WFP's 2018 enterprise risk management policy

Informal consultation

24 July 2018

World Food Programme
Rome, Italy

Executive summary

As a voluntarily funded organization, WFP depends on the confidence of its donors, host governments and many other stakeholders to fulfil its mandate. Despite operating in some difficult environments, WFP aims to maintain its reputation and the trust of its stakeholders by upholding transparency, accountability and high standards of integrity. WFP also operates in very dynamic environments, where needs and the means to fulfil them are continually changing, requiring WFP to adapt and innovate in a sustainable and effective way. Risk is therefore an ever-present consideration in decision-making at WFP.

Risk-informed decisions help to build organizational reliability and resilience. Within this context, enterprise risk management is designed to provide structure, consistency and transparency in risk decision-making across the organization. It provides a framework whereby all risks – strategic, operational, fiduciary and financial – can be identified, assessed and managed in accordance with the organization's appetite for risk.

Risk appetite, and the processes which bring it to life, is an important concept within this policy. For certain risks, such as developing its business model and its desire to innovate, WFP's risk taking may be characterized as "risk hungry"; for others, such as managing fiduciary responsibilities and countering potential fraud and corruption, WFP may be considered highly "risk averse". Achieving common understanding, both internally and among external stakeholders of what risks WFP is comfortable with and those it is not, is a core objective of enterprise risk management implementation. Where WFP is operating within appetite, it may wish to assume more risk within appropriate authority; where it is outside of its risk appetite, it needs to take prompt and effective action to reduce exposure or mitigate risk.

Accountability for taking action and addressing risk is another important element of this policy. Senior management, in particular regional and country directors, have clear responsibilities for owning and managing risk within their remit. Functional directors may also own certain risks, and in their capacity as technical specialists, they are expected to determine the boundaries of risk appetite for their area of specialism and engage with managers who are responsible for decisions. Risk appetite therefore forms the basis for engagement and challenge between "first line" risk decision-makers and "second line" risk specialists. This is designed to strengthen the organization, providing a mechanism whereby risks can be escalated and decisions agreed with appropriate technical input and risk expertise.

To be effective and reinforce the culture of accountability, risk management needs to be an iterative, inclusive and interactive process. Risk assessments need to be informed by regular reporting of risk appetite metrics as well as from more periodic oversight and assurance activities. The risk appetite statements within this policy, therefore, form the basis for internal reporting and escalation of risks and are central to driving the process of continuous improvement.

The risk appetite statements have been updated since they were last revised in 2016. The statements have been consulted and agreed internally with functional specialists who act as Risk Leads for each area of risk. Their "second line" responsibilities outlined within the policy are particularly important in embedding risk appetite throughout the organization, providing advisory support for risk mitigation, and achieving the vision for implementing enterprise risk management at WFP.

Implementation is further cemented by the processes and reporting mechanisms described within this policy for managing risk. Together, embedding of risk appetite, the interaction of first and second line actors, and consistent risk processes, reporting and escalation provide the basis for implementation of enterprise risk management at WFP, building on the architecture of governing bodies, assurance and high-level responsibilities outlined in WFP's 2018 Oversight Framework.[1]

Introduction

Enterprise risk management (ERM) is not new to WFP; the organization's enterprise risk management policy was first introduced in 2005[2] and updated in 2015.[3] 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 were governed through the 2015 policy.

In 2012, WFP prepared and shared its risk appetite statements,[4] identifying the direction for the organization in responding to risk, including at the operational level. The updated risk appetite statements from 2016[5] incorporated the themes/issues that emerged through the quarterly Executive Management Group meetings on risk management since 2012 and built on the deepened understanding of the risks the organization faces.

WFP's 2010 anti-fraud and anti-corruption (AFAC) policy[6] set out WFP's policy and procedures relating to fraud, corruption and/or collusion. The 2015 revision of the AFAC policy[7] expands the definition of fraud and corruption, outlines specific obligations of managers and others, and reinforces guidelines on preventing conflicts of interest.

WFP's innovative culture and mindset to "get things done" are critical strengths and key to achieving its strategic objectives. WFP's ability to execute effectively and deliver change is a source of risk that needs to be well managed. The 2016–2017 oversight reports highlighted the need to strengthen organizational risk assessment and management processes, tools and guidance, including fraud risk assessments, and to ensure that they are embedded in WFP's day-to-day processes. A new Enterprise Risk Management Division was subsequently created in the Resource Management Department in 2017 and is now headed by a Chief Risk Officer.

Vision for enterprise risk management at WFP

1. WFP's mission requires managers to take risk-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 agenda for aid effectiveness. Committed to the 2030 Agenda, WFP, through its Strategic Plan,[8] endeavours to support governments to end hunger among the poorest and most food-insecure people and participate in a revitalized global partnership for sustainable development.

[1] See WFP/EB.A/2018/5-C.

[2] WFP Enterprise Risk Management Policy (WFP/EB.2/2005/5 E/1)

[3] Enterprise Risk Management Policy (WFP/EB.A/2015/5-B)

[4] WFP Enterprise Risk Management: the Risk Appetite Statement (Executive Director's Circular: OED2012/015)

[5] Risk Appetite Statement (WFP/EB.1/2016/4-C)

[6] WFP Anti-Fraud and Anti-Corruption Policy (WFP/EB.A/2010/5-B)

[7] Anti-Fraud and Anti-Corruption Policy (WFP/EB.A/2015/5-E/1)

[8] WFP Strategic Plan (2017–2021) (WFP/EB.2/2016/4-A/1/Rev.2*) – aligned to the achievement of the 2030 Agenda.

2. The aim of this policy is therefore to establish a pragmatic, systematic and disciplined approach to identifying and managing risks throughout WFP that is clearly linked to the achievement of its strategic objectives.

