Fighting Hunger Worldwide

Internal Audit of the Operationalization of WFP's Enterprise Risk Management

Office of the Inspector General
Internal Audit Report AR/17/13

WFP

World Food Programme

wfp.org

Contents

Internal Audit of the Operationalization of WFP's Enterprise Risk Management

I. Executive Summary

Introduction and context

1. As part of its annual work plan, the Office of Internal Audit conducted an internal audit of the operationalization of WFP's Enterprise Risk Management, focused on the period 1 January 2016 to 31 March 2017.

2. WFP's mission requires its managers to take informed decisions that balance risk and opportunity, and, in certain instances, offset one type of risk against another. Transparent and proactive risk-taking and sharing, considering the cost of risk prevention and response, are at the core of the aid effectiveness agenda. The organization is committed to the Agenda 2030 and the Grand Bargain and supports government and community capacities to establish risk management mechanisms. This involves enhancing their ability to transition from crisis response to risk reduction and management.

3. Enterprise Risk Management is not new to WFP; the organization's Enterprise Risk Management Policy was first introduced in 2005 and updated in 2015. Subsequently, WFP also updated its Internal Control Framework, recognizing that key aspects such as its risk management philosophy, objective setting, risk appetite and risk tolerance are now governed through the 2015 policy, and in 2016 by its Risk Appetite Statement.

4. Acknowledging the alignment of these policies with latest industry standards, the audit focused on how WFP's Enterprise Risk Management has been put into practice. The audit took into consideration that WFP, facing ever larger humanitarian needs, is undergoing transformational change. It is aligning its financial and results frameworks to the Sustainable Development Goals, creating a 'line of sight' for better performance management. The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

Audit conclusions and key results

5. WFP has adopted the United Nations reference risk management, oversight and accountability model, applies the Organizational Resilience Management System and participates in the Programme Criticality Steering Group with its recently updated framework. WFP continues to play an active role in shaping the discussion for a United Nations policy framework on risk management and resilience building.

6. The audit found that Enterprise Risk Management in WFP is designed with a clear link to performance management. However, while risk management practices applied are in line with WFP's policy, in day-to-day operations these take an informal approach, often without documentation or consolidation. Operational managers interviewed indicate that currently available tools and processes for Enterprise Risk Management are not necessarily perceived as 'adding value'.

7. Beyond entity-specific performance plans and risk registers, stand-alone guidance, tools and processes (including dedicated staff resources) exist for specific risk categories – as foreseen in the WFP policy – at process level. These siloed efforts (although aligned in principles and language with corporate Enterprise Risk Management policy) contribute to a fragmented, instead of a comprehensive, visibility of WFP's risk exposure. This is because there are no mechanisms and incentives to ensure that this risk information is effectively fed into an organization-wide risk

portfolio view. Examples include the Emergency Preparedness and Response Package or Security Risk Assessments.

8. Without the systematic capturing of residual risks, limited use of key risk indicators and insufficient clarity on assigned responsibilities for risk responses or monitoring the effectiveness of mitigating measures, WFP may miss opportunities to balance risk-taking decisions throughout the portfolio management cycle. More importantly, WFP may also fail to communicate with donors and partners its context-specific risk appetite. As a result, it could miss valuable cost-benefit discussions regarding the means, readiness and agility to remain within acceptable risk tolerance levels.

9. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **partially satisfactory**. Conclusions are summarised in Table 1 by the lines of inquiry defined for the audit:

Table 1: Summary of risks by lines of inquiry

Do ERM processes & procedures:		Risk	
1.	Establish a consistent risk-management framework?	Medium	🟨
2.	Facilitate risk-informed decision-making?	Medium	🟨
3.	Allow WFP to communicate with partners and stakeholders?	High	🟥

10. The audit report contains two high-risk observations and three medium-risk observations. The high-risk observations are:

Leadership and accountability: Scope for improvement was noted regarding leadership, incentive systems and accountability mechanisms for enforcing the use of Enterprise Risk Management tools and processes, for which there had recently been limited investment in training and staff time. The audit noted that some roles and responsibilities were not clear, with performance management tools insufficiently used to assign ownership for risk responses. In addition, Regional Bureaux and Headquarters' second line of defence functions do not systematically review status and effectiveness of mitigating measures. Lacking key risk indicator information and the system support for organization-wide analysis of WFP's risk portfolio, the corporate risk function (within the Division of Performance Management and Monitoring) is intended to be the process expert, analyst, facilitator and custodian of the Corporate Risk Register. It was observed to be dependent on collaboration with, and input from, various risk and control experts, operating in a fragmented manner across WFP.

