Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2017/058

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

The system was yet to achieve integration of end-to-end processing of activities pertaining to contingent-owned equipment

28 June 2017
Assignment No. AT2016/615/04

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

EXECUTIVE SUMMARY

The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the effective implementation of the Electronic Contingent-Owned Equipment (eCOE) system. The audit covered the period from January 2013 to March 2017 and included a review of eCOE implementation by the United Nations Mission in the Republic of South Sudan (UNMISS), the Office of Information and Communications Technology (OICT) and the Department of Field Support (DFS) in the areas of project management and the information and communications technology (ICT) support system.

UNMISS, OICT and DFS had established some good control practices for the implementation and use of the eCOE system. However, some control weaknesses were identified as summarized below. The system was yet to achieve integration of end-to-end processing of activities pertaining to COE.

OIOS made 10 recommendations to address issues identified in the audit, including the following:

DFS needed to:

- Define a project governance mechanism and clarify the source of funding for the integrated system;
- Assign responsibility for uploading the Appendix 1 to Annex C of the Memorandum of Understanding (MOU) into the eCOE system and mitigate risks associated with manual inputs;
- Implement mitigating controls to address the weaknesses identified with input design, master data, mandatory fields, and exception reports;
- Define its reporting requirements and specify procedures for requesting and developing new reports, specify responsibilities for reporting, and ensure that cancelled verification reports are authorized;
- Document procedures for the review and clean-up of master data duplications and draft verification reports;
- Implement mechanisms to control the receipt and assignment of mobile tablets in Galileo/Umoja;
- Undertake a risk assessment to document a user access matrix of roles, define the critical events for logging, and implement periodic monitoring of these events; and
- Undertake a business impact assessment of eCOE processes and document business continuity and disaster recovery procedures in accordance with the eCOE recovery priorities.

OICT needed to:

- Document a mobile device management policy to ensure standard, secure configuration and use of mobile devices; and
- Document a service level agreement that clarifies and defines the chain of support required for the eCOE system.

DFS and OICT accepted the recommendations and have initiated action to implement them.

CONTENTS

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the Electronic Contingent-Owned Equipment (eCOE) system in the United Nations Mission in the Republic of South Sudan (UNMISS).

2. By its resolution 50/222 of 11 April 1996, the General Assembly authorized the implementation of new procedures for determining reimbursement to Member States for contingent-owned equipment (COE). The COE Manual provides detailed policies and procedures for the reimbursement and control of the COE of troop/police contributing countries (TCC/PCC) participating in peacekeeping operations.

3. The verification and control procedures are intended to ensure that the terms of the Memorandum of Understanding (MOU) between the United Nations and the TCC/PCC are met by both parties. Major equipment and self-sustainment standards are defined to ensure operational capability. Reimbursement is dependent upon verification that the material and services provided by the TCC/PCC meet the terms of the MOU.

4. In 2007, the COE Unit of the Logistics Support Division (LSD) of the Department of Field Support (DFS) participated in a series of meetings with the Office of Information and Communications Technology (OICT) and external consultants to determine whether a Customer Relationship Management (CRM) solution could be used to: (i) develop an integrated system for COE that would minimize manual processes; (ii) ensure full integration with the financial management side managed by the Field Budget Finance Division (FBFD) of DFS; and (iii) enable integrated planning processes involving all key COE/MOU stakeholders in the Department of Peacekeeping Operations (DPKO), field missions and DFS. The outcomes of these meetings were the documentation of COE processes and a list of requirements for a new system.

5. In 2008, the Secretary-General's report A/62/510/Rev.1 on information and communications technology (ICT) enterprise systems for the Secretariat worldwide outlined the proposal to automate the service management components of the military and police capacity in field missions. This was to be achieved by integrating the disciplines of finance, logistics as well as strategic and tactical military and police operations, using the CRM solution. Recognizing the benefits of implementing CRM, the General Assembly, in its resolution 63/262, requested the Secretary-General to continue to implement CRM solutions throughout the Secretariat as appropriate and stressed that CRM solutions should be developed and implemented under the authority of the Chief Information Technology Officer to ensure a coordinated approach to the development of enterprise systems.

6. The General Assembly approved $4 million for new CRM initiatives in the Support Account for peacekeeping operations for the year 2009/10, including the system for managing TCC/PCC contributions and the billing of telecommunications services.

7. COE processes cut across several departments, offices and locations. Table 1 below shows the various stakeholders in the COE processes.

