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

DATE: 7 December 2011

REFERENCE: IAD: 11- 00736

FROM: Fatoumata Ndiaye, Director
DE: Internal Audit Division, OIOS

SUBJECT: **Assignment No. AT2011/615/01 – Audit of information and communications technology (ICT) governance and security management in peacekeeping missions**
OBJET:

Overall results relating to the adequacy and effectiveness of ICT governance and security arrangements in peacekeeping missions were partially satisfactory

1. Attached please find the final report on the above-mentioned audit.

2. Annex I shows the status of recommendations. Please note that OIOS will report on the progress made to implement its recommendations in its annual report to the General Assembly and to the Secretary-General annually for important recommendations (nos. 1-3).

3. The audit also identified a number of opportunities for improvement (see Annex-II). While OIOS will not report on the implementation of these opportunities, we encourage you to implement them to improve the efficiency and effectiveness of your operations. OIOS will review their implementation as part of future audits.

4. Please note that under General Assembly resolution 59/272, a Member State may request that the final report be made available. Also note that pursuant to General Assembly resolution 64/263, OIOS has included the complete management response as an appendix to the present report.

5. We wish to express our appreciation to the Management and staff of DFS for the assistance and cooperation extended to the auditors during the assignment.

cc: Mr. Anthony Banbury, Assistant Secretary-General, Department of Field Support
Mr. Choi Soon-hong, Assistant Secretary-General and Chief Information Technology Officer
Mr. Rudy Sanchez, Chief, ICTD, Department of Field Support
Mr. Seth Adza, Operations Review Officer, Department of Field Support
Mr. Zakary Ikiara, Chief, Policy and Oversight Coordination Unit, Department of Management
Mr. Swatantra Goolsarran, Executive Secretary, United Nations Board of Auditors
Mr. Rohan Wijeratne, Deputy Director, United Nations Board of Auditors
Ms. Suzanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwamye, Executive Secretary, IAAC
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS
Ms. Eleanor T. Burns, Chief, Peacekeeping Audit Service, Internal Audit Division, OIOS
Ms. Amy Wong, Programme Officer, Internal Audit Division, OIOS
Mr. Emile Tongunga, Information Systems Officer, OICT

FINAL AUDIT REPORT

Audit of the information and communications technology (ICT) governance and security management in peacekeeping missions

BACKGROUND

The Information and Communications Technology Division (ICTD) in the Department of Field Support (DFS) was established by General Assembly resolution 61/279. In accordance with ST/SGB/2010/2, DFS/ICTD is responsible for supporting the Office of Information and Communications Technology (OICT) in: i) Establishing ICT architecture and standards; ii) Planning and implementing major infrastructure improvements for field operations; (iii) Implementing and supporting Organization-wide applications and major shared field applications; (iv) Providing centralized ICT project management support; (v) Coordinating disaster recovery and business continuity planning for the field; (vi) Reviewing and approving ICT field budget submissions; and (vii) Maintaining strategic oversight of the enterprise data centres and major communications facilities, including review and approval of strategic directions.

Peacekeeping missions include communications and information technology sections for providing local ICT services. ICT related resources for peacekeeping operations for the period from 1 July 2010 to 30 June 2011 are shown in Table 1.

Table 1. ICT related resources for peacekeeping operations for the period from 1 July 2010 to 30 June 2011

	Communications (US Dollars)	**Information Technology (US Dollars)**
MINURCAT	$3,724,000	$1,718,000
MINURSO (from 1 July 2010 to 31 December 2010)	$1,374,400	$1,055,900
MINUSTAH(from 1 July 2010 to 31 December 2010)	$13,515,900	$3,502,200
MONUC (MONUSCO)	$38,511,400	$13,316,200
UNAMID	$53,740,600	$23,590,600
UNDOF	$1,296,500	$755,100
UNFICYP	$844,500	$787,900
UNIFIL	$16,260,000	$4,181,700
UNMIK	$2,199,100	$1,367,400
UNMIL	$13,959,600	$3,900,700
UNMIS	$19,337,100	$15,189,900
UNMIT	$6,202,200	$4,747,600
UNOCI	$16,667,700	$5,681,100
Support of the African Union Mission in Somalia	$14,263,400	$3,679,300
UNLB	$7,977,000	$8,397,300
Support Account (including an amount of $57,033,000 for ERP)	$2,939,400	$79,959,400
Total	**$212,822,800**	**$171,830,300**

During the period 2008 – 2011, the Office of Internal Oversight Services (OIOS) conducted audits of information and communications technology governance and security management in six peacekeeping missions, as follows:

(a) AT2008/620/01 – United Nations Organization Mission in the Democratic Republic of the Congo (MONUC);

(b) AT2008/632/01 – United Nations Mission in Sudan (UNMIS);

(c) AT2009/626/01 – United Nations Mission in Liberia (UNMIL);

(d) AT2009/683/01 – United Nations Stabilization Mission to Haiti (MINUSTAH);

(e) AT2010/672/01 – United Nations Interim Force in Lebanon (UNIFIL); and

(f) AT2010/640/01 – United Nations Operations in Côte d'Ivoire (UNOCI).

OBJECTIVE AND SCOPE

This audit was conducted to assess whether peacekeeping missions implemented adequate risk management, control and governance processes to provide reasonable assurance regarding the effectiveness of ICT governance and security management. The key controls tested for the audit included those related to: (a) risk management and strategic planning; (b) mandates and delegation of authority; (c) regulatory framework; (d) oversight; and (e) disaster recovery and business continuity plans.

AUDIT RESULTS

In OIOS' opinion, risk management, control and governance processes examined were **partially satisfactory** to provide reasonable assurance that ICT governance and security management in peacekeeping missions were adequate and effective.

ICT governance structures in the peacekeeping missions were not operating as expected and appropriate mechanisms for ensuring oversight and coordination of ICT strategic planning in the field were not fully developed. Missions lacked adequate ICT risk and security management processes. The ICT governance, risk and compliance system was not supported by a business case defining strategy and scope. However, DFS developed tools and templates to assist peacekeeping missions in developing business continuity and disaster recovery (BC/DR) plans and training staff. Peacekeeping missions have initiated business continuity and disaster recovery planning activities and are expected to complete them by the end of 2011.