Communication culture and protocols: Scope for improvement was also identified in both internal and external communication. Lacking defined escalation mechanisms, informal channels were used for internal risk and issue escalation, which leave no documented trails for enforcing accountability. Such informal channels also contribute to a culture of a perceived need to keep risk information confidential, instead of encouraging proactive sharing for informed decision-making, organizational analysis and learning. This also applies to external parties, in particular with reference to risk-sharing with partners and stakeholders throughout the country portfolio management cycle.

11. Management has agreed to address the reported observations and work to implement the agreed actions by their respective due dates. The Office of Internal Audit would like to thank managers and staff for their assistance and cooperation during the audit.

Anita Hirsch
Acting Inspector General

II. Context and Scope

Enterprise Risk Management in WFP

12. Acknowledging that the humanitarian imperative requires WFP to operate in risky environments "*where the risks of failing to engage are deemed to outweigh the risks of engagement*"[1], Enterprise Risk Management (ERM) in WFP has been designed as an Executive Board-approved framework (WFP/EB.A/2015/5-B). This framework outlines risk management philosophy, risk appetite and risk tolerance. ERM overarches and informs internal control and risk response choices to best assist the beneficiaries and stakeholders WFP serves: managing and not merely avoiding or transferring risks.

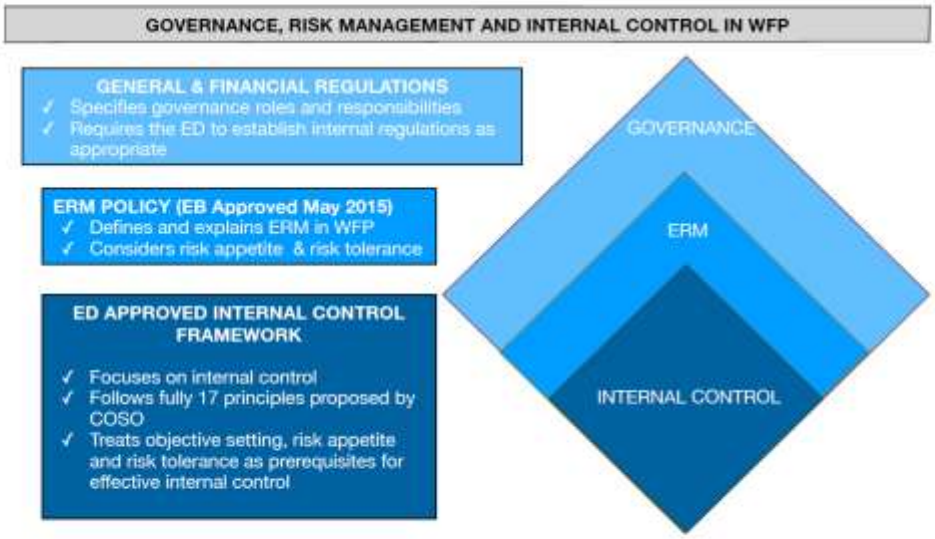
GOVERNANCE, RISK MANAGEMENT AND INTERNAL CONTROL IN WFP
GENERAL & FINANCIAL REGULATIONS
✓ Specifies governance roles and responsibilities
✓ Requires the ED to establish internal regulations as appropriate
ERM POLICY (EB Approved May 2015)
✓ Defines and explains ERM in WFP
✓ Considers risk appetite & risk tolerance
ED APPROVED INTERNAL CONTROL FRAMEWORK
✓ Focuses on internal control
✓ Follows fully 17 principles proposed by COSO
✓ Treats objective setting, risk appetite and risk tolerance as prerequisites for effective internal control
GOVERNANCE
ERM
INTERNAL CONTROL