Table 1: Stakeholders in COE processes

Department/entity	Office
Peacekeeping missions	All field missions with COE
DFS	Field Budget and Finance Division
DFS	Logistics Support Division
DM	Office of Programme Planning, Budget and Accounts (OPPBA), including the Financial Information Operations Service
DPKO	Office of Military Affairs (including the Force Generation Service)
DPKO	Police Division

8. UNMISS was established by Security Council resolution 1996 of 8 July 2011. The COE budget for UNMISS for the financial years 2015/16 and 2016/17 was $1 billion for each financial year.

9. eCOE is the system used by management for verification and control of COE provided by TCC/PCC participating in peacekeeping missions. The system currently has a desktop and mobile application. In 2009, OICT engaged LSD as the stakeholder and subject matter expert to develop an eCOE solution which was deployed to missions in 2010. In 2016, a mobile application for eCOE was piloted at UNMISS to enable data entry at the inspection site using mobile devices and was planned for global deployment by the end of June 2017. A business intelligence module for analytical reporting and reporting on key performance indicators was scheduled for first release in November 2016 and a 'Service Management Reporting module' for major equipment was also in production.

10. The desktop application was a Siebel CRM web application and the mobile application was an Android-based solution integrated with the CRM desktop application. Both had a common Oracle database. eCOE had over 300 registered users and had been used to produce 9,939 verification reports on major equipment and self-sustainment. The system maintained detailed serviceability and inspection records for 1 million items of COE.

11. At the time eCOE was originally planned, core project requirements consisted of: (a) consolidation of multiple COE verification reports and major equipment databases into a single system; (b) replacement of manual/offline processes with automated processes; and (c) integration of the verification and inspection process with the MOU and reimbursement systems.

12. Comments provided by UNMISS, OICT and DFS are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

13. The objective of the audit was to assess the adequacy and effectiveness of governance, risk management and control processes over the effective implementation of the eCOE system.

14. This audit was included in the OIOS 2016 risk-based work plan due to the risks associated with COE, which constituted a significant portion of the peacekeeping budget.

15. OIOS conducted this audit from December 2016 to March 2017. The audit covered the period from January 2013 to March 2017. Based on an activity-level risk assessment, the audit covered risk areas of eCOE implementation in UNMISS, OICT and DFS, which included project management and the ICT support system.

16. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical reviews of data; (d) testing the effectiveness of the project governance,

systems development lifecycle and application controls; (e) walkthroughs of processes and procedures; (f) visit to the field office in Bor, South Sudan; and (g) ICT security tests.

III. OVERALL CONCLUSION

17. UNMISS, OICT and DFS had established some good control practices for the implementation and use of the eCOE system, including: (i) building eCOE on the existing CRM framework; (ii) user access controlled through a centralized identity management system; (iii) functionality for inspection and verification reports; and (iv) facilitation of monthly KPI reporting. However, some control weaknesses were identified with the current system, including: (i) inadequate project management mechanisms; (ii) key processes remaining unintegrated; (iii) completeness, accuracy and authorization of data was not adequately controlled at input; (iv) critical data was not defined; (v) inadequate processing controls and unassigned ownership of master data; (vi) inadequate data security procedures; (vii) user access procedures were not defined; and (viii) business continuity and disaster recovery procedures were yet to be documented.

IV. AUDIT RESULTS

A. Project management

Need to strengthen controls over project management

18. ICT projects in the United Nations Secretariat are governed by the administrative instruction on ICT initiatives (ST/AI/2005/10) and a project management framework based on the best practices defined in the "Projects in Controlled Environments, Version 2" (PRINCE2) methodology. According to this framework, ICT projects should be supported by a business case based on defined standards and approved by an established ICT Committee. This generally required the preparation of a project initiation document (i.e., a complete business case including the rationale and justification for proceeding with the initiative, business requirements, budget, expected benefits, feasibility studies, appraisal of various options, human resources requirements, project plan and risk assessment, and benefits realization).

19. The Secretary-General's report A/62/510/Rev.1 of 2008 on enterprise systems of the Secretariat worldwide outlined the proposal to automate the service management components of the military and police capacity in field missions by integrating finance, logistics as well as strategic and tactical military and police operations using a CRM solution. The project was to deploy a tool to manage the lifecycle of activities required to manage and sustain military and police capacity in field missions.

20. Also in 2008, external consultants were hired to document the business requirements for an integrated COE system to consolidate and replace multiple and disintegrated Lotus Notes databases into a single system, including the Government Claim Management System (GCMS) managed by the MOU and Claims Management Section (MCMS) in DFS. The business requirement document described three modules covering the 'end to end' process (i.e., MOU, inspection and verification, and reimbursements). However, there was limited coordination and collaboration among the various stakeholders in validating the business requirements; only one out of the three modules was deployed (i.e., inspection and verification).

