSPF are shown in *italics*.

II. AUDIT OBJECTIVES

6. The main objective of the audit was to determine whether adequate internal controls are in place to ensure:

- (a) Reliability of pension processing; and
- (b) Confidentiality and integrity of data stored and processed in PENSYS and Content Manager.

An additional objective of the audit was to assess the implementation of previous OIOS audit recommendations regarding the internal controls, functionality and processing of PENSYS.

III. AUDIT SCOPE AND METHODOLOGY

7. The audit was undertaken at UNJSPF Headquarters in New York. Interviews were held with key officers responsible for information technology, pension entitlements and client servicing.

The audit covered the following areas:

- (a) Application environment;
- (b) Data processing and interfaces;
- (c) Data and application ownership;
- (d) Change management;
- (e) Logical access control; and
- (f) Follow-up on the eight PENSYS audit recommendations as previously reported in the OIOS report AS2004/800/04.

8. The PENSYS application is installed on a mainframe computer hosted by the United Nations International Computing Center (UNICC) in Geneva. The general information and communication technology (ICT) controls regarding the UNICC environment will be part of a separate audit engagement. As previously indicated in the OIOS audit report on data security (AT2007/800/01), OIOS obtained from UNICC the Statement on Auditing Standard No. 70 (SAS 70 readiness and gap analysis), issued on February 2007 by the consulting firm Deloitte & Touche, attesting to the overall reliability of the UNICC control environment.

9. OIOS tested and evaluated the overall system of application controls designed and implemented for PENSYS to ensure reliable and secure pension processing. The audit did not include testing of individual beneficiary pension entitlements.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Application environment

PENSYS key ICT functions were not segregated

10. Best practice for the management of applications and systems requires a clear segregation of the main functions dealing with administration, operations, development and maintenance, and security.

11. OIOS found that following PENSYS key ICT functions were not clearly and formally segregated:

- (a) Administration;
- (b) Operations;

-
- (c) Development & maintenance; and
 - (d) Security.

12. For example, the PENSYS operations function was not segregated from the development function and PENSYS security responsibilities, such as reviewing activity logs, were not assigned.

13. While OIOS acknowledges that insufficient resources are limiting UNJSPF's ability to fully segregate the main ICT functions in PENSYS, it is important to note that the current condition increases the risk that users will be able to access data and functionality of systems that they are not authorized to access. They may deliberately or inadvertently make unauthorized changes to data and applications, impacting the integrity of the system.

Recommendations 1 and 2

The UNJSPF Information Management Systems Section should:

(1) Implement compensating controls to mitigate the risks arising from lack of segregation of duties in the key ICT functions of PENSYS. These controls should include:

(a) Logging of all critical activities performed in PENSYS: administration, operations, development & maintenance, and security;

(b) Securing and backing-up the activity log of PENSYS; and

(c) Ensuring the periodic review of the activity logs on a regular basis by an independent function, such as the ICT security officer.

(2) Ensure that the functional requirements of the new pension administration system include the segregation of roles pertaining to administration, operations, development and maintenance, and security.

14. *UNJSPF accepted recommendations 1 and 2 and stated that the UNJSPF Information Management Systems Section will develop a procedure for segregation of duties in the development and production support functions. A centralized log system will be implemented. Critical PENSYS activities will be logged, backed up daily, and reviewed by the ICT Security Officer. In addition, the UNJSPF Information Management Systems Section will work closely with Operations to ensure the functional requirements of the new Integrated Pension Administration System (IPAS) include segregation of roles. Recommendations 1 and 2 remain open pending the implementation of the centralized log system, evidence of regular review of critical PENSYS activities by the ICT Security Officer and inclusion of segregation of roles in the functional requirements of the new IPAS.*

B. Processing and interfaces

Manual processing of data collected from participating entities

15. Due to the lack of data format standards amongst the member organizations, data collection and input of data into PENSYS requires substantial manual processing. Yearly, approximately 260 Excel files and 40 text files are sent to the Fund by e-mail. Manual processing of data is inefficient, error prone, unstable and time consuming.

