UNOPS

Operational excellence for results that matter

Internal Audit and Investigations Group

IAIG Activity Report for 2017 **Annex 1**

Unresolved audit recommendations issued more than 18 months before 31 December 2017

Functional area/audit recommendation description
Finance
1. Strengthen the quality assurance process at the engagement phase and throughout the project cycle to prevent late recognition of defects on physical infrastructure.
General administration
2. Formally define sensitive information and develop a classification system as a foundation for deciding who owns and who may interact with what information in what fashion. A formal information lifecycle should be defined and a current or revised data retention policy and privacy policy should be implemented. This should be supported by appropriate technical measures such as cryptography, digital watermarking and user analytics.
Human resources
3. Ensure that the leave portal in oneUNOPS prevents individual contractors from applying for annual leave that results in a negative balance, as this is not allowable per the policy.
Information and communication technology
4. Perform cyberattack readiness testing to assess levels of preparedness and capability to withstand a possible cyberattack. The scope of threats to UNOPS requires recurrent testing covering the complete structure of UNOPS. This should be done by means of an independent group of experts, ideally without informing the organization that it will be tested, in order to provide a more realistic picture of the organization's cyber security readiness.
Products and services quality management
5. Ensure that quality assurance activities are carried out at the project level to ensure that UNOPS delivers high quality infrastructure. This could include the development and use of standardized quality checklists that identify the minimum required activities at all stages of project delivery and for all types of infrastructure.
6. Enforce ongoing project risk management and strengthen the flow of information between field units and monitoring units.
Project management
7. Implement and enforce the use of a worldwide standard UNOPS drawing system and approval process.
8. Expand the scope of external third party review in the design planning and review phase of infrastructure projects and ensure that design planning guidance is expanded to address other types of infrastructure.
9. Ensure that appropriate corporate and regional oversight exists regarding creation of infrastructure contracts.
10. Share solutions and lessons learned regarding payments to contractors from the Democratic Republic of the Congo with all offices delivering infrastructure projects.
11. Identify and provide guidance on the use of alternative insurance arrangements for infrastructure projects where traditional insurance for work, equipment, material and personnel is cost prohibitive to the contractors.
Strategic management and leadership
12. (a) Establish a formal governance of cyber security that should result in a mandate and a set of responsibilities at the executive level to address cyber security issues; and (b) Establish an organization-wide cyber risk management framework that will inform the development of individual cyber risk management processes within business units. The framework should define policies for information security that are objective, manageable and measurable.
Total number of audit recommendations: 12