21. At the onset of the eCOE initiative in 2008, the required project governance mechanisms (i.e., project board and project initiation document) were absent. There was no evidence to show that: (i) a business case had been prepared; and (ii) a project board had been constituted commensurate with the

project's size and complexity to provide effective oversight and direction. This weakness in project governance resulted in the following:

(i) Although in 2015 a project board was set up for the eCOE system to define and control the project scope, priorities and to ensure that the project's deliverables were aligned with the requirements of the stakeholder group and the General Assembly's mandate, the project board did not operate as expected. It focused primarily on the delivery of the inspection and verification module and the replacement of manual/offline processes with mobile inspection devices. The requirement to integrate all modules of the COE process was not adequately considered and planned.

(ii) In 2016, due to the technical limitations of GCMS, a new initiative led by FBFD was started; it was called the GCMS decommissioning project. The objective of this project was to integrate COE processes, which duplicated that of the eCOE project board. In this regard, OIOS noted the following:

(a) While DFS stated that the GCMS decommissioning project was anticipated to provide an integrated system for COE processes which would involve all stakeholders, this objective overlapped with that of the eCOE project board and was not under the board's oversight even though MCMS (owner of GCMS) was a member of the project board. Without a project board to coordinate and direct the interdependencies of both projects, there was a risk of duplication of effort, and that the objective to deploy an integrated system may not be met.

(b) DFS did not provide any evidence that it had documented a project initiation document describing the business case, plan, coordination and management mechanism for the GCMS decommissioning project in alignment with the General Assembly's mandate to deploy an integrated system.

(iii) OICT indicated that the budget approved for the eCOE project was $3 million and that the actual expenditure was $2.9 million. This budget was near depletion, even though the integrated solution had not been deployed. DFS did not provide evidence demonstrating how it intended to continue to fund the project and the integrated solution.

(iv) The eCOE project board reviewed and updated the 2008 business requirements with minor changes to the original document in 2015. OIOS compared the updated business requirements document against the existing functionality deployed in the eCOE desktop and eCOE mobile applications and noted the lack of integration of all COE systems. Several functionalities had not been deployed, which caused the following:

a. The continued use of separate systems for end-to-end COE processes due to inadequate collaboration amongst all stakeholders caused MOU and verification data to be shared and entered manually between FBFD, OICT, LSD and field missions, resulting in inefficiencies/delays and problems in data quality.

b. There was only a partial upload of MOU data into the eCOE system. The full MOU document was only available by email from the MCMS desk officer, which was then manually uploaded to eCOE and increased the likelihood of error.

c. The periodic upload of MOUs by OICT did not include Appendix 1 to Annex C of the MOU as this was an addition to the MOU which was never in GCMS (from

which MOU data was retrieved and uploaded by OICT). MCMS stated that a business decision was made not to invest any more in enhancing/updating of GCMS because the solution it was built on was outdated.

d. DFS did not define responsibility for ensuring that the Appendix 1 to Annex C of the MOU was uploaded into the eCOE system. This created a situation whereby mission staff had role conflicts by having access to update master data (the 'personnel field', i.e., number of troops and the 'services provided' field).

(v) Critical functionality had not been deployed. The eCOE updated project brief indicated that a total of 79 business requirements out of 188 had not been deployed.

(vi) The eCOE mobile functionality did not currently facilitate the inspection of medical services, which was still being done using paper checklists. DFS explained that the medical services checklists had not been standardized in line with other standard inspection worksheets generated by the eCOE desktop application due to the complexity of medical services.

22. These conditions were caused by the absence of adequate project management controls and may prevent the Organization from achieving the expected benefits of an integrated system.

(1) DFS should: (i) define a project governance mechanism and document a project initiation document for an integrated system that includes end-to-end constituent parts of the COE process; and (ii) clarify the source of funding for the deployment of the integrated system.

DFS accepted recommendation 1 and stated that: (i) with regard to the GCMS decommissioning, the project is being managed under the Umoja Project Management Office guidelines. A project brief and project initiation document is required by the guidelines to kick-off the project. This project will also be inclusive of all associated primary stakeholders; and (ii) the source of funding for this project will be determined upon completion of the technical evaluation of functional requirements, presentation and subsequent selection of a solution option. Recommendation 1 remains open pending receipt of evidence that: (i) a project governance mechanism has been defined and a project initiation document has been prepared covering the end-to-end parts of the COE process; and (ii) the source of funding for the deployment of the integrated system has been clarified.