Local ICT Committees in peacekeeping missions were not functioning as expected

Local ICT Committees responsible for providing direction, control and approval of ICT investments in the peacekeeping missions were either not established or not functioning as expected. Business cases in support of the locally developed applications had not been prepared to detail functional, security, performance and availability requirements.

(1) DFS should: (i) facilitate the establishment and functioning of Local ICT Committees at the mission level and act as a central coordinating body on all ICT matters; and (ii) establish monitoring mechanisms to ensure that peacekeeping missions comply with the Organization's policies and standards for approving business cases.

DFS accepted recommendation 1 stating that guidance will be sent to peacekeeping missions on the establishment of ICT management structures and local ICT review committees. DFS will engage with missions periodically to ensure that no unsanctioned ICT development activities are undertaken. Recommendation 1 remains open pending receipt of the copy of the memorandum sent by DFS to peacekeeping missions and evidence that DFS' monitoring mechanism for the approval of business cases has established satisfactory.

Limited deployment of the Field Support Suite

Local applications in peacekeeping missions were developed without assessing whether the new enterprise-wide applications being developed in the United Nations Secretariat would address the same substantive needs, and how these applications could be integrated. DFS developed the centrally hosted application set, Field Support Suite (FSS), to address missions' common application requirements. In spite of the availability of FSS, the majority of missions still use local applications.

(2) DFS should determine the need for extending the scope of Field Support Suite.

DFS accepted recommendation 2 stating the development and implementation of the Field Support Suite (FSS) was conducted in coordination with the UMOJA Team which sees FSS deployment as an effective mechanism to consolidate data and processes in the field. The implementation of FSS modules to all field missions is underway and scheduled for completion in 2012. Its implementation will result in the decommissioning of local systems that are currently being used to perform similar functions, Local CITS management is kept informed of the enterprise and FSS deployment schedules so that they can adjust the required support and maintenance for local applications accordingly. The scope of the FSS is being extended to meet the business needs of the field and the selection of enhancements and additional modules have been planned in alignment with the Global Field support Strategy as well as through engagement of Headquarters and mission management. FSS is also under consideration as a front end tool to facilitate the data collection and conversions required for UMOJA and IPSAS implementation. Recommendation 2 remains open pending receipt of the assessment conducted by DFS for determining the scope of FSS.

The governance, risk and compliance (GRC) system is not supported by a business case defining strategy and scope

DFS purchased in June 2010 a GRC software for supporting, integrating and aligning its governance, risk assessment and compliance activities. A project of this nature is usually a large and complex initiative involving multiple stakeholders, platforms, technologies and locations, and requires a clear project strategy. However, DFS did not develop a business case for this project and did not document the project scope, cost, requirements and plan in support of its acquisition of this application. Concurrently, OICT was developing a proof of concept for establishing a Secretariat-wide ICT enterprise risk, governance and compliance platform. The two initiatives by OICT and DFS respectively, were not adequately coordinated, exposing the Organization to risks of duplication of investments and waste of resources.

(3) DFS should: (i) ensure that its application for governance, risk and compliance (GRC) is supported by a documented business case in accordance with the established ICT project management procedures; and (ii) implement mechanisms for monitoring the compliance of peacekeeping missions with ICT policies.

DFS partially accepted recommendation 3 stating that a business case is not required for projects under $250,000, in accordance with OICT's portfolio management. Since the cost of the GRC project is below the threshold of $250,000, the procedure followed by ICTD was in compliance with the above quoted guidance. DFS further stated that the implementation of mechanisms for monitoring the compliance of peacekeeping missions with ICT policies is dependent on the development of the platform (E-GRC, electronic governance, risk and compliance) planned by OICT.

The DFS estimate of the GRC project cost does not include the cost of staff required for GRC system implementation (both Headquarters and peacekeeping missions staff). The draft documentation prepared by DFS indicates that the GRC implementation will require two ICT security officers in DFS and one or two ICT security focal points in each field operation. Adding the annual cost of two staff members (i.e., professional staff at P/3 level), which is approximately $154,000, brings the total cost of the initiative to $308,000. This estimate exceeds the threshold of $250,000 required for the preparation of a high level business case. Furthermore, the correct determination of project costs is a necessary element for supporting OICT in completing its proof of concept and deciding which application to adopt for this function. Recommendation 3 remains open pending receipt from DFS of the documented high level business case in support of the GRC project and evidence of mechanisms implemented for monitoring compliance of peacekeeping missions with ICT policies.

Business continuity and disaster recovery need improvement

Business continuity and disaster recovery plans in peacekeeping missions were not documented and tested. However, improvements had been recently made by DFS and DPKO with the establishment of coordination and guidance mechanisms. In 2011, DFS and DPKO's business continuity coordination team established coordination processes and guidelines. Business continuity planning methodology, tools and templates for peacekeeping missions were prepared and business continuity planners of the missions were trained. Peacekeeping missions initiated BC/DR planning activities and expected to complete them by the end of 2011.

(4) DFS should complete the disaster recovery plans of all peacekeeping missions by including: (i) the list of mission critical applications; (ii) the definition of recovery time and point objectives; (iii) alignment with the mission's business continuity plans; and (iv) a standard template for reporting disaster recovery test results.

DFS accepted recommendation 4 stating that guidance for disaster recovery plans is being developed and will be communicated to the field missions. Recommendation 4 remains open pending receipt of mission disaster recovery plans documenting critical applications, recovery time, and point objectives, and a standard template for reporting disaster recovery test results.

ACKNOWLEDEGMENT

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

CONTENTS

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted a horizontal audit of the information and communications technology (ICT) governance and security management processes of the peacekeeping missions. Comments made by Department of Field Support (DFS) are shown in *italics.*

2. In accordance with ST/SGB/2010/2, the Information and Communications Technology Division in DFS is responsible for supporting OICT in: (i) Establishing ICT architecture and standards; (ii) Planning and implementing major infrastructure improvements for field operations; (iii) Implementing and supporting Organization-wide applications and major shared field applications; (iv) Providing centralized ICT project management support; (v) Coordinating disaster recovery and business continuity planning for the field; (vi) Reviewing and approving ICT field budget submissions; and (vii) Maintaining strategic oversight of the enterprise data centres and major communications facilities, including review and approval of strategic directions.

