World Health Organization

Risk Appetite Statement

12-05-2025

A. Pre-amble

An organization's risk appetite expresses the types and amount of risk it is willing to accept in pursuit of its objectives. In other words, it answers the question of how much risk the organization is prepared to face in delivering its strategy.

An effective risk appetite incorporates much more than a one-off policy statement. Its effectiveness lies in the linkage with the established organizational components (strategy, operating model, planning, and resource prioritization), and the concrete application of the risk appetite in decision-making, at all levels of the organization.

Effective management of risks at all levels of the organization will require providing sufficient guidance to decision-makers, by defining clear principles and boundaries, to reduce risk to an acceptable level, and seize opportunities when they arise.

A discussion of risk appetite should address the following questions:

- Organizational Values: What risks will we not accept?
- Strategy: What are the risks we need to take?
- External Stakeholders: What level of risks are they willing to bear?
- Capacity: What resources do we have to manage risks?

Arriving at a risk appetite approach that benefits the organization requires fundamental discussions on the organization's values and direction, and alignment with key stakeholders to reach a shared set of values and priorities.

An actionable framework, based on a fully aligned risk appetite, provides valuable guidance to the management in their daily business decisions.

Implementing risk appetite successfully can bring several benefits to an organization's ability to effectively manage risks and achieve its objectives. These benefits include:

- Helping the organization achieve its strategic objectives by taking on the right kind of risks at the right level, with the right risk responses in place;
- Facilitating better strategic decision-making by requiring Senior Management/governing bodies to consciously consider and articulate the level and type of risk they want to pursue and are willing to accept;
- Bringing consistency across the organization in making risk-related decisions at all levels of the organization, including if and when to escalate risks;
- Ensuring alignment across the entire organization (and with relevant external stakeholders) about what the desired risk level of the organization is;
- Improving overall organizational performance by managing risks appropriately and within the risk appetite.

A.1 Purpose of this document

Contained in this document is **WHO's Risk Appetite Statement**. Its purpose is to articulate WHO's high-level attitude towards risk. This is achieved by expressing the acceptable levels of risk that WHO is willing to accept in pursuit of its mission and is structured across a set of "enablers" named Key Success Factors.

In order to facilitate a thorough understanding of the Risk Appetite Statement, this document includes key definitions, the risk acceptance scales, and high-level mechanisms to operationalize the Risk Appetite Statement effectively, given WHO's current risk maturity.

A.2 Governance

The Risk Appetite Statement document is set and periodically updated by the Global Risk Management Committee (GRMC), with the endorsement of the Global Policy Group (GPG). It is subject to regular review, particularly in response to significant changes in the external environment, organizational context, or strategic objectives that may necessitate a reassessment of acceptable risk levels to support effective decision-making. The document is also shared with the Independent Expert Oversight Advisory Committee (IEOAC) for review, and continuous engagement opportunities are created with Member States to ensure transparency, alignment, and responsiveness to evolving risks and priorities.

B. Definitions and explanation of the Risk Appetite Statement

B1. The following definitions and explanations are key to understanding the WHO Risk Appetite Statement.

Key Success Factors:
Enablers and value drivers that inform day-to-day decision-making throughout WHO.

Risk Appetite:
The aggregate amount (level and types) of risk WHO wants to assume in pursuit of its strategic objectives (and mission).

Risk Appetite Statement:
The document that articulates the current risk appetite of WHO in different areas (namely, Key Success Factors).

Risk Acceptability Scale:
The extent to which the Organization is willing to accept risk, or uncertainty, of a Key Success Factor in order to achieve its mission. See section B2 below for the detailed definitions of the risk acceptability levels.

Risk Capacity:
The maximum risk WHO could bear without serious impairment to its capability to deliver on its mission. It provides an upper boundary to risk appetite.

Risk Criteria:
Risk criteria are terms of reference, used to evaluate the significance or importance of an organization's risks, and calibrated for the organizations risk appetite.

Risk Criticality:
Risk criticality is the total level of risk and is a function of risk impact and probability (i.e., impact

* probability). Residual risk criticality refers to the criticality after the mitigations (including controls) have been applied to reduce the risk. Target risk criticality refers to the target residual risk criticality, based on the risk acceptability level defined for a particular risk.

Risk Owner:
A person or entity with the accountability and authority to manage a risk. This includes identifying the risk, assessing its impact, determining responses, and ensuring the effectiveness of risk treatments.

Risk Trade-offs:
Interplay between various Key Success Factors and risks, when decision-making happens, to determine priorities between Key Success Factors or areas where compromises can be made.

