SAVING LIVES
CHANGING LIVES

Internal Audit of WFP IT Third-Party Risk Management

Office of the Inspector General
Internal Audit Report AR-24-06

World Food Programme

May 2024

Table of Contents

I. Executive summary

Third party risk management

1. As part of its Annual Assurance Plan, the Office of Internal Audit conducted an internal audit of IT third party risk management in WFP. The audit covered the period from 1 January 2023 to 31 December 2023.

2. With over 163 long-term agreements with Information Technology service providers and five major private sector technological partnership agreements, third-party risk management is critical to WFP in managing risks along the life cycle of a third-party vendor, from the sourcing through the due diligence, monitoring of risks to the termination of the contract relationship. Third-party risk management outlines how an organization assesses, selects, and monitors its vendors to ensure that they meet the organization's requirements and standards for quality, security, and compliance.

Audit conclusions and key results

3. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **some improvement needed**[1]. 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.

4. WFP, with its supply chain and technology divisions, has established proper procurement processes and criteria to determine product or service requirements and match them with specific vendor capabilities and pricing. This includes the entire process of soliciting, identifying, evaluating, and contract offering.

5. At the corporate level, initiatives are being coordinated between the Supply Chain and Technology divisions to adopt a comprehensive framework with a consistent approach, empowering WFP to effectively plan, oversee, and enhance its engagements with third-party service providers of food, goods, and services.

6. The current decentralized governance over third-party risk management in WFP has decreased the organization's ability to identify, assess, and manage potential risks posed by third parties. The audit noted that proper third-party risk management (including for IT vendors and partners) was not established within WFP and has yet to become a systematic and formalized process. This has led to incoherent application of standards, unclear roles and responsibilities and an absence of articulation of risk appetite in respect of third parties, aimed at creating alignment among WFP internal stakeholders.

7. Management of the IT partnerships was not standardized and was inconsistent across units, with an inadequate partnership governance framework to effectively assign roles and responsibilities across units.

8. Current due diligence processes for commercial service providers and private partnerships were only focused on financial and reputational risks for partners. These processes were not robust enough to ensure that the third-party's information security, data privacy, and business continuity risks were systematically and properly assessed.

9. Continuous monitoring of third-party relationships to keep third parties accountable for their actions and identify new third-party risks before they become significant issues for the organization was also not part of the existing processes.

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

Actions agreed

10. The audit report contains one high and three medium-priority observations. In consultation with relevant units, the WFP Technology, Partnership, and Supply Chain divisions will be the primary ones leading the implementation of the agreed-upon actions.

11. Management has agreed to address the reported observations and work to implement the agreed actions by their respective due dates.

THANK YOU!

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

II. Context and scope

Third-party risk management in WFP

13. In WFP, business divisions are increasingly reliant on third-party vendors and suppliers to enable growth and support business operations. These partnerships are crucial for the organization, but they also have the potential to expose it to new risks.

14. Information Technology vendor/partners management is a strategic process that involves selecting, managing, and overseeing third-party vendors providing IT products and services. Key functions include vendor selection, contract negotiation, performance evaluation, risk management, and relationship management.

15. Within WFP, several business units contribute to third-party risk management. The WFP Technology Division (TEC) continues to provide services to connect staff, beneficiaries, and donors by relying on technology to drive operational efficiency, innovation, and growth. This dependence on technology requires an effective IT vendor management system, critical to successful IT operations.

16. The Private Partnerships Division (PSP) is responsible for developing the IT partnership framework and assessing the risk-benefit of the opportunity to WFP.

17. The Supply Chain division is responsible for developing and maintaining the governance structures and policies, including standards, procedures, and reporting requirements for the procurement process. The Global Privacy Office (GPO) enables WFP to protect personal data & respect privacy in line with relevant internationally recognized standards & best practices. When requested, the legal unit (LEG) considers security and confidentiality provisions of the contract agreements and provides advice to PSP and the Technology Division (TEC) when signing third-party agreements.

