Fighting Hunger Worldwide

Internal Audit of WFP's Supply Chain Division IT-Based Applications

Office of the Inspector General
Internal Audit Report AR/18/01

WFP
World Food Programme
wfp.org

Contents

		Page
I.	Executive Summary	3
II.	Context and Scope	5
III.	Results of the Audit	6
Annex A – Summary of categorization of observations		11
Annex B – Definition of categorization of observations		12
Annex C – Acronyms		16
Annex D – Application Flowchart- Redacted		
Annex E – Evaluation of technical observations – Redacted		

Internal Audit of WFP's Supply Chain Division IT-Based Applications

I. Executive Summary

Introduction and context

1. As part of its annual work plan, the Office of Internal Audit conducted an audit of WFP's Supply Chain Division information technology (IT) environment and application controls. The focus of the audit was centred on the IT landscape currently in use by the Supply Chain Division, with consequent significant involvement of and interaction with the Information Technology Division. The audit covered the period from 1 January 2016 to 30 June 2017 and looked at prior and subsequent events as required. Fieldwork was performed from 4 September to 27 October 2017 at WFP headquarters in Rome. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

2. The Supply Chain Division manages the entire process of end-to-end planning, sourcing and delivery of assistance, worth an average of USD 3.5 billion per year in food, goods and services for WFP and partners. The Division comprises units that deal with supply chain planning; air, land and sea transport; food procurement, quality and safety; procurement of goods and services; logistics and field support; operational risk management, governance and the United Nations Humanitarian Response Depot.

3. In addition to corporate IT applications such as the Enterprise Resource Planning system, WINGS II, the Division uses several applications it developed in-house or acquired through a service provider to support its business functions. At the start of the audit, the Division was using or developing 31 such applications, with a user focus that varied between corporate, headquarters, field and partners, of which two were in the process of being phased out.

4. A risk-based approach was applied to analyze the 29 active applications and prioritize those most critical and important to the business for a detailed assessment. The 8 applications sampled for the audit and agreed with management were: the in-house developed Supply Chain Import Parity System (SCIPS); Relief Item Tracking Application (RITA); Retailer Onboarding and Contracting (ROC) application and United Nations Humanitarian Response Depot Dashboard; the service provider e-Tendering application, In-Tend; and electronic Flight Management Application, Takeflite; and 2 applications being piloted, Optimus and Quintiq.

Audit conclusions and key results

5. In the management of IT-based applications, the audit noted some positive practices, namely the presence of diversified IT skills and expertise, a noteworthy drive towards continuous research, innovation and improvement on the IT spectrum, and a consolidated process for disaster recovery and business continuity.

6. The absence of a coherent IT governance structure and strategic plan, and the merging of the divisions previously responsible for procurement and logistics, with units of substantially different functions and operational needs, resulted in an IT application environment that did not meet all the expected minimum standards, nor take full advantage of the efficiency and cost effectiveness afforded by integration and synergy.

7. The audit observed that application controls (including input, processing, output, boundary and audit trail controls) for the solutions tested were effective in their design and operation, with a few exceptions. Regarding IT general controls tested at a technical level, the development and change management, infrastructure and network security and operation controls were appropriately designed and functioning. Yet the testing of access controls identified weaknesses with regard to the security parameters, the presence of generic accounts and the absence of procedures for activity log monitoring. At the end of the audit fieldwork, management took immediate steps to address a number of the exceptions reported and was proactively addressing others.

8. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **partially satisfactory/major improvement needed**, i.e. the assessed governance arrangements, risk management and controls were generally established and functioning, but needed major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area and prompt management action will be required to ensure that identified risks were adequately mitigated.

