



AUDIT

OF

INFORMATION AND COMMUNICATIONS TECHNOLOGY MANAGEMENT

IN

UNDP AFGHANISTAN

Report No. 1407
Issue Date: 13 November 2014

Table of Contents

Executive Summary	i
I. About the Office	1
II. Good practice	1
III. Audit results	1
A. Organization/Infrastructure	2
B. Disaster recovery	4
C. Configuration/Software	5
Definitions of audit terms - ratings and priorities	7

Report on the audit of Information and Communications Technology Management in Afghanistan Executive Summary

The UNDP Office of Audit and Investigations (OAI) conducted an audit of UNDP Afghanistan (the Office) from 17 August to 4 September 2014. The audit aimed to assess the adequacy and effectiveness of the governance, risk management and control processes relating to the management of information and communications technology (ICT). Specifically, the audit assessed the extent to which the Office effectively manages its ICT resources and complies with ICT-related UNDP regulations, rules, policies and procedures, particularly relating to the Disaster Recovery Plan, systems security, and software licenses.

The audit covered the activities of the Office from 1 January 2013 to 30 June 2014. The Office recorded programme and management expenditures totalling \$740 million in 2013 and \$387 million in the first half of 2014.

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

Overall audit rating

OAI assessed the Office as **satisfactory**, which means, "Internal controls, governance and risk management processes were adequately established and functioning well. No issues were identified that would significantly affect the achievement of the objectives of the audited entity."

Good practice

The Office had a dedicated system in place for managing its helpdesk, allowing for real-time tracking of the status of requests, production of management information regarding common issues and solutions, and detailed cost recovery regarding work done for projects (Refer to page 1 for details).

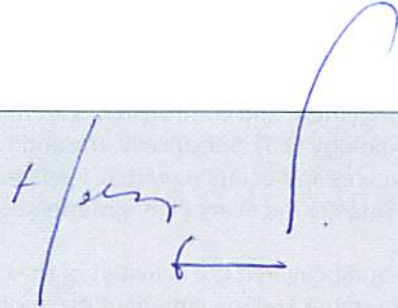
Key recommendations: Total = 4, high priority = 0

The audit did not result in any high (critical) priority recommendations. There are four medium (important) priority recommendations, which means, "Action is required to ensure that UNDP is not exposed to risks that are considered moderate. Failure to take action could contribute to negative consequences for UNDP." These recommendations include actions to address the delay in implementing the defined ICT governance structure, inadequate oversight and coordination over ICT infrastructure of development projects, lack of documentation regarding testing of the Disaster Recovery Plan and back-up of data, and the development/purchase of computer applications without sufficient justification.

Management comments and action plan

The Resident Representative accepted all of the recommendations and is in the process of implementing them. Comments and/or additional information provided had been incorporated in the report, where appropriate.

Issues with less significance (not included in this report) have been discussed directly with management and actions have been initiated to address them.



Helge S. Osttveiten
Director
Office of Audit and Investigations

I. About the Office

The Office is located in Kabul, Afghanistan (the Country). The Office is UNDP's largest programme, globally delivering close to 20 percent of all of UNDP's delivery in one of the world's most insecure environments. The challenges of the Office are significant, both internally and externally, as are the opportunities for sustainable development. The Office's programme and management expenditures totalled \$740 million in 2013 and \$387 million in the first half of 2014.

The Office's ICT Unit is responsible for providing ICT support and services to more than 700 users in Kabul and seven regional offices. The services provided include: (a) development of in-house applications to support the Office's aim in improving efficiency in operations, (b) management of ICT infrastructure, and (c) maintenance of the telephone system. At the time of the audit, the ICT Unit was composed of 1 national officer (head of the unit), 1 international staff member, 1 General Service staff member, and 6 service contract holders. The ICT Unit had three vacant posts.

UNDP's Office of Information Systems and Technology conducted a site-visit in December 2013 to review all aspects of the Office's ICT set-up and made several recommendations to improve the Office's ICT management, including conducting periodic testing of the Office's Disaster Recovery Plan.

II. Good practice

OAI identified a good practice, as follows:

Organization/infrastructure helpdesk management

The Office had a dedicated system in place for managing its helpdesk. Requests for support were entered into an online application, which was used to assign the requests to the first available helpdesk staff member. The online application allowed for real-time tracking of the status of requests through a dashboard presented on a screen. The application also allowed for the production of management information regarding common issues and solutions as well as the speed of the services provided, all used to improve the functioning of the helpdesk. Furthermore, the system allowed for correct cost recovery for the work done for projects, as it tracked issues by project and time spent on resolving these issues.