18. An OIG audit [2] in 2019 found that WFP had not implemented a third-party vendor privacy and security management programme to assign roles and responsibilities across functional teams effectively, and WFP did not maintain an accurate and complete inventory of third parties and associated risks. Though significant progress has been made, WFP has yet to establish a comprehensive third-party risk management framework.

19. In 2021, Supply Chain initiated the Supplier Relationship (SRM) project to develop a comprehensive framework, empowering WFP to effectively plan, oversee, and enhance its engagements with third-party service providers of food, goods, and services. In addition, the project aims to transition from a transactional approach to suppliers to a collaborative and value-driven relationship and to elevate WFP's emphasis on supply chain sustainability and supplier risk management, aligning with the key themes of the WFP Supply Chain Strategic Roadmap 2022-2025. At the time of the audit, the project was in an initial stage with the plan to be gradually rolled out in 2024 and 2025.

Objective and scope of the audit

20. The objective of this audit is to provide assurance on WFP governance, risk management, and controls designed to manage risks associated with information technology third-party vendors and partnerships. Such audits contribute to the Office of Internal Audit's annual and overall assurance statement to the Executive Director on governance, risk management and internal control processes.

[2] Internal Audit of Third-Party Access to WFP's Data and Systems AR/20/02.

21. The following four areas were included in the scope of the audit:

- **Area 1: Strategy and Governance** (IT strategy and alignment of the IT third-party management strategy, roles and responsibilities, policies and procedures, risk management).
- **Area 2: Contracting** (Due diligence, including assessments on dependency, conflicts of interest, vendor/partner selection and validation, contracting including legal template, terms and conditions).
- **Area 3: Relationship Management** (onboarding, performance management, KPIs, communication, and management of contract/partnership and renewal)
- **Area 4: Business continuity/reliance** on third-party vendors, data privacy/information security.

22. The audit scope covered the period from 1 January 2023 to 31 December 2023. Where necessary, transactions and events pertaining to other periods were reviewed. The audit fieldwork was conducted from 29 January to 7 March 2024 at WFP headquarters in Rome.

23. The audit was conducted in conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing.

24. The audit reviewed through a consulting firm compliance and integration of international best practices and internationally recognized framework on IT third-party risk management (including ISO 27036, Information Technology – Security Techniques – Information Security for Supplier Relationships; ISO 27701 – Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management and ISO 22301 – Security and resilience – Business continuity management systems.

III.Results of the audit

Overview of conclusions

25. Table 1 outlines the extent to which audit work resulted in observations and agreed actions. These are classified according to the areas of coverage established for the audit (see paragraph 12) and are rated as medium or high priority; any observations that resulted in low-priority actions are not included in this report.

Table 1: Overview of focus areas, observations, and priority of agreed actions	**Priority of issues/agreed actions**
Focus area 1: Strategy and governance	
Observation 1 Third-party risk management	*High*
Observation 2 Management of IT partners	*Medium*
Focus area 2: Contracting	
Observation 3 Technical Assessment of IT vendors and partners	*Medium*
Focus area 3: Relationship Management	
Observation 4 Monitoring of performance and risks	*Medium*

26. An overview of the actions to be tracked by internal audit for implementation and their due dates can be found in Annex A.

Focus area 1: Strategy and governance

27. WFP across the globe continues to leverage and rely on third-party providers to achieve operational and business objectives. A third-party risk management framework ensures that the risk exposures associated with third parties are managed and monitored according to the organization's risk appetite and governance requirements. Best practices suggest that effective third-party risk management frameworks include adequate policies, procedures, and activities that support it; a structured support system comprising defined roles and responsibilities; a third-party inventory; risk rating criteria; and a risk assessment process and expectations related to third-party risk management controls.

28. At the time of the audit, the procurement unit initiated a Supplier Relationship Management (SRM) project that included establishing a framework for managing risks related to business relationships with third parties.