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	Medium

9. The audit report contains one high-risk observation related to the control environment component, and two medium-risk observations related to specific control activities. The high-risk observation is:

IT governance, oversight and strategy for WFP's Supply Chain Division IT-based applications: the governance over the Supply Chain Division IT-based applications was in most cases delegated to specific units that performed decision-making autonomously on the basis of their individual needs and objectives. The management of data and of the applications was consequently decentralized and not necessarily aligned with the rest of the IT organization.
The audit underlined the absence of a Divisional IT strategic plan that would define, in line with the Corporate IT direction, how Supply Chain's applications contributed to the Organization's strategic objectives, related costs and risks. This contributed to an inadequate definition of how Supply Chain supported its IT-enabled investment programmes, a clear description of IT services and support of its IT assets. The audit also noted the absence of visibility at the Corporate IT level to assess the relevance and adequacy of the controls in place to guide Divisional management's technical governance over Supply Chain applications.

Actions agreed

10. Management has agreed to address the reported observations and is working together with the Information Technology Division 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.

Kiko Harvey
Inspector General

II. Context and Scope

Supply Chain Division's IT-based Applications

12. WFP's Supply Chain Division (OSC) is based at WFP headquarters in Rome and manages the entire process of end-to-end planning, sourcing and delivery of assistance, worth an average of USD 3.5 billion per year in food, goods and services for WFP and partners. The Division comprises units that deal with supply chain planning; air, land and sea transport; food procurement, quality and safety; procurement of goods and services; logistics and field support; operational risk management, governance and the United Nations Humanitarian Response Depot.

13. As a result of the recent merger of the divisions formerly responsible for WFP's procurement and logistics functions, the number of units and their independence from the Information Technology Division (RMT) for managing the acquisition, development and implementation of their IT business solutions have contributed to a varied landscape of IT applications in use across OSC.

- The user focus varied between corporate, headquarter, field and partners.
- Technical support for some OSC applications was in varying degrees provided by RMT while others, such as In-Tend and Takeflite, by the respective service provider.
- User support was a mix of OSC, Global Help Desk and service providers.
- The number of stakeholders and users involved was significant, including several applications used by Cooperating Partners.
- The development of applications also varied, in some cases being performed in-house and in other cases delegated to the service provider.

Objective and scope of the audit

14. The objective of the audit was to evaluate and test the adequacy and effectiveness of the processes associated with OSC's IT general and application controls. This is part of the process of providing an annual and overall assurance statement to the Executive Director on governance, risk management and internal control processes.

15. The audit was carried out in conformance with the *Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing*. It was completed according to an approved engagement plan and took into consideration the preliminary risk assessment exercise carried out prior to the audit.

16. At the start of the audit, there were 31 applications in production, development or in a pilot phase whose functional owner was OSC, of which two were in the process of being phased out. A risk-based approach was applied to analyze all OSC IT-based applications and prioritize those most critical and important to the business. The applications selected and agreed with OSC management for a detailed review were: the in-house developed Supply Chain Import Parity System (SCIPS), Relief Item Tracking Application (RITA), Retailer Onboarding and Contracting (ROC) application and United Nations Humanitarian Response Depot Dashboard; the service provider e-Tendering application In-Tend, and the electronic Flight Management Application, Takeflite. Elements of the criticality and risk exposure attached to the 6 applications in production that were reviewed are provided in Annex E. Another two applications reviewed (Optimus and Quintiq) were being piloted at the time of the audit.

17. The scope of the audit covered IT general and application controls over the applications owned and managed by OSC during the period from 1 January 2016 to 30 June 2017. Where necessary, transactions and events pertaining to other periods were reviewed. The audit fieldwork was conducted at WFP headquarters in Rome.

III. Results of the Audit

18. In performing the audit, positive practices and initiatives were noted, including: presence of diversified IT skills and expertise of staff across OSC; a process for continuous research, innovation and improvement on the IT spectrum brought about by the specific operational requirements of each unit; a coordinated approach to disaster recovery and business continuity planning, which included representatives from the logistics and procurement functions as members of the Organizational Resilience Management Group; and structured and centralized management of changes to the applications that are managed in-house that included the standardization of the change management process using a robust issue management tool that is also used at the corporate level.