16. To address these issues, the Fund has launched two data collection initiatives to increase the number of automated interfaces with participating entities attempting to decrease manual data collection, and to improve timeliness, completeness and accuracy of data. These data collection initiatives are:

(a) "Member Organization Information Sharing Initiatives – Human Resources Interface". This interface will retrieve relevant staff information in order for the Fund to compute contribution amounts. The Human Resources interface is a prerequisite of the Financial interface; and

(b) "Member Organization Information Sharing Initiatives – Financial Interface". Through this interface the Fund will receive detailed monthly contribution reports via the member organizations' payroll systems to reconcile the contribution amounts.

17. The "Member Organization Information Sharing Initiatives – Financial Interface" consists of three phases:

Phase I: Establish secure link with member organizations: During this phase, the Fund will create a new website where a member organization can send or retrieve the year end financial data files.

Phase II: File layout verification: When a member organization sends a financial file to the website, the file layout verification will be performed instantaneously. In case of any format errors, the file will be returned to the organization along with an error report. When there are no errors, the data file will automatically be loaded to the Fund database without manual intervention.

Phase III: Data verification: When a member organization sends a financial file from the website, the system will instantaneously verify the data values. The system will match the key data elements such as pension number and name against PENSYS and in case of any discrepancies, the data file will be returned to the member organization along with an error report. The website will not accept the file until the member organization corrects its data values.

18. These initiatives will replace the current e-mail-based file transfer with a more secure and enhanced file transfer method. In the 2008-2009 biennium, the Human Resources interface is targeted at 75 per cent of the entire participant population, and the Financial interface is targeted at 10 per cent of the entire participant population.

Recommendations 3 and 4

The UNJSPF Information Management Systems Section should:

(3) Ensure that proper documentation is prepared, reviewed and archived for the development, testing, and acceptance of the "Member Organization Information Sharing Initiatives"; and

(4) Ensure that adequate security controls are defined, tested, and implemented in the proposed website for the transmission and retrieval of year end financial data files from UNJSPF member organizations.

19. *UNJSPF accepted recommendations 3 and 4, and stated that the UNJSPF Information Management Systems Section Project Manager will ensure that documentation relating to "Member Organization Information Sharing Initiatives" is properly signed off by the Chief of Operations. The UNJSPF Information Management Systems Section intends to request the ICC Security Officer to work with UNJSPF's Security Officer to monitor and ensure that adequate security controls exist in the proposed website for the transmission and retrieval of year end data. Recommendations 3 and 4 remain open pending documented evidence and sign-off of the "Member Organization Information Sharing Initiatives" and implementation of adequate security controls in the proposed website for the transmission and retrieval of year-end data.*

Manual entry of exchange rates

20. The process of calculating benefits in PENSYS requires a monthly and quarterly input of the United Nations exchange rates with currencies of beneficiaries' countries of residence. These exchange rates were taken from an Excel spreadsheet published monthly on the United Nations Treasury website, and manually entered into PENSYS.

21. Although controls were in place to review these manual entries for accuracy, manual entry of data is inherently inefficient and error prone. OIOS found no errors in the test sample.

Recommendation 5

(5) The UNJSPF Chief of Operations, in collaboration with the Information Management Systems Section, should develop and implement an automated interface with the United Nations Treasury exchange rate system.

