SAVING LIVES
CHANGING LIVES

# Internal Audit of Third-Party Access to WFP's Data and Systems

Office of the Inspector General
Internal Audit Report AR/20/02

February 2020

WFP
World Food Programme

# Contents

# Internal Audit of Third-Party Access to WFP's Data and Information Systems

## I. Executive Summary

1. As part of its annual work plan, the Office of Internal Audit conducted an audit of third-party access to WFP's data and information systems focusing on the period from 1 January 2016 to 31 June 2019. The audit team conducted the fieldwork from 26 August to 27 September 2019 at WFP headquarters in Rome. A sample of four partnerships and contracts was selected to evaluate the adequacy and effectiveness of the processes and controls in place to manage third-party access to WFP's information assets such as data, applications, services and infrastructure. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

2. For the purposes of this assignment, "third-party" refers to any individual or organization external to WFP that interacts with WFP's information assets including applications, services, infrastructure or data. Third-party includes, but is not limited to, technology service providers, programme implementation partners and strategic digital partners.

3. Private sector partnership agreements underline a commitment by WFP to pursue the digital transformation of its operations. Technical assistance and knowledge transfers from partners and service providers bring the expertise, resources and technology the organization needs to solve complex problems in data and information technology. At the time of the audit, WFP had entered into several significant partnership agreements with leading technology companies and relied on a multitude of technology service providers to provide information technology solutions.

4. In entering into these arrangements, WFP must ensure that access to its data and information systems is granted within a framework that enables it to manage potential risks to the confidentiality, integrity and availability of its data and information assets.

### Audit conclusions and key results

5. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **partially satisfactory/major improvement needed**. 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. Prompt management action is required to ensure that identified risks are adequately mitigated.

6. In 2012, WFP established the Private Donors and Partnerships Committee, chaired by the Deputy Executive Director and composed of senior management, to oversee the due diligence process for third parties, review potential partnerships with private donors and make decisions on whether proposed contributions are accepted, and/or partnerships initiated.

7. Over the last two years, WFP's Technology division has increased its IT security governance capabilities through the appointment of a Chief Information Security Officer who oversees a team of IT security professionals to support business units, establish and maintain WFP's IT Security Strategy, and to ensure information assets and systems are adequately protected. In July 2019, the Management Information Systems Steering Committee approved the recruitment of a Data Protection Officer to oversee the formulation and implementation of WFP's Data Protection Strategy and to ensure the adoption of international best practices. At the time of the audit, this recruitment was ongoing.

8. Additional measures were needed to complement these positive developments and establish an effective third-party risk management framework to mitigate the risk of unauthorized access to WFP's systems and data by third parties. WFP had not implemented a third-party vendor privacy and security management programme or applied a consistent approach to contracting, assessing and overseeing the data protection, privacy and information security practices of its partners and vendors. Weaknesses highlighted during the audit included: a lack of third-party risk management governance processes; third-party IT security policies; the absence of a comprehensive inventory of third parties; and the need for a data privacy framework to address privacy risks and identify key areas of control focus.

9. The audit also concluded that the identity and access management processes, related system of controls and risk management practices were not adequate to safeguard WFP from unauthorized third-party access to its data and information systems. Some identity and access management lifecycle weaknesses included: inadequate third-party account management; no monitoring of third-party access to IT production environments and activity logs; lapses in third-party user access removals; and the absence of a network topology that would limit the impact of third-party intrusions within WFP's network.

10. In March 2019, the Technology Division conducted an assessment of identity and access management and identified critical access management issues for its crown jewel applications. The Technology Division proposed several initiatives to mitigate these issues, the adoption of which remained on hold as at the date of this report.

## Actions agreed

11. The audit report contains three high and two medium priority observations. The Technology Division will be the primary lead for implementation of the agreed actions in coordination with the Goods and Services Procurement branch and the Private Donors and Partnerships Committee. Management has agreed to address the reported observations and work to implement the agreed actions by their respective due dates.

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

**Kiko Harvey**
Inspector General

# II. Context and scope

## Third-party management in WFP

13. The growth of WFP's humanitarian and development activities has been accompanied by increasing organizational demands for data and information to help inform decision making and the deployment of resources. Similarly, WFP's business partner landscape continues to increase in breadth and complexity. With an abundance of third parties with deep expertise and broad capabilities, WFP has an opportunity to adopt the latest technologies from leading firms in the private sector.