19. Having evaluated and tested the controls in place, the Office of Internal Audit has come to the following conclusions on the residual risk related to the processes:

Table 3: Conclusions on Risk, by Internal Control Component and Business Process

	Internal Control Component/Business Process	Risk
1.	Control environment	
	Governance and oversight over OSC IT-based applications	High
	Strategic planning	High
	Organisational structure	High
2.	Risk assessment	
	OSC IT risk assessment	Medium
	IT service continuity	Medium
3.	Control activities	
	IT General Controls	Medium
	IT Application Controls	Medium
4.	Information and communication	
	Internal and External communication	Low
5.	Monitoring activities	
	Monitoring of OSC applications	Medium

20. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of *partially satisfactory/major improvement needed*[1].

21. The audit made one high-risk and two medium-risk observations. Tables 4 and 5 present the high and medium risk observations.

Actions agreed

22. Management has agreed to take measures to address the reported observations.[2]

[1] See Annex B for definitions of audit terms.
[2] Implementation will be verified through the Office of Internal Audit's standard system for monitoring agreed actions.

Table 4: High-risk observation

Observation	Agreed action
1 **Control Environment** – IT governance, oversight and strategy for WFP's Supply Chain Division IT-based applications The audit highlighted that the governance of OSC's IT-based applications - encompassing the Division's initiatives, as well as the vendor and applications selection process - is in most cases delegated to the specific owners that perform decision-making autonomously on the basis of their individual needs and objectives. As a result, the landscape of IT applications in support of the Supply Chain process was significantly varied and fragmented. In terms of IT governance, the fragmentation derived from the high degree of initiative allowed to the units that make up the Division. Weakened visibility across OSC of IT applications in use and being piloted by the different units was evidenced by the fragmented/isolated IT initiatives taken by the units. The audit underlined the absence of a written OSC IT strategic plan that would define, in co-operation with relevant stakeholders, how OSC IT-based applications contributed to the Organization's strategic objectives, related costs and risks. This contributed to an unclear definition of how OSC would support its IT-enabled investment programmes, and did not allow for a clear description of IT services provided or the governance of IT assets. The absence of a clearly defined OSC IT strategic plan jeopardized the definition of how OSC objectives were met, the measurements used, the coverage of investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The management of data and of the applications was consequently decentralized and not necessarily aligned with the rest of the IT organization. This, in the absence of an effective centralized IT governance process, may lead to duplication of initiatives (for example, initiatives for the development of data visualization tools and platforms), misalignment of practices, etc., which could also increase IT risks. Technical IT expertise regarding OSC applications is disseminated inside and outside of the units, with irregular involvement of RMT or external providers. The multitude of technical stakeholders concerned and required by operations encompasses the IT infrastructure of applications, system developments, maintenance of the applications as well as data management. The absence of centralized divisional management of IT applications technical governance may also lead to potential risks in terms of costs, management of service level agreements and external service provider oversight. Moreover, the audit highlighted the presence of inconsistent practices among OSC staff and/or units across the various IT-based applications (user management, change	OSC, in collaboration with RMT, will: (a) Finalize an inventory of OSC IT-based applications, and take steps to formalize their relationship and support in consideration of an Enterprise Architecture approach, with specific and clearly set out roles for focal points, and in consideration of the technical expertise required for IT-related matters; (b) Assess the criticality of OSC IT-based applications, that is: perform an appropriate evaluation of the criticality and significance of all applications (as inventoried in (a)), and degree of required compliance with corporate IT policies (or flexibility), as well as identify any application that should be replaced and/or phased out; (c) Determine minimum controls commensurate with the criticality assessment in (b) – with specific consideration to implementing a documented formalized process for the acquisition, development and registration of IT solutions on the basis of internationally-accepted standards, guidelines and best practices, including ISACA's COBIT 5 Framework, as well as in light of RMT's current efforts to provide Functional Units guidance on such, and ensure that this process supports alignment with OSC's divisional objectives; (d) Develop an implementation strategy and structure, capable of addressing the current and future requirements, optimizing IT-based application capabilities and performances, and address the needs in terms of efficiency, technology and costs, improving future investment decisions. A proper divisional structure/responsible service in the organigram will ensure consistency and effectiveness of IT application management through a revision of OSC IT-related practices (user management, change management, segregation of duties, maintenance, disaster recovery/business continuity, etc.) and ensure implementation of minimum controls as defined in (c); and