29. The audit reviewed the IT third-party risk management to evaluate the existence and effectiveness of the core elements of this process: (i) strategy, including alignment with existing strategies and tolerable risk levels and criteria; (ii) inventory of IT third parties; (iii) definition of roles and responsibilities; (iv) policies, operating procedures, guidelines and manuals; (v) methodologies and elements to support risk management (identification, assessment, evaluation, treatment and follow-up); (vi) information security, business continuity and privacy requirements and supporting application criteria.

Observation 1: Absence of a third-party risk management framework

30. The absence of a comprehensive and robust third-party risk management framework continues to hamper WFP's ability to identify, evaluate and control risks related to third parties, vendors, or partners. This is especially the case for IT vendors and partners where the following weaknesses were noted in governance, risk management and policy setting:

31. *Governance, roles, and responsibilities:* The organization has yet to establish a proper framework for the management of IT third-party risks throughout the lifecycle of the relationships. This extends to the process of identification, assessment, evaluation, treatment and monitoring of IT third-party risks, establishing technical requirements, ensuring compliance with technical requirements, and effectively managing third-party performance.

32. Overall, the organization lacks a comprehensive IT vendor/partner sourcing framework that supports existing TEC and other divisions' technology objectives and roadmaps. Such a management framework is necessary to define clear objectives and acceptable risk tolerance levels and to allocate resources and capabilities to manage IT third-party risks.

33. The audit also noted an absence of defined roles and responsibilities across functional teams, which would help drive accountability throughout the organization and provide the basis for the allocation of resources to carry out IT third-party risk management. Critical WFP functions such as TEC's security branch, the Global privacy office (GPO), and legal were not always involved in the establishment of contracts for IT vendors and partners.

34. *Risk management:* Although TEC identified potential threats to IT service delivery and business continuity, there was no corporate risk management process for third-party vendors and partners to ensure that the risk exposure associated with them was managed and monitored according to the organization's risk appetite and governance requirements.

35. *Policies and procedures:* While the due diligence and procurement processes were formalized and documented, other critical policy elements were missing, including guidelines and methodologies for identifying, assessing, categorizing, and managing IT risks. This led to significant gaps in awareness and

understanding among stakeholders involved in IT third-party risk management processes. As a result, potential risks and non-compliance issues within IT third-party relationships were not always identified.

36. *OIG's Internal Audit AR/20/02 on Third-party access to WFP Data and systems,* issued in January 2020, previously highlighted governance gaps impacting IT third-party risk management within WFP. Management actions to address these weaknesses are still outstanding in establishing a comprehensive and efficient third-party risk management framework within WFP.

Underlying cause(s): Limited corporate policies, processes, and resources to manage third-party vendors and partners risks; absence of adequate risk management processes at the corporate level to properly identify and continuously address and monitor IT third-party risks; TEC and other divisions' IT ambitions are not supported by a strategic process that involves identifying, managing, and overseeing risks related to third-party vendors providing IT products and services.

Agreed Actions [High priority]

1) The Supply Chain division:

(i) In coordination with the Technology division, and other relevant divisions, will support the integration of respective third-party risk management needs within the current Supplier Relationship Management project.

(ii) Establish policies, roles, and responsibilities for oversight, management, and support for third-party relationship management.

2) The Technology division, in coordination with the Risk Management Division, will set a risk appetite and key risk indicators for IT third-party selection, management, and services monitoring.

Timeline for implementation

1) 31 March 2025

2) 30 September 2025

Observation 2: Improvement needed in the management of IT partners

37. Management of IT partnerships across units is not standardized, and adequately supported by a comprehensive approach to IT third-party risks. The following weaknesses were noted in the IT partnership process:

38. *Contracting and onboarding of IT partners:* The due diligence process before partnering (in-kind donation) with IT firms was limited to reputational risks and did not include assessing critical IT and operational risks associated with the partner organisations. Additional risks related to conflict of interests, technology dependency and future cost of ownership were not always factored into the decision-making processes.

