RISK MANAGEMENT STRATEGY

Reducing uncertainty around the achievement of WHO's objectives and outcomes

Abstract

This strategy provides a blueprint for WHO's vision and ambition related to Enterprise Risk Management (ERM) within the World Health Organization (WHO). It outlines the path WHO has taken to introduce concrete measures to identify, assess, manage, and monitor risks effectively, and the actions it will take in the short-, medium- and long-term to embed a stronger risk culture and a more enabling risk management process within the Organization.

Office of Compliance, Risk Management and Ethics (CRE)

Contents

I. Definitions 2

II. Background 3

III. Risk management journey to date 4

IV. Risk management vision for the future 5

V. How we will achieve our vision 8

VI. Getting started 14

VII. What investments are needed? 16

VIII. Conclusion and timeframes 18

IX. Annexes 0

i. Risk appetite statement 0

ii. The Three Lines of Assurance Model 12

iii. Prioritized Principal Risks 17

iv. The Reference Maturity Model for Risk Management in the UN System 18

v. The Theory Of Change supporting the Risk Management Strategy 19

I. Definitions

The following definitions and explanations are key to understanding the WHO Risk Management Strategy:

Term	Definition
Compliance	Compliance at WHO is the process of adhering to obligations derived from i. internal rules, policies, and procedures, ii. applicable international standards or regulations and iii. contractual terms with third parties, where violation could result in negatively impacting WHO's organizational objectives, reputation, performance, and ability to deliver on its values and ethical principles.
Internal Control	WHO considers internal control as "a process, designed to provide reasonable assurance to WHO management and stakeholders regarding the achievement of objectives relating to operations, reporting and compliance". The definition is broad and reflects that assurance should be given over more than just financial objectives and financial controls. It includes programme operations, human resources, procurement, travel and safeguarding of assets. It is aimed at the achievement of three objectives: (i) Operations Objectives - related to the effectiveness and efficiency of all operations, (ii) Reporting Objectives - related to the financial and non-financial reporting and its reliability, timeliness, transparency or meeting of other requirements that may be established by WHO; and (iii) Compliance Objectives - related to the WHO's adherence to applicable policies, rules, and regulations.
Assurance	Assurance at WHO relates to the mechanisms contributing to getting confidence over the effectiveness of risk mitigation, in the pursuit of objectives and outcomes. The responsibility for assurance mechanisms is shared among all role-players within the Three Lines of Assurance Model. Assurance is greater when provided by actors not involved with generating the transactions or those not in the primary line, when it comes to managing risks.
Risk Appetite	The aggregate amount (level and types) of risk WHO wants to assume in pursuit of its strategic objectives (and mission).
Risk	Risk can be defined as a potential uncertain event which could affect the achievement of the WHO's objectives and expected results.
Risk Management	Risk management is the process of identifying, prioritizing and responding to risks across an organization. Risk management includes activities to realize opportunities while mitigating threats.
Three Lines of Assurance	The Three Lines of Assurance Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.

II. Background

1. All WHO stakeholders, including the people we serve, Member States, partner agencies, WHO personnel, and donors, rightly have high expectations for strong systems to identify and respond to risks.
2. WHO recognizes that the global environment in which it delivers its mission is becoming increasingly complex and is filled with uncertainty. In recognition of this uncertainty and the impossibility for the Organization to refrain from delivering on its mandate, WHO needs to take calculated risks to successfully achieve its ambitious mission, and the General Programme of Work (GPW).
3. WHO therefore needs to explicitly define an enabling risk appetite and ensure that its approaches, strategies and tools consistently enables its operations, in line with that appetite. WHO will not be able to achieve the results as defined in its GPW and in the Sustainable Development Goals (SDGs) if the Organization is "risk averse" or "risk blind". Accordingly, WHO must define effective ways to understand the risks it faces and manage them to maximize results.
4. In defining and implementing those fit-for-purpose risk management approaches across its Results Based Management (RBM) System and operations, WHO will be able to minimize surprises which derail achievement of results and undermine its related financing.
5. The key question is: "How do we achieve this?" Incorporating leading practices, including from across the United Nations for an effective risk management system, this Strategy outlines a framework to ensure WHO's Enterprise Risk Management (ERM) system is fit-for-purpose to enable the achievement of its objectives in line with its risk appetite.