Observation	Agreed action
management, segregation of duties, maintenance, etc.). Accountability is maintained on a unit level, but absence (incompleteness or obsolescence) of written procedures and guidelines was a recurring element in our observations. Underlying cause: Inherited separated initiatives and IT-based applications: the recent modifications in the organizational structure of the Division, the presence of several units with substantially different functions and the operational needs-based development of IT-applications have all hindered the effective implementation of a coherent IT governance structure within the Supply Chain organization relative to IT-based applications. Absence of comprehensive and centralized OSC IT strategic planning processes and effective governance procedures resulted in an inability to thoroughly evaluate and monitor project investments and also resulted in the inability to support informed decision-making on OSC IT projects and costs.	(e) Establish monitoring controls: Determine the roles, responsibilities and processes for the monitoring of non-standard or suspicious activities.

Table 5: Medium-risk observations

Observation	Agreed action
2 **General IT Controls** – Access Security In the review of the general IT control environment for IT-based applications, the audit noted the following exceptions deemed to be of medium risk. The table below identifies with an X which exceptions apply to which application. (A) The log-in password of several of the sampled applications were not in line with the security parameters required in WFP corporate policies; (B) Some non-uniquely identifiable accounts were in use (i.e. presence of generic accounts); and (C) There were no activity log procedures to allow to retrace and verify the various steps for each process, including the date and time of input and the user identification for each online or batch transaction. The security configurations identified above assist the organization in preventing unauthorized access to systems, masking of identities through the use of untraceable user identification, and identifying the activities of users who access WFP applications.	OSC, in collaboration with RMT, will: (a) Ensure overall compliance with the logical security parameters set out in WFP's corporate policies regarding password controls for in-house developed applications and, based on the criticality associated to "off-the-shelf" applications, and if considered technically feasible and cost-effective, negotiate with the vendor any required modification to bring it in line with the corporate standards and criteria; (b) Redesign roles to avoid generic users (using distinct identity and passwords in compliance with corporate policies), and design appropriate mitigating controls in the case an exception is required; and (c) Perform a periodic user review, and strengthen and monitor the process whereby administrators review user accounts and related privileges and de-activate dormant accounts.

	Application[3]	Password policy (A)	Generic users (B)	Monitoring end-user activity logs (C)
			X*	
		X*	X*	
		X*	X*	
		X	X*	
		X	X	X
		X	X	

*OSC took immediate steps to analyse the exception brought to its attention by the audit and appropriate corrective action was taken or planned at the time of the audit report issuance.

[3] Redacted under the WFP Policy for Disclosure of Oversight Reports - WFP/EB.2/2012/4-A/1 paragraph 13.

	Observation	Agreed action
	The need to strengthen specific IT controls required consideration of the criticality of each application as well as whether these are "off-the-shelf" applications where customization comes at a cost. These considerations are reflected in the agreed actions. Underlying cause: Inadequate monitoring to ensure that password security controls for OSC's IT applications remained aligned with those set in the corporate IT policies and procedures or good practices. Incomplete implementation of system security configurations. Lack of a process and resources to consistently and periodically monitor activity logs and an operational risk management approach.	
3	**Application Controls** – Retroactive processing on the Takeflite application The analysis conducted on the processing of data of the Takeflite application showed that the application allowed the booking of a flight for a past date and that the system allowed one to insert a retroactive date. In an emergency situation management explained flexibility may be required to record flights ex post. The system however also allowed the adding of passengers retroactively to an existing flight. Underlying cause: Inappropriate functional design brought about by specific operational needs.	OSC will implement specific application settings in Takeflite to prevent the insertion of retroactive flights/passengers. Monitoring controls will be introduced to detect the insertion of retroactive dates.