3. In accordance with DFS policy directive on ICT security, business continuity and emergency preparedness strategy, DFS/ICTD is also responsible for administering a programme of work comprised of: (i) ICT security policies, procedures, standards, baselines, guidelines and plans; (ii) risk assessment and management; (iii) coordination, monitoring, compliance, certification and continuous improvement; and (iv) ICT security awareness and training programme.

4. The Communications and Information Technology Section (CITS) established in each peacekeeping mission provides ICT services locally. ICT related resources for peacekeeping operations for the period from 1 July 2010 to 30 June 2011 are shown in Table 1.

Table 1. ICT related resources for peacekeeping operations for the period from 1 July 2010 to 30 June 2011

	Communications (US Dollars)	**Information Technology (US Dollars)**
MINURCAT	$3,724,000	$1,718,000
MINURSO (from 1 July 2010 to 31 December 2010)	$1,374,400	$1,055,900
MINUSTAH(from 1 July 2010 to 31 December 2010)	$13,515,900	$3,502,200
MONUC (MONUSCO)	$38,511,400	$13,316,200
UNAMID	$53,740,600	$23,590,600
UNDOF	$1,296,500	$755,100
UNFICYP	$844,500	$787,900
UNIFIL	$16,260,000	$4,181,700
UNMIK	$2,199,100	$1,367,400
UNMIL	$13,959,600	$3,900,700
UNMIS	$19,337,100	$15,189,900
UNMIT	$6,202,200	$4,747,600
UNOCI	$16,667,700	$5,681,100
Support of the African Union Mission in Somalia	$14,263,400	$3,679,300
UNLB	$7,977,000	$8,397,300
Support Account (including an amount of $57,033,000 for ERP)	$2,939,400	$79,959,400
Total	**$212,822,800**	**$171,830,300**

II. AUDIT OBJECTIVE

5. This audit was conducted to assess whether DFS and peacekeeping missions implement adequate risk management, control and governance processes to provide reasonable assurance regarding the effectiveness of ICT governance and security management. The key controls tested for the audit included those related to: (a) risk management and strategic planning; (b) mandates and delegation of authority; (c) regulatory framework; (d) oversight; and (e) disaster recovery and business continuity plans. For the purpose of this audit, OIOS defined these key controls as follows:

(a) Risk management and strategic planning – those controls that are designed to provide reasonable assurance that effective mission ICT strategies have been put in place and ICT risks are identified and assessed, and that action is taken to mitigate or anticipate risks.

(b) Mandates and delegation of authority – those controls that are designed to provide reasonable assurance on the clarity of the authority, roles and responsibilities for managing ICT resources and operations in the peacekeeping missions.

(c) Regulatory framework – those controls that are designed to provide reasonable assurance that policies and procedures exist to guide ICT operations and manage ICT security.

(d) Oversight – those controls that provide for supervision and evaluation of the mission's ICT activities for ensuring that threats and opportunities are identified and appropriate response or action plans are drawn to minimize risks and take advantage of opportunities.

(e) Disaster recovery and business continuity plans – those controls that are designed to provide reasonable assurance that disaster recovery and business continuity plans exist to ensure that ICT operations of the peacekeeping missions can withstand crisis and continue to operate within a reasonable time frame.

III. AUDIT SCOPE AND METHODOLOGY

6. This audit was cross-cutting and included a review of ICT governance and security management in six peacekeeping missions and DFS/ICTD, as follows:

a. AT2008/620/01 – United Nations Organization Mission in the Democratic Republic of the Congo (MONUC, April – June 2008);

b. AT2008/632/01 – United Nations Mission in Sudan (UNMIS, September – November 2008);

c. AT2009/683/01 – United Nations Stabilization Mission to Haiti (MINUSTAH, September – December 2009);

d. AT2009/626/01 – United Nations Mission in Liberia (UNMIL, November 2009 – January 2010);

e. AT2010/640/01 – United Nations Operations in Côte d'Ivoire (UNOCI, October 2010);

f. AT2010/672/01 – United Nations Interim Force in Lebanon (UNIFIL, November 2010 – January 2011); and

g. AT2011/615/01 - Audit of ICT governance and security management in DFS/ICTD (March – May 2011).

7. The audits conducted in the peacekeeping missions included: (a) review of policies, standard operating procedures and guidelines; (b) interviews with representatives and staff from substantive areas and the Mission's support offices; (c) vulnerability tests on selected critical hosts and scans of the Mission's network; and (d) visits to ICT installations and off-site backup locations.

8. The audit conducted in DFS/ICTD included a review of policies, standard operating procedures, guidelines and reports, and interviews with relevant staff involved in the ICT governance and security management.

9. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of written policies and procedures, and also whether they were implemented consistently.

IV. OVERALL ASSESSMENT

10. In OIOS' opinion, risk management, control and governance processes examined were **partially satisfactory** to provide reasonable assurance regarding the effectiveness of ICT governance and security management. ICT governance bodies in the missions were not operating as expected. DFS/ICTD developed a field support strategy based on the establishment of global and regional service centres, reorienting organizational structures and service delivery mechanisms towards a shared services model, including for ICT operations. However, mechanisms for ensuring oversight and coordination of ICT strategic planning in peacekeeping missions were yet to be developed. Missions lacked adequate ICT risk and security management processes. The ICT governance, risk and compliance system was not supported by a business case defining strategy and scope. Business continuity and disaster recovery (BC/DR) plans were not properly documented and tested in the missions. However, DFS and DPKO developed tools and templates to assist the missions in developing BC/DR plans and training staff. Peacekeeping missions have initiated BC/DR planning activities and are expected to complete them by the end of 2011.

V. AUDIT RESULTS

A. Role and responsibility of DFS/ICTD in support of peacekeeping missions

11. The role and responsibility of DFS/ICTD in mitigating the systematic control weaknesses indentified across the peacekeeping missions were audited in accordance with its mandate.