III. Risk management journey to date

1. The importance of risk management in achieving results was institutionalized by WHO's reform process, as defined at the 64th World Health Assembly in 2011. In 2014, the 'Compliance, Risk Management and Ethics' (CRE) department was established as part of this reform, with the objective of pursuing excellence across the three levels of the Organization in an effective, efficient, transparent, and accountable way.

2. Risk management is not new in WHO. The 2015 WHO Accountability Framework clearly includes risk management as a key pillar. The first Executive Board paper on risk management, including a corporate risk register, was submitted to the EB in May 2013.[1] A Corporate Risk Management Policy was issued in November 2015.[2] WHO has been publishing its Principal Risks annually since 2017 on its website. Moreover, between 2015 and May 2022, various governing bodies and their subsidiaries have issued 60 recommendations/requested actions of the Secretariat on risk management/risk statements[3].

3. Since 2017, WHO has institutionalized, through its corporate risk register and internal control self-assessment checklist, an annual assessment of risks and key controls across the Organization. Dedicated risk management functions were also created in each of the regions, and in some programmes, to support risk management activities.

4. The introduction of these risk-related activities were initially judged appropriate and sufficient. However, in the past decade, the complexity of WHO's work has evolved, with increased demands for WHO's engagement in health emergency preparedness and response, beyond its initial focus on normative work. This operating environment calls for adaptation, particularly given the nature of risks that have emerged, such as those demonstrated by the sexual abuse and exploitation allegations in the Democratic Republic of the Congo, as documented in the Independent Commission report[4] in 2021.

5. WHO now faces increased operational risks, which require a different, expanded and more proactive approach: risk management cannot be a separate administrative process but must be embedded into the daily decision-making of all actors who contribute to delivering health outcomes, informing their strategic and operational choices as well as related resource prioritization. This includes not only WHO's personnel, but also its partners who help the Organization implement and deliver on its mission (i.e., Member States, International Non-Governmental Organizations (INGOs) or Non-Governmental Organizations (NGOs)).

[1] https://apps.who.int/gb/ebwha/pdf_files/EB133/B133_10-en.pdf

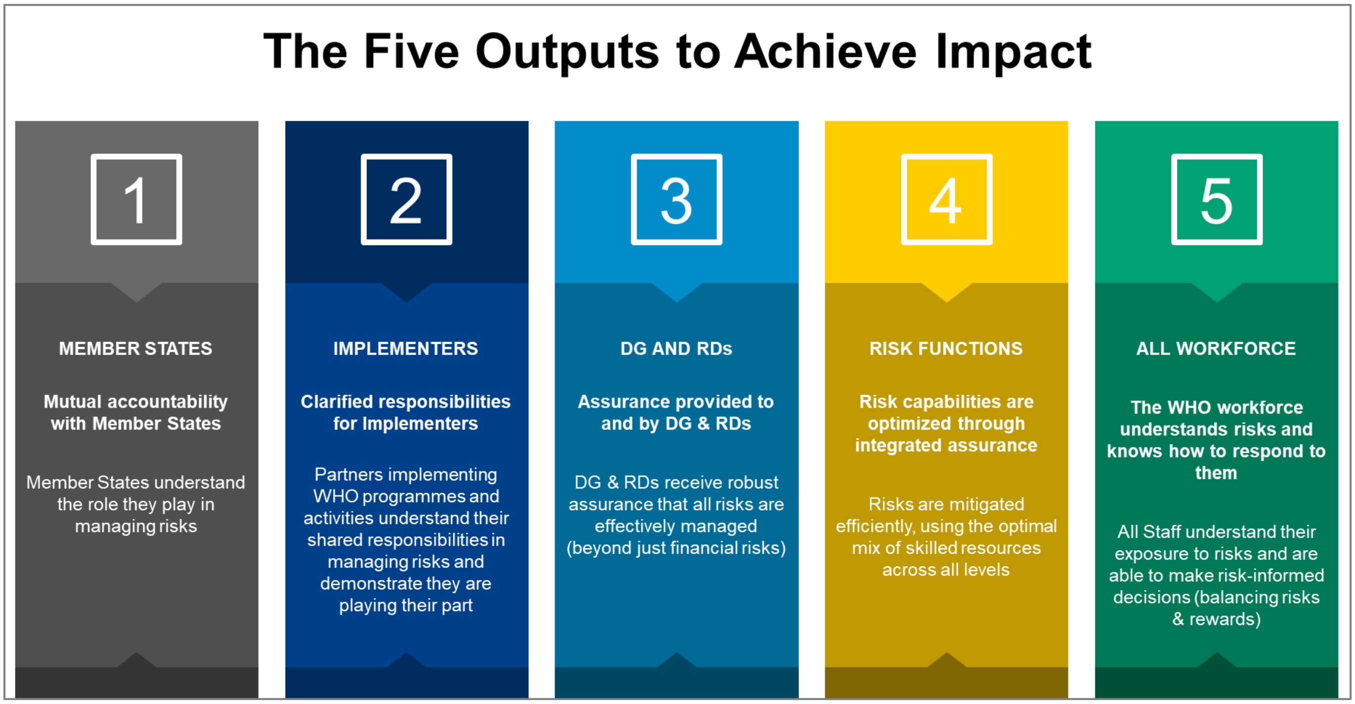
[2] https://intranet.who.int/homes/cre/documents/corporateriskpolicy.pdf

