**Unresolved audit recommendations issued more than 18 months before 31 December 2018**

|  |
| --- |
| **Functional area/audit recommendation description** |
| **Finance** |
| 1. Commit all transactions posted to the general ledger (GL) to a workflow and make these subject to approval in accordance with the delegation of authority (DoA), not only related to payments, but to GL postings.
 |
| 1. Make it mandatory to attach supporting documentation in oneUNOPS, as it is difficult for the approver to assess the validity of the entries. Suitably qualified personnel independent of the journal entry preparation and recording process should follow an established programme to monitor and test significant or unusual journal entries for evidence of inappropriate management override or bias.
 |
| 1. Implement a Treasury Management System to support: dealing and settlement activities of foreign exchange (FX) deals; monitoring of cash balances and short-term investment activities; liquidity forecasting, including cash replenishment processes; and FX risk hedging and reporting (should UNOPS adopt an FX hedging programme).
 |
| **Human resources** |
| 1. Ensure a full reconciliation of data migrated from legacy systems to oneUNOPS. This includes formal documentation of the reconciliation. Formalization of the payroll validation should be strengthened, ensuring clear 1:1 reconciliation and documentation.
 |
| 1. Ensure that all changes to transactions, both those that relate to data and those that relate to documents in the workflow, trigger the ICA workflow again.
 |
| **Information and communication technology** |
| 1. Perform cyberattack readiness testing to assess levels of preparedness and capability to withstand a cyberattack. The scope of threats to UNOPS requires recurrent testing covering the complete structure of UNOPS. This should be done by an independent group of experts, without informing the organization that it will be tested, in order to provide a more realistic picture of the organization’s cyber security readiness.
 |
| 1. Leverage the native Windows full disk encryption (Bitlocker) on all UNOPS laptops, taking into account that an encryption key management process should be in place in order to prevent compromising the availability of the corporate laptops and the information they store.
 |
| **Procurement** |
| 1. Create an automatic flag in oneUNOPS for UNGM flagged suppliers. Ensure a two-step control by independent users to validate suppliers to be flagged. Ensure that on a regular basis it is checked whether all flagged suppliers in UNGM are flagged correctly in oneUNOPS. Ensure a careful check of the financial information for all active unflagged suppliers.
 |
| 1. The DoA level entry in the system should be subjected to workflow, and approval by at least two independent users.
 |
| 1. Include robust requisite for procurement strategy in the Procurement Manual. This could include a threshold for significant procurement actions, upon which a strategy is mandatory.
 |
| **Project management**  |
| 1. Enforce ongoing project risk management and strengthen the flow of information between field units and monitoring units.
 |
| 1. 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.
 |
| **Total number of aged audit recommendations: 12\*** |
| \*All 12 recommendations stem from thematic reviews and two thirds pertain to enhanced functionality and/or data in IT tools.  |

\*