INTERNAL AUDIT DIVISION

AUDIT REPORT

Audit of the Galileo System at the United Nations Logistics Base in Brindisi, Italy

1 July 2008
Assignment No. AT2007/610/02

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE

TO: Ms. Susana Malcorra, Under-Secretary-General
A: Department of Field Support

DATE: 1 July 2008

REFERENCE: IAD: 08- 01464

FROM: Dagfinn Knutsen, Director
DE: Internal Audit Division, OIOS

SUBJECT: **Assignment No. AT2007/610/02 - Audit of the Galileo System at the United Nations Logistics Base**
OBJET:

1. I am pleased to present the report on the above-mentioned audit.

2. Based on your comments, we are pleased to inform you that we will close recommendations 5 and 7 in the OIOS recommendations database as indicated in Annex 1. In order for us to close the remaining 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. Your response indicated that you did not accept recommendation 2. In OIOS' opinion however, this recommendation seeks to address significant risk areas. We are therefore reiterating it and request that you reconsider your initial response based on the additional information provided in the report.

4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as critical (i.e., recommendations 2, 3, and 6) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Ms. Jane Holl Lute, Assistant Secretary-General, Department of Field Support
Mr. Rudy Sanchez, Chief, Communications and Information Technology Service
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Maria Gomez Troncoso, Officer-in-Charge, Joint Inspection Unit Secretariat
Mr. Jonathan Childerley, Chief, Oversight Support Unit, DM
Mr. Byung-Kun Min, Programme Officer, OIOS

INTERNAL AUDIT DIVISION

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, PEACEKEEPING AUDIT SERVICE:
Eleanor T. Burns, Chief: Tel: +917.367.2792, Fax: +212.963.3388,
e-mail: burnse@un.org

EXECUTIVE SUMMARY

Audit of the Galileo System at the United Nations Logistics Base

OIOS conducted an audit of The Galileo Inventory Management System at the United Nations Logistics Base (UNLB), Brindisi. The overall objective of the audit was to ensure that:

a) Access to critical programmes and data is secure and restricted to authorized personnel only;
b) The network environment is secured physically and logically;
c) Change management controls exist;
d) Data migration is appropriate, complete and accurate;
e) Procedures exist to ensure the accuracy, completeness, and timely processing of system jobs; and
f) A business impact assessment has been completed and business continuity plans developed and approved for all supported business processes.

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

OIOS found that in general, Galileo's operations were well structured and monitored, with clearly defined processes for change management, service availability, and resource capacity. Adequate controls had been implemented to ensure that data migrated from the legacy systems to Galileo was accurate.

The review of Galileo's configuration and settings, however, presented some control weaknesses, which could expose both the system and data to potential security breaches, if not addressed by management. In particular, OIOS identified that:

i) There was no dedicated resource and clearly assigned officer responsible for information and communication security at UNLB, with particular responsibility for the information security of the Galileo system;
ii) The transmission of network traffic and information was not secure;
iii) Data integrity controls were not validated;
iv) There were limited reviews and monitoring of the audit trail logs;
v) A Business Impact Assessment had not been completed;
vi) The Disaster Recovery facility was inappropriately located in the same location as the main site; and
vii) There are weak inventory reconciliation procedures in place.

To ensure that these weaknesses are addressed, UNLB/Communications and Information Technology Services (CITS) management should:

a) Allocate dedicated resources and assign clear responsibility for information and communication system security at UNLB;
b) Conduct a thorough risk assessment of the risks posed by traffic traveling 'in clear text' over the network and implement a secure standard protocol

(Hyper-text-transfer-protocol over secure socket layer, https) for communication;

c) Ensure the complete validation of all functional controls implemented in Galileo, with particular regard to data integrity checks;

d) Undertake a more frequent review of the audit trail logs;

e) Undertake and document a Business Impact Assessment for the Galileo system; and

f) Review and update the Disaster Recovery Plan with a view to relocating the 'off site' location.