[3] IEOAC (11), PBAC (10), EB (2), IOAC (7), External Auditor (18), JIU (11), and ICSEA (1)

[4] Final Report of the Independent Commission on the review of sexual abuse and exploitation during the response to the 10th Ebola virus disease epidemic in DRC

IV. Risk management vision for the future

Risk Management should enable WHO colleagues and partners to create impact and achieve results, and not be perceived as preventing the organization from achieving positive health outcomes. Therefore, for WHO to effectively manage its risks, it should build a risk-aware culture, where risk management informs decision-making affecting the GPW outcomes and is embedded into its Results Based Management system, to be an integral part of strategic planning, implementation, and resource prioritization at all levels. To achieve this goal, the following elements were identified as key outputs that must be achieved through implementation of the Risk Management Strategy.



The Five Outputs to Achieve Impact

1

MEMBER STATES

Mutual accountability with Member States

Member States understand the role they play in managing risks

2

IMPLEMENTERS

Clarified responsibilities for Implementers

Partners implementing WHO programmes and activities understand their shared responsibilities in managing risks and demonstrate they are playing their part

3

DG AND RDs

Assurance provided to and by DG & RDs

DG & RDs receive robust assurance that all risks are effectively managed (beyond just financial risks)

4

RISK FUNCTIONS

Risk capabilities are optimized through integrated assurance

Risks are mitigated efficiently, using the optimal mix of skilled resources across all levels

5

ALL WORKFORCE

The WHO workforce understands risks and knows how to respond to them

All Staff understand their exposure to risks and are able to make risk-informed decisions (balancing risks & rewards)

Figure 1: Vision and ambition for Enterprise Risk Management, namely, the Five Outputs to Achieve Impact