39. In addition, the Technology Industry Engagement (TIE) committee meetings, which establish gateways into IT partnerships and assess their risks and benefits, have not been held since 2022.

40. *Assessment of IT partnerships:* At the time of the audit fieldwork, TEC was not always involved in onboarding new IT partners to ensure alignment with the organization's IT strategy, IT architecture, IT existing solutions landscape, IT security policies and guidelines.

41. *IT Partnership inventory:* There was no clear definition of what constitutes a technological partnership within WFP. Even though a repository of private partnerships exists, it does not include a complete list of IT partnerships, WFP Innovation's unit associations or relevant IT relationships in-country offices.

Underlying cause(s): Absence of a third-party risks management framework to support the selection, onboarding, and management of IT partners' risks; no formalized process to systematically involve technical teams in the selection of IT partners; and de-prioritization of the TIE committee meetings.

Agreed Actions [Medium priority]

The Private Partnership division, in coordination with the Technology division and WFP Innovation Accelerator unit will:

(i) Formalize an IT partnership framework that includes a centralized role for private partnerships in managing IT private partnerships, a clear definition and harmonized use of existing inventories and tools of IT partnerships across interested and accountable parties and a mechanism to review and approve IT partnerships.

(ii) Establish a process which involves the Technology division applicable units for reviews and inputs during due diligence and the management processes of third IT partners.

Timeline for implementation

31 December 2024

Focus area 2: Contracting

42. The audit reviewed the management of contracts with IT third parties to evaluate the adequacy and effectiveness of: (i) controlled repository -centralized or distributed- of agreements with IT third parties; (ii) definition of roles and responsibilities; (iii) technical clauses for information security, business continuity and privacy; (iv) technical clauses for performance monitoring and relationship management; (v) supporting policies, operating procedures, and manuals.

43. The following observations were noted from a sample of ten IT vendors' contracts and 5 IT partnership agreements reviewed.

Observation 3: Absence of technical assessment of IT vendors and partners

44. Current due diligence processes for both commercial service providers and private partnerships are focused on financial, capability to operate for vendors and reputational risks for partners. These processes were not robust enough to ensure the third-party's information security risks, data privacy and business continuity risks were systematically and properly assessed.

45. *Assessment of IT vendors:* The IT vendor management process did not include in the pre-tender stage an analysis of potential risks that could arise from (i) the relationship with the IT vendor or (ii) the service or solution it provides. The audit found in only one out of ten contracts sampled that WFP performed a financial risk analysis to ensure the third-party's ability to provide critical services to the organization.

46. *IT Third parties' compliance with IT security standards:* IT security assurance reports, typically used as a reference note for compliance with industry IT security standards, were not requested by WFP. In the cases where the IT vendor provided such reports, the audit found that technical teams did not review them to provide assurance or follow up on the IT third-party IT security risks and posture. In addition, information security and data privacy annexes were not systematically added to the IT contract agreements.

Underlying cause(s): Inadequate resource allocation to support IT vendor selection processes; absence of a clear and formalized process to consistently assess, review and identify risks related to third-party IT vendors; inability to identify critical business impact and business continuity risks in the IT vendors' due diligence process.

Agreed Actions [Medium priority]

The Technology division, in collaboration with the Supply Chain Division, will establish clear IT requirements and checklists in the Goods and Services procurement manual to ensure that technical assessment and adequate procurement processes are consistently and thoroughly performed before and after establishing a relationship with IT third parties.

Timeline for implementation

30 June 2025

Focus area 3: Relationship Management

47. Management best practices define effective vendor relationship management as a continuous "to establish and nurture the links between the organization and its stakeholders at strategic and tactical levels. This includes the identification, analysis, monitoring, and continual improvement of relationships with and between stakeholders."[3]

48. The WFP procurement process requires conducting an IT vendor assessment at the end of a long-term agreement. Such assessments are necessary to enable WFP to track vendor performance over time and to support renewal decision-making.