14. Best practices suggest a due diligence screening process should be undertaken by a strategic working group before WFP enters into agreements with third parties. This assessment should provide management with the information needed to address qualitative and critical aspects of potential third-party agreements, mitigate potential risks and help determine how the partnership would support the achievement of WFP's strategic goals. The Legal Office (LEG) conducts the due diligence research and screening of potential partners under the oversight of the Private Donors and Partnerships Committee, chaired by the Deputy Executive Director.

15. Within WFP, several business units contribute to third-party relationship management. The Information Security Branch of the Technology Division (TECI) is responsible for enacting policies and standards related to information security that apply to all users, including third parties, and may be called upon to provide post-factum third-party relationship assessments. The Private Sector Partnerships Division (PGP) and the IT Resource Management Branch of the Technology Division (TECR) are responsible for developing and maintaining the governance structures necessary to implement vendor/partner management policies including standards, procedures and reporting requirements. When requested, LEG considers security and confidentiality provisions of the contract agreements and provides advice to PGP and the Technology Division (TEC) when signing third-party agreements.

16. Recent audits and advisories carried out by the Office of Internal Audit (OIGA)[1] found that WFP's data protection and privacy needed to be anchored in the organizational structure and embedded within business processes. This extended to the establishment of a privacy and data protection framework whereby WFP may grant third-party access to its data and information systems in a controlled manner. Though significant progress has been made on beneficiary data management, WFP has not yet established a comprehensive privacy and data protection framework as a foundation for robust corporate policies and practices.

## Objective and scope of the audit

17. The overall objective of this audit was to assess WFP's governance, internal controls and risk management practices when granting third-party access to its data and information systems.

18. The audit scope included examining contracts and partnership agreements, on a sample basis, to assess the arrangements between service providers, partners and WFP relating to data access and management. The audit chose a sample of four partnerships and contracts. Two additional contracts were reviewed to test monitoring controls and assurance mechanisms. These samples were chosen

[1] Internal Audit of Beneficiary Management AR/17/17; Internal Audit of WFP's SAP (WINGS II) GRC Access Control and Related Modules AR/17/16 and Advisory Assignment on Data Protection and Privacy AA/19/02.

after a rigorous risk assessment exercise that considered both qualitative and quantitative risk elements of the population of identifiable third parties, representing a cross-cutting sample of different agreements and partnership types. Third-party access to beneficiary data through SCOPE or other systems was excluded from the scope of this audit as these were covered in the Internal Audit of SCOPE IT General and Application Controls (Audit Report AR/17/18) completed by OIGA in 2017.

19. Based on the engagement-specific risk assessment, the audit scope covered the following three lines of enquiry:

    **Line of enquiry 1:** Are governance mechanisms, internal controls and risk management practices in place and operating effectively to facilitate the management of third-party access to WFP's data and systems?

    **Line of enquiry 2:** Are controls and assurance mechanisms in place and operating effectively to verify and monitor the implementation of agreed upon obligations and commitments entered into by partners and service providers regarding access to/and use of WFP's systems and data?

    **Line of enquiry 3:** Are IT security controls (preventive, detective and corrective) in place and operating effectively to ensure WFP's data and systems are only accessible to authorized users?

20. 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 risk assessment exercise carried out prior to the audit.

21. The scope of the audit covered 1 January 2016 to 31 June 2019. Where necessary, transactions and events pertaining to other periods were reviewed.

22. The audit fieldwork carried out at WFP's headquarters in Rome took place from 26 August to 27 September 2019.

# III. Results of the audit

## Audit work and conclusions

23. The audit work was tailored to WFP's third-party management context and the governance objectives set by the IT Security and Data Privacy Policy, considering the different findings of WFP's second and third lines of defence functions on data privacy management.

24. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **partially satisfactory/major improvement needed**.[2] The assessed governance arrangements, risk management and controls were generally established and functioning but needed major improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issue(s) 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.

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

## Gender maturity

25. OIGA, in supporting management efforts in the areas of gender, separately reports its assessment of gaps identified relating to gender. This audit raised no gender-related observations.