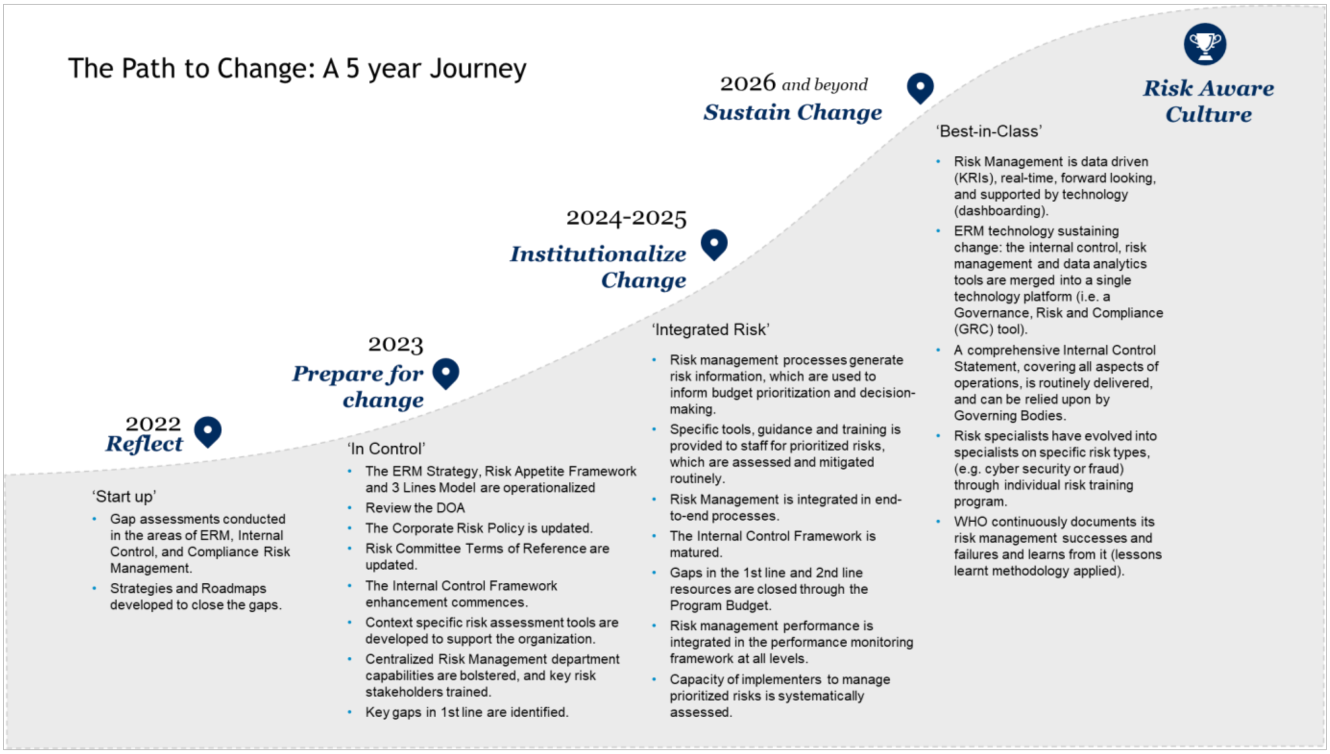
1. **Mutual accountability with Member States** – WHO and its Member States have a mutual accountability in delivering health outcomes. In so doing, they also have mutual accountability to manage the uncertain events which may affect those health outcomes, i.e., risks.
   - This takes the form of agreeing a Programme Budget which clearly defines the risks faced when delivering the GPW, and
   - Prioritizing the resources in Programme Budget and other voluntary contributions aimed at maintaining risks within acceptable limits, as defined by the Risk Appetite Framework (outlined in Annex i) and the Organization's Results Based Management policies and procedures.

2. **Clarified responsibilities of Implementing Partners in managing risks within their control** – WHO delivers health outcomes through implementing partners (including MOHs, Non-State actors, etc.). The effective management of risks by WHO will therefore be highly dependent on WHO's ability to assess the capacity[5] of those implementing partners to identify, prevent and mitigate risks and its ability to monitor the effective management of risks during the implementation of health programmes. This will require implementing partners to commit to facilitating WHO's assessments and monitoring activities, including, where needed, though external assurance mechanisms (e.g., external risk and assurance reviews, on-site spot-checks of implementing partners, and compliance reviews, etc.)
3. **The Director-General (DG) and Regional Directors (RDs) can attest to the effective management of risk at all levels** – the DG and RDs should be enabled to provide reasonable assurance to external stakeholders that risks are effectively identified and managed in all key operations and decisions contributing to the GPW. This will require:
   - Recognition that Principal Risks (i.e., fraud and corruption, SEAH etc…) require a more centralized and harmonized approach in defining mitigations and executing oversight (including compliance) led by the Global Risk Management Committee,
   - Risk management processes to be integrated into the Organization's Results-based management and business operations of the Organization (including into the new ERP),
   - Roles and responsibilities at the three levels of the Organization to be clearly defined and efficiently distributed in terms of risk identification and performance of checks and balances (i.e., controls), and
   - Compliance checks to adherence with policies and procedures, and risk informed challenging mechanisms with the objective of generating robust and integrated assurance on which the Director-General and RDs can rely on, in line with the Three Lines of Assurance Model referenced in Annex ii
4. **All three levels (Countries, regions and HQ) are capacitated with sufficient resources** – in the form of Risk, Compliance and Assurance specialists in place where risks are higher and capacity is limited – risks are mitigated efficiently, using the optimal mix of skilled resources from all three levels and lines of assurance.
5. **All staff can make risk-based decisions –** all staff (across all levels of the Organization) are equipped with the guidance and resources needed to identify risks and base their decisions on a calculated balance between *risks and rewards* (i.e., pursued health impact or benefits).