12. As per its mandate, DFS/ICTD provides strategic guidance, coordination and support for ICT in the missions. In particular, DFS/ICTD is responsible for supporting OICT in: (i) Establishing ICT architecture and standards; (ii) Planning and implementing major infrastructure improvements for field operations; (iii) Implementing and supporting Organization-wide applications and major shared field applications; (iv) Providing centralized ICT project management support; (v) Coordinating disaster recovery and business continuity planning for the field; (vi) Reviewing and approving ICT field budget submissions; and (vii) Maintaining strategic oversight of the enterprise data centres and major communications facilities, including review and approval of strategic directions.

13. Furthermore, in accordance with DFS policy directive on ICT security, business continuity and emergency preparedness strategy, DFS/ICTD is also responsible for administering a programme of work comprised of: (i) ICT security policies, procedures, standards, baselines, guidelines and plans; (ii) risk

assessment and management; (iii) coordination, monitoring, compliance, certification and continuous improvement; and (iv) ICT security awareness and training programme.

B. Risk management and strategic planning

14. ICT security risks and vulnerability assessments were not performed in any of the missions. Although DFS developed a risk management policy and risk management guidelines in 2008, this document was still in draft. A sample threat catalog and risk assessment methodology was developed in UNLB in the context of its information security management system. However, this methodology had not been adopted by the peacekeeping missions. While DFS/ICTD performed some security risk assessment activities in peacekeeping missions based on the request of the missions, the reports on these risk assessments were not available at the time of the audit.

15. DFS/ICTD created an ICT security reporting workspace allowing security practitioners to collaborate and share information about security incidents. The ultimate goal of this initiative was to mitigate the risk of security breaches not detected in a timely manner. This repository included guidelines and best practices for managing security incidents. The tool, which requires manual input, enables the ICT security focal points of each mission to provide a monthly report describing the overall status of the local ICT security, as well as details of the current operational environment and risks.

16. DFS advised that:

> *The establishment of an ICT risk management framework falls within the purview of OICT. In accordance with paragraphs 35 (i) and (j) of the information and communications strategy for the United Nations Secretariat (A/62/793) dated 9 April 2008, OICT is responsible for among others to: (a) oversee the assessment and management of ICT risks for the Organization; and (b) develop and maintain the information security policy of the Organization and monitor compliance across organizational units; and*
>
> *It was expected that by June 2011, a comprehensive information security framework would have been finalized by OICT. However, since this framework is still in progress, in the absence of the Organization-wide framework or any specific security plans and guidance, DFS developed a departmental ICT security framework and supporting high-level policies in 2009, the implementation of which is being conducted in a phased approach taking into account the risk based priorities as well as existing capacities in field missions. DFS has established mechanisms to monitor the effectiveness of ICT risk management in peacekeeping missions through the various ICT policy directives as well as the ICT organization structure to facilitate effective and timely monitoring of ICT risks in peacekeeping missions. The revised DPKO/DFS Risk Assessment Policy and the standard operating procedures related to ICT Security Governance and Management Structure are in the final stages of approval, copies of which were provided to OIOS.*

C. Mandates and delegation of authority

Local ICT Committees in peacekeeping missions were not functioning

17. The responsibilities of DFS/ICTD and the Local ICT Committees are described as follows:

Table 1: Responsibilities of DFS/ICTD and Local ICT Committees

DFS/ICTD	Local ICT Committee
Supporting OICT in: (i) Establishing ICT architecture and standards; (ii) Planning and implementing major infrastructure improvements for field operations; (iii) Implementing and supporting Organization-wide applications and major shared field applications; (iv) Providing centralized ICT project management support; (v) Coordinating disaster recovery and business continuity planning for the field; (vi) Reviewing and approving ICT field budget submissions; and (vii) Maintaining strategic oversight of the enterprise data centres and major communications facilities, including review and approval of strategic directions	(i) Review, approve and prioritize all ICT initiatives and projects proposed by the mission; (ii) Ensure that initiatives and projects are substantively aligned with departmental or office goals and objectives, and with the achievement of an approved programme of work; and (iii) Consolidate similar ICT requests and works with ICT to reduce duplication of effort.

18. Missions had dedicated local application development units, which, in some cases, developed a high number of local applications. For example, UNOCI and MONUC developed 31 and 43 applications respectively. Some of these applications provided support to critical administrative processes of the missions. However, the following control weaknesses were identified in the development, use and support of these applications:

- Business cases in support of the locally developed applications had not been prepared to detail functional, security, performance and availability requirements. Therefore, these applications had not been reviewed or approved by the Local ICT Committee for ensuring strategic alignment and efficient use of resources.

- Although OICT developed and published a project management handbook and DFS/ICTD prepared corresponding guidelines and templates, the applications developed in the missions did not follow any project management methodology or professional standard for software development.

- The OICT project management handbook provided a methodology and templates to assess the security requirements of the applications. DFS/ICTD also developed an "ICT system security assessment questionnaire" for performing post-implementation security assessments. However,

security assessments were not performed during the development of applications at the mission level.

- Business impact analyses were not performed for assessing the consequences deriving from the unavailability of the locally developed applications. Disaster recovery plans of local applications were either incomplete or had not been tested.

- There was no formal process for identifying and classifying information stored or processed on locally developed applications in accordance with the provisions of the Secretary General's bulletin ST/SGB/2007/6 (Information sensitivity, classification and handling). However, an initiative was launched by the Peacekeeping Information Management Unit of DPKO, DFS/ICTD and the Archives and Record Management Section for developing an information sensitivity toolkit. While the toolkit addressed the requirements established in the Secretary-General's bulletin ST/SGB/2007/6, operating procedures for implementing the toolkit in the missions were not available at the time of the audit.

Recommendation 1

(1) DFS/ICTD should: (a) facilitate the establishment and functioning of Local ICT Committees at the mission level and act as a central coordinating body on all ICT matters; and (b) establish monitoring mechanisms to ensure that peacekeeping missions comply with the Organization's policies and standards for approving business cases.

19. *DFS accepted recommendation 1 stating that guidance will be sent to peacekeeping missions on the establishment of ICT management structures and local ICT review committees and DFS will engage with missions periodically to ensure that no unsanctioned ICT development activities are undertaken.* Recommendation 2 remains open pending receipt of the copy of the memorandum sent to peacekeeping missions and evidence of established monitoring mechanism for the approval of business cases.