22. *UNJSPF accepted recommendation 5 and stated that the UNJSPF Information Management Systems Section intends to automate the interface with the UN Treasury exchange rates upon receipt of business requirements and functional specification from the data owner. Recommendation 5 remains open pending automation of the interface with the UN Treasury exchange rates.*

Manual entry of cost of living adjustments

23. The process of calculating benefits in PENSYS requires, at least twice a year, the manual input of the consumer price indices (CPI) of beneficiaries' countries of residence. The CPIs are manually copied from the United Nations Monthly Bulletin of Statistics, to an Excel spreadsheet, which calculates the cost of living adjustments (COLA). Once calculated, the adjustments are manually entered into PENSYS. Although controls are in place to review the correctness of the Excel calculations, and the accuracy of the data entry into PENSYS, the process is inefficient and error prone.

Recommendations 6 and 7

The UNJSPF Chief of Operations, in collaboration with the Information Management Systems Section, should:

(6) Develop and implement an automated interface with the statistics system of the Department of Economic and Social Affairs to automatically upload Consumer Price Indices.

(7) Develop and implement a functionality in PENSYS to automate the calculation of cost of living adjustments.

24. *UNJSPF accepted recommendations 6 and 7 and stated that the Information Management Systems Section intends to automate the interface with the UN Statistics system to upload the CPIs and automate the cost-of-living adjustment indices upon receipt of business requirements and functional specification from the data owner. The cost and effort involved will be weighed against the fact that PENSYS will likely be replaced in the context of IPAS, in which case the recommendations will be incorporated in the scope of that project. Recommendations 6 and 7 remain open pending automation of the interface with the UN Statistics system to upload the CPIs and the automation of the cost-of-living adjustment indices.*

Lack of quality of data input from United Nations ICT systems

25. The PENSYS system is populated with participant data extracted from the human resources systems of over 70 participating UN reporting entities (United Nations Secretariat, Funds, Programmes, Peacekeeping Missions and Specialized Agencies) on a yearly basis. The data validation and error identification controls implemented by the Fund have identified a significant number (more than 10,000) of participant reconciliation exceptions in the data received from several human resources systems. Examples of these reconciliation exceptions include:

-
- (a) Differences in entitlement start dates,
 - (b) Differences in contribution amounts,
 - (c) Differences in start of service (employee contract) dates, and
 - (d) Use of old pension numbers (instead of the new retirement numbers).

26. The Fund transmits the participant reconciliation exception reports to participating organizations on a yearly basis, requesting them to resolve the identified discrepancies. Since participating organizations often do not take sufficient action, many of these exceptions remain unresolved for a number of years, thus creating delays in the calculation of benefits when staff members separate or retire from their organizations. OIOS already reported on the criticality of this finding in the audit report AS2006/800/02, on Financial Accounting and Reconciliation.

Recommendation 8:

(8) The UNJSPF Secretariat should escalate the criticality of the problems relating to unresolved errors in participant data to the highest level of management in the relevant UNJSPF member organizations.

27. *UNJSPF accepted recommendation 8 and stated that current efforts to clean data at the operational level are continuing. In light of the experience that results from those efforts, UNJSPF will be able to escalate the issue with other organizations indicating where the principal areas of concern lie. The necessary communication will be drafted after the current exercise is completed and in the wake of the year end exercise. Recommendation 8 remains open pending communication with other UN organizations indicating where the principal areas of concern lie.*

C. Data and application ownership

Unclear ownership of data and applications

28. Clear roles and responsibilities should be assigned to data and application owners to ensure the quality of data and the effectiveness of the application processing. These responsibilities usually include the definition of requirements for data classification, processing, security and retention.

29. UNJSPF has a process owner procedure, based on the General Procedure N.2001-66, dated 31 July 2001. However, there were no clear terms of reference for the ownership of PENSYS applications and the data pertaining to benefit calculations, payments, participants and contributions. Examples of data for which a owner was not identified include:

- (a) Cost of living differential (COLD) factors;
- (b) Mid-month exchange rates; and
- (c) 36-month average exchange rates.

Recommendation 9

(9) The UNJSPF Chief of Operations should define and allocate ownership of PENSYS data and application modules, and define the requirements for data classification, processing, documentation, training, security and retention.