(2) DFS should: (i) assign responsibility for uploading the Appendix 1 to Annex C of the MOU into the eCOE system for completeness; and (ii) mitigate the risks associated with manual inputs/uploads pending the deployment of an integrated system by embedding a workflow process for the independent review of manual inputs and amendments to processed data.

DFS accepted recommendation 2 stating that the GCMS decommissioning project has identified the business requirements and the new design will include the roles and responsibilities of each stakeholder for input and controls. Recommendation 2 remains open pending receipt of evidence that: (i) responsibility has been assigned for uploading Appendix 1 to Annex C of the MOU into the eCOE system; and (ii) the risks associated with manual inputs/uploads pending the deployment of an integrated system have been mitigated.

B. ICT support system

Need to strengthen controls over system design

23. ICT best practices (i.e., Control Objectives for Information and Related Technologies – COBIT) recommend that user requirements should be documented and detailed enough for a system design to include applications controls (i.e., authorization, input, processing and output) to ensure accuracy, completeness, timeliness, availability, and auditability of data.

24. The eCOE system was developed based on business requirements documented by an external consultant and updated by LSD. However, these documents were not based on a risk assessment to establish adequate controls for input, processing, and output before OICT translated the requirements into the system's design.

25. OIOS noted the following weaknesses in input controls which prevented the applications from ensuring data integrity:

(i) The system did not ensure the capture of mandatory data. There was blank data in fields (description, status, subtype and unit) described as critical by COE staff in UNMISS.

(ii) Data inputs were not always validated for consistency in the eCOE mobile application.

(iii) There was no notification process when units changed the name/equipment as a result of unit decommissioning/reconfiguration.

(iv) Data quality tests conducted by OIOS identified instances of multiple equipment with duplicate serial numbers, and test data in the production environment, and inconsistency in input nomenclature which allowed the acceptance of any value.

26. Processing controls and the ownership and responsibilities for the update of master data were not adequately defined. Master data updates and changes were done by UNMISS, OICT and the COE Unit of LSD. The following weaknesses were noted in this regard:

(i) The COE Manual was uploaded into the eCOE system and was used as a data source for populating standard rates (for reimbursements) and calculated rates in the MOU "tab". OIOS re-performed the calculations manually and observed that the calculated rate and the factors applied referred to the 2011 COE Manual instead of the values in the currently applicable 2014 Manual.

(ii) There was duplication of master data (i.e., unit fields) as a result of the migration of data from the old Lotus Notes COE database, which may cause the use of obsolete master data.

(iii) The requirements for process exception reports were not adequately defined for consistency.

27. These conditions were due to inadequate controls for input, processing, and output which may lead to the production of inaccurate information.

(3) DFS, in collaboration with OICT, should: (a) implement mitigating controls to address the weaknesses identified with input design; (b) assign ownership for master data; (c) ensure that all master data required for processing are captured by the system; (d) ensure that mandatory fields

are defined and the system is configured to capture the input of mandatory data; and (e) define exception reports for consistency.

DFS accepted recommendation 3 and stated that: (i) the GCMS decommissioning project has already identified the business requirements to address the weaknesses identified by OIOS. The new system will be robust, and include roles and responsibilities of each stakeholder and define access by functional group; (ii) ownership (and revision/update) of designated master data will be determined during the GCMS decommissioning project across the various processes and sub-processes; and (iii) the weaknesses identified by OIOS will be addressed in the GCMS decommissioning project by the MOU Functional Group, which is involving participants from LSD, FBFD, OPPBA and the Office of Military Affairs. Recommendation 3 remains open pending receipt of evidence that: (i) mitigating controls have been implemented to address the weaknesses in input design; (ii) ownership has been assigned for master data; (iii) all master data required for processing are captured by the system; (iv) mandatory fields have been defined and the system is configured to capture the input of mandatory data; and (v) exception reports have been defined for consistency.

Need to strengthen reporting requirements and procedures

28. An appropriate design of reporting requirements should ensure the availability, completeness, integrity and confidentiality of output data. Further, the impact of data outputs on other programmes and recipients should be adequately assessed.