## Observations and actions agreed actions

26. Table 1 outlines the extent to which audit work resulted in observations and agreed actions. These are classified according to the lines of enquiry 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 enquiry, observations and priority of agreed actions** | **Priority of issues/agreed actions** |
|---|---|
| **Line of enquiry 1: Are governance mechanisms, internal controls and risk management practices in place and operating effectively to facilitate the management of third-party access to WFP's data and systems?** | |
| *1. Third-party governance and risk management framework* | *High* |
| *2. Third-party due diligence process* | *Medium* |
| **Line of enquiry 2: Are controls and assurance mechanisms in place and operating effectively to verify and monitor the implementation of agreed upon obligations and commitments entered into by partners and service providers regarding access to/and use of WFP systems and data?** | |
| *3. Third-party security controls and assurance mechanisms* | *Medium* |
| **Line of enquiry 3: Are IT security controls (preventive, detective and corrective) in place and operating effectively to ensure WFP's data and systems are only accessible to authorized users?** | |
| *4. Third-party user identity and access management* | *High* |
| *5. Third-party user logging and monitoring of activities* | *High* |

27. The five observations of this audit are presented in detail below.

28. Management has agreed to take measures to address the reported observations.[3] An overview of the actions to be tracked by internal audit for implementation, their due dates and their categorization by WFP's risk and control frameworks can be found in Annex A.

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

## Line of enquiry 1: Are governance mechanisms, internal controls and risk management practices in place and operating effectively to facilitate the management of third-party access to WFP's data and systems?

29. Best practices suggest that effective management of third-party access includes gaining an understanding of the risks that each third-party may represent and implementing safeguards to reduce the risk of errors or malicious activities. According to WFP's Corporate IT Security Policy, "WFP information is maintained on the principles of integrity, confidentiality, availability and accountability. This information should be available when required, accessible by authorized personnel, and trusted to be authentic while maintaining assigned confidentiality".

30. The audit reviewed WFP's corporate policies and guidelines on IT security, data classification, roles and responsibilities of stakeholders involved in third-party management, and support and oversight mechanisms by the second line of defence.

31. At the time of the audit, TECI had started updating and working on new policies and processes, which will enhance decision making and information reporting on third-party risk management.

### Observation 1: Third-party governance and risk management framework

32. At the time of the audit, WFP had not implemented a third-party vendor privacy and security management programme to apply a consistent approach to contracting, assessing and overseeing the data protection, privacy and information security practices of its partners and vendors. The following weaknesses were noted in WFP's third-party management process:

33. *Governance* – There was no third-party management governance framework to effectively assign roles and responsibilities across functional teams; help drive accountability throughout the organization; and provide the basis for the allocation of resources to carry out a third-party risk management programme. Instead, WFP evaluated third parties on a case-by-case basis using a variety of systems, policies and approaches. At the time of the audit, only TEC had an active role in the management of third-party risks. Business systems owners had limited involvement in the process and were not monitoring third-party access to data (refer to Observation 5).

34. *Risk management* – There was no dedicated risk management process for third-party vendor and partner access to WFP's data and systems to ensure that the risk exposure associated with third parties was managed and monitored according to the organization's risk appetite and governance requirements.

35. *Policies and procedures* – There was no comprehensive third-party management policy. Instead, several policies (including the IT Security and Data Privacy policies) made some references to third parties. A formalized security programme was not available to provide a description of the organizational, technical and security capacity and systems needed to manage third parties; neither were processes in place to deal with data breaches and incident management involving third parties.

36. *Third-party inventory* – WFP did not maintain an accurate and complete inventory of third parties and associated risks. A third-party review process was not established to prioritize and allocate resources to monitor the third parties that should receive the most attention to mitigate IT security and business continuity risks. With a few exceptions, application owners could grant third parties access to specific applications and systems without formal internal controls and the oversight of TEC, thus increasing the challenge of managing third-party risks.

37. *Data classification and privacy framework* – Although WFP had designed a Data Classification Policy which included a classification framework, a list of responsibilities for identifying sensitive data and descriptions of the various data classification levels was not established. Information was not always

classified in terms of its value, sensitivity and criticality. At the business unit level, controls had not been implemented to identify information that should not be disclosed to third parties. OIGA's Advisory Assignment AA/19/02 on *WFP Data Protection and Privacy: General Data Protection Regulation Benchmarking,* issued in November 2019, also highlighted data privacy and protection weaknesses reported in the benchmarking assessment related to organization-wide policy gaps, data risks, quality management frameworks, processes and tools. WFP senior management agreed a series of recommendations to address these weaknesses.