III. Audit results

Satisfactory performance was noted in one area:

- Systems Security – Ownership & Data Access. The physical security of the Office's server room as well as the storage site for back-up tapes was more than adequate, and the rooms were equipped with smoke detectors and temperature controls. Access to the Office's network was protected by means of a firewall. Furthermore, data was protected by a centrally installed and enforced anti-virus system and back-up software.

OAI made four recommendations ranked medium (important) priority.

Low priority issues/recommendations were discussed directly and agreed with the Office and are not included in this report.

Medium priority recommendations, arranged according to significance:

- (a) Set up the ICT governance structure as outlined in the ICT governance document and have the ICT Board carry out the responsibilities assigned to them (Recommendation 1).
- (b) Improve disaster recovery documentation and maintenance of back-up tapes (Recommendation 3).
- (c) Improve oversight over the ICT infrastructure of development projects (Recommendation 2).
- (d) Conduct a needs assessment and/or cost-benefit analysis before purchasing/developing software applications (Recommendation 4).

The detailed assessment is presented below, per audit area:

A. Organization/Infrastructure

Issue 1 Defined ICT governance structure not fully implemented

According to the Information Technology Governance Institute, a recognized professional body, effective ICT governance will result in improved business performance as well as compliance with external requirements. Effective ICT governance requires a range of enablers with carefully prescribed roles, responsibilities and accountabilities that fit the style and operational norms specific to an operational entity. These include an appropriate culture and behavior, guiding principles and policies, organizational structures, well-defined and managed governance and management processes, the information required to support decision making, supporting solutions and services, and appropriate governance and management skills.

The Office had prepared a comprehensive document outlining the set-up and implementation of ICT governance in the Office, but the governance structure had not been implemented at the time of the audit. One of the governance bodies identified in the ICT governance document was the ICT Board. Though the ICT governance document had been prepared in July 2013, the first meeting of the ICT Board did not take place until July 2014. Consequently, none of the responsibilities assigned to the ICT Board (e.g. approval of the ICT work plan, review of business automation requirements, and review of the progress of ICT projects) had been carried out.

According to the Office's management, meetings with heads of units to discuss ICT issues had taken place in the period between drafting the ICT governance document and the first meeting of the ICT Board, and that these meetings could have been considered the predecessors to the ICT Board. However, these meetings did not lead to implementation of the responsibilities assigned to the ICT Board, which was only established in July 2014.

Not implementing the ICT governance structure could negatively impact the Office's leverage of its ICT resources.

Priority	Medium (Important)
Recommendation 1:	
Set up the ICT governance structure as outlined in the ICT governance document and have the ICT Board carry out the responsibilities assigned to them.	
Management action plan:	
The Office will implement the ICT governance structure as outlined in the ICT governance document and	

have the ICT Board carry out the responsibilities assigned to them.

Up to the time of the ICT audit, ICT matters were discussed in the weekly meetings of the heads of operations units, which also included project Operations Managers on a bi-weekly basis. Following the audit, the second formal ICT Board meeting was held on 15 September 2014. In this meeting, the Terms of Reference of the Board were discussed. The Terms of Reference will be finalized in the third meeting scheduled on 6 November 2014.

Estimated completion date: 2 January 2015

Issue 2 Inadequate oversight over ICT infrastructure of development projects

To increase the effective and efficient use of ICT resources, its management must not be limited to ICT resources used by the Office, but where applicable, include ICT resources used by development projects as well.

The ICT Unit had limited to no oversight over the ICT infrastructure (ICT systems/ICT procurement/disaster recovery etc.) of the development projects managed by the Office, specifically with regard to those projects that had their own ICT staff. Furthermore, coordination with regard to management of the ICT infrastructure between the ICT Unit and ICT staff of the development projects was limited. Although the projects managed by the Office might be responsible for their own ICT infrastructure, OAI was of the opinion that the Office as well as the projects could benefit from coordination and/or oversight by the ICT Unit to improve efficiency and effectiveness, by for example, coordinating maintenance visits to the region and/or ensuring that all projects have a Disaster Recovery Plan in place, or where possible, piggyback on the Office's Disaster Recovery Plan.

Lack of coordination and oversight with regard to the use of ICT resources within the Office as well as the projects managed by the Office could lead to inefficient and ineffective use of ICT resources, ultimately leading to additional costs for the organization.