Limited deployment of the Field Support Suite

20. Local applications in peacekeeping missions were developed without assessing whether the new enterprise-wide applications being developed in the United Nations Secretariat (Enterprise Resource Planning/UMOJA; Inspira Talent Management; Customer Relationship Management and Enterprise Content Management) would address the same substantive needs, and how these applications could be integrated.

21. DFS created a centralized e-Assets system for sharing information about technology systems developed across the United Nations Secretariat. However, this initiative was not supported by a process instructing missions on when and how to consult the e-Assets system. DFS acknowledged this problem and issued a field application development strategy to all missions in a memo dated 29 June 2009. The same strategy was also reflected in the global field support strategy. One of the components of this strategy was the introduction of a Field Support Suite (FSS), composed of a modular set of applications designed to support work-flow and business functions common to all missions. To facilitate the rapid development of these centralized systems, DFS established a development capacity in UNLB and in Entebbe.

22. The expected benefits of the strategy for centralizing the application development in support of peacekeeping missions' operations, included: (i) quicker implementation; (ii) upgrades and process improvements; (iii) more reliable and stable use; (iv) improved coordination and communication across missions in key areas; and (v) improved security and disaster recovery.

23. FSS initially covered seven applications: i) electronic movement of personnel; ii) personnel check-in; iii) personnel check-out; iv) e-training management system; v) travel expense claims; vi) electronic passenger booking system; and vii) cargo management request. This list was later extended with five additional applications (education grant claims; identification cards; travel authorization forms; eLeave and tracking software assets). Considering the large number of applications in some field missions (i.e. UNOCI, MONUC, UNMIL, UNIFIL developed 31, 43, 34 and 37 applications, respectively), it was not clear whether the current scope of FSS is adequate for addressing the needs of the peacekeeping missions.

24. Furthermore, the deployment and usage rate of the FSS across the missions is behind the initial deployment plan, which had a target date for implementation in all missions by the fourth quarter of 2010. Table 2 shows the deployment status of FSS across the missions based on its implementation as of March 2011. Details of deployment status in each mission are listed in Annex-V.

Table 2: Deployment summary of FSS application across missions

	Deployment Rate of FSS Applications across missions (Number of applications in FSS=12)	
Missions	**Number of deployed FSS applications Q1-2011**	**Forecasted number of deployed applications Q2-2011**
MINUSTAH	3	5 (41%)
MONUSCO	6	8 (66%)
UNIFIL	3	3 (25%)
UNMIL	1	1 (8%)
UNMIS	4	8 (66%)
UNOCI	1	1 (8%)

Recommendation 2

(2) DFS/ICTD should determine the need for extending the scope of Field Support Suite.

25. *DFS accepted recommendation 2 stating that the development and implementation of FSS was conducted in coordination with the UMOJA Team which sees FSS deployment as an effective mechanism to consolidate data and processes in the field. The implementation of FSS modules to all field missions is underway and scheduled for completion in 2012. Its implementation will result in the decommissioning of local systems that arc currently being used to perform similar functions, Local CITS management is kept informed of the enterprise and FSS deployment schedules so that they can adjust the required support and maintenance for local applications accordingly. The scope of the FSS is being extended to meet the business needs of the field and the selection of enhancements and additional modules have been planned in alignment with the Global Field support Strategy as well as through engagement of Headquarters and mission management. FSS is also under consideration as a front end tool to facilitate the data collection and conversions required for UMOJA and International Public Sector Accounting Standards (IPSAS) implementation*. Recommendation 2 remains open pending receipt of the assessment conducted by DFS/ICTD for determining the scope of FSS.

D. Regulatory framework

Policies, procedures and guidelines were out-dated and not easily accessible

26. Peacekeeping missions did not consistently document or follow the policies, standard operating procedures and guidelines related to ICT operations. Periodic ICT security risk assessments were not performed and controls for ensuring compliance with minimum security standards were not in place in the majority of the missions. DFS/ICTD developed an ICT security framework including security policies and guidelines. However these documents were not accessible from the Policy and Practice Database of DFS and DPKO. In addition, the ICT security framework was not supported by proper security planning and risk management processes.

27. DFS/ICTD developed ICT policies and guidelines in accordance with the United Nations provisions established in the Secretary-General's bulletin ST/SGB/2004/15 on the use of information and communications technology resources and data; ST/SGB/2007/6 on information sensitivity, classification and handling; and standard best practices for information security (i.e., ISO 27000 series). These policies were formally communicated to the missions with the memo reference 2009-UNHQ-026289. However, ICT procedures in peacekeeping missions were not aligned with those defined at Headquarters by OICT and DFS/ICTD. In addition, there was no formal review process for ensuring periodic update of policies and procedures in the missions.

28. Although ICT policy directives were approved by the Director of DFS/ICTD in November 2009, they had not been updated and did not reflect the latest provisions established with the new ICT strategy of the United Nations Secretariat (A/62/793). In addition, ICT policies and guidelines were not accessible from the Policy and Practice Database of DFS and DPKO, which has a search capability. Some of the policies were published on DFS/ICTD intranet site however the following guidelines and standard operating procedures were not published:

- Draft ICT access control policy (working draft);
- ICT system security assessment questionnaire;
- Equipment disposal guideline;
- Recovery of ICT resources of data; and
- Draft guideline for ICT security model and life cycle.

29. **DFS could improve the awareness of ICT-related policies, standard operating procedures and guidelines by publishing them on the intranet web site of DFS/DPKO containing the peacekeeping policy framework.** *DFS stated that policies, standard operating procedures and guidelines which are still in draft form have to be reviewed and finalized before they are posted on the DFS/DPKO intranet. However DFS/ICTD conducts security awareness programmes and advises all missions of current documentation that are posted on the DFS/ICTD webpage.*

Absence of a global ICT security plan

30. In four of the six missions audited, clear responsibilities for ICT security were not defined and assigned to a dedicated staff member. Additionally, in all audited missions ICT security procedures were either not documented or not implemented, resulting in several cases of non-compliance.

31. Maintaining the integrity of information and protecting ICT assets require an effective security management process to minimize the business impact of security vulnerabilities and incidents. In this regard, OIOS tested whether the following controls existed and functioned as expected:

- Establishing an information security framework;
- Aligning information security strategies with business strategies;
- Assigning ICT security roles and responsibilities;
- Defining ICT security policies, standards and procedures;
- Conducting periodic analysis of vulnerabilities and implementing mitigating controls;
- Translating risk and compliance requirements into an overall ICT security plan (security policies and procedures together with appropriate investments in services, personnel, software and hardware);
- Testing and monitoring ICT security mechanisms; and
- Implementing oversight processing of the information security function.