29. Although some predefined reports had been designed in eCOE, there was no evidence that DFS had adequately defined its reporting requirements and the availability of eCOE as a reporting and analytical tool to analyze performance and provide management reports. For instance, the system was embedded with functionality to calculate reimbursement rates. OIOS received mixed opinions as to the relevance of this functionality. LSD and MCMS stated that this function was not required as it could provide misleading information, whereas UNMISS stated it was required because it provided senior management with information for decision making. In addition, the following control weaknesses were identified with regard to reporting:

(i) UNMISS stated that reporting demands have not been adequately met by eCOE as there were reports required by the Mission which could not be generated from the system.

(ii) There were multiple tools in place for reporting, i.e., eCOE and business objects (BO) without clarification as to who was responsible for ownership/integrity of data appearing in the reports and the procedure for requesting the development of new reports. The use of multiple tools (i.e., eCOE and BO) leads to duplication of data sets and increased data integrity risks from potential errors. In order to examine the integrity of data and the outputs from both tools, OIOS did a comparison between the eCOE reports and the COE quarterly reports generated from BO. OIOS observed discrepancies between the two outputs.

(iii) There were several verification reports in draft status since 2014, and cancelled verification reports that had been certified. However, there was no visibility to ascertain whether the verification report was approved for cancellation. This may cause confusion and affect system performance if there are no procedures for cleanup.

30. This condition points to the need for adequate analysis of reporting requirements and definition of clean up procedures to mitigate the risks of management's inability to monitor performance, inefficiencies and potential fraud.

(4) DFS should: (a) define its reporting requirements for eCOE; (b) specify responsibilities for reporting; (c) define procedures for requesting and developing new reports; and (d) ensure that cancelled verification reports are authorized.

DFS accepted recommendation 4 and stated that it will establish a set of standard reports on data quality and consistency and clarified that output requirements for eCOE are defined through the eCOE project board. DFS further stated that it will ensure that cancelled verification reports are authorized. Recommendation 4 remains open pending receipt of evidence: (a) defining the reporting requirements for eCOE; (b) specifying responsibilities for reporting; (c) defining procedures for requesting and developing new reports; and (d) ensuring that cancelled verification reports are authorized.

(5) DFS, in collaboration with OICT, should document procedures for the review and clean-up of master data duplications and draft verification reports.

DFS accepted recommendation 5 and stated that in collaboration with OICT, it will document the data clean-up process for the draft verification reports and global lookup tables, as well as the procedure for the review of data load, which includes dealing with duplications. Recommendation 5 remains open pending receipt of evidence demonstrating the documentation of procedures for the review and clean-up of master data duplications and draft verification reports.

Need to define mobile device management procedures

31. ISO/IEC 27001 recommends the documentation of a mobile device management policy to address the risks associated with the use of mobile devices. The policy should define the registration/de-registration of mobile devices, physical security requirements, technical security requirements (including remote connections, software control, access control, encryption at rest/in-transit), and it should also define the business requirements for the use of mobile devices.

[redacted].

33. OIOS brought these security issues to the attention of the UNMISS Communication and Information Technology Section (CITS) and OICT during the audit. Both OICT and UNMISS CITS provided evidence that some of these weaknesses had been resolved and draft guidelines had been issued to the Mission. OICT also stated that a draft administrative instruction is currently with the Office of Human Resources Management to address this issue at the Organization level.

34. This condition was caused by the lack of a mobile device management policy which posed the risks of unreliable data, unauthorized access to the eCOE system, and unauthorized modification of data.

(6) OICT, in collaboration with DFS, should formally document a mobile device management policy to ensure the standardized, secure configuration and use of mobile devices.

OICT accepted recommendation 6 and stated that the mobile device policy has been developed and it is currently pending formal approval. Recommendation 6 remains open pending receipt of evidence of a formal mobile device management policy to ensure the standardized and secure configuration and use of mobile devices.

Weak controls over the inventory of mobile tablets

35. The international ICT security management standards adopted by the United Nations Secretariat (ISO/IEC 27001) recommend that information processing assets should be identified and an inventory should be maintained to reduce the risks from environmental threats, hazards, and unauthorized use.

36. Twelve mobile tablets were in use by the UNMISS COE Unit of which six were provided by OICT and six were procured locally. However, the six provided by OICT were not recorded in Galileo/Umoja. Inadequate controls over the inventory of mobile tablets may result in their loss or misuse.

(7) UNMISS should implement mechanisms to control the receipt and assignment of mobile tablets in Galileo/Umoja.