Internal & External factors:
The likelihood of a risk materializing is based on several factors (i.e. causes). If these factors are in place, a risk is more likely to occur or materialize. Among these factors, some can be directly controllable by WHO (i.e., internal factors), whereas others are outside of WHO's direct control (i.e., external factors).

B2. Detailed definitions of the risk acceptance scale

The definition of the risk acceptance scale and key parameters within the risk acceptance scale definition, to guide our thinking on choosing a level.

Level	Risk Acceptability Definition*	Acceptable Risk Criticality
Averse	**A Significant level of risk** cannot be accepted as such, and **mitigation must immediately be developed and implemented**, to bring the **residual risk to as low as reasonably possible (ALARP)**, (i.e. target risk level) taking into account the relative importance of internal and external factors. The exposure to **internal factors** should be reduced **immediately**. Where the **external factors** cannot be controlled, **robust prevention, detection and contingency planning measures** must be put in place. If the residual risk criticality cannot be realistically reduced to the target level **within available resources, consideration** should be given to **stopping or reducing the scope of the related activity**	**Moderate, Low**
Minimal	**A Significant level of risk** cannot be accepted as such, and **mitigation must be developed as soon as possible** to bring the **residual risk to as low as reasonably possible (ALARP)**, (i.e. target risk level), taking into consideration the relative importance of internal and external factors. The exposure to **internal factors** should be reduced **as soon as possible,** and **resources should be allocated** accordingly to achieve that. Where the **external factors** cannot be controlled **robust prevention, detection and contingency planning measures** must be put in place.	**Moderate, Low**

Cautious	**A Significant level** of risk **can be accepted** in pursuit of impact, taking into consideration the relative importance of internal and external factors. The exposure to factors should be brought to at least **a moderate level** of risk criticality **within reasonable timelines**. The related risk should be **monitored regularly** to ensure that any change in circumstances is detected and that opportunities for mitigation are identified and implemented, where necessary, to maintain an optimal balance between risks and expected benefits (e.g., impact).	**Significant, Moderate, Low**
Open	**A Severe level** of risk **can be accepted** in pursuit of impact, taking into consideration the relative importance of internal and external factors. The exposure to **internal factors may remain unmitigated temporarily**, if necessary, to seize opportunities. The related risk must be **monitored periodically**, however, to ensure that any change in circumstances is detected and any unintended consequences acted upon appropriately.	**Severe, Significant, Moderate, Low**

C. WHO's Risk Appetite Statement

WHO's Overall Attitude to Risk in non-emergency and stable environments

WHO's mission, to help people attain the highest possible standards of health, requires **operating in complex or changing environments** where avoiding all forms of risks is impossible. The Organization takes risks in pursuit of opportunities, especially when pursuing innovation in public health, developing life-saving interventions or responding to emerging global health needs.

Accordingly, WHO's overall attitude is to **take calculated risks**. This means **balancing risks and impact** as a basis for decision making when facing uncertainty. Recognizing that uncertainty may negatively affect the Organization's success, WHO sets its risk appetite by defining the **drivers of its success** (called "Key Success Factors") and describing the level of acceptability the Organization has for risks affecting any of the core principles in WHO's success factors.

WHO recognizes that all risks affecting its Key Success Factors, if not managed effectively, **may result in reputational damage** or may **negatively impact its brand**, hence the importance of achieving consistency in applying the WHO risk management framework in daily activities and decision-making.

Defined in the paragraphs below are the **zero-tolerance policies** within WHO, and risk acceptability levels for each of the Key Success Factors.

Zero-tolerance policies within WHO

In addition to WHO's Risk Acceptability Levels for its Key Success Factors, zero tolerance policies are applied to some risks. These include Sexual misconduct not prevented or addressed (SEAH), Fraud and Corruption (including money laundering and financing terrorism), contracting and partnering with the tobacco industry or non-State actors working to further the interests of the tobacco industry, engagement with the arms industry and financing terrorism.

Where WHO has expressed zero-tolerance, WHO commits to maintaining a clear and firm stance in responding to a report/indication of a risk having materialized by: (i) actively following up on the incidents (including investigation), (ii) taking appropriate corrective actions (including disciplinary actions, sanctions and recovery of funds lost as relevant) and (iii) ensuring that appropriate lessons-learnt exercises are conducted to improve processes and minimize the re-occurrence of such incidents.

To achieve this, WHO will take a firm stance to ensure that its staff and partners are aware of their responsibilities and will be held accountable.