32. DFS/ICTD developed a security, business continuity and emergency preparedness strategy as an umbrella policy describing the ICT policy and security framework. This document contained basic rules for implementing DFS policies addressing ICT security and business continuity threats, standards, procedures, baselines, guidelines and plans. The policy also defined processes, accountabilities, roles and responsibilities. However, the document was outdated and did not reflect the latest Organization-wide ICT strategy. In accordance with this document, DFS/ICTD has the responsibility to assist data owners in designing and maintaining security and continuity plans for ensuring that adequate level of security and availability is provided for all data.

33. In 2008, DFS/ICTD developed a project security lifecycle framework. This framework described the required ICT security activities for each phase of system development, with requirements for access control, awareness and training, logging, configuration management, contingency planning, identification and authentication, system and service acquisition, physical and environmental protection, and media protection. These controls were mapped against DFS policies and standards. The framework, however, was not supported by adequate procedures for guiding peacekeeping missions through its adoption and implementation. Although DFS/ICTD prepared a work plan for its security section, this plan included a list of activities limited to the section and, therefore, did not contain the necessary information about the actions that peacekeeping missions are expected to take for implementing the ICT security framework. A comprehensive ICT security plan defining the activities of the peacekeeping missions was lacking.

34. In the period 2008-2010, DFS/ICTD organized 19 ICT security training initiatives in UNLB. These were mostly focused on the security of specific software or general security certifications of the mission staff.

35. DFS/ICTD developed a draft (1 March 2011) ICT security model providing instructions to CITS sections in each mission for establishing an ICT specific security governance and management structure.

This proposed structure comprised centralized security controls and decentralized security administration functions. Responsibilities for these functions were described as follows:

- A centralized control function, encompassing policies, procedures, overall direction, prioritization and establishment of organizational structures designed to provide reasonable assurance that the department's security objectives will be achieved, undesired events prevented and risks minimized to acceptable levels; and

- A decentralized security administration for the implementation and operation of ICT security in accordance with policy and standards requirements in the missions and UNLB, including day to day operational activities.

36. The ICT security and compliance function in several peacekeeping missions were understaffed. DFS/ICTD supported the establishment of field missions' information security units in the document "CITS Vision for the period 1 July 2008 - 30 June 2009". DFS/ICTD stated that although dedicated ICT security resources were requested in the context of the support account budget, these resources were not approved by the General Assembly. DFS/ICTD developed ICT security job descriptions and submitted them to the Office of Human Resources Management (OHRM). At the time of the audit, their approval was still pending. Once approved, these job descriptions will be used as the starting point for issuing ICT security vacancy announcements in all peacekeeping missions.

37. The issue of ICT security governance and information security framework has been discussed by the ICT-management coordination group (ICT-MCG) of the United Nations Secretariat, in February 2011. The following decisions were made:

- The front office of OICT will include information security in a new Secretary-General's bulletin being developed (estimated issuance Dec 2011);

- OICT will complete a comprehensive information security framework by June 2011; and

- All Departments, Offices Away From Headquarters and Regional Commissions' ICT Units will initiate information security discussions with their Local ICT units, with a view at advancing business ownership of risk and cost mitigation.

38. *DFS stated that it will develop departmental security plans following the receipt of the global ICT security plan from OICT. In the absence of such a plan, DFS/ICTD will continue the phased implementation of the Departmental security framework within its available capacities.* Based on the review of the DFS ICT security model and phased implementation initiated by DFS/ICTD, OIOS is not issuing additional recommendations in this area.

E. Oversight

Compliance with DFS policies and standard operating procedures was not monitored

39. The audits conducted in missions during the period 2008-2011 showed that, in most cases, missions did not follow standard operating procedures in alignment with the policies and guidelines established at Headquarters by DFS and OICT. For example, five of the six audited missions did not implement the criteria defined in the DFS access control policy resulting in several security weaknesses. The list of recommendations addressing cases of non-compliance is included in Annex IV. Missions accepted all audit recommendations issued.

40. In 2009, DFS/ICTD established an ICT security compliance and certification policy defining compliance requirements in accordance with the United Nations security policies and standards (including technical standards). According to this policy, there should have been annual compliance planning, periodic assessments and compliance reporting.

41. In order to strengthen the compliance capacity on ICT security matters, DFS/ICTD issued guidance to the peacekeeping missions for establishing ICT security focal points and usage of the ICT security reporting workspace. However, DFS/ICTD had not established a systematic monitoring and review process for identifying cases of non-compliance of peacekeeping missions with the established policies, procedures and guidelines, and assessing their causes. Missions either did not fully document the local standard operating procedures for their ICT operations or did not implement measures based on existing policies causing non compliance.

42. **DFS could improve the monitoring process of ICT security in peacekeeping missions by establishing reporting requirements, frequency and metrics.** *DFS stated that Mission ICT units develop their work plans in response to strategic guidance from Headquarters, mission mandates and operational imperatives. Missions are discrete programmatic entities. As such, DFS/ICTD monitors the actions taken by missions in respect to strategic guidance. While the elements of their work programme related to operational imperatives must be executed in accordance with policies and standards established by United Nations Headquarters, they are not subject to monitoring by DFS/ICTD.*

The ICT governance, risk and compliance (GRC) system is not supported by a business case defining strategy and scope

43. DFS/ICTD purchased in June 2010 a governance, risk and compliance (GRC) software for supporting, integrating and aligning its governance, risk assessment and compliance activities. DFS/ICT described the objectives of this initiative as follows:

- Improve compliance with security policies and standards;
- Formulate, review, publish and distribute security policies;
- Map security controls to policies;
- Report on policy compliance department-wide;
- Enhance field missions' capabilities to more effectively address malware threats;
- Improve DFS/ICTD's capability to effectively identify and address ICT security risk;

- Maintain an inventory of ICT assets and asset classifications; and

- Conduct risk assessments and compliance reporting through automatic collection and evaluation of data related to vulnerabilities and configuration of ICT resources.