Priority	Medium (Important)
Recommendation 2:	
Improve oversight over the ICT infrastructure of development projects by:	
<ul style="list-style-type: none"> (a) having the Office's ICT Unit carry out oversight over the ICT infrastructure of development projects to the extent possible; and (b) improving coordination between the ICT Unit and ICT staff of development projects with regard to the implementation and management of the development projects' ICT infrastructure. 	
Management action plan:	
The Office has already taken action to ensure compliance with the recommendation. The Office will take the following actions to implement this recommendation:	
<ul style="list-style-type: none"> (a) A memo from the Senior Deputy Country Director – Operations will be sent to all Project Managers/Programme Officers, indicating that all ICT related procurement requests need to be cleared by the Office's ICT Unit. Equally, at the project design stage and annual work plan stage, provisional budgets for ICT goods and services should be discussed and cleared by the ICT Unit. 	

Further, the ICT Unit will conduct spot checks of the projects' ICT infrastructure, including disaster risk management provisions, and will provide recommendations for improvement, where needed.

- (b) The ICT Unit is also increasing its involvement in securing economies of scale by being involved as key participants in the development of the Terms of Reference and subsequent evaluation of the Long Term Agreement procurement process for the provision of Fiber Optic-based and VSAT internet services covering all of the projects' internet connectivity needs. This process is expected to achieve more than 30 percent savings in connectivity charges. The Long Term Agreement procurement process is in its final stages and is in the process of being submitted to the Advisory Committee on Procurement.

Estimated completion date: 8 February 2015

B. Disaster recovery

Issue 3 Lack of documentation regarding testing of Disaster Recovery Plan and back-up of data

According to the 'UNDP Programme and Operations Policies and Procedures,' the Disaster Recovery Plan should include information about business requirements, back-up arrangements, and recovery procedures. In addition, Country Offices need to ensure that the plan is kept up-to-date and is regularly tested. Furthermore, the 'UNDP Programme and Operations Policies and Procedures' prescribe that the maximum Recovery Point Objective (description of the acceptable amount of data loss; usually measured in days, occasionally in hours) shall not be more than 1 week or 168 hours and that a backup schedule for every critical ICT system shall be developed in accordance with the Recovery Point Objective for that system. Backup media that facilitates such Recovery Point Objective shall be stored off-site.

Tests of the Office's Disaster Recovery Plan conducted by the ICT Unit were not adequately documented, making it impossible for OAI to assess whether the objectives of the test had been achieved and, where necessary, appropriate action had been taken to address deficiencies identified during the test. The Office had provided a write-up of two tests conducted in 2013 and 2014. However, a review of the documentation provided showed that it had been prepared on 1 September 2014 while the audit was ongoing (18 August to 4 September 2014) and not at the time of the test (15 August 2013 and 4-7 March 2014), thereby defeating the purpose of documenting test results. Furthermore, back-up of data was not properly documented. No information was kept regarding what was backed-up and when, nor was the content of the off-site safe containing all back-up tapes documented. Additionally, it was noted that the latest version of the back-up of user data stored in the safe was more than two months old.

Without an up-to-date and regularly tested Disaster Recovery Plan, and without properly documented back-up data, it would be difficult for the Office to recover its information systems in the event of a systems failure or disaster.

Priority	Medium (Important)
Recommendation 3: Improve disaster recovery documentation and maintenance of back-up tapes by: <ul style="list-style-type: none"> (a) documenting testing of the Disaster Recovery Plan timely and adequately; (b) keeping a log of the data back-ups performed by the ICT Unit, including an overview of the back-up tapes stored in the off-site safe; and (c) storing the latest version of back-up tapes, which preferably should be not more than one week old, in the off-site safe. 	
Management action plan: The Office has already taken action to ensure compliance with the recommendation. <ul style="list-style-type: none"> (a) Starting 15 November 2014, the standard Disaster Recovery Plan testing template will be used to document the Disaster Recovery Plan test results on a quarterly basis. (b) Implemented. Following the audit recommendation, a log recording system for the data centre in the main office and HUB offices (location of offsite storage) was established on 15 September 2014. A log recording system for back-ups has been created to explain the details, such as time and type of the back-up, including its testing information. (c) Implemented. Back-ups are done on a daily and weekly basis. Back-up tapes in the off-site safe are replaced on a weekly basis. This task is carried out by the LAN administrators. 	
Estimated completion date: 15 November 2014	
OAI Response OAI acknowledges the action taken by management; this will be reviewed at a later stage as part of the standard desk follow-up process of OAI.	