3. Specifically, WFP's enterprise risk management vision is to:

   - maintain a consistent risk management framework through which risks can be identified, analysed, addressed, escalated and accountability assigned;

   - achieve a common understanding of WFP's risk exposures in relation to its appetite for risk, to be able to articulate the organization's risk profile coherently internally as well as externally to donors and external stakeholders; and

   - establish a culture where risk management is linked to implementing WFP's Strategic Plan and considered proactively in operational decision-making.

4. WFP's enterprise risk management framework is based on the 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO)[9] ERM framework, which integrates the relationship between risks, strategy and performance. WFP's ERM activities build upon the five components of COSO:

   i) **Governance and culture:** Governance and culture together underpin all the components of enterprise risk management. Governance, as laid out in WFP's 2018 Oversight Framework,[10] establishes oversight responsibilities and reinforces accountabilities across the three lines of defence. Culture is reflected in the subsequent transparency and quality of risk decision-making.

   ii) **Strategy and objective setting:** WFP's risk appetite is aligned to the achievement of WFP's Strategic Plan and country-level strategic plans[11] and supports the achievement of objectives in day-to-day operations and in setting priorities.

   iii) **Performance:** WFP identifies and assesses risks that affect the ability to achieve its strategic objectives, and prioritizes and responds to them according to their severity and considering WFP's risk appetite. The organization's portfolio of risk exposures – its *risk profile* – is continually monitored.

   iv) **Review and revision:** WFP seeks to continuously improve and build resilience in managing risk, and its control environment is expected to evolve as it seeks to align its risk profile with its risk appetite.

   v) **Information, communication and reporting:** WFP adapts and continuously develops its risk appetite measures to improve risk information and drive more risk-sensitive decisions. This helps to embed a productive risk culture across the organization.

[9] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) document *Enterprise Risk Management – Integrating with Strategy and Performance* (www.coso.org). COSO is sponsored by five major professional associations in the United States of America: the American Accounting Association; the American Institute of Certified Public Accountants; the Financial Executives Institute; the Institute of Internal Auditors; and Institute of Management Accountants. COSO first published its enterprise risk management integrated framework in September 2004. A revised version of this Framework was published in June 2017.

[10] WFP oversight framework (WFP/EB.A/2018/5-C*)

[11] Policy on country strategic plans (WFP/EB.2/2016/4-C/1/Rev.1*)

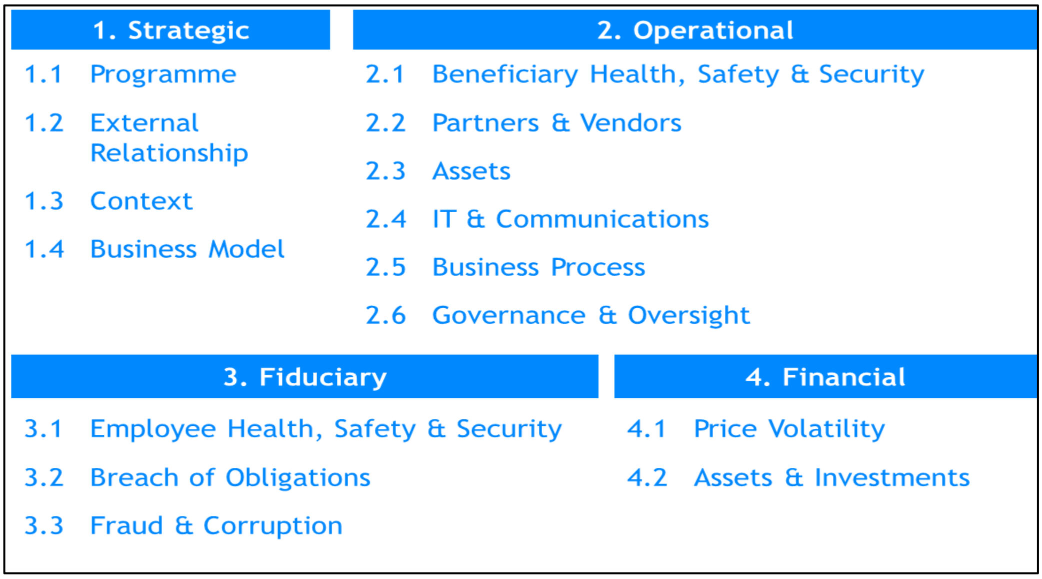
Key areas of risk for WFP

5. WFP has developed a new risk categorization framework to assist management at all levels as well as to improve risk analysis. The framework enables offices and operations to identify risks using a common language across WFP.

6. Risks are classified into four[12] primary categories: strategic, operational, fiduciary and financial. Reputational risk is defined as a consequential risk whereby risks occurring in any category could negatively impact WFP's reputation.

7. Within these four categories, 15 risk areas covering the scope of WFP's enterprise risk management have been defined.

Figure 1: WFP's risk categorization



1. Strategic	2. Operational
1.1 Programme	2.1 Beneficiary Health, Safety & Security
1.2 External Relationship	2.2 Partners & Vendors
1.3 Context	2.3 Assets
1.4 Business Model	2.4 IT & Communications
	2.5 Business Process
	2.6 Governance & Oversight

3. Fiduciary	4. Financial
3.1 Employee Health, Safety & Security	4.1 Price Volatility
3.2 Breach of Obligations	4.2 Assets & Investments
3.3 Fraud & Corruption	

8. **Strategic risks** refer to those that have an impact on WFP's ability to achieve strategic goals, objectives and plans. Within the programme area, risks include the design of country strategic plans (CSPs) and the availability of suitable employee skills, as well as sufficient resources that allow the achievement of optimum results. Building and maintaining external relationships with national governments, sister United Nations agencies and other partners is critical to achieving the Sustainable Development Goals (SDGs) and commitments toward achieving zero hunger. Risks related to external relationships also include donor funding capacity and threats to funding posed by potential misrepresentation of WFP's priorities or objectives in the media.