Figure 1: Governance, ERM and Internal Control relationships as outlined in WFP's Internal Control Framework (ED Circular)

13. 13. WFP's humanitarian goals are to provide life-saving assistance where it is needed most using innovative approaches and working in partnership to end hunger. These goals require its managers to take informed decisions that balance risk and opportunity, and in certain instances offset one type of risk against another[2]. Committed to the Agenda 2030 and the Grand Bargain, WFP takes active part in system-wide discussions; for example, the UN High-Level Committee on Programmes, which acknowledges that "an innovative, multi-hazard and cross-pillar approach to assessing and managing risks to sustainable development was indeed required more than ever"[3], and the UN High-Level Committee on Management which, considering a heightened threat environment and committing to duty of care, prominently placed risk management in the approach of 'how to deliver'[4].

14. The necessity for further 'Strengthening Enterprise Risk Management and WFP's Internal Control Culture' became the theme of a dedicated WFP Global Management Meeting on 30 March 2017. The entire WFP management team reaffirmed their commitment to embedding the principles of risk management and internal control into day-to-day work and discussed actions to move towards a stronger culture of risk-informed management.

[1] Text in *italics* is cited from WFP Enterprise Risk Management Policy (WFP/EB.A/2015/5-B)
[2] WFP – like other aid or assistance actors – has adopted the categories of contextual, operational and institutional risks; and in designing and managing its country portfolios WFP is regularly obliged to mediate between short-term fiduciary concerns and long-term sustainability goals or advocate for the cost-effectiveness of prevention over mitigation actions.
[3] Agenda item 1 of High-level Committee on Programmes at its 32nd session (CEB-2016-6-HLCP32).
[4] HLCM Strategic Plan 2017-2020.

Objective and scope of the audit

15. The Office of Internal Audit (OIGA) included an audit of WFP's ERM in its 2017 work plan since several audits as well as advisory work in 2016 highlighted the need to strengthen organizational risk assessment and management processes, tools and guidance, including fraud risk assessment, to ensure that these are embedded in WFP's day-to-day operations and effectively used to drive risk-based dialogue and decision-making.

16. During the planning phase of this audit, OIGA considered WFP's operating context, current developments and ongoing change initiatives. Recognizing the role of WFP's ERM to help adequately calibrate (considering the cost of control) between risk taking and risk aversion to steer the organization towards improved performance, OIGA assessed WFP's ERM Policy against the Committee of Sponsoring Organizations of the Treadway Commission (COSO) standards[5].

17. In view of the general alignment of WFP's ERM Policy with best-practice standards, the audit was scoped to focus on operationalization of the policy, which foresees risk management to be implemented at:

- *process level*[6]*;*
- *unit level (country office (CO), regional bureau (RB) or headquarters (HQ) division); and*
- *corporate level*[2].

18. Feedback was obtained through surveys and audit interviews from all levels of the organization. Detailed audit testing covered the period from 1 January 2016 to 31 March 2017, but also looked at earlier and later events, as needed. The testing also covered risk management practices not necessarily captured in ERM tools and processes maintained by the Strategy Implementation and Risk Management branch of the Performance Management and Monitoring division (RMP).

19. Through its ERM Policy, WFP aims to ensure *that its operating environment supports effective levels of control. This involves: i) identification of current and emerging risks; ii) provision of guidance on how to respond to risks in line with WFP's risk appetite; iii) escalation of risks as required; and iv) communication of risks and mitigation actions to stakeholders. The goal is optimal management of activities and achievement of objectives in the complex environments in which WFP operates*[2]. The audit followed lines of inquiry derived from these characteristics and goals outlined in WFP's policy (refer to table B.1 in Annex B) which were designed to provide a means of enquiring whether Enterprise Risk Management processes and procedures in WFP:

(1) Establish a *consistent risk-management framework through which risks can be identified, analysed and addressed, and accountability assigned*?

(2) Facilitate risk-informed decision-making where *decisions to engage are based upon analyses of the benefits of engagement and the costs of risk mitigation*?

