

Principal Risks

(as of 12 May 2025)



Principal Risks are risks that:

- (i) may affect the achievement of WHO's objectives (including GPW14 implementation), and**
- (ii) require alignment and coordination in their response and mitigation across the three levels of the Organization.**

The Principal Risks are the result of a “bottom-up” risk identification process, as captured in WHO’s corporate Risk Management Tool, complemented by a comprehensive “top-down” review, conducted by the Global Risk Management Committee (GRMC). As per previous years, the identification process included analysis of the GPW14 risk factors and benchmarking against peer agencies. This year’s top-down review integrated the latest global and organizational context through interviews with senior decision-makers across the Organization to ensure the 2025 Principal Risks accurately reflect WHO’s internal and external risk landscape.

As part of the increasing risk management maturity process, this year’s analysis categorizes Principal Risks into primary and secondary risks. The secondary risks are contributing to the primary ones. The Principals Risks are presented below by criticality level further to the assessment by the Global Risk Management Committee. The first table showcases the top five Principal Risks by criticality level and the second table lists the remaining Principal Risks.

Management establishes mitigation measures, and future risk response strategies are outlined to reduce the residual risk to levels aligned with WHO’s risk appetite. The risks are discussed and updated regularly under the leadership of the Global Risk Management Committee.

As part of WHO’s risk management journey, risk descriptions and related action plans are continuously refined and discussed among regional networks within WHO, to facilitate the operationalization and monitoring of the residual risk exposure by Global risk owners.

The update of Principal Risks is therefore a dynamic and iterative process. As a result, the list below only provides a snapshot of WHO’s risk profile, at the date of publication. This list evolves over time.

Top Five Principal Risks (by criticality level)

RISK No.	RISK SHORT NAME	RISK DESCRIPTION
1	Global health and WHO's legitimacy undermined (including societal polarization)	Global health and WHO's legitimacy (including recognition of its leadership / coordination role in international health) is undermined due to geopolitical instability, a comparative advantage not recognized amongst other players and/or scepticism towards multilateralism, negatively impacting its ability to leverage consensus-based mechanisms and its resource mobilization efforts.
	1.1 Weak capacity of Implementing Partners (including fragile country capacity)	Dependency on Implementing Partners with limited, and rapidly declining capacity (including Ministries of Health and stakeholders at country level) may lead to incomplete execution of WHO's delivery of programmes.
	1.2 Mistrust in Science and WHO (includes misinformation and disinformation)	Mistrust in science and in the positive impact of WHO's health activities, with misinformation and disinformation campaigns amplified by social media targeting health, may result in decreased effectiveness and reach of WHO's health policies and guidelines in certain communities and in loss of public and Member States' trust.
	1.3 Ineffective partner engagement	An ineffective partner engagement strategy and model may lead to duplication of efforts, heightened competition among health agencies, and an inability to leverage each other's strengths to effectively address health topics.
	1.4 Communication Risk	Lack of effective internal and external communication strategies leading to (i) WHO's added value not being recognized by other stakeholders, and/or (ii) inconsistencies in responding to emerging issues across the three levels of the Organization.
2	Inflexible, unpredictable and non-diversified financing, along with significant reductions in funding	Insufficient flexible and predictable financing and reliance on a limited number of donors increases the exposure to funding cuts impacting significantly key functions and programmes as well as continuity of operations.
3	Inability to rapidly define a fit for purpose organizational structure to address public health needs and WHO's Constitution	Inability to design swiftly an operational structure delivering WHO's constitutional mandate in an evolving global context due to: <ul style="list-style-type: none"> i. Challenges in prioritizing strategic technical areas ii. The need to embrace innovation in health matters (e.g. e-health, Artificial Intelligence)
	3.1 Business Management System (BMS) transition	In the context of current organizational changes, BMS development falling short on delivering its expected operational and efficiency results, thus failing to support the Organization in addressing today's global health needs.
	3.2 Quality and excellence of WHO's normative work compromised	WHO's normative and technical work compromised, negatively affecting WHO's ability to deliver GPW results and reputation.
4	WHO's inability to adequately support Member States in the event of a rapid resurgence of infectious diseases or health emergencies	Failure to adequately support Member States and manage rapid resurgence of infectious diseases (including inability to interrupt wild Polio virus transmission) or multiple, simultaneous health emergencies affecting the Organization's reputation.
5	Fraud and corruption	Fraud and corruption cases involve the misuse of funds by staff and non-staff, potentially leading to the inability to implement WHO activities in an effective, efficient, and economical manner; and to major donor and Member States, outrage and loss of confidence in WHO's ability to manage funds.

Other Principal Risks (by criticality level)

RISK No.	RISK SHORT NAME	RISK DESCRIPTION
6	Inability to equip WHO with a fit for purpose and qualified workforce	Difficulty in establishing high performing and fit for purpose technical workforce to sustain current and future WHO's activities which may hamper WHO's ability to fulfil its core mandate.
7	Strained workforce mental health and well-being	Strained WHO workforce well-being and mental health may result in lack of motivation, mental strain, physical health deterioration, and staff burnout which ultimately results in reduced organizational performance.
8	Breach in data protection and privacy and leakage of WHO confidential information	Intentional or unintentional leakage and misuse of personal identifiable information and/or WHO confidential information (perpetrated internally or by external actors) due to a lack of appropriate data protection mechanisms and resources.
9	Inability to demonstrate results and impact	Inability to demonstrate WHO's results and impact with a fit for purpose results chain responding to the latest global health needs, affecting WHO's ability to maintain its comparative advantage in the Global Health architecture and reliability for donors.
10	Vulnerable supply chain disruptions	With the current international trade landscape, failure to deliver quality health products timely and at budgeted costs in WHO programmes in response to country needs.
11	Sexual misconduct not prevented or addressed	Inability to prevent, detect and manage cases of sexual misconduct, including, but not limited to sexual exploitation, sexual abuse and sexual harassment (SEAH) thereby harming people and affecting the reputation of the Organization.
12	Abuse of power and harassment	Abuse of power and harassment in WHO's workplace may lead to deterioration of WHO's staff well-being and the establishment of an environment of acceptance impacting the reputation of the Organization as a United Nations health agency.
13	Business services disruptions 13.1 Cybersecurity breach	Incidents (e.g. natural disasters, security-related threats, armed conflicts) with the potential of interrupting or halting the normal functioning of essential services within WHO may lead to discontinuity of operations including major financial losses, inability to deliver programmes, harm to staff safety, and loss of data. Cybersecurity attack significantly compromising critical HQ, Regional, and/or Country information systems, WHO digital assets or critical data leading to discontinuity of operations, financial losses, legal claims, and/or damaged reputation.
14	Climate, Environmental and Social Safeguards Risk	Inability to address the health impacts of climate change globally and within WHO health programmes, thus undermining (i) WHO's ability to act fully as the directing and co-ordinating authority on international health (as mandated by its Constitution) in this field, or (ii) inadvertently causing negative environmental and social impacts to the communities WHO serves.