30. *UNJSPF accepted recommendation 9 and stated that a detailed analysis of data ownership per module and application will be drawn up. Identification of data across UNJSPF's databases, and responsibilities for its ownership will be key in the implementation of an IPAS project and will be part of the pre-implementation tasks. For CPI, foreign exchange and COLD factor data the responsibilities will be delineated between Payments Unit, FSS and PECSS, and interdependencies, if any, between data sets should be explicitly addressed in reviewing the make up of the databases. In addition, IMSS will document all changes in the calculations of benefits and payments using its Change Management System and will include notifications to PECSS, Finance, and Executive Office. Recommendation 8 remains open pending the results of the analysis of data and application ownership, classification, processing, documentation, training, security, and retention.*

Need for PENSYS end-user documentation and training

31. The long-term maintenance and support of system applications is ensured by comprehensive and duly updated end-user documentation and training initiatives.

32. UNJSPF has taken significant steps to ensure an adequate level of support for the PENSYS system with the completion of the following initiatives:

- (a) PENSYS technical documentation, centrally stored in UNJSPF's Knowledge System (Quickplace Database); and
- (b) Data model and data dictionary, detailing the PENSYS database set-up.

33. However, in a number of instances, PENSYS end-user documentation and training material were not readily available and/or up-to-date. Users made and referred to personal notes for newly introduced benefits calculation rules and operating procedures. The unavailability of standard documentation in support of these calculations constitutes a major limitation that became particularly significant during the recent feasibility study of the new pension administration system. In addition, the incomplete documentation has an adverse impact upon the quality of reference material for purposes of training and operational support.

34. UNJSPF has recently developed a plan for the first half year of 2009 to document the benefit calculation models and how these models should be used during the development of the new pension administration system.

Recommendations 10 and 11

The UNJSPF Chief of Operations, in collaboration with the Information Management Systems Section, should:

(10) Ensure that PENSYS end-user documentation and training material is completed, updated and made readily available to the end-user. Documentation and reference materials should be designed for all levels of expertise, written in plain language and easily accessible.

(11) Review, update, and formally sign-off on all system documentation, including operational procedures and training material.

35. *UNJSPF accepted recommendations 10 and 11 and stated the UNJSPF Information Management Systems Section project managers will work with data owners to ensure all future new projects will be fully documented and that end-user training will be completed and readily available. Current procedural documentation will be formalized from desk manuals for inclusion in the Knowledge Management System. A training officer will be recruited. This post will be located in the Executive Office and duties will include management of the UNJSPF training programmes and the development of training materials. Together with a further post of a Learning Management System IT Engineer who will be responsible for design of a training platform, existing materials will be reviewed and where necessary improved. Training courses will be developed from the material captured or created to set up a forum where knowledge of the Fund's complex processes can be captured and shared between past, current and future staff. In addition, the COO will sign off on all system documentation on the recommendation of both the manager directly responsible for the area and the UNJSPF Information Management Systems Section staff responsible. Recommendations 10 and 11 remain open pending completion of PENSYS documentation and end-user training materials, as well as a formal procedure for the Chief of Operations to review, update, and formally sign-off on all system documentation, including operational procedures and training material.*

D. Change management

Informal change management procedures

36. The Fund recently implemented a change management system and procedure to keep track of all ICT-related changes, including modifications of the PENSYS system. Historical changes to PENSYS and user acceptance tests, however, have not been formally and systematically documented and archived. Therefore, OIOS was not able to determine whether all changes to PENSYS have been properly tested and reviewed.

37. The Fund provided the audit team with a series of e-mails as evidence of user acceptance tests conducted for 12 changes since 2000, including:

-
- (a) Calculation of the 80% minimum guarantee for two-track benefits;
 - (b) 0.5% reinstatement of initial cost of living adjustment;
 - (c) Second 0.5% reinstatement;
 - (d) Special measure for Turkey regarding the initial local currency pension; and
 - (e) Work-type 524 (E10 calculation for two track-cases).