9. WFP's dual mandate and its strategic alignment with the 2030 Agenda involves responding to the needs of the most vulnerable, while simultaneously promoting longer-term food and nutrition security. WFP must respond to contextual risks related to conflicts, natural disasters and economic crises, necessitating a high degree of adaptability. As an integral part of its progress towards the 2030 Agenda and United Nations reform, WFP must also periodically review and adjust its business model, offering innovative solutions that not only aim to address drivers of conflict and protracted emergencies, but also to promote sustainable food systems in transitional or middle-income countries.

[12] The Enterprise Risk Management Policy (WFP/EB.A/2015/5-B) identified three risk categories: contextual, programmatic and institutional.

10. **Operational risks** relate to the implementation and execution of WFP's activities. As WFP strives to meet the needs of vulnerable people to food insecurity and malnutrition, it manages risks related to the quality of its assistance, including risks related to protection of affected civilian populations.

11. As WFP collaborates with international and local government counterparts, non-governmental partners, commercial vendors and sub-contractors, risks may occur in relation to the availability and capacity of these partners, as well as additional risks relating to the quality of their work, security constraints and access to affected areas.

12. WFP seeks to protect its assets from deliberate harm or accidents, as well as ensure that its information systems are safeguarded from the impacts of utility outages, systems failures and cyber threats, including the loss or misuse of personal data.

13. WFP's business processes continue to be affected by changes in its operating environment. WFP manages risks such as disruption in food or cash supply chains, delays in programme delivery, or inability to scale up or down in line with implementation needs. Its governance and oversight mechanisms affecting decision-making, particularly in volatile environments in the field, also need to be resilient.

14. **Fiduciary risks** encompass breaches of obligations in terms of ethics and standards of conduct by WFP and its partners, failure to implement policies, and unauthorized activities including breaches of delegation. Risks related to fraud and corruption may be internal or external to WFP and include misappropriations of cash and other assets as well as misrepresentation and fraudulent reporting. WFP's duty of care to its employees is also a fiduciary risk: their health, safety and security must be managed from an occupational health and well-being perspective.

15. **Financial risks** are typically related to currency and exchange rate concerns, adverse pricing, and inefficient use or misutilization of financial or other assets.

Risk appetite at WFP

16. WFP's risk appetite reflects its overall approach to risk management, affirming its commitment to identify, measure and manage risks as it seeks to reach the people vulnerable to food insecurity and malnutrition while at the same time safeguarding resources. WFP's mission towards zero hunger requires risk taking and operating in difficult environments, including conflict zones. The question is often not whether to engage, but how to engage in a way that minimizes and contains risk while maintaining conformance with the humanitarian principles.[13] WFP therefore places a strong emphasis on a risk-aware culture that relies on management judgment to make decisions that enhance value, deliver on its humanitarian and development objectives, and is aligned with WFP's core values.

17. WFP's appetite for risk is articulated in a series of statements linked to its risk areas. Each risk appetite statement reflects the intent to manage risks. This allows WFP to share risks with partners and stakeholders and engender proactive engagement in operational decision-making. While WFP's risk appetite is developed corporately, context-specific appetite or tolerance levels are set with due consideration of risk impact and cost of control. Risks that are deemed out of appetite will be escalated to the next level of authority.

[13] The humanitarian principles of humanity, neutrality, impartiality and independence are formally adopted in General Assembly resolution 46/182 (adopted in 1991) and General Assembly resolution 58/114 (adopted in 2004).

18. Risk appetite statements serve as guiding principles for managers and:

- allow analysis, response and monitoring of their risks;
- inform their day-to-day decisions and prioritization of resources;
- support the establishment of performance targets for their areas of responsibility; and
- enable them to carry out WFP's mission within boundaries for risk management and with respect for the core values of the organization.

19. WFP's risk appetite statements:

Strategic risks	
1.1 Programme	WFP responds in the context of international consensus on needs. It is committed to designing evidence-based, robust and gender-sensitive country strategic plans, in partnership with host governments, donors, civil society and other key stakeholders. WFP will continue to develop funding partnerships to align its resources with implementation priorities, including modality choice. WFP recognizes that in its humanitarian and development mission, enhanced employee skills are required and need to be rapidly mobilized. WFP invests in training, sourcing of employees with the required skills and mechanisms to deploy them rapidly.
1.2 External relationships	WFP works closely with many strategic partners, whether donor governments, other United Nations entities, non-governmental organizations, civil society organizations and private sector organizations. WFP commits to share information and communicate pro-actively with all its strategic partners. Exposure to media attention and public perception may negatively impact WFP's reputation. WFP is committed to ensure that any false allegations are correctly addressed while maintaining transparency and building trust with all partners and stakeholders.
1.3 Context	WFP needs to provide principled and effective assistance in a variety of contexts. WFP invests in emergency preparedness activities based on early warning and response protocols. WFP recognizes the importance in certain circumstances of deploying employees and assets prior to a potential humanitarian emergency.
1.4 Business model	WFP continuously seeks to foster a creative and innovative culture that allows the organization to accelerate its contribution to achieve the SDGs. WFP manages its execution risks in this dynamic environment through increased investment in new approaches, technologies and expertise, as well as the implementation capacity to take solutions to scale.