TABLE OF CONTENTS

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of The Galileo Inventory Management System at the United Nations Logistics Base (UNLB), Brindisi. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The Galileo Inventory Management System is an in-house developed application. It is an automated system that manages United Nations owned equipment as part of the supply chain process within the United Nations field support operations.

3. The application is physically hosted in the UNLB data center. The support of the Galileo system is provided as a joint effort between the Department of Field Support (DFS) and United Nations International Computing Centre (UNICC), which provides central support from UNLB, and by Local Administrators at the mission sites. The statistics for the application are as follows:

- 4,488 registered active users (As of 10 October 2007)
- 4,650 documents created per day
- 24,000 major transactions per day
- 479,990 asset records with a value of $1,6 billion
- $400 million in expendables

4. The application is deployed in 15 Peacekeeping missions, 6 Special Political Missions, UNLB and UNHQ (New York).

5. Comments made by the UNLB/Communications and Information Technology Service (CITS) administration are shown in *italics*.

II. AUDIT OBJECTIVES

6. The main objectives of the audit were to determine whether:

(a) access to critical programmes and data within the information system is secure and restricted to authorized users based on appropriate identification, authentication and authorization;

(b) the network environment is secured physically and logically;

(c) controls are in place to ensure that modifications to the system environment are made using a structured policy, have appropriate authorizations, are well documented, and are tested before migration into production;

(d) controls exist to ensure that data migrated to or from other systems via interfaces are validated and retain integrity;

(e) management have implemented procedures to ensure the accuracy, completeness and timely processing of system jobs; and

(f) a business impact assessment has been completed and business continuity plans developed and approved for all supported business processes.

III. AUDIT SCOPE AND METHODOLOGY

7. Interviews were held with key officers responsible for processes and assets. Documentation was obtained and reviewed so as to ascertain the Galileo system's operating environment. Tests were performed on all key control areas to confirm the existence and effectiveness of controls, as well as to enable the identification of threats, risks and vulnerabilities.

8. The audit covered the following areas:

a) Policies & procedures;
b) Allocation of ICT related responsibilities;
c) Effectiveness of input, processing & output controls;
d) Business continuity management; and
e) Management of information security incidents and improvements.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Information security

9. UNLB/CITS issued and documented information security policies and procedures. However, OIOS found that there is no dedicated officer tasked with overseeing and managing the risks associated with the application and its security issues. In addition, there was no evidence of systematic monitoring of advisory updates pertaining to IT security threats and vulnerabilities. The potential impact of this condition is that security breaches or vulnerabilities may not be routinely investigated and remedial action promptly taken.

Recommendation 1

(1) UNLB/CITS should allocate a dedicated resource to act as a focal point for the Galileo IMS. Furthermore, the focal point should be assigned clear responsibility for the information and communication system security of Galileo IMS. In the interim, existing technical staff should be tasked with the responsibilities of checking mailing lists containing updated information regarding IT security threats and vulnerabilities.

10. *UNLB/CITS accepted recommendation 1 and stated that it has requested for the establishment of an Information Security Management position in the UNLB budget for the financial period 2008/2009. Pending the approval of this, DFS has assigned a technical support staff to monitor and act upon any known security threats, both for the ICT infrastructure and applications.* Recommendation 1 remains open pending the allocation of a dedicated resource for information security management.

B. Network security

Security of data transmission

11. Galileo is a web based application that is implemented over an insecure network protocol (hyper-text-transfer-protocol, http). Hence the confidentiality and integrity of the data transmitted over the network can be easily breached. In particular, user identification and passwords entered in by users whilst logging on to the application can easily be intercepted by any individual with moderate computer expertise and can be used to access the application without authorization. This condition exposes the application to the risk of unauthorized access and malicious attacks.

Vulnerability assessment procedures

12. Penetration testing activities are conducted at UNLB by the Network Control Center, managed by the International Computing Center. These activities, however, are not based on defined policies and systematic procedures for a proactive security programme. The absence of defined terms of reference for the systematic review of security risks could result in: a) the failure of firewall rules to reflect the Organization's security policy; b) undetected unauthorized modifications of security requirements; and c) security breaches not detected in a timely manner.