C. Configuration/Software

Issue 4 Development/purchase of computer applications without sufficient justification

As per UNDP's Financial Regulations and Rules, the following general principles must be given due consideration while executing procurement on behalf of the organization: best value for money; fairness, integrity, transparency; effective international competition, and the interest of UNDP. In line with these principles offices should in case of development or purchase of ICT systems start with a needs assessment/feasibility study to ensure that the system to be developed/purchased addresses actual needs of the office and does so in the most efficient and effective way.

The Office had purchased a number of software applications (e.g. vehicle tracking system priced at approximately \$138,000 and room management system priced at \$5,000) and developed (or was in the process

of developing) a number of SharePoint applications (e.g. procurement process automation) for which the Office had recruited two individuals. All purchases and developments were driven by needs identified by the Senior Deputy Country Director – Operations. However, evidence of a proper needs assessment and/or cost-benefit analysis could not be provided by the Office. Furthermore, the ICT Unit was only involved in the procurement process after the decision to purchase the vehicle tracking system had been made. The valid issues raised by the ICT Unit relating to the purchase and implementation of the system had not been addressed. The concerns included the potential consequences/effect the use of the system might have on the performance of the Office's network (system is web-based), questions regarding data security and back-up and questions regarding the potential future involvement of the ICT Unit with the system (in case the Office decided to have the system hosted in-house).

Office management indicated that the vehicle tracking system was purchased to facilitate cost recovery of vehicle usage for transportation provided to national staff to and from the Office, for which they had to pay. The tracking system would allow the Office to easily allocate usage of the vehicles to individuals. Additionally, management indicated that the added advantage of this system was its ability to track vehicles and movement of staff from a security perspective. Furthermore, it was argued that given the number of vehicles in use by the Office (around 34) and the cost of each individual vehicle (around \$200,000), the cost of the system was relatively low.

Although the cost of the system might be considered low in relation to the total cost of all vehicles managed by the Office, OAI did not consider this to be a justification for purchasing the system without a needs assessment and/or cost-benefit analysis. Finally, although it was mentioned that one of the reasons for purchasing the vehicle tracking system was its ability to track vehicles and movement of staff from a security perspective, at the time of the audit the system was not used for this purpose, diminishing its usefulness.

Purchasing and/or developing software applications without conducting a needs assessment and/or cost-benefit analysis increases the risk that the selected system might not be the most efficient and/or effective solution for the problem at hand, leading to inefficient/ineffective use of resources.

Priority	Medium (Important)
Recommendation 4:	
Conduct a needs assessment and/or cost-benefit analysis before purchasing/developing software applications. Once the ICT Board is functioning, the proposed actions in this regard should be assessed and endorsed by the ICT Board.	
Management action plan:	
The Office will ensure compliance with the recommendation for future software development opportunities.	
As mentioned under Recommendation 2, a memo will be issued that requires that all ICT related procurement plans and actions be cleared by the ICT Unit. The ICT Unit will review the plans in view of needs and cost-benefits. The ICT Board will set criteria for the types of procurement (e.g. purchasing price threshold) that will need to be discussed and approved by the ICT Board.	
Estimated completion date: 8 February 2015	

Definitions of audit terms - ratings and priorities

A. AUDIT RATINGS

- **Satisfactory** Internal controls, governance and risk management processes were adequately established and functioning well. No issues were identified that would significantly affect the achievement of the objectives of the audited entity.
- **Partially Satisfactory** Internal controls, governance and risk management processes were generally established and functioning, but needed improvement. One or several issues were identified that may negatively affect the achievement of the objectives of the audited entity.
- **Unsatisfactory** Internal controls, governance and risk management processes were either not established or not functioning well. The issues were such that the achievement of the overall objectives of the audited entity could be seriously compromised.

B. PRIORITIES OF AUDIT RECOMMENDATIONS

- **High (Critical)** Prompt action is required to ensure that UNDP is not exposed to high risks. Failure to take action could result in major negative consequences for UNDP.
- **Medium (Important)** Action is required to ensure that UNDP is not exposed to risks that are considered moderate. Failure to take action could contribute to negative consequences for UNDP.
- **Low** Action is desirable and should result in enhanced control or better value for money. Low priority recommendations, if any, are dealt with by the audit team directly with the Office management, either during the exit meeting or through a separate memo subsequent to the fieldwork. Therefore, low priority recommendations are not included in this report.