Operational risks	
2.1 Beneficiary health, safety and security	WFP actively seeks to protect beneficiaries from harm, including exploitation, abuse and gender-based violence. It aims to develop sustainable programmes and infrastructure. It will take prompt action to protect beneficiaries and affected populations, imposing high standards on itself and its partners, and ensuring safe and accessible complaints and feedback mechanisms are in place. WFP seeks to respond to the particular needs of women, men, girls and boys on a timely basis with consistent standards of food assistance. WFP manages its supply chain and costs of delivery by integrating food quality and safety standards.
2.2 Partners and vendors	WFP will conduct due diligence on all partners and vendors and will monitor ongoing performance. Where availability, capacity or implementation quality of partners or vendors is limited or inadequate, WFP will work to build their capacity to comply with its standards.
2.3 Assets	WFP will maintain minimum operational safety and security standards to safeguard its fixed assets and inventories. WFP will continuously assess risks of loss of assets and inventories, and invest in embedding processes, systems and enhanced safety and security measures where appropriate.
2.4 Information technology and communications	WFP invests in systems resilience and improved functionality to deliver cost-effective operations. WFP will continue to enhance cyber security measures to counter risks of data loss/misuse or system disruption. WFP sees innovation as a strength and actively seeks to adopt new technology, and addresses associated risks through governance mechanisms, testing and change release controls.
2.5 Business process	WFP invests in the resilience of its supply chain with clear accountabilities for all elements of the critical path, including robust supplier due diligence and quality assurance monitoring. WFP's ability to sustain heightened operations is reviewed after the first 90 and 180 days of an emergency. WFP promotes a culture of change to continually enhance its operations and prioritizes change initiatives to focus resources and minimize disruption.
2.6 Governance and oversight	WFP operates in dynamic environments and must make timely decisions, often at the field level. Technical and functional experts support managers in making decisions, and accountabilities are reinforced by internal governance processes, including regular risk monitoring, reporting, evaluation and, where required, escalation.

Fiduciary risks	
3.1 Employee health, safety and security	WFP will assess employee health, safety and security risks in the context of programme criticality and its duty of care. In the event of a critical incident, WFP will take action in line with the United Nations security framework and revise procedures accordingly.
3.2 Breach of obligations	WFP commits to the highest standards of ethics and conduct and seeks to uphold humanitarian principles, in addition to applicable rules and regulations across all its operations. In doing so, it relies on the commitment of all its employees, who are held personally accountable. WFP commits to take firm action where there has been a material breach of WFP standards. WFP commits to abide by its contractual obligations with donors and other stakeholders. WFP is obliged to verify its adherence to its obligations on an ongoing basis.
3.3 Fraud and corruption	WFP is investing in its management side anti-fraud and anti-corruption (AFAC) capability and ongoing employee training to deter and detect potential instances and limit any impacts. WFP commits to investigating substantive reports of violations of the AFAC policy and taking appropriate disciplinary action/sanctions when allegations are substantiated. In addition, WFP will take measures for corrective action, including, but not limited to, recovery of WFP losses.

Financial risks	
4.1 Price volatility	WFP restricts its exposure to commodity price and currency fluctuations by managing its major exposures centrally, within strict procedures and financial limit frameworks.
4.2 Assets and investments	WFP manages its investment portfolios with professional managers under strict investment policies, matching the investment principles of security, liquidity and return with the nature of the funds being invested. It monitors exposures against guidelines daily and reports on performance and risk to the Investment Committee on a monthly basis. WFP commits to monitor the utilization of its key assets, financial and non-financial. Where constraints exist, WFP will proactively engage with stakeholders to manage resources as efficiently as possible.

Risk roles and responsibilities at WFP

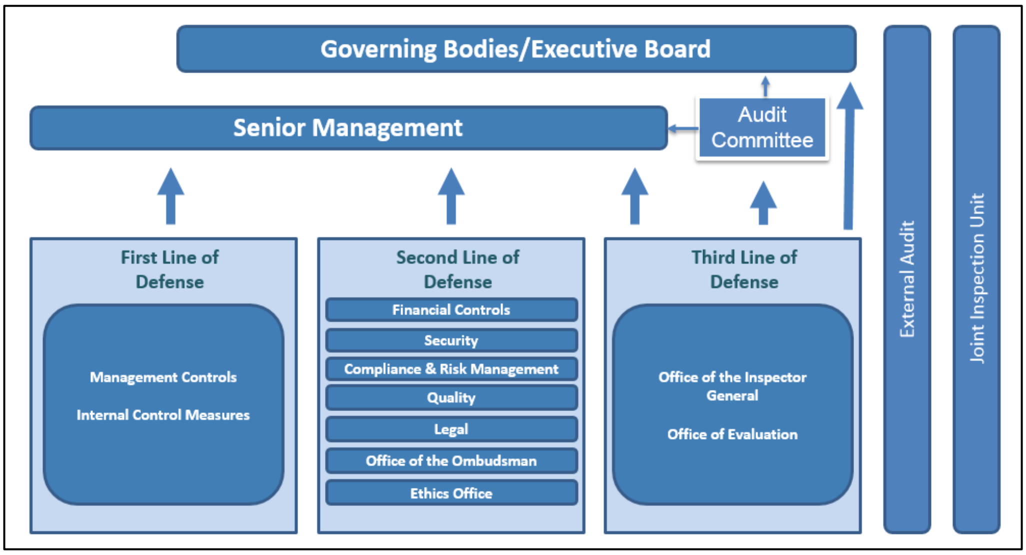
20. WFP’s 2018 oversight framework defines its governance and oversight architecture. While formal governing bodies hold senior management to account for risk management, on a day-to-day basis risk management is everyone’s responsibility. Managers and employees who fail to consider risk in the planning, implementation and refining of their activities will face obstacles in achieving their objectives. Effective risk management engages employees at all levels and allows risks to be escalated to the appropriate level of decision-making.

21. **Three lines of defence:** WFP has adopted the three lines of defence model.[14] Under the model, risk roles and responsibilities are distributed by activity between “first line” risk decision-makers who own and manage risk as part of day-to-day work, “second line” managers and functional Risk Leads who monitor risk and controls, set standards and define overall risk appetite, and “third line” independent assurance. All actors within the three lines

[14] WFP’s oversight framework follows the “Three Lines of Defence Model” adopted by the High-Level Committee on Management in 2014.

of defence are accountable to the Executive Director,[15] who in turn is accountable to the Executive Board.

Figure 2: Three lines of defence



22. **The Executive Board:** As a governing body, the Board is responsible for setting policies, providing direction and overseeing implementation through its oversight role. To support Board accountability, the membership is regularly updated on implementation of the enterprise risk management policy and the critical risks that WFP is facing, including emerging risks and trends. Risk management information will be included in country strategy documents submitted to the Board and in regular reporting (e.g. quarterly operational updates).