38. Ineffective change management and incomplete testing of changes could result in unauthorized and unreliable changes, and may impact the integrity of the system. Moreover, ineffective change management impedes the requirements analysis process for the new pension administration system as undocumented requirements are difficult to reuse.

Recommendations 12 and 13

The UNJSPF Information Management Systems Section, in collaboration with the Pension Entitlement and Client Servicing Section, should:

(12) Document the specifications of all PENSYS calculations in the new change management system. This should also include updated technical and functional documentation, user acceptance test results and sign-off.

(13) Ensure that all changes pertaining to automatic calculations of benefits and payments, whether using PENSYS or the future pension administration system, are:

- (a) Adequately documented and archived; and**
- (b) Properly signed-off by the appropriate application or data owner.**

39. *UNJSPF accepted recommendations 12 and 13 and stated that documentation of the specifics of all PENSYS calculations would, depending on the specific application, involve PECSS and/or FSS (as the case may be). Calculations will be documented in a General Procedure so that all future changes will follow the same documented procedure. Documentation for the changes as from 1 January 2009 will be reflected in the new change management system; previous changes will be accumulated, filed and reflected in the change management system when time and resources permit. Other changes that were recommended by the Pension Board in 2008 will be documented if and when approved by the General Assembly. Each procedure documenting change will promulgate a requirement that such changes be tested and signed off by the appropriate officer. The UNJSPF Information Management Systems Section Change Management system (implemented in November 2008) requires that technical and functional specifications, user acceptance results and user sign-off are attached to all Requests for Change (RFC). It is the intention of the UNJSPF Information Management Systems Section that any new request for change to the automatic calculation of benefits and payments must follow the established*

System Development Methodology (SDM) strictly. Recommendations 12 and 13 remain open pending documented evidence of the specifications and changes to all automated PENSYS calculations.

E. Logical access control

Need to implement a role-based access control

40. The logical access control of the PENSYS system is based on defined profiles and user groups. However, a formal access policy for both PENSYS and Content Manager was not in place.

41. In addition, there was no procedure to ensure that user access to applications remains appropriate and in line with the current job description. Neither was there a procedure in which the Information Technology Unit is formally notified of employees separating or changing job within UNJSPF.

42. A comprehensive table of all employee roles and their corresponding access profiles in PENSYS did not exist. Such a table would assist management in monitoring user access and determining whether duties have been properly segregated.

43. The lack of the above procedures and controls increases the risk that users will be able to access data and functionality of systems that they should not have access to. This condition exposes UNJSPF to the risks of deliberate or inadvertent unauthorized changes to data. In this regard, OIOS noted the following:

- (a) Instances where access rights were still being granted to employees who left the organization (for example employees who retired);
- (b) Instances where access rights were not in line with (changes in) current employee roles and responsibilities;
- (c) User groups to which no users were assigned; and
- (d) Users with special access, not associated to a particular user group.

Recommendations 14 to 17

(14) The UNJSPF Information Management Systems Section, in collaboration with all UNJSPF Section and Unit Chiefs, should effectively implement role-based access control by drafting and implementing a formal access policy for all mission critical systems. This policy should, at a minimum, include:

- (a) A comprehensive list of all employee roles and the corresponding required access profiles for each application appropriate to their role and responsibilities;**

(b) All applications that users may access, including PENSYS, Content Manager, and the financial system (Lawson);

(c) A description of responsibilities for how to remove or update system access in case an employee leaves the organization or changes role; and

(d) Approval by the Chief Executive Officer / designated officer.

(15) The UNJSPF Information Management Systems Section, in collaboration with all UNJSPF Section Chiefs should develop and implement a procedure for the periodic review of users' access rights, to confirm their appropriateness.

(16) The UNJSPF Information Management Systems Section should develop and implement a procedure to monitor, analyze, independently review, and securely archive access logs to mission critical applications, including PENSYS.