Recommendations 2 and 3

UNLB/CITS should:

(2) adopt and implement a secure standard protocol for the communication channels supporting Galileo; and

(3) develop and document policies and procedures for the conduct of regular vulnerability assessments at the UNLB site. These policies should require a consistent analysis of the results, the determination of any remedial action necessary to mitigate risks, and a follow-up report about their implementation.

13. *UNLB/CITS did not accept recommendation 2, stating that the austere locations of field missions require communication to be conducted over low-bandwidth, high latency satellite links which therefore means that the implementation of the recommendation may seriously affect performance. DFS*

stated that because Galileo is only accessible over the intranet, the user ID and password information cannot be easily intercepted. However, DFS proposes to implement a standard protocol for authentication processes.

14. OIOS acknowledges the challenges identified by UNLB/CITS in the implementation of the recommendation, and also the positive initiative to establish a secure authentication process. Nonetheless, the strategic relevance of secure and reliable communications requires that adequate safeguards be put in place. Furthermore, DFS observed that "Galileo is only accessible over the intranet". This condition does not mitigate the risks to which the information is exposed to. These risks include:

i) the vulnerability of the insecure connection. When remote users in the mission connect to Galileo, all data, including their credentials (i.e. login and password) is transmitted without protection through both the upload and download links. An "eavesdropping attack" performed in the geographical area where the download link is received, would compromise the confidentiality of all data transmitted, including the credentials of the user; and

ii) the over-reliance on the security of the internal environment. Relevant statistics in the information security domain have demonstrated that the highest percentage of security breaches occurs within the organization. Therefore, in the absence of additional mitigating controls, the fact that Galileo is accessible over the intranet constitutes an inherent risk to the security of the application and the data within. On the basis of these considerations, OIOS reiterates recommendation 2 and requests that UNLB/CITS reconsiders its initial response based on the additional information provided.

15. *UNLB/CITS accepted recommendation 3 and stated that the establishment of the Information Security Management position will allow UNLB/CITS to actively engage in a comprehensive information security management program.* Recommendation 3 remains open pending the development of policies and procedures for the conduct of regular vulnerability assessments.

C. Data integrity

Data integrity

16. Galileo contains automated procedures to check the integrity, accuracy and reliability of the input, processing, and output of data. However, OIOS noted that the automated procedures to control data integrity (i.e. data integrity checks, reliability of queries and reports, and traceability of transactions), as defined in the original functional requirements of the system, have not been validated and confirmed by the application owners. This condition exposes sensitive data to the risks of inaccuracy, incompleteness, misuse, and unauthorized access.

Audit trail

17. The Galileo system generates audit trails and logging mechanisms of database transactions. However, OIOS noted that these data and information are reviewed only once a month, and are not integrated with the change, incident, and problem management process established at UNLB/CITS. This condition exposes the Organization to the risk of errors and problems going undetected for a considerable amount of time.

Recommendations 4 and 5

UNLB/CITS should:

(4) perform a complete validation of all functional controls implemented in Galileo with particular regard to data integrity checks, to ensure the correctness of all rule-related requirements, reliability of queries and reports, and clear traceability of transactions; and

(5) develop and implement procedures for a more frequent review (i.e. on a weekly basis) of audit trails and logging information, to ensure timely review of unusual patterns and changes. These procedures should be integrated with the change, incident, and problem management process of the information technology infrastructure of UNLB.

18. *UNLB/CITS accepted recommendation 4 and stated that a validation exercise is in progress and will be completed by October 2008.* Recommendation 4 remains open pending the completion of the validation exercise and the forwarding of documentary evidence to OIOS.

19. *UNLB/CITS accepted recommendation 5 and stated that the recommendation has been implemented as of 27 February 2008.* Based on the action taken by UNLB/CITS, recommendation 5 has been closed.

