Fighting Hunger Worldwide

Internal Audit of WFP's SAP (WINGS II) GRC Access Control and Related Modules – Executive Summary

Office of the Inspector General
Internal Audit Report AR/17/16

WFP
World Food Programme
wfp.org

Internal Audit of WFP's SAP (WINGS II) GRC Access Control and Related Modules

I. Executive Summary

Introduction and context

1. As part of its annual work plan for 2017, the Office of Internal Audit conducted an audit of SAP GRC (Governance, Risk and Compliance) Access Control and related modules implemented in WFP's Enterprise Resource Planning (ERP) system, the WFP Information Network and Global System (WINGS II). The audit focused on the period from 1 January 2016 to 30 April 2017. It looked at events prior to and after this period as required. The audit team conducted the field work between 18 May and 27 June 2017 at WFP headquarters in Rome.

2. WINGS II incorporates SAP as the ERP platform and is designed to provide a seamless integration between the various critical business functions, including programme/project planning and implementation, procurement, supply chain, finance, travel and human resources.

3. As WFP's processes are increasingly supported by WINGS II and the information available in this system, a set of internal controls and technical solutions that prevent and detect any attempts at unauthorized access and alterations are necessary to safeguard the confidentiality, integrity and availability of such data and programmes. The WINGS II security system is based on the concept of authorizations, a role-based access control system and various types of permissions. Starting from this technological context and stakeholder requirements, WFP implemented the SAP GRC Access Control solution to provide an integrated access control framework that defined the Segregation of Duties and Critical Access risks, and apply a mitigation strategy for managing all access right risks.

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

Audit conclusions

5. The implementation of SAP GRC and consequent improvement of workflows in Identity and Access Management offered WFP several advantages. WFP's Information and Technology Division (RMT) approached the project as a basic technology implementation and as a risk transformation initiative with the involvement of Subject Process Experts from the business side. Implementation allowed for the transfer of Segregation of Duties and Critical Access conflict decisions from RMT and an Information Technology perspective to the Subject Process Experts on the business side. It defined and helped to enforce the relationship between the business tasks in WFP's processes and the roles in WINGS II. RMT implemented and enforced an authorization workflow that granted permission to access administrative users (Firefighter IDs) to the GRC platform with the objective of mitigating the risks of serious operational failures or financial fraud.

6. As WFP has completed the "Get Clean" phase, it needs to ensure a governance framework is in place and functioning to maintain the benefits achieved so far and capitalize on its investment ("Stay Clean" and "Stay in Control" – refer to Annex D). Such governance framework requires representation from the IT/technical provider and the business units who own and operate the various modules that make up WINGS II. It would define risk mitigation in line with the corporate one and ensure its consistent application. It would ensure the assignment of risks to the correct Risk Owners, an effective application of user access rights and the correct mapping of critical actions and Segregation of Duties violations.

7. While organizational policies and SAP best practices set out the optimal Segregation of Duties profile for each role, organizational set-up and staffing levels in headquarter business units and country offices may not always allow the desired level of segregation as defined in the GRC ruleset. Such instances would be reported by SAP GRC as a "conflict". Responsible management is expected to continually assess the severity of the resulting risk and define a mitigation strategy for the correct alignment between risks and mitigating controls.

8. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of *partially satisfactory*. Conclusions are summarized in Table 1, according to internal control component.

Table 1: Summary of risks by Internal Control Component

Internal Control Component		Risk
1.	Control environment	High
2.	Risk assessment	Medium
3.	Control activities	Medium
4.	Information and communication	Low
5.	Monitoring activities	High

Key results of the audit

Audit observations

9. The audit report contains one high-risk and four medium-risk observations. The high-risk observation is:

Governance framework for control over Segregation of Duties and Critical Access risk owners and a strategy for mitigated users: Although the system went live in February 2017, a governance framework over SAP GRC and related processes with representatives from the business and IT stakeholders was not yet in place and a strategy for the review of all the mitigated users with Segregation of Duties and Critical Access risks had not been defined and implemented. Of the nine main business process areas, only the Finance Division had identified a strategy for the risk mitigation of Segregation of Duties and Critical Access users in conflict. Mitigated users were not yet listed in SAP GRC and therefore RMT was unable to provide the Subject Process Experts with the required mitigated user report for monitoring non-compliance.

Actions agreed

10. Management has agreed to address the reported observations and is working to implement the agreed actions by their respective due date.

11. The Office of Internal Audit would like to thank managers and staff for the assistance and cooperation during the audit.

Anita Hirsch
Director, Office of Internal Audit
and Acting Inspector General