23. **The Executive Director:** The Executive Director is ultimately accountable for the enterprise-wide implementation of risk management. Ensuring that WFP's strategic objectives are met requires the Executive Director's direct sponsorship of the risk management process. The Executive Director:

i) promotes the development of a culture that supports effective risk management and innovation and that encourages effective risk taking in line with WFP's risk appetite;

ii) integrates risk management into major programmes and functions and advocates funding so that it is embedded within decision-making across the organization;

iii) ensures that risks are managed effectively across all of WFP, which includes identifying, analysing, responding to, reviewing and reporting on risks;

iv) owns risk decision-making and assigns accountability to employees for managing risks within their areas of responsibility, levels of authority and competence; and

v) allows for the systematic review of risk management to ensure its effectiveness and adherence to WFP's risk appetite.

[15] WFP Oversight Framework (WFP/EB.A/2018/5-C*)

24. **Regional directors:** Regional directors lead the implementation of risk management activities in each region and perform both first and second line roles: as senior risk decision-makers for their region; and as managers of oversight and technical support activities provided to country offices. Specifically, regional directors:

i) are accountable for implementing risk management effectively in all WFP offices and operations within their region and assign risk owners at the regional level;

ii) ensure that country office employee skills and experience are appropriate for the risks the country faces;

iii) proactively manage the risks and prioritization related to scarce financial resources in the region;

iv) are accountable for the security of WFP employees, operations, premises and assets throughout the region;

v) monitor early warning indicators and maintain a level of emergency preparedness;

vi) define and monitor appropriate risk appetite metrics for their region in consultation with functional Risk Leads;

vii) chair a regular regional risk discussion to review risk information, including indicators, appetite metrics and follow-up on mitigation measures;

viii) are accountable for effective implementation within their region of all internal and external oversight and compliance recommendations; and

ix) maintain an oversight role throughout the region and sponsor regional oversight and technical support to countries.

25. **Country directors:** Country directors lead and advocate for a WFP country office to ensure the effective implementation of the corporate and their own country strategy, as well as the resourcing and delivery of WFP programmes and activities. As such, their role is primarily risk decision-making, but they also maintain an oversight role over functional areas within their countries. Country directors:

i) are accountable for implementing risk management effectively for all WFP offices and operations within their country and assign risk owners at the country office level;

ii) provide effective leadership in risk management and ensure that suitable employees are assigned accountability for managing the risks within their areas of responsibility and authority;

iii) define and monitor appropriate risk appetite metrics for their country in consultation with functional Risk Leads;

iv) chair a regular country risk discussion to review risk information, including indicators and appetite metrics and follow-up on mitigation measures; and

v) lead the effort to ensure that internal and external oversight and compliance recommendations are effectively addressed within their country.

26. **Functional directors and managers as Risk Leads:** Functional management, whether in headquarters, regional bureaux or country offices provide leadership within a specialized function, and act as Risk Leads for their area of risk specialism. They are actively involved in formulating WFP corporate strategies, policies and plans, including effective implementation of WFP programmes and activities. They may have first line risk decision-making responsibilities as well as second line oversight responsibilities. Specifically, functional directors:

    i) are accountable for implementing risk management effectively within their function;

    ii) demonstrate ownership, promote and deploy WFP corporate initiatives and strategies;

    iii) act in an assigned emergency response capacity as required to meet emergency food assistance needs;

    iv) ensure that employees are trained to manage the risks within their areas of responsibility and authority at all levels of the organization;

    v) set standards, provide guidance and define overall risk appetite for their area of risk specialism;

    vi) proactively engage with first line owners of risk and support them in specifying suitable risk appetite metrics and agree thresholds and escalation protocols; and

    vii) are responsible to monitor and act upon aggregated and specific risk information from other reporting entities and take the lead to ensure that internal and external oversight and compliance recommendations are efficiently addressed for their function.

27. **Chief Risk Officer:** The Chief Risk Officer reports to the Chief Financial Officer[16] and manages the Enterprise Risk Management Division, which provides leadership for the organization’s adoption of best risk management practices and the continuous improvement of its internal control environment. The Chief Risk Officer oversees the implementation of enterprise risk management as a second line of defence accountability and:

    i) provides overall vision, leadership and direction for enterprise risk management;

    ii) represents and communicates WFP’s strategies and policies for risk management to senior management, members of WFP’s Executive Board and other stakeholders;

    iii) recommends the adoption of risk appetite statements and protocols for reporting and escalation and de-escalation of risk exposures to the Executive Board;

    iv) establishes the methodologies and tools for identifying, assessing, monitoring and reporting on WFP’s risk exposures;

    v) sponsors the enterprise risk management framework, including the operation of the three lines of defence and the adherence to and use of risk appetite measures;

    vi) oversees risk ownership and accountability both for first line risk decision-makers and second line Risk Leads for specific categories of risk;

    vii) leads efforts to embed risk management across the organization and evolves enterprise risk management tools and competencies to continually develop risk management in line with leading best practice;

[16] The Chief Financial Officer is also the Assistant Executive Director, overseeing the Resource Management Department.

viii) acts as a focal point for best practice sharing on enterprise risk management at the inter-agency level;

ix) is the second line *lead* for anti-fraud and anti-corruption (AFAC), setting standards, providing training and agreeing risk appetite measures for AFAC monitoring at the corporate level as well as assisting headquarters functions and field operations to develop suitable metrics; and

x) manages the interface with the third line of defence on the corporate implementation of risk management, and responds to scrutiny concerning risk management from external parties, including the External Auditor, the Joint Inspection Unit and donors.