44. A project of this nature is usually a large and complex initiative involving multiple stakeholders, platforms, technologies and locations. These initiatives usually involve a large number of staff and include asset-based risk assessments, threat and dependency modeling, technical auditing and gap analysis. This complexity requires a clear project strategy, scope and adequate involvement of resources from missions. However, DFS/ICTD did not develop a business case for this project and did not define a project scope, requirements and plan. DFS/ICTD did not have the required documentation (i.e. business case, project plan, statement of work, etc.) in support of its acquisition of this application.

45. Concurrently, OICT has been developing a proof of concept for establishing a Secretariat-wide ICT enterprise risk, governance and compliance platform. The two initiatives being undertaken by OICT and DFS in this domain were not adequately coordinated, exposing the Organization to risks of duplication of investments and waste of resources.

Recommendation 3

(3) DFS/ICTD should: (i) ensure that its application for governance, risk and compliance (GRC) is supported by a documented business case in accordance with the established ICT project management procedures; and (ii) implement mechanisms for monitoring the compliance of peacekeeping missions with ICT policies.

46. *DFS partially accepted recommendation 3 stating that a business case is not required for projects under $250,000, in accordance with OICT's portfolio management. Since the cost of the GRC project is below the threshold of $250,000, the procedure followed by DFS/ICTD was in compliance with the above quoted guidance. DFS further stated that the implementation of mechanisms for monitoring the compliance of peacekeeping missions with ICT policies is dependent on the development of the platform (E-GRC, electronic governance, risk and compliance) planned by OICT.*

47. The DFS estimate of the GRC project cost does not include the cost of staff required for the GRC system implementation (both Headquarters and peacekeeping missions). The draft documentation prepared by DFS/ICTD indicates that the GRC implementation will require two ICT security officers and one or two ICT security focal points in each field operation. Adding the annual cost of two staff members (i.e., professional staff at P/3 level), which is approximately $154,000, brings the total cost of the initiative to $308,000. This estimate is well above the threshold of $250,000 required for the preparation of the high level business case. Furthermore, the correct determination of project costs is a necessary element for supporting OICT in completing its proof of concept and deciding which application to adopt for this function. Recommendation 3 remains open pending receipt of the documented high level business case in support of the GRC project and evidence of mechanisms implemented for monitoring compliance of peacekeeping missions with ICT policies.

F. Business continuity and disaster recovery planning

Business continuity and disaster recovery need improvement

48. Business continuity and disaster recovery plans in peacekeeping missions were not documented and tested. However, improvements have been recently made by DFS and DPKO with the establishment of coordination and guidance mechanisms. In 2011, DFS and DPKO's business continuity coordination team established coordination processes and guidelines. Business continuity planning methodology, tools and templates for peacekeeping missions were prepared and business continuity planners of the missions were trained. Peacekeeping missions have initiated BC/DR planning activities and expect to complete them by the end of 2011.

49. In general, in the the six peacekeeping missions audited, business impact analyses were not performed and critical business processes, disaster recovery scenarios and required resources not defined. The disaster recovery plans of the missions were not aligned with their business continuity requirements. Disaster recovery plans were partially tested (i.e., did not include all the defined scenarios) and the results not documented.

50. In November 2010, DFS and DPKO, in coordination with the Department of Management (DM), developed a business continuity planning methodology, tools and templates for peacekeeping missions. UNMIL was selected as pilot mission. A workshop was organized in UNMIL for the purpose of training staff on the methodology and tools as well as performing the activities such as business continuity risk assessment; identification of critical business processes, key recovery assets and core applications; documenting business continuity plan and disaster recovery plan; and performing the test exercise. The workshop was successfully completed with expected outputs.

51. Based on the feedback from the UNMIL workshop, the DPKO-DFS business continuity coordination team performed a formal analysis of training needs for defining competencies and generic job profiles of the business continuity planners. In April 2011, the team organized a course for training business continuity planners in the field missions. The training was held in UNLB and focused on the policy, methodology, tools and techniques that business continuity planners should be following. DPKO, DFS and the Department of Political Affairs (DPA) were involved in the coordination of the training. There were 21 participants from 15 field missions. Some field missions were unable to send participants to the training due to the lack of funding.

52. DFS/DPKO issued a memo (14 April 2011) to peacekeeping missions requesting development of business continuity plans by 30 June 2011 and their submission to Headquarters for quality review. It was also planned that some missions, due to their size and complexity, would receive direct assistance from the business continuity coordination team. United Nations Assistance Mission in Afghanistan (UNAMA) and UNOCI have not been included in the June 2011 deadline because of the current crisis situation in these missions.

53. The disaster recovery coordination team of DFS/DPKO developed a plan template and issued a comprehensive questionnaire to all missions for collecting information about their critical applications, infrastructure (hardware and software), location of data, test exercises and test results. Members of the disaster recovery coordination team participated in the business continuity workshops in both UNMIL and UNLB.

54. Since business continuity plans of the missions are being developed, existing disaster recovery plans need to be updated and aligned upon completion of the business continuity requirements, including

critical information and required recovery time and point objectives. Although the disaster recovery coordination team prepared a standard disaster recovery plan template, currently not all mission disaster recovery plans were in standard template. Results of the disaster recovery test activities were not reported in a standard format.

Recommendation 4

(4) DFS/ICTD should complete the disaster recovery plans of all peacekeeping missions by including: (i) the list of mission critical applications; (ii) the definition of recovery time and point objectives; (iii) alignment with the mission's business continuity plans; and (iv) a standard template for reporting disaster recovery test results.

55. *DFS accepted recommendation 4 stating that guidance for disaster recovery plans is being developed and will be communicated to the field missions.* Recommendation 4 remains open pending receipt of mission disaster recovery plans documenting critical applications, recovery time, and point objectives, and a standard template for reporting disaster recovery test results.

G. Summary of control weaknesses identified in the audits of peacekeeping missions

56. The systemic issues identified in the peacekeeping missions, corresponding audit recommendations and status are listed in Table 2.