Underlying cause(s): Missing corporate framework for third-party risk management; lack of ownership of the overall third-party management process; lack of adherence to the Data Classification Policy by WFP business units; lack of IT data mapping identifying external systems involved in processing data; and corporate risk appetite on third-party management not set.

**Agreed Actions** [High priority]

The Data Protection Officer should formulate an implementation plan for the completion of recommendations 1, 2 and 3 put forward in OIGA's Advisory Assignment AA/19/02 on *WFP Data Protection and Privacy: General Data Protection Regulation Benchmarking*, issued in November 2019.

In implementing these actions, the Data Protection Officer should implement a proactive and comprehensive approach to third-party risk management, including establishing third-party risk policies, principles and risk tolerances, as well as roles and responsibilities for oversight, management and support to third-party relationship owners and associated risk management processes.

**Timeline for implementation**

31 December 2020

## Observation 2: Third-party due diligence process

38. Best practices suggest it is necessary to conduct appropriate due diligence for any third-party such as contractors, suppliers and others prior to completing the vendor onboarding process. The Private Donors and Partnerships Committee is responsible for overseeing due diligence processes carried out by LEG, and for reviewing potential partnerships with private donors. TEC may be called upon to identify and assess the information security risks of the proposed contribution or partnership, in most cases post-factum. The Committee decides whether proposed contributions are accepted, or partnerships initiated. For commercial service providers, the Goods and Services Procurement Manual calls for different mechanisms to assess service providers depending on the type of procurement process to be followed. In this regard, the audit noted:

39. *Information gathering* – Due diligence processes for both commercial service providers and private partnerships identified red flags and reputational risks associated with potential agreements. However, these processes were not consistent, thorough or robust enough to ensure the third-party's information security risks and control environment were properly assessed or understood. WFP did not request third-party security policies and standards and assurance reports in all cases. These are needed to properly assess the third-party's platforms and key processes including access controls and business continuity. Business units did not request that vendors and partners complete security control questionnaires to gain assurance that proper controls were in place to protect WFP's data and services.

40. Requests for proposals and requests for quotation for commercial contracts did not set IT security standards, or expectations for their disclosure to WFP, by potential service providers.

41. *Dependency risks* – Conducting due diligence, internal control assessments and projecting the cost of potential services are critical steps in managing third parties. This is particularly important for partnerships that provide donations in the form of technology tools, training and expert advice as some of these partnerships may later turn into commercial agreements with WFP. Key technology solutions currently under development with partners are likely to require the acquisition of licences and services after the end of the partnership agreement with these entities, yet there were no projections of potential future costs, or a fair and transparent comparison against alternative service providers. For example, WFP entered into a partnership agreement with a vendor for data visualization software initially provided for free and widely adopted by the organization; the agreement eventually turned into a commercial relationship.

42. *Due diligence team* – The potential impact of data security on the organization requires that stakeholders from different WFP divisions, including the Enterprise Risk Management Division (RMR) and TEC, participate in the due diligence and decision-making process to help improve the screening and onboarding, risk assessment and continuous monitoring of potential partners and vendors. RMR and TEC were not participating consistently in due diligence processes and were not standing members of the Private Donors and Partnerships Committee.

Underlying cause(s): Due diligence processes mainly focused on reputational risks, with limited consideration of operational, data, cybersecurity, financial and business continuity risks, etc.; absence of dedicated subject matter expert(s) to oversee third-party access risks; and lack of standard operating procedures to assess and onboard third-party partners and vendors.

**Agreed Actions** [Medium priority]

a) The Chair of the Private Donors and Partnership Committee, with the assistance of the Data Protection Officer and TEC, will propose a review of the ED's Circular OED2012/016 and update the Committee's operating procedures to ensure that standard IT and data security checklists and requirements are part of the due diligence process, when relevant, allocating responsibilities with due consideration of potential conflicts of interest.

b) The Goods and Services Procurement Unit (OSCG) will collaborate with TEC to ensure that scope of work of presented to vendors during the tendering process, includes standard IT and data security checklists and requirements for preliminary screening and technical evaluation of potential suppliers with access to WFP's systems and data.