28. The Chief Risk Officer manages the enterprise risk management function, whose activities include, but are not limited to:

i) ownership of the enterprise risk management framework and implementation for risk appetite measures and escalation and de-escalation protocols for incidents as well as appetite measures;

ii) recommending the boundaries and escalation triggers for first line decision-making and determination of the ongoing engagement of second line Risk Leads with those in the first line;

iii) definition of assessment methodologies, relevant processes and controls, and the mechanism for prioritizing risk by level of materiality;

iv) determination and dissemination of corporate risk policies and guidance for implementation;

v) development of toolsets, including systems and their specifications for capturing risk information and reporting on risks issues and mitigating actions;

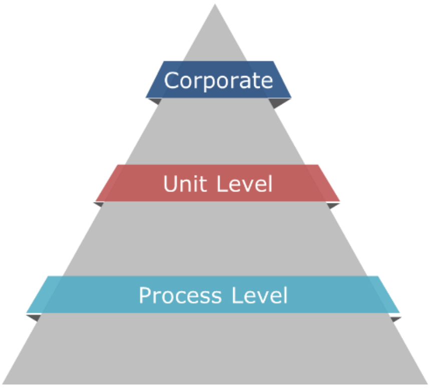
vi) preparation of the Executive Director’s Statement on Internal Control to highlight significant risk and internal control matters; and

vii) preparation of regular senior management oversight reports follow-up of outstanding actions.

29. The Chief Risk Officer also has functional responsibility for risk and compliance advisory employees in regional bureaux and country offices. The criteria for the establishment of these roles include contexts with high inherent risks, complex operations, where there are high levels of resource use, where there are employee capacity issues or in countries with high levels of systemic corruption.

30. Risk and compliance advisers are senior professional-level risk employees who provide advice and guidance and also challenge in a second line capacity to first line risk decision-makers, both in central functions and in field operations. While risk and compliance advisory roles in regional bureaux and field operations may report locally to regional and country directors, their direction and functional priorities must be agreed centrally by the Chief Risk Officer. Embedded within operations, these employees provide proactive and real-time support to regional and country directors in fulfilling their risk and compliance obligations, as well as assurance that risk management is being implemented consistently across all regions and specifically in high-risk locations.

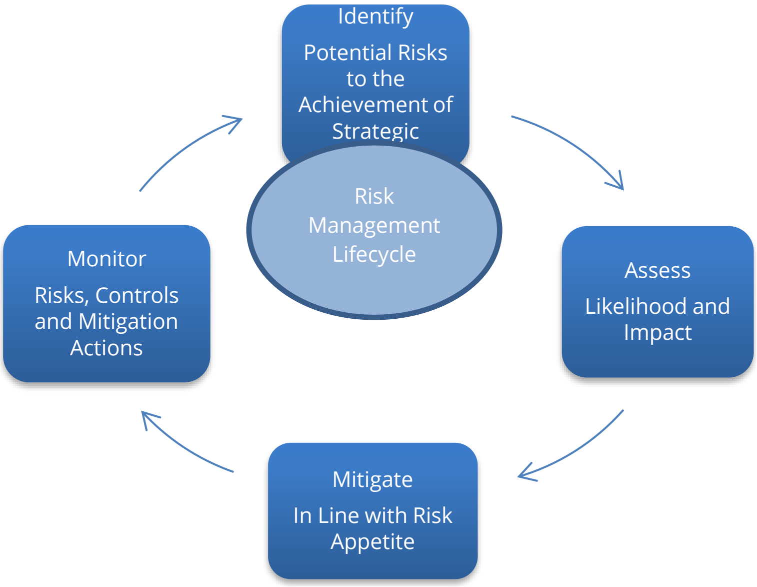
Risk processes at WFP



31. The intention of structured risk processes is to instill discipline to include risk considerations as part of decision-making and planning/resource allocation exercises. The nature of risk assessment and impetus of mitigating actions will differ depending on the area of organizational focus. Examples of process-level risk management, such as security risk management or emergency preparedness and response management, is about understanding the risks in specific areas of WFP's work. These are focused on key risk areas and usually require understanding of detailed process steps. Process dependencies also need to be understood end-to-end so that risks are captured comprehensively along the value chain.

32. At the unit level, all relevant risks must be considered. Risk review processes are integrated with the annual performance planning processes, and should also be informed by process-level risk assessments.

33. Risk management at the corporate level is coordinated centrally by the ERM function directly with function heads and focuses on monitoring and analysing business-unit risk assessments, identifying risks for WFP as a whole, and considering potential events that may impede the achievement of WFP's strategic objectives. Results of corporate-level risk assessments are presented to the Executive Management Group through the Corporate Risk Register.[17] This focuses executive management on the key risks for WFP, ensures accountability for addressing risks, and facilitates decision-making and implementation of mitigating actions.


Identify
Potential Risks to the Achievement of Strategic
Risk Management Lifecycle
Assess
Likelihood and Impact
Mitigate
In Line with Risk Appetite
Monitor
Risks, Controls and Mitigation Actions

[17] The Corporate Risk Register is updated, taking into consideration the risks that occur globally and with the contribution of all corporate risk owners and mitigation action owners. A review of the corporate risks and upcoming issues is presented to the Executive Management Group three times a year.

34. **Risk identification:** Risks may arise at any time and be identified from numerous sources – as part of planning exercises (whether at corporate, country or programme level), risk assessment exercises (e.g. risk reviews, oversight missions or assurance work), external events (e.g. incidents or risks occurring at other United Nation agencies, non-governmental organization partners or government), or internal incidents and escalations (breaches of appetite or unanticipated events). While any employee may identify a risk, first line risk decision-makers own risks applicable to their area and are therefore responsible for identifying all relevant and potentially material risks. They are supported in this process by second line Risk Leads who provide advice, guidance and challenge for specialist areas of risk. All relevant and potentially material risks (i.e. which affect the delivery of strategic objectives) should be captured as they arise and at least twice yearly as part of the performance planning process and risk review update.