[5] Capacity refers to the people, processes, and systems

Guiding the implementation of this Strategy is a Theory of Change (refer to Annex v), reflecting the activities above leading to the desired results and facilitating the development of a results framework and monitoring and evaluation framework for the Strategy.

V. How we will achieve our vision



The Path to Change: A 5 year Journey

2022 *Reflect*

'Start up'

- Gap assessments conducted in the areas of ERM, Internal Control, and Compliance Risk Management.
- Strategies and Roadmaps developed to close the gaps.

2023 *Prepare for change*

'In Control'

- The ERM Strategy, Risk Appetite Framework and 3 Lines Model are operationalized
- Review the DOA
- The Corporate Risk Policy is updated.
- Risk Committee Terms of Reference are updated.
- The Internal Control Framework enhancement commences.
- Context specific risk assessment tools are developed to support the organization.
- Centralized Risk Management department capabilities are bolstered, and key risk stakeholders trained.
- Key gaps in 1st line are identified.

2024-2025 *Institutionalize Change*

'Integrated Risk'

- Risk management processes generate risk information, which are used to inform budget prioritization and decision-making.
- Specific tools, guidance and training is provided to staff for prioritized risks, which are assessed and mitigated routinely.
- Risk Management is integrated in end-to-end processes.
- The Internal Control Framework is matured.
- Gaps in the 1st line and 2nd line resources are closed through the Program Budget.
- Risk management performance is integrated in the performance monitoring framework at all levels.
- Capacity of implementers to manage prioritized risks is systematically assessed.

2026 *and beyond* *Sustain Change*

'Best-in-Class'

- Risk Management is data driven (KRIs), real-time, forward looking, and supported by technology (dashboarding).
- ERM technology sustaining change: the internal control, risk management and data analytics tools are merged into a single technology platform (i.e. a Governance, Risk and Compliance (GRC) tool).
- A comprehensive Internal Control Statement, covering all aspects of operations, is routinely delivered, and can be relied upon by Governing Bodies.
- Risk specialists have evolved into specialists on specific risk types, (e.g. cyber security or fraud) through individual risk training program.
- WHO continuously documents its risk management successes and failures and learns from it (lessons learnt methodology applied).

Risk Aware Culture

Figure 2: Our approach to achieving our vision by 2026

a) 2022 Reflect

Reflecting on the Current State

Much of 2021 and 2022 were used to reflect on the current state of Risk Management within WHO, with two main outcomes:

i. Formal gap assessments were conducted (using external service providers), in the areas of the Internal Control (including a focus on Fraud and Corruption), Compliance, and Risk Management (with additional work done around developing a Risk Appetite Framework).

ii. Strategies and Roadmaps have since been developed to close gaps. Significant gaps will be closed through the implementation of this ERM strategy, and what follows in sections b) to d) below.