**Timeline for implementation**

a) 31 January 2021

b) 30 June 2020

## Line of enquiry 2: Are controls and assurance mechanisms in place and operating effectively to verify and monitor the implementation of agreed upon obligations and commitments entered into by partners and service providers regarding access to/and use of WFP systems and data?

43. Best practices suggest organizations manage potential risks and obtain reliable and independent assurance when services are outsourced to third parties. One of the most effective ways for third-party organizations to communicate information about their risk management and controls is through security certificates (e.g. International Organization for Standardization standards [ISOs]), service auditor reports or assurance reporting (e.g. ISAE 3402, SSAE 16 -SOC 1, ISAE 3000, SOC 2 and SOC 3) provided to their client organizations.

### Observation 3: Third-party security controls and assurance mechanisms

44. A review of third parties' assurance reports was not conducted by TEC for the agreements sampled. There was no evidence that WFP had obtained reasonable assurance from third parties that their IT internal controls were adequately designed or worked effectively before or after entering into these agreements. Specific audit clauses were not present in the agreements, which would allow WFP to access evidence of third-party compliance with the terms and conditions set therein. Audit clauses were limited to the UN general terms and conditions and did not include the right to audit clauses, reporting of security breaches to WFP or the requirement to provide internal control assurance reports. TEC stated that the current set of technologies and equipment donated in kind to WFP may have capabilities to harvest data and information.

45. *Case study* –WFP uses a software-as-a-service cloud-based solution to manage its tendering processes. The vendor for this solution did not provide independent and objective assurance reports regarding its IT internal controls upon request from the auditors. Therefore, WFP could not gain assurance that potential risks related to the security, availability, processing integrity, confidentiality and privacy of WFP's data in the tendering system had been effectively identified and mitigated. While the vendor stated it was ISO 27001 certified, no additional information was sought by WFP to corroborate the validity, current state or scope of the ISO certification. At the time of the audit, neither a contract nor a service level agreement was in place with this vendor, although payments of approximatively USD 500,000 had been made for services rendered over the past ten years. OIGA alerted OSCG to these issues and was informed that OSCG was working to establish a contract with the vendor.

Underlying cause(s): Standard UN terms and conditions not fit for partnership and service agreements of a technical nature; and absence of mechanisms and processes to gain assurance from third parties regarding their internal controls, and to corroborate their compliance with agreed upon IT internal controls.

**Agreed Actions** [Medium priority]

a) The Data Protection Officer, in coordination with TEC and relevant units, will:

- establish the roles and responsibilities required to risk assess through data protection impact assessments the agreements with donors and partners, and contracts with services providers, that potentially grant third-party access to WFP's systems and data; and

- for highly sensitive contracts, establish a process granting WFP the right to request and review IT assurance reports from third-party service providers from the due diligence stage and periodically throughout the lifecycle of the agreement or contract.

b) OSCG, with the assistance of TEC, will obtain independent and objective assurance regarding the tendering software vendor's IT security controls before entering into any agreements in the future.

**Timeline for implementation**

a) 31 December 2020

b) 30 September 2020

## Line of enquiry 3: Are IT security controls (preventive, detective and corrective) in place and operating effectively to ensure WFP's data and systems are only accessible to authorized users?

46. An Identify and Access Management (IAM) framework should be in place to ensure the right access is granted to the right people at the right time. According to the Information Systems Audit and Control Association (ISACA), effective governance along with role management, authentication, user profiling and integration capabilities are key to implementing an effective IAM framework. Best practices also suggest that logging and monitoring user activities are key controls when working and collaborating with third parties. WFP's Information Technology Security Policy states that "All WFP systems [should be] configured to monitor and log system access. Event details [should be] stored and periodically reviewed". In March 2019, TEC conducted an IAM assessment, identifying the main criticalities for every system and proposing key recommendations, the adoption of which remained on hold at the time of this audit report.

### Observation 4: Third-party user identity and access management

47. The audit reviewed a sample of four partnerships and contracts to ensure WFP's data and systems were only accessible to authorized users. The following weaknesses were noted:

48. *Third-party account management* – WFP's user access policies and procedures require active directory (AD) credentials to clearly distinguish accounts associated with internal or external users. Sixty-four of 18,212 AD active user accounts were marked as external; this was substantially lower than the 400 users identified as external by OIGA when comparing the AD to the Human Resources master data.