Annex A – Summary of categorization of observations

The following table shows the categorization ownership and due date agreed with the auditee for all the audit observations. This data is used for tracking audit findings and monitoring the implementation of agreed actions.

Observation		Risk categories			Underlying cause category	Owner	Due date
		ICF	WFP's Management Results Dimensions	WFP's Risk Management Framework			
1	**Control Environment –** IT governance, oversight and strategy for WFP's Supply Chain Division IT-based applications	Operational Strategic	Processes and Systems	Institutional	Guidelines Best practices	OSC	31 December 2018
2	**General IT Controls** – Access Security	Operational	Processes and Systems	Programmatic	Compliance Guidance	OSC	30 June 2018
3	**Application Controls** – Retroactive processing on the Takeflite application	Operational	Processes and Systems	Programmatic	Compliance Guidance	OSC	30 June 2018

Annex B – Definition of categorization of observations

1. Rating system

1. Internal control components and processes are rated according to the degree of related risk. These ratings are part of the system of evaluating the adequacy of WFP's risk management, control and governance processes. A rating of one of the following four categories is reported for each audit: effective/satisfactory; partially satisfactory/some improvement needed; partially satisfactory/major improvement needed; or ineffective/unsatisfactory. These categories are defined as follows:

Table B.1: Rating system

Engagement rating	Definition
Effective / Satisfactory	The assessed governance arrangements, risk management and controls were adequately established and functioning well to provide reasonable assurance that the issues identified by the audit were unlikely to affect the achievement of objectives of the audited entity/area.
Partially satisfactory / Some improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning well, but needed improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issue(s) identified by the audit are unlikely to significantly affect the achievement of the objectives of the audited entity/area. Management action is recommended to ensure that identified risks are adequately mitigated.
Partially satisfactory / Major improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning, but need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.
Ineffective / Unsatisfactory	The assessed governance arrangements, risk management and controls were not adequately established and not functioning well to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area. Urgent management action is required to ensure that the identified risks are adequately mitigated.

2. Risk categorization of audit observations

2. Audit observations are categorized by impact or importance (high, medium or low risk) as shown in Table B.4 below. Typically audit observations can be viewed on two levels: (1) observations that are specific to an office, unit or division; and (2) observations that may relate to a broader policy, process or corporate decision and may have broad impact.[4]

[4] An audit observation of high risk to the audited entity may be of low risk to WFP as a whole; conversely, an observation of critical importance to WFP may have a low impact on a specific entity, but have a high impact globally.

Table B.2: Categorization of observations by impact or importance

High risk	Issues or areas arising relating to important matters that are material to the system of internal control. The matters observed might be the cause of non-achievement of a corporate objective, or result in exposure to unmitigated risk that could highly impact corporate objectives.
Medium risk	Issues or areas arising related to issues that significantly affect controls but may not require immediate action. The matters observed may cause the non-achievement of a business objective, or result in exposure to unmitigated risk that could have an impact on the objectives of the business unit.
Low risk	Issues or areas arising that would, if corrected, improve internal controls in general. The observations identified are for best practices as opposed to weaknesses that prevent the meeting of systems and business objectives.

3. Low risk observations, if any, are communicated by the audit team directly to management, and are not included in this report.

3. WFP's Internal Control Framework (ICF)

4. WFP's Internal Control Framework follows principles from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Integrated Internal Control Framework, adapted to meet WFP's operational environment and structure. The Framework was formally defined in 2011 and revised in 2015.

5. WFP defines internal control as: "a process, effected by WFP's Executive Board, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, compliance."[5] WFP recognises five interrelated components (ICF components) of internal control, all of which need to be in place and integrated for them to be effective across the above three areas of internal control objectives.