Technical Excellence

WHO shall act as the "directing and coordinating authority on international health work"[8] by, delivering public health decisions and services of the ***highest quality*** (i.e., relevant, evidence-based, and swiftly) with the view to create ***measurable impact for people***. In doing so, the Organization prioritizes the interest of the people it serves before its own, and seeks to maintain ***objectivity and independence*** when making public health decisions. In delivering its work, the Organization will apply the principles of ***transparency, accountability, inclusion*** and will aim to ***respect the dignity and human rights*** of the people it serves. Risks emerge where these principles are put at stake.

Risk Acceptability – **Minimal** – **Significant** levels of risk affecting the core principles underlying Technical Excellence cannot be accepted as such, and mitigation must be developed **as soon as possible** to bring the residual risk to **as low as is reasonably possible**, taking into consideration the relative importance of internal and external factors. The exposure to internal factors should be **reduced as soon as possible** and resources should be allocated accordingly to achieve that target.

Examples of risks that impact this key success factor – Non-adherence to WHO Quality, Norms and Standards; Gaps in health data; and Ineffective response to health emergencies.

Partnerships

WHO is a Member State Organization existing in an ecosystem of partners in which each plays a crucial role in achieving the Sustainable Development Goals (SDGs). Therefore, its success in fulfilling its function, as the directing and coordinating authority on international health work[9], will depend on its ability to maintain ***effective collaboration and trust*** with its Member States, donors, the United Nations (UN), UN specialized agencies, high-level political forums, other state-related entities, non-State actors, civil society and communities. In addition, WHO recognizes the critical importance of **maintaining and building the trust** placed in it by the public.

Risk Acceptability – **Open** – A **Severe** level of risk affecting the core principles underlying Partnerships **can be accepted** in pursuit of impact, taking into consideration the relative importance of internal and external factors. This means that WHO accepts to explore non-traditional partnerships and take a higher level of risks to Partnership where the search of innovative approaches requires to do so. WHO will however establish the necessary safeguards to ensure that integrity risks that could emerge from innovative partnerships are carefully assessed and managed in line with its appetite on compliance and Integrity.

Examples of risks that impact this key success factor – Undue influence exercised by external parties; Infodemics/Misinformation; UN system approaches negatively affecting WHO's ability to achieve results.

[8] WHO constitution, Chapter II
[9] WHO constitution, Chapter II

Financial Sustainability

WHO's financial resources are deployed to execute its vision, mission, and strategic priorities. The success of its work will depend on its ability to ***finance, in a sustainable manner, the key activities and core functions*** required to deliver the General Programme of Work (GPW).

Risk Acceptability – **Cautious** – A **significant level** of risk affecting the core principles underlying Financial Sustainability **can be accepted** in pursuit of impact, taking into consideration the relative importance of internal and external factors. The exposure to factors should be brought to at least a moderate level of risk criticality within reasonable timelines, taking into consideration the relative importance of internal and external factors and the availability of resources. This means that WHO will (i) advocate to its Member States that activities with the highest impact to its core mission of "directing and coordinating authority on international health work" be properly funded and (ii) adjust plans proactively where needed to stay financially sustainable. If funding gaps arise, solutions like non-traditional resource mobilization or reprioritization will be quickly explored.

Examples of risks that impact this key success factor – Initiating strategic or critical activities before financing is fully received in situations where good predictability of funding exist within a biennium.

People Health, Safety and Wellbeing

WHO shall fulfill its **duty of care** towards its workforce and the people it serves, when delivering its mission, by **protecting them from harm and promoting their wellbeing**.

Risk Acceptability – **Minimal** – **Significant** levels of risk affecting the core principles underlying People Health, Safety & Wellbeing cannot be accepted as such, and mitigation must be developed **as soon as possible** to bring the residual risk to **as low as is reasonably possible**, taking into consideration the relative importance of internal and external factors. The exposure to internal factors should be **reduced as soon as possible** and resources should be allocated accordingly to achieve that target. This means that WHO will put in place systems and procedures aimed at fulfilling the principles of duty of care, while recognizing that its commitment to this principle stands independently of external circumstances or expectations of specific outcomes. WHO will put in place the necessary measures to uphold this fundamental ethical responsibility which by no means represents an obligation of results.

Examples of risks that impact this key success factor - Sexual misconduct not prevented or addressed, Staff morale and wellbeing, Breach of data privacy.