49. Internal/external user attributes were not backed by characteristics and criteria as there was no technical distinction between a domain account activated for an employee or a third-party user. Internal and external users had the same default access to applications, services and data available through AD including WFP's intranet (and all information and data found therein), virtual private network connections and some shared drives, etc. This exposes potentially sensitive and confidential data to unauthorized access.

50. *Third-party access to production environment* – For all the cases reviewed, third-party users had access to the production environment, with administrative privileges in some instances. In two cases, the audit

noted that third-party contractors had performed troubleshooting and bug-fixing activities directly in the production environment, raising the risk of unauthorized changes to systems. In one case, the contractor's duties included the joint administration of a database system for data encryption and sanitization, thus increasing the risk of unauthorized access to sensitive data. At the time of the audit, there were no compensating controls such as periodic oversight and monitoring processes to ensure WFP's data and information systems were only accessed by authorized users on a restricted basis. Vendors providing cloud services, including software-as-a-service solutions, had not been assigned technical limitations in accessing WFP's data stored in their systems, increasing the risk of unauthorized access to sensitive information[4].

51. *Third-party access removal* – Dormant user accounts increase the exposure of WFP's data and systems to unauthorized access. There were gaps in the process to deactivate user credentials of separated third-party users. Hiring business units were not consistently notifying TEC when third-party users were separated. The audit detected more than 90 active third-party users that had not logged into WINGS for at least 30 days, and a further 100 users that had never logged in at all.

52. *Network segmentation* – TEC was in the process of reviewing WFP's network architecture at the time of the audit. TEC aims to limit the impact of intrusions by using segmentation and segregation. However, the audit noted that this approach was not consistently applied throughout the organization's network infrastructure. The only servers under appropriate isolation were the ones hosting the crown jewels applications. Third-party users connecting to other areas of WFP's network could still access many systems and data outside the scope of agreed upon activities.

53. *Data upload controls* – There is a risk that controls designed to prevent the unauthorized transfer of Personal Identifiable Information (PII) outside WFP's network perimeter may be circumvented. There were ongoing efforts to anonymize, encrypt and sanitize data before it was transferred to and accessed by third parties. However, the platforms reviewed in the audit had internal control weakness that allowed data, including PII data, to be uploaded without robust preventive or detective controls.

Underlying cause(s): The IAM framework review was never completed due to a lack of clear ownership over the project; and lack of clear roles and responsibilities, guidelines and expectations in the management of third-party access to WFP's data and systems.

**Agreed Actions** [High priority]

TEC will:

a) Present the IAM framework options and a recommendation on the model to be adopted to the Management Information Systems Steering Committee (MISSC).

b) On a risk-based basis, and in coordination with the Data Protection Officer, perform periodic third-party user reviews with business units to confirm active third-party personnel.

**Timeline for implementation**

31 January 2021

[4] OIGA is currently finalizing an audit of Cloud Computing in WFP.

## Observation 5: Third-party user logging and monitoring of activities

54. The review of the systems for third-party user logging and monitoring highlighted the following issues:

55. User activity logging and monitoring were inconsistently applied across WFP systems. Decisions on what and how to log and monitor user activities were assigned to systems and application owners; however, their level of responsibility for the process, or role relating to IT security was not clear. This led to monitoring gaps.

56. There was no active monitoring strategy. For the cases reviewed, monitoring of third-party activities was only conducted through the operating systems' default rules and was not based on a proper risk assessment and strategy.

57. While there were some instances of adequately designed audit trails and mechanisms to alert TEC of third-party activities in WFP's production environment, these were found to be ineffective as resources were not allocated to actively review logs and properly address detected issues.

58. The lack of a proper logging and monitoring framework increases the risk that malicious activities perpetrated by third-party users go undetected, until the effects are visible and, often, irreversible.

Underlying cause(s): Unclear roles and responsibilities in the management of systems logs and activities; absence of clear guidelines for active logging and monitoring of systems and applications; inadequate oversight of critical IT systems; and logging and monitoring costs not part of the total cost of ownership of IT systems.

**Agreed Actions** [High priority]

TEC will:

a) Establish guidelines to specify what systems information must be logged (mandatory, discretionary, unnecessary) and how logging should be implemented and monitored.

b) Inform the application owners of their roles and responsibilities regarding the monitoring of logs to detect unauthorized third-party user activities.