Table B.3: Interrelated Components of Internal Control recognized by WFP

1	Control Environment:	Sets the tone of the organization and shapes personnel's understanding of internal control.
2	Risk Assessment:	Identifies and analyses risks to the achievement of WFP's objectives though a dynamic and iterative process.
3	Control Activities:	Ensure that necessary actions are taken to address risks to the achievement of WFP's objectives.
4	Information and Communication:	Allows pertinent information on WFP's activities to be identified, captured and communicated in a form and timeframe that enables people to carry out their internal control responsibilities.
5	Monitoring Activities:	Enable internal control systems to be monitored to assess the systems' performance over time and to ensure that internal control continues to operate effectively.

4. Risk categories

6. The Office of Internal Audit evaluates WFP's internal controls, governance and risk management processes, to reach an annual and overall assurance on these processes in the following categories:

[5] OED 2015/016 para.7

Table B.4: Categories of Risk – based on COSO frameworks and the Standards of the Institute of Internal Auditors

1	Strategic:	Achievement of the organization's strategic objectives.
2	Operational:	Effectiveness and efficiency of operations and programmes including safeguarding of assets.
3	Compliance:	Compliance with laws, regulations, policies, procedures and contracts.
4	Reporting:	Reliability and integrity of financial and operational information.

7. To facilitate linkages with WFP's performance and risk management frameworks, the Office of Internal Audit maps assurance to the following two frameworks:

Table B.5: Categories of Risk – WFP's Management Results Dimensions

1	People:	Effective staff learning and skill development – Engaged workforce supported by capable leaders promoting a culture of commitment, communication and accountability – Appropriately planned workforce – Effective talent acquisition and management.
2	Partnerships:	Strategic and operational partnerships fostered – Partnership objectives achieved – UN system coherence and effectiveness improved – Effective governance of WFP is facilitated.
3	Processes and systems:	High quality programme design and timely approval – Cost efficient supply chain enabling timely delivery of food assistance – Streamlined and effective business processes and systems – Conducive platforms for learning, sharing and innovation.
4	Programmes:	Appropriate and evidence based programme responses – Alignment with government priorities and strengthened national capacities – Lessons learned and innovations mainstreamed – Effective communication of programme results and advocacy.
5	Accountability and funding:	Predictable, timely and flexible resources obtained – Strategic transparent and efficient allocation of resources – Accountability frameworks utilized – Effective management of resources demonstrated.

Table B.6: Categories of Risk – WFP's Risk Management Framework

1	Contextual:	External to WFP: political, economic, environmental, state failure, conflict and humanitarian crisis.
2	Programmatic:	Failure to meet programme objectives and/or potential harm caused to others though interventions.
3	Institutional:	Internal to WFP: fiduciary failure, reputational loss and financial loss through corruption.

5. Causes or sources of audit observations

8. Audit observations are broken down into categories based on causes or sources:

Table B.7: Categories of Causes or Sources

1	Compliance	Requirement to comply with prescribed WFP regulations, rules and procedures.
2	Guidelines	Need for improvement in written policies, procedures or tools to guide staff in the performance of their functions.
3	Guidance	Need for better supervision and management oversight.
4	Resources	Need for more resources (for example, funds, skills, staff) to carry out an activity or function.
5	Human error	Mistakes committed by staff entrusted to perform assigned functions.
6	Best practice	Opportunity to improve in order to reach recognized best practice.

6. Monitoring the implementation of agreed actions

9. The Office of Internal Audit tracks all medium and high-risk observations. Implementation of agreed actions is verified through the Office of Internal Audit's system for the monitoring of the implementation of agreed actions. The purpose of this monitoring system is to ensure management actions are effectively implemented within the agreed timeframe to manage and mitigate the associated risks identified, thereby contributing to the improvement of WFP's operations.

Annex C – Acronyms

In-Tend	An on-line e-Tendering application supporting the tender process
RITA	Relief Item Tracking Application, a web-based tool developed in-house
ROC	Retailer and Onboarding Contracting application, developed in-house
RMT	WFP's Information Technology Division
SCIPS	Supply Chain Import Parity System, developed in-house
Takeflite	An electronic Flight Management Application (e-FMA)
OSC	WFP's Supply Chain Division
WFP	World Food Programme
WINGS II	WFP Information Network and Global System, WFP's ERP system