D. Disaster recovery and business continuity

Business impact analysis

20. OIOS noted that a business impact assessment had not been fully completed as at the time of the audit. An assessment had only been conducted though informal meetings. Notes of the meetings have not been documented, and only a final classification of the criticality of applications was made available to OIOS. Furthermore, the criticality ranking was not supported by any defined criteria or terms of reference used to undertake the ranking analysis. The absence of a systematic business impact analysis could lead to failures in recovering critical mission applications and services in a timely manner, inability to determine alternative solutions in response to adverse events, and lack of required recovery.

Disaster recovery plan

21. A disaster recovery strategy and procedures were in place for the recovery of Galileo data in the event of a disaster. However, OIOS noted that: i) a structured business impact analysis had not been completed; and ii) the disaster recovery procedures identified as 'off site' location, for the continuation of operations in case of disaster, was the same campus hosting the application within UNLB. As a consequence of this condition, a disaster affecting the UNLB campus will also affect the 'off site' continuity location identified for the Galileo system. In this event, UNLB would not be able to ensure the continuity of operations and its support to the mission sites. In this regard, OIOS noted that two proposals are currently being reviewed for off-site locations: a) the creation of a UNLB twin site to be located in Valencia, Spain; and b) the use of UNHQ computing infrastructure in New York.

Recommendations 6 and 7

UNLB/CITS should:

(6) document a Business Impact Analysis for Galileo (as well as the other mission critical applications) in accordance with a structured approach and pre-defined methodology, such as the one documented in the guidelines issued by UNHQ Information and Technology Services Division; and

(7) relocate the 'off site' location for the continuity of operations of systems such as Galileo, to UNHQ New York, pending the review and approval of the twin-site in Valencia, Spain.

22. *UNLB/CITS accepted recommendation 6 and stated that a Business Impact Analysis for Galileo will be completed by 30 September 2008.* Recommendation 6 remains open pending the completion of the Business Impact Assessment and the forwarding of evidence to OIOS to confirm completion.

23. *UNLB/CITS accepted recommendation 7 and stated that UNHQ has been selected as the "off Site" location.* Based on the action taken by UNLB/CITS, recommendation 7 has been closed.

E. New Enterprise Resource Planning (ERP) system

24. The Secretary General has recently submitted to the General Assembly a proposal (A/62/510) for the phased implementation and deployment of the new enterprise resource planning (ERP) system. It is expected that in the near future many legacy systems, including Galileo, will be gradually replaced by the new ERP system. It is necessary to define clear responsibilities and procedures to adequately prepare for the transition into the new system and the migration of data from the enterprise-wide applications currently in use.

Recommendation 8

(8) UNLB/CITS should create a working group with the objective of defining criteria and procedures to review the data currently contained in the Galileo database, and ensure timely conduct of data validation, clean-up, and consolidation in preparation for the transition to the new ERP system.

25. *UNLB/CITS accepted recommendation 8 and stated that the implementation of a working group is subject to a final determination of the date of implementation of ERP.* Recommendation 8 remains open pending the creation of the working group.

V. ACKNOWLEDGEMENT

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

ANNEX 1

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
1	O	Allocation of a dedicated resource for information security management.	Not provided
2	O	Implementation of a secure standard protocol (i.e. https) for the communication channels supporting Galileo, and implementation of a secure standard protocol for authentication.	Not provided
3	O	Development of policies and procedures for the conduction of regular vulnerability assessments.	31 December 2008
4	O	Completion of the validation exercise for all functional controls in the Galileo system.	October 2008
5	C	Action completed.	Implemented
6	O	Completion of the Business Impact Assessment.	30 September 2008
7	C	Action completed.	Implemented
8	O	Creation of a working group with the objective of defining criteria and procedures to review the data currently contained in the Galileo database, and ensure timely conduction of data validation, clean-up, and consolidation in preparation for the transition to the new ERP system.	Not provided

1. C = closed, O = open
2. Date provided by UNLB/CITS in response to recommendations.