**Timeline for implementation**

31 January 2021

# Annex A – Summary of observations

The following tables shows the categorization, 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.

| | | Categories for aggregation and analysis: | | | | |
|---|---|---|---|---|---|---|
| **High priority observations** | | **WFP's internal audit universe** | **WFP's Governance, Risk & Control logic: Risks (ERM)** | **Processes (GRC)** | **Implementation lead** | **Due date(s)** |
| 1 | Third-party governance and risk management framework | Risk management | IT & Communications risks | Risk management | DPO | 31 December 2020 |
| 4 | Third-party user identity and access management | Security administration/controls over core application systems | IT & Communications risks | Technology | TEC | 31 January 2021 |
| 5 | Third-party user logging and monitoring of activities | Security administration/controls over core application systems | IT & Communications risks | Technology | TEC | 31 January 2021 |

| | | Categories for aggregation and analysis: | | | | |
|---|---|---|---|---|---|---|
| **Medium priority observations** | | **WFP's internal audit universe** | **WFP's Governance, Risk & Control logic: Risks (ERM)** | **Processes (GRC)** | **Implementation lead** | **Due date(s)** |
| 2 | Third-party due diligence process | ICT governance and strategic planning | IT & Communications risks | Technology | DED<br>OSC | a) 31 January 2021<br>b) 30 June 2020 |
| 3 | Third-party security controls and assurance mechanisms | Security administration/ controls over core application systems | IT & Communications risks | Technology | DPO<br>OSC | a) 31 December 2020<br>b) 30 September 2020 |

# Annex B – Definitions of audit terms: ratings & priority

## 1 Rating system

The internal audit services of UNDP, UNFPA, UNICEF, UNOPS and WFP adopted harmonized 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.<br>Issue(s) identified by the audit were unlikely to significantly affect the achievement of the objectives of the audited entity/area.<br>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.<br>Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area.<br>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.<br>Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area.<br>Urgent management action is required to ensure that the identified risks are adequately mitigated. |

## 2 Priority of agreed actions

Audit observations are categorized 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 organization 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.[5]

[5] 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 Categorization by WFP's audit universe

WFP's audit universe[6] covers organizational entities and processes. Mapping audit observations to themes and process areas of WFP's audit universe helps prioritize 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 (GRC) logic

As part of WFP's efforts to strengthen risk management and internal control, several corporate initiatives and investments are underway. In 2018, WFP updated its Enterprise Risk Management Policy,[7] and began preparations for the launch of a risk management system (Governance, Risk & Compliance – GRC – system solution).

As a means to facilitate the testing and roll-out of the GRC system, audit observations are mapped to the new risk and process categorizations as introduced[8] by the Chief Risk Officer to define and launch risk matrices, identify thresholds and parameters, and establish escalation/de-escalation protocols across business processes.

[6] A separately existing universe for information technology with 60 entities, processes and applications is currently under review, its content is summarized for categorization purposes in section F of Table B.3.
[7] WFP/EB.2/2018/5-C
[8] As per 1 January 2019, subsequent changes may not be reflected in 2019 audit reports.

**Table B.4: WFP's new ERM Policy recognizes 4 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 mobilization and partnerships |
| 2 | Sourcing | Food, Non-food, Services |
| 3 | Logistics | Transportation, Warehousing |
| 4 | Delivery | Beneficiaries 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 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

| | |
|---|---|
| AD | Active Directory |
| ERM | Enterprise Risk Management |
| GRC | Governance, Risk and Control |
| IAM | Identify and Access Management |
| ISAE | International Standard for Assurance Engagements |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| LEG | Legal Office |
| MISSC | Management Information Systems Steering Committee |
| OIGA | Office of the Inspector General Internal Audit |
| OSCG | Goods and Services Procurement Unit |
| PGP | Private Sector Partnerships Division |
| PII | Personal Identifiable Information |
| RMR | Enterprise Risk Management Division |
| SOC | System and Organization Controls |
| SSAE | Statement on Standards for Attestation Engagements |
| TEC | Technology Division |
| TECI | Technology Division Information Security Branch |
| TECR | Technology Division IT Resource Management Branch |
| WFP | World Food Programme |