(17) The UNJSPF Information Management Systems Section, in collaboration with all UNJSPF Section Chiefs, should develop and implement a procedure for reporting and addressing access violations to systems and applications, including PENSYS.

44. *UNJSPF accepted recommendations 14, 15, 16 and 17, and stated that the UNJSPF Information Management Systems Section intends to work with the data owners to define an access policy for PENSYS, the Lawson system and the Content Manager system. The access policy will be reviewed on a collaborative basis between the operations area and the UNJSPF Information Management Systems Section. Once the access log is implemented, it will be used as a basis for monitoring user access rights. The UNJSPF Information Management Systems Section intends to develop and implement a procedure to log, monitor, analyze and securely archive all access logs and will assign the ICT Security Officer to independently review the access logs. The UNJSPF Information Management Systems Section also intends to work with the Section Chiefs to develop and implement a procedure for addressing security violations. In addition to post facto reporting of violations, proactive and contemporaneous monitoring of system access and potential harmful intrusion will continue to be monitored within the UNJSPF Information Management Systems Section. Recommendations 14, 15, 16 and 17 remain open pending implementation of: a) role-based access control, defining an access policy for PENSYS, the Lawson system and the Content Manager system; b) a procedure for the periodic review of users' access rights; c) a procedure to log, monitor, analyze and securely archive all access logs; d) a procedure for the independent review of access logs; and e) a procedure for reporting and addressing security violations.*

F. Status of previous OIOS audit recommendations on PENSYS

45. OIOS verified and confirmed that all previous recommendations issued on the PENSYS system in audit report AS2004/800/04, have been implemented. This includes the recommendation to perform an in-depth study of PENSYS redevelopment.

V. ACKNOWLEDGEMENT

46. We wish to express our appreciation to the Management and staff of UNJSPF for the assistance and cooperation extended to the auditors during this assignment.

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
1	<p>IMSS should implement compensating controls to mitigate the risk deriving from lack of segregation of duties in the key ICT functions of PENSYS. These controls should include:</p> <ul style="list-style-type: none"> a) logging of all critical activities performed in PENSYS: administration, operations, development & maintenance, and security; b) securing and backing-up the activity log of PENSYS; and, c) ensuring the periodic review of the activity logs on a regular basis by an independent function, such as the ICT security officer. 	Operational	High	O	Implement the centralized log system, and provide evidence of the regular review of critical PENSYS activities by the ICT Security Officer.	31/12/2009
2	<p>IMSS should ensure that the functional requirements of the new pension administration system include the segregation of roles pertaining to administration, operations, development and maintenance, and security.</p>	Governance	High	O	Document the functional requirements of the new IPAS, including segregation of duties pertaining to administration, operations, development and maintenance, and security.	31/12/2009
3	<p>IMSS should ensure that proper documentation is prepared, reviewed and archived for the development, testing, and acceptance of the "Member Organization Information Sharing Initiatives".</p>	Operational	Medium	O	Provide evidence that documentation is prepared, reviewed and archived for the development, testing, and acceptance of the "Member Organization Information Sharing Initiatives", and it has been signed off by the Chief of Operations.	31/12/2009
4	<p>IMSS should ensure that adequate security controls are defined, tested, and implemented in the proposed website for the transmission and retrieval of year-end</p>	Operational	Medium	O	Implement adequate security controls in the proposed website for the transmission and retrieval of year-end data.	31/12/2009