DFS accepted recommendation 7 and stated that the required mechanisms for the receipt and assignment of tablets in Galileo/Umoja are established and that the current threshold asset policy for tablets is $500, regardless of life expectancy. DFS further stated that if the tablets cost over the established threshold, they will be tracked in Galileo/Umoja. Otherwise, the Mission asset manager will maintain accountability for the tablets, and the tablets will be tracked outside of Umoja. OICT, in coordination with the Information Communication and Technology Division (ICTD), are addressing the issues of data accountability and prevention of unauthorized access. An Administrative Instruction and Technical Procedure on Mobile Devices have been drafted and are pending issuance by OICT. OIOS notes that these assets contain sensitive data and a mobile application, which are deemed to be configurable items. In this regard, the mechanism for tracking the receipt, use and movement of these assets should be formalized if they are under the threshold for tracking in Galileo/Umoja. Recommendation 7 remains open pending receipt of evidence that procedures have been established in the pending mobile device management policy to control the receipt and assignment of mobile tablets.

Need to strengthen data security procedures

37. The United Nations project management framework includes a requirement to define information security controls in the design of any system. These controls pertain to confidentiality, integrity, availability, auditability and user accessibility of data.

38. DFS had not performed a risk assessment to define its user access requirements and critical activities (i.e., user activities, exceptions, faults and information security events) that required logging and monitoring. The following weaknesses were noted in this regard:

(i) DFS had partially defined user access procedures in the document "Field eCOE verification procedures". However, this document did not provide guidance for mapping user access based on a matrix of roles and responsibilities to ensure that incompatible roles were not assigned. OICT used its own judgement in defining user access controls embedded into the system. User access requirements should be defined by the business owners because they have a better understanding of their critical roles and potential conflicts.

(ii) Some logs were maintained for changes to equipment. However, DFS had not adequately defined what critical events it needed to log and monitor (i.e., edit, modify and delete of eCOE data and transactions).

39. The absence of a risk assessment and related controls to determine user access requirements and critical activities requiring logging may cause data loss, unauthorized access, unauthorized modifications to data, and unreliable information.

(8) DFS should undertake a risk assessment to: (a) document a user access matrix of roles and responsibilities to ensure that incompatible roles are not assigned in the eCOE system; and (b) define the critical events for logging and implement periodic monitoring of these events.

DFS accepted recommendation 8 and stated that the scope of COE operations varies from mission to mission. In some cases, there is only one staff member who performs all COE roles, i.e., updates missing MOU values in eCOE, conducts inspection, and approves and submits verification reports for certification. In these cases, it is not possible to segregate roles. The outcome of the GCMS decommissioning project should relieve field staff of MOU data entry. Nevertheless, a generic user access matrix could be documented in collaboration with OICT for large missions. Recommendation 8 remains open pending receipt of evidence of a risk assessment to: (i) document a user access matrix of roles and responsibilities to ensure that incompatible roles are not assigned in the eCOE system as far as practicable; and (ii) define the critical events for logging and implement periodic monitoring of these events.

Need to strengthen business continuity and disaster recovery procedures

40. COBIT recommends the development of detailed business continuity and disaster recovery procedures for any application deployed in the Organization.

41. DFS had not performed a business impact assessment and defined its business continuity requirements for eCOE (i.e., recovery time objective and recovery point objective). OICT had implemented the same recovery procedures it used for the Umoja system and will apply the same recovery prioritization during a disaster recovery incident. eCOE operational priorities and risks may differ from that of Umoja. Also, there was no procedure for ensuring the retention of data on the mobile application and its recovery in the event of a disaster recovery incident.

42. The lack of business impact assessment and disaster recovery procedures may result in data losses.

(9) DFS, in collaboration with OICT, should undertake a business impact assessment of the eCOE processes and document business continuity and disaster recovery procedures in accordance with the eCOE recovery priorities.

DFS accepted recommendation 9 and stated that it will take necessary action to implement the recommendation. Recommendation 9 remains open pending receipt of evidence that a business impact assessment of eCOE processes has been undertaken, and business continuity and disaster recovery procedures have been documented in accordance with the eCOE recovery priorities.

Support procedures need to be defined

43. COBIT recommends documenting procedures for managing service requests in a standard manner to support agreed-upon service levels (SLA) and ensure continuous operations. The procedures should also: (i) include monitoring and escalation processes based on agreed-upon SLAs for classification and prioritization of any reported issue (i.e., incidents, service requests); and (ii) ensure that the end-to-end life cycle of requests/incidents is monitored and escalated appropriately by the service desk.

44. OICT deployed the pilot eCOE mobile application to UNMISS in 2016 and provided deployment support. However, the chain for continuous support after deployment (i.e. hardware, software and infrastructure) was not clarified between OICT and UNMISS CITS.

