SAVING
LIVES
CHANGING
LIVES

Internal Audit of WINGS Upgrade

Office of the Inspector General
Internal Audit Report AR/21/19

WFP
World Food
Programme

October 2021

Contents

Internal Audit of WINGS Upgrade

I. Executive summary

Objective and scope of the audit

1. As part of its annual work plan, the Office of Internal Audit conducted an audit of the WFP Information Network and Global Systems (WINGS) upgrade. WINGS seamlessly integrates several elements within WFP's enterprise resource planning system (based on SAP software) to manage the organisation's critical business functions, including procurement, supply chain, finance, travel and human resources. The upgrade to WINGS was prompted by the announcement of the end of technical support by the vendor of WFP's SAP running version, and the associated need to move from an Oracle to a HANA database. The upgrade project started on 1 October 2019 and ended with the go-live phase on 2 November 2020.

2. The types of changes associated with a major upgrade such as this bring about significant risks of operational disruptions, compromised integrity of the migrated data, and/or gaps in IT security, automated and access controls. The audit concentrated on the following control areas, plus their associated risks and related mitigations: (i) project management and governance; (ii) training and awareness; (iii) integration and impact analysis, data conversion and data quality; (iv) access management; and (v) change management.

3. Lines of enquiry defined for the audit were: 1) was the WINGS upgrade process adequately supported and monitored to meet business and security requirements?; 2) were mechanisms in place to effectively integrate WINGS with WFP's environment, evaluate the impact of changes, and detect and mitigate any risks to the completeness, accuracy and consistency of the data being transferred?; 3) did the WINGS configuration meet WFP's requirements and best practices regarding access security?; and 4) were change management controls and mechanisms adequately designed and implemented to mitigate unauthorised changes to WINGS?

Audit conclusions and key results

4. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **effective / satisfactory**. The assessed governance arrangements, risk management and controls were adequately established and functioning well, to provide reasonable assurance that issues identified by the audit were unlikely to affect the achievement of the objectives of the audited entity/area.

5. The WINGS upgrade applied project management best practices, including appropriate governance, risk management, and business continuity planning. These resulted in the complete and accurate migration of data and configuration settings, with no significant delays in implementing the project or disruptions during the restoration of system functionalities to end-users of WINGS.

6. SAP's configuration parameters and system settings, including the clients in the production environment, were found to be properly designed, allocated and implemented to prevent unauthorised changes to programs and system configurations; however, there were opportunities to close configuration gaps for high-privilege, debug and authorisation access accounts that are used to update, maintain or make changes to some tables and the system. These were provided to users who may not have needed them for undefined timelines, or were not locked when not in use as per best SAP practices. Analysis by the audit team of the user activity logs determined that these privileged accounts had only been used for upgrade project-related purposes. Concerns related to lack of review of activity logs were already raised in an internal audit report on WINGS in 2017[1].

[1] Internal audit of WFP's SAP (WINGS II) GRC Access Controls and Related Modules (AR/17/16).

7. There were opportunities to update WINGS end-user manuals and establish training programmes. While not impacting the delivery of the upgrade or changes to the database technology, end-user manuals and training are important elements supporting the effective use of the platform.

Actions agreed

8. The audit report contains two medium priority observations. The Technology Division will be responsible for the implementation of the agreed actions, coordinating with the SAP basis team at the United Nations International Computer Center. Management has agreed to address the reported observations and work to implement the agreed actions by their respective due dates.

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

II. Context and scope

WFP Information Network and Global Systems (WINGS) upgrade and configuration

10. WINGS is WFP's tailored SAP enterprise resource planning (ERP) platform designed to integrate the organisation's various critical business functions such as procurement, supply chain, finance, travel and human resources. WINGS aims to improve business units' transparency and reporting capabilities through access to a single source of information accessible to users. This enables WFP to monitor activities effectively and optimise resources globally, to maintain stronger oversight and meet business requirements.