- **Performance planning:** Risk management is an integral part of performance management and is linked to performance targets – identifying, quantifying, prioritizing and deciding on how to manage risks related to the achievement of objectives.
- **Risk reviews:** Risks are identified for each office, region and headquarters division using WFP's risk categorization, including scenario examples to describe each type of risk and how it might manifest itself for a given area. Risk Leads may provide input for each risk area/category; the reviews are then owned/approved by country, regional, and corporate/functional directors.

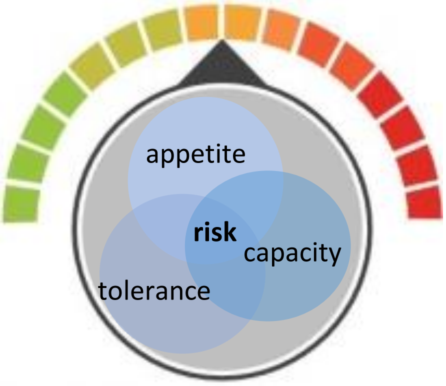
35. **Risk assessment:** Risks identified in risk reviews are assessed to understand the materiality of each risk to the achievement of WFP's strategy and defined objectives, and to support the selection of the risk response. Risk appetite serves as the basis for assessing and responding to risks. For instance, a risk would be considered out of appetite if it poses a serious threat to the achievement of WFP`s strategic objectives. The assessment of risk takes the existing control environment into account and determines:

- The **likelihood** (frequency) of the risk occurring. When assessing likelihood, consideration is given to the future probability which may be informed by the frequency of occurrence in the past and validated by data gathered about the control environment from risk indicators, incidents and audit/evaluation or management/oversight issues. It can range from very unlikely to very likely.
- The **impact** (severity) of the event on WFP's objectives if it occurs. The impact scale considers the four risk categories and assesses the impact based on the following: outcome and impact for strategic (including reputational) risks; operational continuity and resilience as well as safety and security for operational risks; legal/regulatory and fraud and corruption aspects for fiduciary risks; and monetary loss/deficit for financial risks. Impact scales range from negligible to critical.
- Risk **prioritization**, based on the combined assessment of likelihood and impact and whether the assessed risk is within appetite.

36. **Risk mitigation:** Risks that are outside of the context-specific appetite will require specific mitigation actions; these are recorded in risk reviews with responsibilities assigned for implementation and followed up against agreed target dates. Accountability for completion of actions rests with country, regional or functional directors who own the risk review. For certain risks, there may be no suitable action, in which case the appropriate director must determine whether the risk can be avoided altogether or if it can be accepted. For risks within appetite, actions are not required, but directors may choose to pursue a greater

degree of risk provided it furthers the achievement of WFP objectives. WFP's responses to risk are summarized below:[18]

- **Avoid –** An activity may be terminated if it is out of appetite and deemed too risky. Choosing avoidance suggests management has not been able to identify a response that would reduce the risk to an acceptable level of severity.
- **Reduce –** Mitigating action is taken to reduce the likelihood and/or potential impact of the risk to bring the risk within appetite. This typically involves implementation of controls, and for material risks may also require organizational or process changes.
- **Share –** Mitigating action is taken to reduce the likelihood and/or potential impact of the risk by sharing elements of the risk. Outsourcing to third-party specialists or service providers, for instance, may share execution and implementation risks (but not fully the reputational impacts). Similarly, the financial impact of some risks may be mitigated by insurance.
- **Accept –** Risk is accepted without the need for any further mitigating measures. This applies when risk is within appetite, but sometimes also when a risk is out of appetite but there is no feasible mitigation. Acceptance of risks that are out of appetite requires appropriate director level approval and for material risks is escalated to the Executive Management Group.
- **Pursue –** Provided a risk is within appetite, or there is a clearly agreed path to meet appetite, an increased level of risk may be pursued to achieve strategic objectives and/or improve performance. A decision by a director to increase risk where it is already out of appetite will be escalated to the Executive Management Group.



37. **Risk monitoring:** Risks are continually monitored at all levels of the organization and their likelihood and potential impacts validated by various information sources – e.g. incidents, risk indicator metrics linked to appetite, audit/evaluation findings and management/ oversight issues. Looked at holistically and analysed for trends and root causes, this risk information captures the *risk profile* for a functional area, thematic area or for a specific operation, and can then be compared to appetite for each risk category. The process of continuous monitoring across field offices, regional bureaux and by headquarters brings risk management to life and supports management in making more informed decisions and allocating resources. It also provides an essential feedback loop to continually reassess risks in a dynamic environment and trigger escalation and mitigating action where risks drift outside of appetite. For example, country offices, through regular risk reviews, are expected to monitor the implementation of risk mitigation actions and country/context specific risk metrics against risk appetite. These risk reviews are typically conducted concurrently with performance planning and management processes.

[18] Previously, WFP responded to risk in four ways; Accept, Control, Avoid, Transfer. To align this Policy to the updated 2017 COSO ERM Framework guidance, WFP has adopted the five risk responses noted within the guidance.

Risk escalation and reporting

38. **Risk escalation:** Risks deemed to be particularly high and significantly out of appetite are described as being out of risk tolerance and requiring escalation. Risk tolerances may be in the context of a major incident or a risk indicator breaching a certain threshold, or may be a high-risk issue highlighted by an oversight body. Formal escalation, as well as de-escalation, is important since it drives transparency to accountable managers and defines the protocols of engagement and interaction between first and second line actors. Jointly, this improves the quality of risk responses and decision-making.

39. Risk Leads, with support from the Enterprise Risk Management Division, are responsible for aggregation and monitoring of gaps in the management of their risk specialisms. This supports informed decision-making by senior managers and provides an analysis of priority oversight issues based on a review from internal audits, proactive integrity reviews, fraud and corruption-related investigations, policy evaluations and evaluation syntheses, and external audit and Joint Inspection Unit reports.