45. iNeed is the enterprise system used for raising service requests. The majority of eCOE issues up to January 2017 were logged as "other", which did not provide the necessary visibility and did not allow effective tracking of multiple issues before they developed into problems. However, OICT provided evidence that necessary changes had since been made to address this issue.

46. There were inadequate procedures to manage requests for investigation of reimbursement discrepancies from TCC/PCC. As a result, requests could not be tracked in a consistent manner. OICT stated that it had already documented a proposal to implement iNeed for DFS' tracking of all COE-related issues that were brought up either by missions, through OICT or directly from Member States and it was awaiting LSD consideration of the proposal to implement iNeed.

47. The lack of an adequate SLA for the eCOE system may result in service delays and complaints.

(10) OICT, in collaboration with DFS, should document a service level agreement that clarifies and defines the chain of support required for the eCOE system.

OICT accepted recommendation 10 and stated that it is currently working on the SLA. Recommendation 10 remains open pending receipt of evidence that a SLA has been established clarifying and defining the chain of support required for the eCOE system.

V. ACKNOWLEDGEMENT

48. OIOS wishes to express its appreciation to the management and staff of UNMISS, OICT and DFS 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

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	DFS should: (i) define a project governance mechanism and document a project initiation document for an integrated system that includes end-to-end constituent parts of the COE process; (ii) clarify the source of funding for the deployment of the integrated system.	Important	O	Receipt of evidence that: (i) a project governance mechanism has been defined and a project initiation document has been prepared covering the end-to-end parts of the COE process; and (ii) the source of funding for the deployment of the integrated system has been clarified.	31 March 2018
2	DFS should: (i) assign responsibility for uploading the Appendix 1 to Annex C of the MOU into the eCOE system for completeness; and (ii) mitigate the risks associated with manual inputs/uploads pending the deployment of an integrated system by embedding a workflow process for the independent review of manual inputs and amendments to processed data.	Important	O	Receipt of evidence that: (i) responsibility has been assigned for uploading Appendix 1 to Annex C of the MOU into the eCOE system; and (ii) the risks associated with manual inputs/uploads pending the deployment of an integrated system have been mitigated.	31 March 2019
3	DFS, in collaboration with OICT, should: (a) implement mitigating controls to address the weaknesses identified with input design; (b) assign ownership for master data; (c) ensure that all master data required for processing are captured by the system; (d) ensure that mandatory fields are defined and the system is configured to capture the input of mandatory data; and (e) define exception reports for consistency.	Important	O	Receipt of evidence that: (i) mitigating controls have been implemented to address the weaknesses in input design; (ii) ownership has been assigned for master data; (iii) all master data required for processing are captured by the system; (iv) mandatory fields have been defined and the system is configured to capture the input of mandatory data; and (v) exception reports have been defined for consistency.	31 March 2019
4	DFS should: (a) define its reporting requirements for eCOE; (b) specify responsibilities for reporting;	Important	O	Receipt of evidence: (a) defining reporting requirements for eCOE; (b) specifying	31 March 2018

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.
[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[3] C = closed, O = open
[4] Date provided by UNMISS, OICT and DFS in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
	(c) define procedures for requesting and developing new reports; and (d) ensure that cancelled verification reports are authorized.			responsibilities for reporting; (c) defining procedures for requesting and developing new reports; and (d) ensuring that cancelled verification reports are authorized.	
5	DFS, in collaboration with OICT, should document procedures for the review and clean-up of master data duplications and draft verification reports.	Important	O	Receipt of evidence demonstrating the documentation of procedures for the review and clean-up of master data duplications and draft verification reports.	31 March 2018
6	OICT, in collaboration with DFS, should formally document a mobile device management policy to ensure the standardized, secure configuration and use of mobile devices.	Important	O	Receipt of evidence of a formal mobile device management policy to ensure the standardized and secure configuration and use of mobile devices.	31 March 2019
7	UNMISS should implement mechanisms to control the receipt and assignment of mobile tablets in Galileo/Umoja.	Important	O	Receipt of evidence that procedures are established in the pending mobile device management policy to control the receipt and assignment of mobile tablets.	Not indicated
8	DFS should undertake a risk assessment to: (a) document a user access matrix of roles and responsibilities to ensure that incompatible roles are not assigned in the eCOE system; and (b) define the critical events for logging and implement periodic monitoring of these events.	Important	O	Receipt of evidence of a risk assessment to: (i) document a user access matrix of roles and responsibilities to ensure that incompatible roles are not assigned in the eCOE system as far as practicable; and (ii) define the critical events for logging and implement periodic monitoring of these events.	31 March 2018
9	DFS, in collaboration with OICT, should undertake a business impact assessment of the eCOE processes and document business continuity and disaster recovery procedures in accordance with the eCOE recovery priorities.	Important	O	Receipt of evidence that a business impact assessment of eCOE processes has been undertaken, and business continuity and disaster recovery procedures have been documented in accordance with the eCOE recovery priorities.	31 March 2018
10	OICT, in collaboration with DFS, should document a service level agreement that clarifies and defines the chain of support required for the eCOE system.	Important	O	Receipt of evidence that a SLA has been established clarifying and defining the chain of support required for the eCOE system.	31 March 2019