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
5	data. The UNJSPF Chief of Operations, in collaboration with IMSS, should develop and implement an automated interface with the United Nations Treasury exchange rate system.	Operational	Medium	O	Automate the interface with the UN Treasury exchange rates.	31/12/2009
6	The Chief of Operations, in collaboration with IMSS, should develop and implement an automated interface with the statistics system of the Department of Economic and Social Affairs to automatically upload Consumer Price Indices.	Operational	Medium	O	Automate the interface with DESA systems to access CPI data.	31/12/2009
7	The Chief of Operations, in collaboration with IMSS, should develop and implement a functionality in PENSYS to automate the calculation of Cost of Living Adjustments.	Operational	Medium	O	Automate the cost-of-living adjustment indices upon receipt of business requirements and functional specification from the data owner.	31/12/2009
8	The UNJSPF Secretariat should escalate the criticality of the problem relating to unreconciled participant data to the highest level of management in the relevant UNJSPF member organizations.	Governance	High	O	Provide documented evidence of the communication issued to the UNJSPF member organization regarding unreconciled data.	31/12/2009
9	The Chief of Operations should define and allocate ownership of PENSYS data and application modules, and define the requirements for data classification, processing, documentation, training, security, and retention.	Operational	High	O	Document the results of the detailed analysis of data ownership per module and application, including the definition of the requirements for data classification, processing, documentation, training, security, and retention.	31/12/2009
10	The Chief of Operations, in collaboration with IMSS, should ensure that PENSYS end-user documentation and training material is updated, completed and readily available to the end-user. Documentation and reference materials should be designed for all levels of expertise, written in plain language and easily accessible.	Operational	Medium	O	Document the end-user training procedure.	31/12/2009

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
11	The Chief of Operations, in collaboration with IMSS, should review, update, and formally sign-off on all system documentation, including operational procedures and training material.	Operational	Medium	O	Formalize the procedure for the Chief of Operations to review, update, and formally sign-off on all system documentation, including operational procedures and training material.	31/12/2009
12	IMSS, in collaboration with PECSS, should document the specifications of all PENSYS calculations in the new change management system. This should also include updated technical and functional documentation, user acceptance test results and sign-off.	Operational	High	O	Document the specifications of all PENSYS calculations in the new change management system, including updated technical and functional documentation, user acceptance test results and sign-off.	31/12/2009
13	IMSS, in collaboration with PECSS, should ensure that all changes pertaining to automatic calculations of benefits and payments, whether using PENSYS or the future pension administration system, are: (a) adequately documented and archived; and (b) properly signed-off by the appropriate application or data owner.	Operational	High	O	Document all changes pertaining to automatic calculations of benefits and payments in the new change management system.	31/12/2009
14	IMSS, in collaboration with all UNJSPF Section and Unit Chiefs, should effectively implement role based access control by drafting and implementing a formal access policy for all mission critical systems. This policy should at least include: (a) a comprehensive list of all employee roles and the corresponding required access profiles for each application appropriate to their role and responsibilities; (b) all applications that users may access, including PENSYS, Content Manager, and the financial system (Lawson); (c) a description of responsibilities how to remove or update system access in case an	Governance	High	O	Implement role based access control and define an access policy for PENSYS, the Lawson system and the Content Manager system.	31/12/2009

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
	employee leaves the organization or changes role; and, (d) approval of the Chief Executive Officer / designated officer.					
15	IMSS, in collaboration with all UNJSPF Section Chiefs, should develop and implement a procedure for the periodic review of users' access rights, to confirm their appropriateness.	Operational	High	O	Implement a procedure for the periodic review of users' access rights.	31/12/2009
16	IMSS should develop and implement a procedure to log, monitor, analyze, independently review, and securely archive access logs to mission critical applications, including PENSYS.	Operational	Medium	O	Implement a procedure to log, monitor, analyze and securely archive all access logs. Assign the ICT Security Officer to independently review the access logs.	31/12/2009
17	IMSS, in collaboration with all the UNJSPF Section Chiefs, should develop and implement a procedure for reporting and addressing access violations to systems and applications, including PENSYS.	Operational	High	O	Implement a procedure for reporting and addressing security violations.	31/12/2009

1. C = closed, O = open

2. Date provided by UNJSPF in response to recommendations.