11. In 2016 SAP announced the end of vendor technical support to the SAP version run by WFP and planned move of its database layer from Oracle to HANA by 2024. This prompted the initiation of an upgrade project managed by WFP's Technology Division (TEC).

12. The WINGS upgrade was formally proposed by TEC, with TEC starting the design analysis phase of the project from October 2019, and approved by the Strategic Resource Allocation Committee in December 2019. TEC is the overall custodian of WINGS, facilitating the development of required system changes and functionality, performing maintenance, and providing corrections to system issues. TEC also handles all user access support, network connectivity and IT security administration. The project started on 1 October 2019 and ended with the go-live phase on 2 November 2020.

13. The upgrade was designed to bring about multiple benefits, including increased maintenance and improved service level and performance monitoring by the SAP vendor. Furthermore, as reported by TEC, the upgrade resulted in (i) improved tracking, accountability and documentation for all requests; and (ii) a reduction of bottlenecks due to the synergy created by the effective collaboration between business users and the TEC analyst and developer during the entire upgrade and configuration process.

14. The SAP basis team at the United Nations International Computer Center was responsible for all activities related to the database migration and controls over migrated WINGS data and objects.

15. The system was released, and all the interfaces were successfully restarted for business activity on 2 November 2020.

Objective and scope of the audit

16. The objective of the audit was to provide assurance on the adequacy and operating effectiveness of controls, governance mechanisms and risk management frameworks related to the WINGS upgrade. Such audits contribute to an annual and overall assurance statement provided to the Executive Director on governance, risk management and internal control processes.

17. 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 considered the risk assessment exercise carried out before the audit. The audit fieldwork took place from 5 to 30 July 2021 at WFP headquarters in Rome.

18. The scope of the audit covered the period from 1 October 2019 to 30 April 2021. Where necessary, transactions and events pertaining to other periods were reviewed.

19. The audit team carried out structured interviews and documentation reviews. In addition, the audit included (i) a review of project management and governance related to the upgrade process; and (ii) an analysis and review of general IT controls in WINGS to determine whether they were designed and operating effectively to mitigate potential risks that could impede business operations. In particular, analytical reviews and data analysis of the configuration parameters of SAP S4/HANA and HANA database (DB) systems were carried out, focusing on access security requirements, authorisation profiles and change management controls. The Office of Internal Audit (OIGA) used an Automated Controls Testing Tool (ACTT) to automate data extraction directly from the SAP S4/HANA and HANA DB environments related to the configuration parameters and populations (users, changes, data and table characteristics).

20. The engagement-specific risk assessment focused on five control areas: (i) project management and governance; (ii) training and awareness; (iii) integration and impact analysis, data conversion and data quality; (iv) access management; and (v) change management. Based on these, the audit scope covered the following four lines of inquiry (LoIs):

- **LoI 1:** Was the WINGS upgrade process adequately supported and monitored to meet business and security requirements?
- **LoI 2:** Were mechanisms in place to effectively integrate WINGS with WFP's environment, evaluate the impact of changes, and detect and mitigate any risks to the completeness, accuracy and consistency of the data being transferred?
- **LoI 3:** Did the WINGS configuration meet WFP's requirements and best practices regarding access security?
- **LoI 4:** Were change management controls and mechanisms adequately designed and implemented to mitigate unauthorised changes to WINGS?

21. Prior internal audits of WINGS included baseline security[2] and GRC Access Control and Related Modules.[3] Considering the role of WINGS in the production of WFP's financial statements, the external auditor has included regular reviews of WINGS.[4]

[2] AR/2016/07 – June 2016.

[3] AR/17/16 – See Footnote 1.

[4] 2020: https://executiveboard.wfp.org/document_download/WFP-0000127476;
2019: https://docs.wfp.org/api/documents/WFP-0000115483/download/

III.Results of the audit

Audit work and conclusions

22. Based on the results of the audit, the OIGA has come to an overall conclusion of **effective / satisfactory**[5]. The assessed governance arrangements, risk management and controls were adequately established and functioning well, to provide reasonable assurance that issues identified by the audit were unlikely to affect the achievement of the objectives of the audited entity/area.