b) 2023 Preparing for change

Ten key actions to shape the system

1. **Key Action 1: The Global Policy Group (GPG) endorses the Risk Strategy and Risk Appetite Framework**, for further endorsement by Member States through the Programme, Budget, and Administration Committee (PBAC) and the Executive Board. This will facilitate the operationalization of the Risk Appetite Framework within WHO and will serve as guidance to staff on how to formalize risk & rewards assessments (i.e., the balance between risks and the rewards associated with the public health impact/benefits pursued) to guide decision-making and resource prioritization. In particular, the Secretariat will systematically apply the risk appetite framework implementing it with due diligence processes, and decisions escalated to committees guiding strategic or scientific decision-making potentially affecting global health outcomes and/or the Organization's reputation
2. **Key Action 2: Reflect Risk appetite in the 2024 Programme Budget** – The Programme Budget has been prepared to highlight areas where WHO has lower risk acceptability, and where (consequently) funds are needed to build and capacitate the necessary systems (people, processes, technology, etc.) to keep risks within acceptable levels (e.g., for high priority risks like PSEAH and other Prioritized Principal Risks[6]), recognizing the critical role of the Output Delivery Teams role in identifying risks, and in ensuring that the funds needed for mitigation are prioritized.
3. **Key Action 3: Update tools to manage collaboration with implementing partners** – WHO defines the required capabilities of Implementing partners (including Ministries of Health (MOH)) and creates (or updates where relevant) tools to assess the capacity of implementing partners to manage high risk areas and monitor them (see section VI).
4. **Key Action 4: Enhance the internal control framework** – Formalize a global and unified set of checks and balances (i.e., controls) and related accountability matrices (RACI Charts/Risk & Controls Matrices) for key processes underlying prioritized Principal Risks, with clear responsibilities defined at the three levels. The scope of this enhanced internal control framework would go beyond financial assurance to provide broader assurance over the achievement of the General Programme of Work, in line with the latest UN reform. This would provide a very practical tool for effectively operationalizing accountability in a decentralized environment such as WHO's.
5. **Key Action 5: Review the Delegation of Authority (DoA)** – Review and refine the Delegation of Authority (DoA) to reflect at all levels (DG to RD, ADG and Directors, RD to WRs and in job descriptions

[6] As defined in Annex ii, and updated annually

and performance objectives of team leads and staff) the obligation to identify, assess, and mitigate risks (at a minimum the Principal Risks), and ensure internal controls are operating effectively. This will only be effective if more granular expectations on risk identification, assessment and mitigation are defined and communicated to operationalize the authority delegated and facilitate monitoring.

6. **Key Action 6: Operationalize a "Three Line of Assurance Model"** – Adapting WHO's "three lines of assurance" model for accountability (see Annex ii), by mapping existing functions and roles which contribute to managing risks, to ensure complementarity of roles and responsibilities, and thereby minimize gaps and duplications. The aim is to clarify, for key organizational processes and risks, clear roles and responsibilities, through the following broad classifications, which will be mapped by roles:
   i. **1st Line of Assurance**: the front-line managers in charge of delivering on a daily basis WHO programmes and activities while maintaining an effective balance of risks and rewards in their decisions; they are responsible for implementing the necessary controls to manage identified risks, for supervising their execution and for ensuring related routine compliance with rules and regulation. Given WHO's decentralized nature, with policy makers located at Headquarters, and operations implemented at the Headquarter, regional and country level, dedicated roles or teams may be required to support front line managers in their duty to review control measures in a harmonized manner and ensure their correct execution in high-risk areas (called in this document the 1.5 Line of Assurance).
   ii. **2nd Line of Assurance**: the Risk management and compliance teams which provide expertise, advice, tools/techniques on matters of risk management, assurance, and compliance. They are responsible for providing consolidated reports on the effectiveness of internal controls, risk management and state of compliance within the organization.
   iii. **3rd Line of Assurance**: The Internal audit and Evaluation functions which provide assurance to the WHO governing bodies on the performance of 1st and 2nd Lines.

   To accomplish and enable this framework, a mapping of key functions contributing to manage risks across the 1st and 2nd line and the three levels of WHO is required and surge capacity will be established to fill identified gaps (including capacitating country offices for core functions (e.g. procurement, finance, monitoring evaluation finance, security, IT etc) and using a "roster" of talent ready to be drawn on, at short notice, especially in high-risk countries, programmes, and activities).

7. **Key Action 7: Formalize a network of risk champions** within the existing first line functions in each division, department, and countries, with harmonized Terms of Reference to monitor/report back on the risk management activities **and increase the capacity and skills of the risk, assurance, and**

compliance functions in the second line. These would involve: (i) making available Risk and Assurance advisors to countries and programmes operating in high-risk environments as a support to decision-making, (ii) strengthening the capacity of regional and headquarters' risk management functions to provide risk management tools and guidance to countries and programmes and (iii) strengthening the Global compliance program and other early alert systems to facilitate more regular verifications regarding the operating effectiveness of controls using various testing and monitoring techniques..