(3) Allow WFP to *communicate with partners and stakeholders about the level of risk it is prepared to accept, and to be proactive in taking decisions on sharing risk and developing joint mitigation actions*?

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 before the audit.

[5] Principles outlined in the proposed update to COSO's ERM Framework: *Enterprise Risk Management — Aligning Risk with Strategy and Performance* (Exposure Draft) & WFP's Internal Control Framework based on COSO components.

[6] Examples of processes include the emergency preparedness and response exercise (focused on contextual risks), security risk assessments (contextual and programmatic risks) and financial risk management (institutional risks).

III. Results of the Audit

21. In performing the audit, the following positive practices and initiatives were noted:

Table 2: Positive practices and initiatives

Control Environment

- The ERM Policy overarches WFP's Internal Control Framework, which has been implemented in line with the UN reference risk management, oversight and accountability model.
- Risk management is a day-to-day activity, actively embraced in WFP culture; various tools and processes exist beyond the Corporate Risk Register and entity risk logs.
- A mandatory manager certification process (Internal Control Framework compliance) reminds WFP managers of their risk management responsibilities, including fraud risk.

Risk Assessment

- WFP has defined and recently updated its Corporate Risk Appetite Statement, intended to guide risk tolerance, which is publicly shared with stakeholders.
- The Integrated Road Map (IRM) introduces a Strategic Review for programme design that provides a comprehensive analysis of the challenges facing a country.
- Emergency operations (Levels 2 and 3) have defined protocols to ensure the involvement of experienced managers in risk-informed decision-making.
- For other operations there are an increasing number of fora (working groups, etc.) to discuss risk cross-functionally.

Control Activities

- WFP's ERM Policy foresees risk logs at a strategic level and at operational (entity/unit) levels to define and monitor risk responses. At the strategic level, the Executive Management Group (EMG) regularly reviews the Corporate Risk Register.
- WFP applies the UN Organizational Resilience Management System (Crisis Management and Business Continuity Management) as core elements.
- For certain risks at the core of WFP's business (i.e. contextual risks) the organization has:
  - built renowned expertise;
  - put in place a standardized, risk-informed approach for preparedness and response; and
  - generated cost awareness (return on investment studies) for prevention versus treatment.
- For a number of institutional risks (including for example cash-based transfers, partnership or supply chain management) new tools and/or guidance are under development.

Information and Communication

- WFP's Corporate Risk Register and Risk Appetite Statement are shared and discussed with the Audit Committee and the Executive Board.
- WFP performs lessons learned exercises (corporate listening exercises) aimed at identifying the successes and areas for improvement of corporate emergency responses. These inform future emergency responses, reviews, protocols, processes and policies.
- There is active WFP engagement in inter-agency and other fora for joint risk language and approaches; for example http://www.inform-index.org/.

Monitoring Activities

- There are efforts to prioritize oversight (second and third line of defence) based on risk register data, plus parallel risk identification and oversight prioritization processes exist.
- The Corporate Risk Register is fed by risk and oversight analyses.

22. Having evaluated and tested the controls in place, the Office of Internal Audit has concluded on the residual risk related to each of the lines of inquiry defined for the audit (see Table 1 above) and also by internal control component; these results are presented in Annex B.

23. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of *partially satisfactory*[7].

24. The audit report contains two high-risk observations and three medium-risk observations. Tables 3 and 4 below present the high and medium-risk observations respectively.

Action agreed

25. Management has agreed to take measures to address the reported observations.[8]

[7] See Annex C for definitions of audit terms.

[8] Implementation will be verified through the Office of Internal Audit's standard system for monitoring agreed actions.