Observations and actions agreed

23. Table 1 outlines the extent to which audit work resulted in observations and agreed actions. These are classified according to the lines of inquiry (LoIs) established for the audit and are rated as medium or high priority; observations that resulted in low priority actions are not included in this report.

Table 1: Overview of lines of inquiry, observations and priority of agreed actions	**Priority of issues/agreed actions**
LoI 1: Was the WINGS upgrade process adequately supported and monitored to meet business and security requirements?	
Update of the end-user manuals and training	*Medium*
LoI 2: Were mechanisms in place to effectively integrate WINGS with WFP's environment, evaluate the impact of changes, and detect and mitigate any risks to the completeness, accuracy and consistency of the data being transferred?	
No observations raised	*N/A*
LoI 3: Did the WINGS configuration meet WFP's requirements and best practices regarding access security?	
Access management and debug authorisation	*Medium*
LoI 4: Were change management controls and mechanisms adequately designed and implemented to mitigate unauthorised changes to WINGS?	
Incorporated within the observation included in LoI 3	*NA*

24. The two observations of this audit are presented in detail below.

25. Management has agreed to take measures to address the reported observations.[6] An overview of the actions to be tracked by internal audit for implementation, their due dates and their categorisation by WFP risk and control frameworks can be found in Annex A.

[5] See Annex B for definitions of audit terms.

[6] Implementation will be verified through OIGA's standard system for monitoring agreed actions.

LoI 1: Was the WINGS upgrade process adequately supported and monitored to meet business and security requirements?

26. The audit reviewed the project management and governance for the WINGS upgrade process to verify that: (i) documentation was formalised and shared with relevant stakeholders; (ii) upgrading and data migration processes were adequately supported by qualified SAP third-party vendors for development, testing, go-live and post-go-live activities; (iii) monitoring activities before, during and after the upgrading phase were performed to assess the upstream impact and resolve deviations; and (iv) training and awareness activities, including the update of standard operating procedure manuals, were planned and implemented for all personnel impacted by the upgrade, configuration and data migration.

27. The audit concluded that project management and governance activities during the upgrade from one SAP version to another, including the definition of stakeholders, allocation of roles and responsibilities, and implementation strategies, were adequately documented and promptly communicated. Continuous status monitoring, periodic reporting to stakeholders by TEC and timely resolution of deviations occurred throughout the project period.

28. WINGS upgrade information was periodically communicated to stakeholders. There were opportunities to improve end-user manuals and provide specific training for staff impacted by the upgraded system.

Observation 1: Update of WINGS end-user manuals and training

29. WINGS end-user manuals issued between 2007 and 2008 were last updated in July 2009. They were not updated after the 2020 WINGS upgrade.

30. Additionally, no training for end-users addressing configuration-related changes was planned or implemented. While not impacting the delivery of the upgrade nor changes to the database technology, end-user manuals and training are important elements supporting the effective use of the platform.

Underlying cause(s): Responsibilities and accountabilities have not been defined between TEC and business units regarding updating WINGS user manuals and training.

Agreed Actions [Medium priority]

TEC, in collaboration with relevant business units, will update end-user manuals and provide WINGS-specific end-user training.

Timeline for implementation

31 December 2022

LoI 2: Were mechanisms in place to effectively integrate WINGS with WFP's environment, evaluate the impact of changes, and detect and mitigate any risks to the completeness, accuracy and consistency of the data being transferred?

31. The WINGS upgrade involved implementing a complex change management process to (i) evaluate the impact on the existing system landscape and infrastructure, and (ii) mitigate the risks related to data quality, completeness and accuracy of data migration. The audit reviewed the results of the project risk assessment and business scenarios, and regression and user acceptance testing.