Compliance and Integrity

WHO expects **its workforce and stakeholders it engages with** to "Act with Integrity", meaning that they must act in the best interest of WHO and People's health, in line with WHO's values and code of conduct. As an organization, WHO is committed to **complying with its internal and external commitments**, which include internal policies, rules, regulations and procedures, donor agreements or applicable international regulations.

Risk Acceptability – **Minimal** – **Significant** levels of risk affecting the core principles underlying Compliance & Integrity cannot be accepted as such, and mitigation must be developed **as**9

soon as possible to bring the residual risk to **as low as is reasonably possible**, taking into consideration the relative importance of internal and external factors. The exposure to internal factors should be **reduced as soon as possible** and resources should be allocated accordingly to achieve that target. This means that WHO will enforce its established rules, regulations and ethical conduct, ensure transparency, and act quickly to correct any breaches. Where risks arise, swift measures will be taken to protect trust and accountability.

Examples of risks that impact this key success factor – Fraud and corruption; and Breach of WHO's rules and/or international regulations and professional standards.

Business Continuity and Operational Efficiency

WHO recognizes that successfully delivering on its mission depends on its ability to ensure its ***freedom to operate***, to secure the ***operating continuity of its critical systems and functions,*** as well as to deliver administrative services in an ***efficient manner to enable*** its activities.

Risk Acceptability – **Cautious** – A **significant level** of risk affecting the core principles underlying Business Continuity and Operational efficiency **can be accepted**, in pursuit of impact, taking into consideration the relative importance of internal and external factors. The exposure to factors should be brought to at least a moderate level of risk criticality within reasonable timelines, taking into consideration the relative importance of internal and external factors and the availability of resources. This means WHO will maintain agile systems to ensure efficiency in support of highest public health impact and quickly fix vulnerabilities that could disrupt critical services.

Examples of risks that impact this key success factor – Cybersecurity failure; Loss of data; Security incidents affect the continuity of WHO operations; Unfit administrative processes and systems; Supply chain disruptions; and Ineffective Transformation.

WHO's Overall Attitude to Risk during crises or Health Emergencies

In a health crisis, the expectation from Member States, and other key stakeholders, is that WHO will immediately deploy its resources to deliver the required support to countries in the form of emergency response operations. The speed with which WHO is expected to deliver on its mission involves ***greater complexity***, and an ***inherently riskier environment***, in which it is difficult to maintain the same level of risk acceptance, as compared to serving under stable environments.

As such, WHO is generally willing to consider ***accepting a greater level of risk during a Health Emergency***. When delivering health services during a graded health emergency, the levels of risk acceptability may be higher than the ones set for stable and non-emergency environments.

In emergency situations, Senior Management[10] at the three levels of the Organization where relevant ***jointly defines the risk acceptability levels, upfront*** (e.g., at the onset of a graded emergency) and document why the risk acceptability levels defined for non-emergency situations cannot be maintained. Once the levels of risk acceptability are endorsed by Executive Management[11], the designated officers in charge of the operational oversight of a graded emergency response ensure that the appropriate mitigations are reflected in the operational plans and implementation of the given Response. All mitigations embedded in the activities contributing to these emergency responses should be consistent with the agreed level of risk acceptability agreed.

For both acute and protracted phases of an emergency or crisis, zero-tolerance policies promulgated at the level of the Organization will, however, still be maintained and adhered to, unless authorized by the Executive Management.

[10] following the delegations of authority, roles and responsibilities as set out in the current Emergency Response Framework

[11] As set out in the current Emergency Response Framework.

D. Operationalizing WHO's Risk Appetite

i) Trade-offs/dilemmas

Delivery on WHO's Mission is the "Raison d'être" of the Organization. When delivering its mission, WHO may face complex situations such as engaging in a new initiative or program, or when prioritizing the investment of resources (whether financial, human resources, or the time of personnel) between activities. ***When facing dilemmas, WHO will balance the level of risk inherent to its activities with the level of impact expected from those activities***, to define the appropriate level of risk acceptability, while adhering to its zero-tolerance policies.

At the onset of an initiative or program (including graded emergencies), the level of risk acceptability set in pursuit of impact will be discussed and agreed with relevant stakeholders (both internal and external) and approved by the appropriate levels of authority.

ii) Operational implications:

WHO's Risk Appetite provides an ***indication of the amount of risk*** that WHO is willing to take to seize opportunities and deliver impact. Choosing a risk acceptance level also provides guidance in terms of the ***level of mitigation or control required for an activity or process, to effectively manage the residual risk***.