Table 3: High-risk observations

Observation	Agreed Action
1 **Leadership and accountability** The audit noted strong interest and appetite from WFP managers for risk management. This was considered to be a core leadership skill, critical for allowing the organization to identify and pursue innovative solutions, to ensure controls are adjusted to varying contexts and operating priorities, and to gear WFP's delivery towards the best results for the people it serves. However the audit also observed significant variation in leadership preferences for the use of ERM tools and processes, and varying degrees of knowledge and understanding of the ERM framework. Risk identification, response and escalation were in many instances observed to take an informal approach, without documentation or consolidation. In practice the zero cost roll-out strategy for the 2015 ERM Policy, the 'Fit for Purpose' decentralization initiative, and the decommissioning in 2016 of a planned ERM IT system resulted in: • Tasks related to maintaining risk registers being assigned as add-on responsibilities to focal points, and limited investment in staffing resources, time and training after 2014; • Risk and control ownership not being assigned at the appropriate level, and/or those owners not being held sufficiently accountable through existing performance management tools; • Development of stand-alone guidance, tools and processes for specific risk categories, which although aligned in principles and language with the corporate ERM policy operate in silos, and in some cases outside HQ, almost in competition with the tools and processes used for ERM. Recent efforts by various HQ divisions to strengthen risk management practices have further contributed to the fragmentation in risk documentation; and • Varying use of the Corporate Risk Register (CRR) and entity-specific risk registers at HQ, RB and CO-level by HQ functions for risk analysis and priority setting. The Strategy Implementation and Risk Management branch of RMP was intended to be the process expert, analyst, facilitator and custodian of the CRR. However the audit observed that, lacking key risk indicator information and system support for organization-wide analysis of WFP's risk portfolio, the unit was dependent on collaboration with and input from various risk and control experts operating in a fragmented way across the organization. Underlying Cause Weak leadership and accountability mechanisms. Some roles and responsibilities are not clear and/or were assigned without consideration for required seniority. Inadequate incentive systems for use of ERM tools and processes. Limited investment in training and staff time for ERM.	(1) OED will, in consultation with the EMG, clarify roles and responsibilities and where applicable the required level of seniority of: i. First line of defence risk managers at CO, RB and HQ levels, which should ensure the right risk information is collected and shared to then be acted upon; ii. Second line of defence experts in RBs and HQ (in specific functional areas), which should include quality assurance and review of risk registers, monitoring of countries with function-specific risks, advice on appropriate mitigation measures as well as analysis, consolidation and further escalation of risks; and iii. The corporate ERM function, which should act as ERM process expert, facilitator and custodian of tools, and have appropriate access to the analysis undertaken by experts in all functional areas to allow for prioritization of strategic risks in the CRR and overview of operational risks across WFP (entity-level risk registers). (2) RMP will update and implement improved ERM facilitation and training (especially for CO management jointly with HRM) and liaise with other HQ functions (such as ETO, OIG, PG and others) where risk/control-specific training is needed or where external partners require training on ERM.

2 **Communication culture and protocols**

While the audit observed that risk and issue escalation happens on a day-to-day basis and through various management channels, such informal communication mechanisms leave no trails for enforcing accountability, which is especially unclear in cases of risk sharing. This in turn inhibits the organization from learning and avoiding repetitive errors. The lack of clear indications as to when risk escalation is required (when residual risk is beyond local 'risk management authority') contributes to the accountability issues outlined in observation 1 and could impede awareness and management of risks at adequate levels.

With respect to inhibitors for sharing risk information in WFP's culture context, certain functions flagged a need for treating certain issues confidentially, which current risk logs do not facilitate. While this argument may be justified for certain specific risks, for most risks more clear information sharing is preferable (see also observation 5).

The audit noted that an ongoing internal discussion to strengthen risk management and internal control places emphasis on enforcing compliance without necessarily giving sufficient attention to putting in place the systems, rules, norms, culture and incentives to ensure the right risk information is collected and shared to then be acted upon.

Audit interviews also highlighted the need at CO and functional level for:

- More frequent and structured cross-functional discussion of risk in order to obtain guidance and support if needed (refer also to observation 4: risk appetite and its application to context),
- Better information flow on risk analysis as well as on the prioritized, strategic risks from the CRR (refer also to observation 1: role of risk/control experts for analysis, and to observation 5: aggregate portfolio view of risks across the organization).

In the SDG operating environment, with a growing focus on working with partners (including host governments), WFP has to increasingly rebalance risk choices to achieve shared objectives. It also has to communicate its choices adequately. A culture that inhibits proactive discussion of risks and the need for controls may also inhibit valuable cost-benefit discussions on what it requires to be prepared or agile, or to remain within acceptable risk tolerance levels.