32. During the upgrade project, all WFP business units were involved through respective focal points, reporting internally on all system activities and performance. Business units were responsible for ensuring the continuity of critical business activities during the No Automated System Available (NASA) period during which they were unable to record transactions in SAP. Business units were also responsible for identifying and developing dedicated procedures and offline tools to be deployed in case of extended NASA periods. The focal points also performed checks and activities on the production environment during the NASA period to verify that no major or evident bugs would compromise activities once the upgrade went live. The cutover phase initially planned for August 2020 occurred in October 2020 due to delivery delays of hardware and servers attributable to the COVID-19 pandemic.

33. There was no detectable business impact as a result of these delays. The downtime period was scheduled to allow for the upgrade of the WINGS production server. Some services were unavailable, while others were partially available. Reporting platforms based on business warehouses, HANA and DOTS (WFP's data warehouses) had a planned NASA period due to the parallel upgrade of WINGS and the SAP Landscape Transformation Replication Server. This prevented the server's data injection from systems such as the Country Office Tool for Managing Effectively (COMET) and WINGS.

34. TEC defined a rollback strategy and recovery plan designed to respond to the risk of serious issues and problematic events occurring by precautionarily defining mitigating actions (contingency plans) and action plans to be executed in the event of severe issues. The two potential scenarios included (i) rolling back to a previous stage of SAP upgrade (restore to a certain point) and (ii) rolling back to the non-upgraded system on Oracle (as a worst-case scenario). The project was delivered without the need to activate either rollback strategy.

35. Data quality was evaluated through the functionalities test results of the upgraded WINGS, with no anomalies noted on the migrated data. At the end of the upgrade process, business focal points analysed and certified that the migrated data, transactions and interfaces were complete. Additionally, they provided incident updates and reported that the quantitative and qualitative objectives defined at the beginning of the process were achieved. The final successful results of the regression and user acceptance tests were used as the basis for the go-live business decision for the upgraded system.

36. These results highlighted that adequate mechanisms were put in place to effectively integrate WINGS with WFP's environments. The risk assessment was instrumental in minimising the impact of the upgrade on the business. All existing interfaces with other systems were successfully restarted after the upgrade.

37. The audit did not identify any reportable issue within this LoI.

LoI 3: Did the WINGS configuration meet WFP's requirements and best practices regarding access security?

38. The audit performed reviews and data analysis of SAP S4/HANA and HANA DB systems configuration parameters through ACTT. The analysis found that user access security controls related to user identification mechanisms and system authentication were adequately designed and operating effectively for internal and external users. In particular:

- Password parameters met WFP's requirements and best practices (including a minimum password length and complexity, expiration, and account lockout).
- Access to SAP security administrative functions was authorised and appropriately restricted.

39. The audit also analysed user access management implemented in WINGS to verify that (i) users did not have access privileges beyond those necessary to perform their duties, and that there was adequate segregation of duties; and (ii) systems were adequately configured or updated to restrict system access only to authorised users.

Observation 2: Access management and debug authorisation

40. **Authorisation profile**: Granting direct update access to tables to end-users is not recommended following SAP best practices. The audit noted that some accesses to table updates were not adequately restricted to users based on the "need to know" principle. Access was provided to staff profiles in some business units that may not have needed it.

41. **Generic account access configuration**: High-privilege profiles should be assigned only to nominal user accounts based on their job responsibilities. Some high-privilege accesses were granted to generic accounts configured as "S" service users, which indicated that they could log and make changes to the system. It was also noted that these access profiles were not locked upon completion of any tasks performed in WINGS ("migration" user).

42. **Standard SAP accounts access configuration**: Vendor-provided and generic accounts may require access to SAP to perform various actions and access to these accounts should be appropriately restricted and controlled. Such user accounts with highly powerful privileges should either be set as type "B" system or locked when not in use. On the contrary, standard SAP IDs (DDIC and SAP*) were configured as "S" service users, which indicated that they could also be used to log and make changes to the system. Further, these accounts were active at the time of the audit.

43. **Debug authorisation profile:** Debug access in the production environment should be assigned only to emergency/firefighter users when relevant, as it works as a "back door" to the SAP system, granting super-user privileges. When required, specific accounts can temporarily be granted debug access with change permission via a controlled and monitored process. The audit noted that debug access was granted to users in business functions who should not have had it. Additionally, several of these profiles were nominal end-users, and their access was active and permanently enabled.