APPENDIX I

Management Response

ANNEX II

Management Response

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	DFS should: (i) define a project governance mechanism and document a project initiation document for an integrated system that includes end-to-end constituent parts of the COE process; (ii) clarify the source of funding for the deployment of the integrated system.	Important	Yes	USG, DFS	First quarter of 2018	DFS' comments are reflected in the report.
2	DFS should: (i) assign responsibility for uploading the Appendix 1 to Annex C of the MOU into the eCOE system for completeness; and (ii) mitigate the risks associated with manual inputs/uploads pending the deployment of an integrated system by embedding a workflow process for the independent review of manual inputs and amendments to processed data.	Important	Yes	USG, DFS	First quarter of 2019	DFS' comments are reflected in the report.
3	DFS, in collaboration with OICT, should: (a) implement mitigating controls to address the weaknesses identified with input design; (b) assign ownership for master data; (c) ensure that all master data required for processing are captured by the system; (d) ensure that mandatory fields are defined and the system is configured to capture the input of mandatory data; and (e) define exception reports for consistency.	Important	Yes	USG, DFS	First quarter of 2019	DFS' comments are reflected in the report.
4	DFS should: (a) define its reporting requirements for eCOE; (b) specify responsibilities for reporting; (c) define	Important	Yes	Director, LSD	First quarter of 2018	(a), (b), and (d): DFS will establish a set of standard reports on data quality and consistency.

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

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

ANNEX II

Management Response

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	procedures for requesting and developing new reports; and (d) ensure that cancelled verification reports are authorized.				(c): Implemented	(c): DFS wishes to clarify that output requirements for eCOE are defined through the eCOE Project Board.
5	DFS, in collaboration with OICT, should document procedures for the review and clean-up of master data duplications and draft verification reports.	Important	Yes	Director, LSD	First quarter of 2018	DFS' comments are reflected in the report.
6	OICT, in collaboration with DFS, should formally document a mobile device management policy to ensure the standardized and secure configuration and use of mobile devices.	Important	Yes	Chief, Global Operations Division	First quarter of 2019	The mobile device policy has been developed and it is currently pending formal approval.
7	UNMISS should implement mechanisms to control the receipt and assignment of mobile tablets in Galileo/Umoja.	Important	Yes	DMS, UNMISS	Implemented	The required mechanisms for the receipt and assignment of tablets in Galileo/Umoja are established by UN asset management policies. The current threshold asset policy for tablets is USD500, regardless of life expectancy. If the tablets cost over the established threshold, they will be tracked in Galileo/Umoja. Otherwise, the Mission asset manager will maintain accountability for the tablets, and the tablets will be tracked outside of UMOJA. OICT, in coordination with ICTD, are addressing the issues of data accountability and prevention of unauthorised access. An AI and Technical Procedure on Mobile Devices have been drafted and are pending issuance by the Office of the

ANNEX II

Management Response

Audit of the Electronic Contingent-Owned Equipment system in the United Nations Mission in the Republic of South Sudan

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						Chief Information Technology Officer (CITO).
8	DFS should undertake a risk assessment to: (a) document a user access matrix of roles and responsibilities to ensure that incompatible roles are not assigned in the eCOE system; and (b) define the critical events for logging and implement periodic monitoring of these events.	Important	Yes	Director, LSD	First quarter of 2018	DFS' comments are reflected in the report.
9	DFS, in collaboration with OICT, should undertake a business impact assessment of the eCOE processes and document business continuity and disaster recovery procedures in accordance with the eCOE recovery priorities.	Important	Yes	Director, LSD	First quarter of 2018	DFS' comments are reflected in the report.
10	OICT, in collaboration with DFS, should document a service level agreement that clarifies and defines the chain of support required for the eCOE system.	Important	Yes	Chief, Enterprise Application Centre - Bangkok	First quarter of 2019	OICT is currently working on the SLA.