Unclear communication and/or understanding of WFP's risk appetite and/or insufficient alignment of the appetite with donor expectations increases the potential for reputational risk to materialize.

Underlying Cause ERM policy not clear on escalation/de-escalation guidelines. Lack of communication protocols for risk-related information to both internal and external parties.

RMP will:

(a) Develop guidelines on escalation/de-escalation to complement and augment the otherwise comprehensive ERM policy. These will include guidance on responsibility for higher-level risk and control owners to elevate risks where residual risks are beyond a local 'risk management authority'.

(b) In collaboration with relevant partnership divisions, define protocols for sharing risk information with partners and donors using shared language[9].

[9] For example, utilization of www.inform-index.org, linking UNDAF/UNCT/HRP risk logs as well as those of clusters to WFP-specific risk registers.

Table 4: Medium-risk observations

	Observation	Agreed Action
3	**Key risk indicators and use of alerts and feedback loops** The ERM infrastructure does not facilitate a portfolio view of risks nor a documented escalation process (which however may exist in day-to-day communication and informal feedback mechanisms). The audit also noted that there are limited other tools (for example reports, dashboards, or information sources) which provide alerts about emerging or pertaining risks. Where key risk indicators (KRIs) exist, there is no clear linkage to ERM tools and processes: • Acceptable variance in performance is not defined or not used as a KRI; • There is limited analysis of actual incidents compared to risks monitored and overall exposure; and • There is a risk that donor, partner or beneficiary concerns flagged through various channels (for example, complaint mechanisms) may be acted upon individually without a link to feed information regarding risk priorities or risk management capacity into ERM structures. Notwithstanding effective use of risk analysis (including review of oversight findings) feeding the CRR, the audit noted that risk registers remained quite static. In some instances, the CRR had started to replace entity-level risk registers for certain HQ-divisions, defeating the purpose of prioritizing/differentiating strategic versus operational risks. The above points result not only in inefficiencies; they may also result in insufficient prioritization of mitigating actions or recurrence of risks, which may impact WFP's reputation. Underlying Cause Few KRIs are defined and monitored; without such KRIs the definition of risk tolerance levels that translates WFP's risk appetite statement into meaningful guidance lacks an important building block. Limited benchmarking and analysis of changes in stakeholder perceptions and practices.	RMP will: (a) Work with functional experts to define KRIs (for example, red flags, inacceptable variations in performance, risk tolerance ranges and thresholds) to improve internal feedback loops and alerts and respective monitoring. These KRIs will be used as metrical ranges or thresholds to enhance guidance related to the Corporate Risk Appetite. (b) Define, in collaboration with PG, external alert mechanisms (for example, based on risk discussions in operational briefs for quarterly Executive Board briefings) as well as feedback loops (such as donor feedback on proposals or findings from verification exercises, partners' assessments regarding WFP's risk sharing).
4	**Residual risk, risk appetite and its application to context** Acknowledging that WFP operates in various contexts with varying internal capacity, and that there are also significant variations in the risk appetite of WFP's diverse donors in those varying contexts, the audit observed that balancing risk choices without a clear context-specific communication tool proves difficult. There is a strong trend towards increasing donor scrutiny (including earmarking of funding, additional reporting requirements and in certain cases specific due diligence/verification exercises) with a potential negative impact on overhead cost and/or adherence to aid-effectiveness principles and commitments.	RMP will: (a) In liaison with the IRM project introduce country portfolio-specific risk appetites within the ranges of corporate risk appetite thresholds. These will provide for more effective internal management and review (including internal review at the design stage documenting the assessment of risk exposure as well as of WFP's and partners' risk capacity) and improve communication with donors and partners.