44. The audit noted that the Governance Risk and Compliance (GRC) system implemented in 2017 was used in a complementary way to mitigate and manage segregation of duties and critical access risks, significantly increasing the ability of TEC to detect issues with the account access configuration. Further analysis by the

audit team of the user activity logs determined that privileged accounts were only used for project-related purposes.

45. Management was informed of these findings and was actively taking remediation actions at the time of this report.

Underlying cause(s): Rights to modify or update tables and SAP system accounts and debug authorisation access not included in the periodic review of the access profiles.

Agreed Actions [Medium priority]

TEC will review access user accounts and profiles, including the rights to modify or update tables and debug access in the review activity; remove access from unauthorised users; and establish a process to perform these reviews periodically.

Timeline for implementation

31 December 2021

LoI 4: Were change management controls and mechanisms adequately designed and implemented to mitigate unauthorised changes to WINGS?

46. The audit performed analytical reviews and data analysis of the SAP S4/HANA and HANA DB system configuration parameters, using ACTT. The production client and system settings were configured to prevent unauthorised changes to programs and configuration based on the analysis performed. Client and system setting changes were logged, monitored, and approved by management. Additionally, maintenance and support tickets were managed via the SAP Solution Manager tool ChaRM GSM. There were opportunities for improvement on the management of debug access accounts as detailed in observation 2; otherwise, no further observations were identified within this LoI.

Annex A – Summary of observations

The following tables shows the categorisation, ownership and due date agreed with the auditee for all the audit observations raised during the audit. This data is used for macro analysis of audit findings and monitoring the implementation of agreed actions.

Medium priority observations		Categories for aggregation and analysis:			Implementation lead	Due date(s)
		WFP's Internal Audit Universe	WFP's Governance, Risk & Control logic:			
			Risks (ERM)	Processes (GRC)		
1	Update of WINGS end-user manuals and training	Security administration/ controls over core application systems	IT & Communications risks	Technology	TEC	31 December 2022
2	Access management and debug authorisation	Security administration/ controls over core application systems	IT & Communications risks	Technology	TEC	31 December 2021

Annex B – Definitions of audit terms: ratings & priority

1 Rating system

The internal audit services of UNDP, UNFPA, UNICEF, UNOPS and WFP adopted harmonised audit rating definitions, as described below:

Table B.1: Rating system

Rating	Definition
Effective / satisfactory	The assessed governance arrangements, risk management and controls were adequately established and functioning well, to provide reasonable assurance that issues identified by the audit were unlikely to affect the achievement of the 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 were 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 Priority of agreed actions

Audit observations are categorised according to the priority of agreed actions, which serve as a guide to management in addressing the issues in a timely manner. The following categories of priorities are used:

Table B.2: Priority of agreed actions

High	Prompt action is required to ensure that WFP is not exposed to high/pervasive risks; failure to take action could result in critical or major consequences for the organisation or for the audited entity.
Medium	Action is required to ensure that WFP is not exposed to significant risks; failure to take action could result in adverse consequences for the audited entity.
Low	Action is recommended and should result in more effective governance arrangements, risk management or controls, including better value for money.

Low priority recommendations, if any, are dealt with by the audit team directly with management. Therefore, low priority actions are not included in this report.

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.[7]

[7] 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.

To facilitate analysis and aggregation, observations are mapped to different categories:

3 Categorisation by WFP's audit universe

WFP's audit universe covers organisational entities and processes. Mapping audit observations to themes and process areas of WFP's audit universe helps prioritise thematic audits.