40. Risk escalation also takes place upon the activation of a *WFP emergency response*. Two corporate coordination bodies exist to facilitate WFP's internal coordination of emergency response operations. The Strategic Task Force and the Operational Task Force are internal coordination bodies that meet for major emergencies (Level 3 and 2), to support informed decision-making and facilitate efficient and effective coordination. The task forces address operational issues and refer strategic issues to executive management. Major risks to emergency response are escalated to these task forces to ensure that there is adequate follow-up.

41. **Risk reporting:** Effective risk management requires a continual process of capturing and sharing risk information that flows up, down and across WFP's three lines of defence. Risk reporting is therefore required at the headquarters/functional, regional and country level, based around risk categories and supported by relevant risk data within the framework of context-specific risk appetite. Risk Leads are expected to support the reporting process in line with functional oversight responsibilities.

   - **The Executive Management Group:** The Executive Management Group (EMG), chaired by the Executive Director, is responsible for ensuring that WFP manages risk effectively, in particular risks that affect WFP as a whole. The Enterprise Risk Management Division coordinates risk discussions with mitigation action owners at the corporate level for review by the EMG three times a year. The Corporate Risk Register and the Global Risk Profile Report are circulated internally in WFP following a review by the EMG and are subsequently shared with the Audit Committee.

   - **The Audit Committee and the Executive Board:** Regular briefings are provided to the Audit Committee and the Executive Board. The Enterprise Risk Management Division coordinates risk-related discussions with the Audit Committee. These communications and updates focus on key risks affecting the achievement of WFP's mission and strategy. Joint Management/Executive Board working groups are also established as needed to address critical matters, including sexual exploitation and harassment, and abuse of power. The Executive Board has an opportunity to review risks and mitigation actions during the country strategy documentation approval process, while operational briefings provide them a review of the risks impacting large-scale emergencies.

- **External stakeholders:** WFP shares pertinent risk information with external stakeholders, such as donors and cooperating partners as it strives, in partnership, to achieve strategic objectives in a given country. Specific protocol directives[19] will define the scope of the risk information to be shared with partners and donors.

Policy dissemination and review

42. The Enterprise Risk Management Division commits to working with managers in country offices, regional bureaux and headquarters to widely disseminate the policy, with special emphasis on the first and second line responsibilities for risk management across all levels of the organization. The Division will closely work with the Risk Leads on the analysis of key risk metrics, embedding of measures and reporting specifications in line with WFP's risk appetite statements, and agree on escalation criteria for risk appetite indicators and major incidents.

43. General and specialized ERM training will provide employees at all levels basic and enhanced knowledge about their roles and responsibilities for risk management and internal controls. Employees who take on specific risk review functions in the first and second lines of defence are trained to update their risks, risk assessment tools and techniques, mitigation actions and key risk metrics for their office or function. Risk education includes regular quality assurance risk reviews, thus ensuring a consistent approach to risk management across the organization.

44. Resourcing for the corporate focus on strengthening enterprise risk management across the organization was provided and approved by the Executive Board through the Management Plan 2018–2020 in November 2017. This was based on a comprehensive enterprise risk management agenda, proposing several priority work streams to be led or coordinated by the Enterprise Risk Management Division. Funded activities aim to strengthen risk management and internal controls across the organization, investing in improved frameworks for ERM and oversight, and the tools needed to support ERM, the application of internal controls, and capabilities within WFP for the prevention of fraud and corruption.

45. Monitoring of the implementation of the ERM policy will be conducted based on key performance metrics and reported regularly internally to senior management and annually to the Executive Board.

46. This enterprise risk management policy will be assessed according to policy evaluation standards as established by the Office of Evaluation.

Definitions

47. WFP's definitions of key terms used in this policy: [20]

    - **Enterprise risk management:** Common organization-wide arrangements for implementing and embedding risk management activities. This includes, *inter alia*, the culture, capabilities and practices integrated with strategy setting and performance, which the organization relies on to manage risk to create, preserve and realize value.

    - **Incident**: Occurrence of an event or series of events which have an impact on the organization and its objectives, usually negatively.

[19] Under development at the time of drafting this policy.

[20] WFP has adapted these definitions from the 2017 Committee of Sponsoring Organizations of the Treadway Commission (COSO) document *Enterprise Risk Management – Integrating with Strategy and Performance,* September 2017.

- **Impact:** The result or effect of risk crystallizing. There may be a range of possible impacts associated with a risk; usually impacts are negative to the strategy or objectives.
- **Internal control:** A process, effected by an entity's board of directors, management and other employees, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance. Internal control is one component of enterprise risk management.
- **Opportunity:** An action or potential action that creates or alters goals or approaches for creating, preserving and realizing value.
- **Performance management:** The measurement of efforts to achieve or exceed the strategy and objectives.
- **Risk:** The possibility that an event of a given impact will occur, adversely affecting the achievement of objectives. A material risk is deemed to have a significant impact on the achievement of WFP's objectives.
- **Risk appetite:** The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
- **Risk Lead:** A second line actor, usually a director or manager within a central function, who has specialist knowledge of a particular risk and supports first line risk decision-makers with policies and appetite for managing a particular risk.
- **Risk tolerance:** A limit to the type and amount of risk that an organization can accept, requiring a response/action and internal escalation.
- **Risk escalation:** Risk escalation is a process employed that addresses the need to report and provide transparency into significant risks to the most appropriate level where decisions can be made regarding a response.
- **Risk capacity:** The maximum amount of risk that an entity can absorb in the pursuit of strategy and objectives. The concept should be considered when analysing risks.
- **Risk owner:** The first line decision-maker with the accountability, authority and responsibility to manage risks in their span of control.
- **Risk portfolio:** A view of risks across a defined set of risk categories and/or organizational units.
- **Risk profile:** A composite view of the risk assumed at a particular level of the organization, or aspect of the business, that positions management to consider the types, severity and interdependencies of risks and how they may affect performance relative to the strategy and objectives.