	Audit interviews highlighted that while WFP actively searches for innovative solutions and effective delivery mechanisms for the various contexts, the ERM framework was not cited as a mechanism to facilitate re-thinking of processes and controls during programme design and implementation, but rather as a bureaucratic tool to give assurance to risk-averse internal and external stakeholders. From existing risk registers it is difficult to obtain a clear view on residual risk and the status of risk responses (refer also to observation 5). While WFP's ERM policy is designed to facilitate risk-informed decision-making, the audit observed this practice to happen either without documentation or not in an easily accessible way to provide for strategic review, to ensure the right information is collected and shared, and that it is acted upon to ensure that residual risk remains at acceptable cost within agreed appetite. Underlying Cause The risk appetite statement is too generic to function as guidance tool. Risk registers in the annual performance planning (APP) (where not embraced as key management tool within the programme cycle) are perceived as tick-box exercises filled for compliance purposes. Appropriateness and status of mitigating measures (residual risk) are not formally tracked and monitored.	(b) Provide clear guidance on how risk registers should be used in the annual planning and reporting cycle foreseen in the IRM roll-out in order to monitor on a timely and regular basis: i. Changes to the identified threats and opportunities which were the basis for defining the specific risk appetite, to ensure their updates; and ii. The status of implementation and effectiveness of mitigation measures and residual risks with respect to a country portfolio-specific risk appetite.
5	**System support** Since the decommissioning of a planned and partially rolled out risk and performance database, WFP implements its ERM with the use of Excel spreadsheets/Word documents as part of the APP and review process. The audit noted that this process is resource-intensive and has the following shortcomings: • Unless actively shared (within an office and to higher levels), risk registers are not visible within the organization; the lack of visibility creates pervasive CO/RB challenges to gain warranted HQ management/policy maker attention; • The risk register template is not perceived as sufficiently simple and intuitive. Free text risk descriptions and currently available classifications inhibit aggregation and a portfolio view (for instance, experts in HQ, RBs and RMP do not have cross-cutting views on risks); • The audit noted few instances where emerging risks were added to risk registers on a timely basis. (Such risks were often handled outside of the ERM system); and • The timing of the APP exercise, which embeds risk assessment (December-February) and the lack of a time gap between submission deadlines for COs, RBs and HQ units impedes review and analysis, and ultimately overall acceptance of the usefulness of the tool. Underlying Cause No formal ERM tool (database). Current risk taxonomy does not facilitate aggregation and review. Periodic review of risk registers is not well anchored in business processes.	RMP will, building on the lessons learned from the planned and partially rolled-out risk and performance database and a review of the risk register template, implement an online and real-time database which will facilitate risk management processes and ensure: i. An aggregate portfolio view of risks across the organization; ii. Enforced accountability (including mitigation action tracking and automation of escalation); iii. Real-time and multi-user access, thereby facilitating capture of emerging risks and elimination of data entry clerk roles; and iv. Confidentiality aspects (viewing rights) while maximising internal visibility of risk information.

Annex A – Summary of categorization of observations

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

Observation		**Risk categories**					
		WFP's ICF	**WFP's Management Results Dimensions**	**WFP's Risk Management Framework**	**Underlying cause category**	**Owner**	**Due date**
1	Leadership and accountability	Compliance	People Accountability and Funding	Institutional	Resources Guidance	OED RMP	31 December 2017 31 July 2018
2	Communication culture and protocols	Reporting Operational	Partnerships	Institutional	Guidance	RMP	31 July 2018
3	Key risk indicators and use of alerts and feedback loops	Strategic Operational	Accountability and Funding	Operational	Best practice	RMP	31 July 2018
4	Residual risk, risk appetite and its application to context	Strategic Operational	Programmes	Operational	Guidelines	RMP	31 July 2018
5	System support	Reporting Operational	Processes and Systems	Institutional	Guidelines	RMP	31 July 2018