Table B.3: WFP's 2019 audit universe (themes and process areas)

A	Governance	Change, reform, and innovation; Governance; Integrity and ethics; Legal support and advice; Management oversight; Performance management; Risk management; Strategic management and objective setting.
B	Delivery	(Agricultural) Market support; Analysis, assessment, and monitoring activities; Asset creation and livelihood support; Climate and disaster risk reduction; Emergencies and transitions; Emergency preparedness and support response; Malnutrition prevention; Nutrition treatment; School meals; Service provision and platform activities; Social protection and safety nets; South-south and triangular cooperation; Technical assistance and country capacity strengthening services.
C	Resource Management	Asset management; Budget management; Contributions and donor funding management; Facilities management and services; Financial management; Fundraising strategy; Human resources management; Payroll management; Protocol management; Resources allocation and financing; Staff wellness; Travel management; Treasury management.
D	Support Functions	Beneficiary management; CBT; Commodity management; Common services; Constructions; Food quality and standards management; Insurance; Operational risk; Overseas and landside transport; Procurement – Food; Procurement - Goods and services; Security and continuation of operations; Shipping - sea transport; Warehouse management.
E	External Relations, Partnerships and Advocacy	Board and external relations management; Cluster management; Communications and advocacy; Host government relations; Inter-agency coordination; NGO partnerships; Private sector (donor) relations; Public sector (donor) relations.
F	ICT	Information technology governance and strategic planning; IT Enterprise Architecture; Selection/development and implementation of IT projects; Cybersecurity; Security administration/controls over core application systems; Network and communication infrastructures; Non-expendable ICT assets; IT support services; IT disaster recovery; Support for Business Continuity Management.
G	Cross-cutting	Activity/project management; Knowledge and information management; M&E framework; Gender, Protection, Environmental management.

4 Categorization by WFP's governance, risk & compliance logic

Audit observations are mapped to WFP's risk and process categorizations.

Table B.4: WFP's new ERM Policy recognises four risk categories and 15 risk types

1	Strategic	1.1 Programme risks, 1.2 External Relationship risks, 1.3 Contextual risks, 1.4 Business model risks
2	Operational	2.1 Beneficiary health, safety & security risks, 2.3 Partner & vendor risks, 2.3 Asset risks, 2.4 ICT failure/disruption/attack, 2.5 Business process risks, 2.6 Governance & oversight breakdown
3	Fiduciary	3.1 Employee health, safety & security risks, 3.2 Breach of obligations, 3.3 Fraud & corruption
4	Financial	4.1 Price volatility, 4.2 Adverse asset or investment outcomes

Table B.5: The GRC roll-out uses the following process categories to map risk and controls

1	Planning	Preparedness, Assessments, Interventions planning, Resource mobilisation and partnerships
2	Sourcing	Food, Non-food, Services
3	Logistics	Transportation, Warehousing
4	Delivery	Beneficiary management, Partner management, Service provider management, Capacity strengthening, Service delivery, Engineering
5	Support	Finance, Technology, Administration, Human resources
6	Oversight	Risk management, Performance management, Evaluation, Audit and investigations

5 Monitoring the implementation of agreed actions

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.

OIGA monitors agreed actions from the date of the issuance of the report with regular reporting to senior management, the Audit Committee and the Executive Board. Should action not be initiated within a reasonable timeframe, and in line with the due date as indicated by Management, OIGA will issue a memorandum to Management informing them of the unmitigated risk due to the absence of management action after review. The overdue management action will then be closed in the audit database and such closure confirmed to the entity in charge of the oversight.

When using this option, OIGA continues to ensure that the office in charge of the supervision of the unit who owns the actions is informed. Transparency on accepting the risk is essential and the Enterprise Risk Management Division is copied on such communication, with the right to comment and escalate should they consider the risk accepted is outside acceptable corporate levels. OIGA informs senior management, the Audit Committee and the Executive Board of actions closed without mitigating the risk on a regular basis.

Annex C – Acronyms

ACTT	Automated Controls Testing Tool
DB	Database
ERP	Enterprise Resource Planning
GRC	Governance, Risk and Compliance
IT	Information Technology
LoI	Line of Inquiry
NASA	No Automated System Available
OIGA	Office of Internal Audit
TEC	Technology Division of WFP
WINGS	WFP Information Network and Global Systems
WFP	World Food Programme