Table 2. Control weaknesses identified in the audits of ICT governance and security management in peacekeeping missions

Systemic control weakness	Critical/Important/ Opportunity for Improvement	Action Recommended	Status (as of November 2011)
Lack of ICT strategic planning and monitoring	Critical	Develop mission specific ICT strategy and monitoring procedures	MONUSCO: Implemented UNIFIL: In progress UNMIL: In progress UNMIS: Implemented UNOCI: In progress
Lack of ICT risk management	Important	Establish an ICT risk management framework for identifying risks and implement mitigating controls	MINUSTAH: In progress MONUSCO: Implemented UNIFIL: Implemented UNMIL: Implemented UNMIS: Closed without implementation UNOCI: In Progress
ICT Committee not established or non functioning	Important	Establish an ICT Local Committee in accordance with the governance framework issued by OICT	MINUSTAH: In progress MONUSCO: Implemented UNIFIL: Implemented UNMIL: In progress UNMIS: Implemented UNOCI: In progress

Lack of project management methodology	Important	Adopt and implement the ICT project management methodology “Prince II”, established by OICT	MONUSCO: Implemented UNIFIL: Implemented UNMIL: In progress UNMIS: Implemented UNOCI: In progress
Incomplete ICT standard operating procedures	Important	Complete, document and monitor the implementation of standard procedures for ICT operations	MINUSTAH: In progress MONUSCO: Implemented UNIFIL: In progress UNMIL: In progress UNMIS: Implemented UNOCI: In progress
Inadequate ICT security management	Critical	Assign responsibilities for conducting periodic ICT security vulnerability testing and implement corresponding mitigating measures	MONUSCO: Implemented UNIFIL: Implemented UNMIL: In progress UNMIS: Closed without implementation UNOCI: In progress
Incomplete and untested business continuity and disaster recovery plans	Critical	Complete the mission business continuity and disaster recovery plans with the list of critical functions and supporting systems. Assign responsibilities and conduct periodic tests of the plans.	MINUSTAH: In progress MONUSCO: In progress UNIFIL: In progress UNMIL: In progress UNMIS: Implemented UNOCI: In progress

ANNEX I
STATUS OF RECOMMENDATIONS
Audit of ICT governance and security management in peacekeeping missions

Recom. no.	Recommendation	Risk category	Critical/ important	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
1	DFS/ICTD should: (i) facilitate the establishment and functioning of Local ICT Committees at the mission level and act as a central coordinating body on all ICT matters; and (ii) establish monitoring mechanisms to ensure that peacekeeping missions comply with the Organization's policies and standards for approving business cases.	Governance	Important	O	Receipt of the copy of the memorandum sent to peacekeeping missions and evidence that monitoring mechanisms for the approval of business cases have been established satisfactorily.	31 Dec 2011
2	DFS/ICTD should determine the need for extending the scope of Field Support Suite.	Information Resources	Important	O	Receipt of the assessment conducted by DFS with the regard to the extension of the FSS.	31 Dec 2014
3	DFS/ICTD should: (i) ensure that its application for governance, risk and compliance (GRC) is supported by a documented business case in accordance with the established ICT project management procedures; and (ii) implement mechanisms for monitoring the compliance of peacekeeping missions with ICT policies.	Compliance	Important	O	Receipt of the documented high-level business case in support of the GRC project and evidence of mechanisms implemented for monitoring compliance of peace keeping missions with ICT policies.	Not indicated

[1] Critical recommendations address significant and/or pervasive deficiency or weakness in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

4	DFS/ICTD should complete the disaster recovery plans of all peacekeeping missions by including: (i) the list of mission critical applications; (ii) the definition of recovery time and point objectives; (iii) alignment with the mission's business continuity plans; and (iv) a standard template for reporting disaster recovery test results.	Operational	Important	O	Receipt of the mission disaster recovery plans which include list of mission critical applications, recovery time and point objectives, standard template for reporting disaster recovery test results.	31 Dec 2011

[1] Critical recommendations address significant and/or pervasive deficiency or weakness in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

ANNEX II
OPPORTUNITIES FOR IMPROVEMENT
Audit of ICT governance and security management in peacekeeping missions

Para. no.	Opportunity for improvement	Client's comments
27	DFS/ICTD could improve the awareness of ICT-related policies, standard operating procedures and guidelines by publishing them in the intranet web site of DFS/DPKO containing the peacekeeping policy framework.	*DFS stated that Policies, SOPs and guidelines which are still in draft form have to be reviewed and finalized before they are posted on the DFS/DPKO intranet. However DFS/ICTD conducts security awareness programmes and advises all missions of current documentation that are posted on the DFS/ICTD webpage.*
40	DFS/ICTD could improve the monitoring process of ICT security in peacekeeping missions by establishing reporting requirements, frequency and metrics.	*DFS stated that Mission ICT units develop their work plans in response to strategic guidance from Headquarters, mission mandates and operational imperatives. Missions are discrete programmatic entities. As such, DFS/ICTD monitors the actions taken by missions in respect to strategic guidance. While the elements of their work programme related to operational imperatives must be executed in accordance with policies and standards established by United Nations Headquarters, they are not subject to monitoring by DFS/ICTD.*

ANNEX-III
Field Support Suite Implementation Status (March 2011)

Mission	CI	CO	eMOP	ePBS	F10	eTMS	eLeave	e-CMR	e-CBS	Ed. Grant	ID Card	PT8
MINUSTAH	Deployed	Deployed	Impl. In Progress (Q2 2011)	Impl. In Progress (Q2 2011)		In Use	Not Planned					
MONUSCO	In Use	In Use	In Use (partially)	In Use (partially)		In Use	Not Planned	Q2 2011	Q2 2011	In Use		
UNIFIL	Deployed	Deployed				In Use	Not Planned					
UNMIL										In Use		
UNMIS	Impl. In Progress (Q2 2011)	Impl. In Progress (Q2 2011)	In Use (Partially)	In Use (Partially)		In Use	Not Planned	Q2 2011	Q2 2011	In Use		
UNOCI										In Use		

Legend:
CI: Personnel check-in
CO: Personnel check-out;
eMOP: Electronic movement of personnel
ePBS: Electronic passenger booking system
F10:: Travel expense claims
eTMS: Training management system
eLeave: Leave request system
e-CMR: Cargo management request
E-CBS: Tracking software assets
Ed-Grant:: Education grant claim
ID-Card: ID card system
PT8:Travel authorization form