Annex B – Conclusions on risk by process areas reviewed

Table B.1: Conclusions on risk by audit process areas and by lines of inquiry

Do ERM processes & procedures in WFP[10]:	**Design of WFP's Policies**	**Operationalization of WFP's Policies**		**Observations 1-5**				
		ERM tools (corporate and unit-level risk registers)	**Other processes**					
(1) Establish a *consistent risk-management framework through which risks can be identified, analysed and addressed, and accountability assigned*? 🟨				**1**	**2**	**3**	**4**	**5**
i) identification of current and emerging risks	✓	O	O				M	M
ii) provision of guidance on how to respond to risks in line with WFP's risk appetite	✓	O	O	H		M		
iii) escalation of risks as required	✓	x	O		H			M
(2) Facilitate risk-informed decision-making where *decisions to engage are based upon analyses of the benefits of engagement and the costs of risk mitigation*? 🟨				**1**	**2**	**3**	**4**	**5**
The goal is optimal management of activities and achievement of objectives in the complex environments in which WFP operates	✓	O	O		H			M
(3) Allow WFP to *communicate with partners and stakeholders about the level of risk it is prepared to accept, and to be proactive in taking decisions on sharing risk and developing joint mitigation actions*? 🟥				**1**	**2**	**3**	**4**	**5**
iv) communication of risks and mitigation actions to stakeholders	✓	x	x	H	H	M	M	

Legend: ✓ No issue noted **O** Scope for improvement **x** Issues identified **H** – High **M** - Medium

[10] Text in *italics* is cited from WFP Enterprise Risk Management Policy (WFP/EB.A/2015/5-B)

Annex C – Definition of categorization of observations

1. Rating system

1. Internal control components and processes are rated according to the degree of related risk. These ratings are part of the system of evaluating the adequacy of WFP's risk management, control and governance processes. A rating of satisfactory, partially satisfactory or unsatisfactory is reported in each audit. These categories are defined as follows:

Table C.1: Rating system

Engagement rating	Definition	Assurance level
Satisfactory	Internal controls, governance and risk management practices are adequately established and functioning well. No issues were identified that would significantly affect the achievement of the objectives of the audited entity.	Reasonable assurance can be provided.
Partially Satisfactory	Internal controls, governance and risk management practices are generally established and functioning, but need improvement. One or several issues were identified that may negatively affect the achievement of the objectives of the audited entity.	Reasonable assurance is at risk.
Unsatisfactory	Internal controls, governance and risk management practices are either not established or not functioning well. The issues identified were such that the achievement of the overall objectives of the audited entity could be seriously compromised.	Reasonable assurance cannot be provided.

2. Risk categorization of audit observations

2. Audit observations are categorized by impact or importance (high, medium or low risk) as shown in Table C.2 below. Typically audit observations can be viewed on two levels: (1) observations that are specific to an office, unit or division; and (2) observations that may relate to a broader policy, process or corporate decision and may have broad impact.[11]

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

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

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

3. WFP's Internal Control Framework (ICF)

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

5. WFP defines internal control as: "a process, effected by WFP's Executive Board, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, compliance."[12] WFP recognises five interrelated components (ICF components) of internal control, all of which need to be in place and integrated for them to be effective across the above three areas of internal control objectives.

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

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

4. Risk categories

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

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

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

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

[12] OED 2015/016 para.7

Table C.5: Categories of risk – WFP's Management Results Dimensions

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

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

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

5. Causes or sources of audit observations

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

Table C.7: Categories of causes or sources

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

6. Monitoring the implementation of agreed actions

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 so as to manage and mitigate the associated risks identified, thereby contributing to the improvement of WFP's operations.

Annex D – Acronyms

APP	Annual Performance Planning
CBT	Cash-Based Transfers
CO	Country Office
CO RR	Country Office Risk Register
CRR	Corporate Risk Register
COSO	Committee of Sponsoring Organizations of the Treadway Commission[13]
EMG	Executive Management Group
ERM	Enterprise Risk Management
EPRP	Emergency Preparedness and Response Package
ETO	Ethics Office
HLCM	(United Nations) High-Level Committee on Management
HLCP	(United Nations) High-Level Committee on Programme
HRP	Humanitarian Response Plan
ICF	Internal Control Framework
IRM	Integrated Road Map
OIG	Inspector General & Oversight Office
OIGA	Office of Internal Audit
PG	Partnership, Governance and Advocacy Department
RBs	Regional Bureaux
RMP	Performance Management and Monitoring Division
RMPS	Strategy Implementation and Risk Management Branch
UN	United Nations
UNDAF	UN Development Assistance Framework
UNCT	UN Country Team
WFP	World Food Programme

[13] A joint initiative of five private sector organizations (www.coso.org) dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.