WHO personnel must ***implement the controls necessary to ensure that the risk remains within agreed boundaries (i.e., as indicated by agreed target risk levels)*** indicated by the risk acceptance levels. The level of risk accepted will also have consequences in terms of frequency and extent of monitoring and oversight, reporting, delegation of authority, resources, freedom to innovate, change management and communications.

iii) Mitigation and Escalation

The WHO risk taxonomy (i.e. categorization of the types of risks potentially threatening WHO's objectives, Figure 1) is mapped against the primary Key Success Factors and related risk acceptability levels. Where the residual risk levels remain within acceptability levels, it may be tolerated or exploited for strategic benefits. If not, risk owners are required to mitigate the risks to reduce them to the agreed limits.

Where mitigation is ineffective, and risk owners are not able to put in place new mitigation actions because of limited delegation of authority, insufficient resources, lack of expertise, or other limitations, escalation protocols described in the WHO Enterprise Risk Management policy apply.

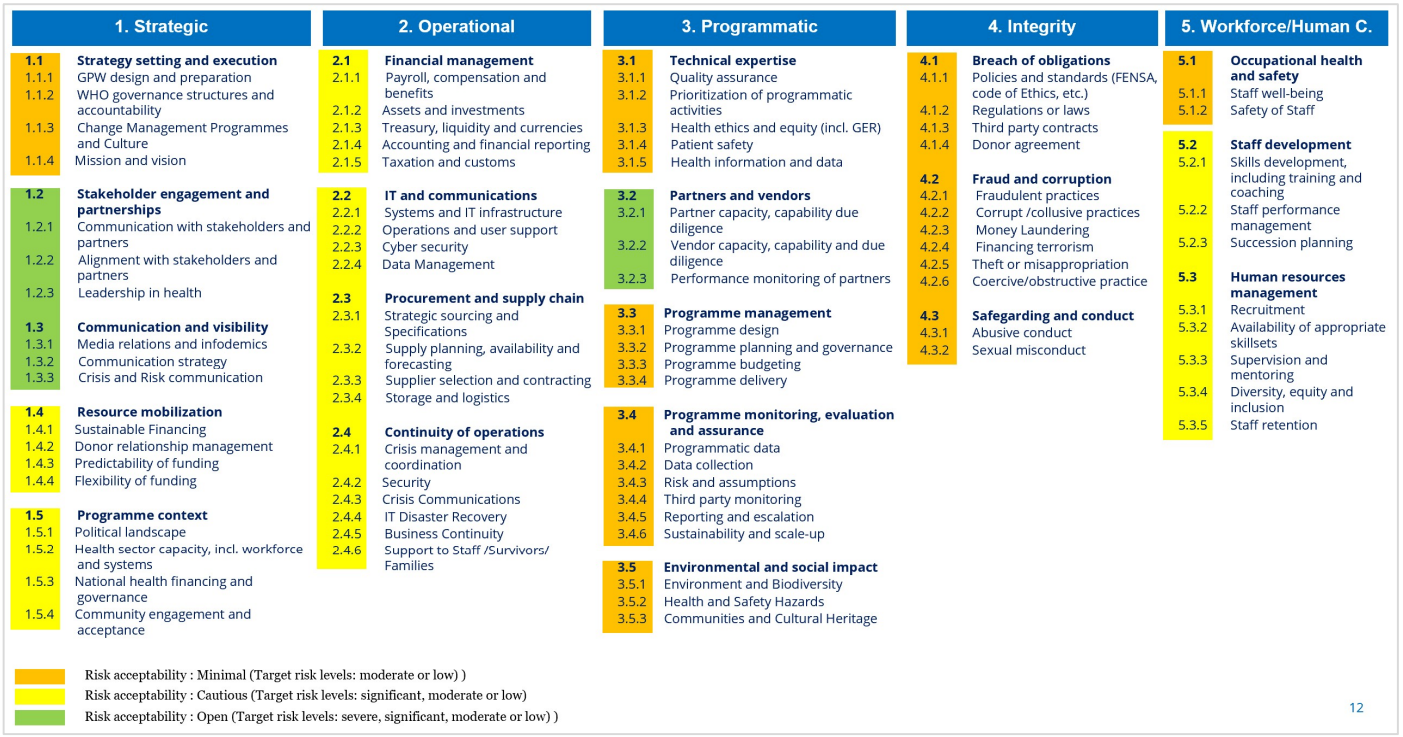

Figure 1: Risk Appetite mapped over the Risk Taxonomy