49. The Office of Internal Audit reviewed the IT third-party relationship process to assess the existence and effectiveness of (i) a process for monitoring and managing vendor performance and compliance with service level agreements; (ii) a process for monitoring and managing technical requirements for information security, business continuity and privacy; (iii) an offboarding management process; and (iv) policies, operating procedures, guidelines and support manuals.

Observation 4: Monitoring of IT third parties' performance and risks requires improvement

50. The audit noted that there was no continuous evaluation and monitoring of IT vendor and partner performance to ensure service quality, adherence to contractual requirements and compliance with international IT standards and regulations.

51. *Compliance with service level agreements:* There was no monitoring of compliance or existence of applicable or expected information security, business continuity and privacy requirements of the IT third-party service or product during the relationship. Monitoring of compliance with service level agreements and other performance metrics during the relationship was not formalized or performed with sufficient frequency.

52. *Policies and guidelines:* There were no standard operating procedures (SOP), guidelines, or manuals for ongoing risk management, review of applicable technical requirements, or monitoring service level agreements. There were no documented processes to define or guide the IT third-party relationship model and service operation procedures.

[3] Best management practices from the Information Technology Infrastructure Library (ITIL) framework

53. *Data retention clause:* WFP Data removal and destruction (from third-party systems and solutions) following the end of the business relationship are not included in WFP contracts. As WFP's data retention policy is not up to date, this limits the organization's ability to set an IT third-party's retention policy and creates privacy risks in its dealings with IT third parties.

Underlying cause(s): Lack of a structured framework and governance for managing third-party relationships; absence of standardized procedures for continuous performance monitoring.

Agreed Actions [Medium priority]

1) The Technology division will establish, following the implementation of the IT third-party relationship management process, standard and operating procedures, for applicable technical requirements, and monitoring of service level agreements.

2) The Technology division, in coordination with the Legal division, will include clauses related to WFP data retention, removal, and destruction in applicable contracts.

Timeline for implementation

1) 30 June 2025

2) 31 December 2025

Annex A – Agreed action plan

The following table 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 the macro analysis of audit findings and monitoring the implementation of agreed actions.

#	Observation	Focus Area	Owner	Priority	Timeline for implementation
1	Third-party risk management	Area 1: Strategy and governance	Supply Chain & Technology Divisions	High	31 March 2025 30 Sept 2025
2	Management of IT partners	Area 1: Strategy and governance	Private Partnerships	Medium	31 Dec 2024
3	Technical Assessment of IT third-party vendors and partners	Area 2: Contracting	Technology Division	Medium	30 June 2025
4	Monitoring of performance and risks	Area 3: Relationship Management	Technology Division	Medium	30 June 2025 31 Dec 2025

Annex B – Definitions of audit terms: ratings & priority

1 Rating system

The internal audit services of UNDP, UNFPA, 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.
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.
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 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 a 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.

3 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.

Office of Internal Audit monitors agreed on actions from the date of the issuance of the report with regular reporting to senior management, the Independent Oversight Advisory 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, the Office of Internal Audit 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, the Office of Internal Audit 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. Office of Internal Audit informs senior management, the Audit Committee and the Executive Board of actions closed without mitigating the risk on a regular basis.

Annex C – Acronyms

GPO	WFP Global Privacy Office
INKA	WFP Innovation Accelerator
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LEG	WFP Legal Office
OIG	Office of the Inspector General
RMD	Risk Management Division
SOC	System and Organization Controls reports
SOP	Standard operating procedures
PSP	WFP Private Sector Partnership
SRM	WFP Supply Chain 's Supplier Relationship Project
TEC	Technology Division
TEC R	Resource Management Branch of the Technology unit
TEC I	Information Security Branch of the Technology Division
TIE	WFP Technology Industry Engagement Committee
WFP	World Food Programme