8. **Key Action 8: Train key risk stakeholders** (e.g., Risk Owners (i.e., ADGs, Directors, Team Leads), Risk Focal Points, WRs and DAFs, etc.) on the application and use of the Risk Appetite framework, thus equipping them with the tools needed to make risk informed decisions daily.
9. **Key Action 9: Develop context specific risk assessment tools** to support staff at all levels in understanding the factors which may increase the exposure to the Prioritized Principal Risks in a consistent manner (e.g., as done in 2022 for SEAH, using where possible Key risk indicators, including the integration of the Corporate Risk register into the new ERP design).
10. **Key Action 10: Update the Corporate Risk Policy and harmonize the terms of Reference for Risk Management committees across the three levels:** the updated policy would highlight changes to the methodology needed to operationalize the newly defined Risk Appetite framework; terms of references for Regional and local committees where relevant (including for high-risk programmes) would be adapted to allow for coordinated monitoring of the risk and assurance agenda across the three levels.

c) 2024-2025 Institutionalizing Change
Building a risk aware culture within WHO

Our objective in this phase is to enable systematic identification and analysis of risks, with sound comparison of expected health impact as a cornerstone of effective risk management. This requires the integration of risk assessment into Results Based Management (RBM) (i.e., planning, implementation, and performance assessment processes) across the Organization:

1. **Risk management incorporated into workplans:** All budget centers and programmes prepare their workplans with due consideration to risks that may affect their objectives; the new risk management tool in the System for Programme Management (SPM) is available to facilitate the incorporation of risk mitigation into operational planning.

2. **Key Business Owners in the first line provide annual assurance:** Key business owners at all levels of the Organization provide annual compliance, risk, and assurance reports to the Global Risk & Assurance function (through regional risk and assurance) on the operating effectiveness of the global key controls adopted in 2023. Key business owners and cadence of reporting will be based on the Terms of Reference of the Local, Regional and Global Risk Management Committee.
3. **An annual compliance, risk and assurance plan for monitoring of prioritized risks and controls is defined and driven by a Chief Risk Officer (CRO) role:** compliance, risk and assurance functions assess risk and control mechanisms for high-risk areas based on the global Compliance, Risk and Assurance plan defined by the global function, headed by the CRO and complemented with regional specifics; regional compliance, risk and assurance managers' report their activities in a transparent manner to the Global Function, following harmonized Terms of Reference. They ideally report to RDs, building on the annual compliance and assurance reports received from the 1st and 1.5 lines of assurance (where existing) and relevant additional verifications. Where direct reporting line to RDs is not feasible, clear safeguards are established to guarantee that the compliance, risk and assurance function can operate and report without limitations, with sufficient authority (i.e. levels of seniority), resources free access to RDs and broad coverage of the regions' activities. Global and regional Compliance, risk and assurance functions also report to the Global and regional Risk Management committees respectively.
4. **Risk management and assurance is linked to performance assessments:** Risk information informs performance assessments at budget centers level (e.g., country/department performance) through established Key Performance/Key Risk Indicators and individual levels (staff ePMDS objectives and related performance).
5. **Capacity of implementing partners to manage prioritized risks is systematically assessed:** Will include joining the UN partner portal beyond for SEAH related risks, where WHO will join efforts of other UN organizations in assessing partners' capacity.

d) 2026 Sustaining Change

Sustaining change beyond 2026

1. **Information and Dashboarding**: With the roll-out of the new ERP system, senior management at all levels have access to dynamic and comprehensive risk information in a transparent manner which informs decision-making in a dynamic manner (e.g., risks at all levels, Key Risk Indicators by countries, etc.). Dynamic risk information dashboards and risk appetite, tolerance (or criteria) is proactively used across WHO's operations.
2. **ERM Technology:** The internal control, risk management and data analytics tools are merged into a single technology platform (Governance Risk and Compliance tool) to be integrated with the new ERP.
3. **Continuous Improvement:** The Organization continuously documents its risk management successes and failures and learns from it.

VI. Getting started

Key principles for a smooth operationalization

a) **Focusing on Quick Wins (the 10 Actions):** The 10 actions proposed in section IV a) “2023 – Getting ready for change” (above) will be prioritized

b) **Risk-based prioritization:** In a context of constrained funding within WHO, it may not be possible to tackle all risks at the same time. The principle of risk-based prioritization will be applied when investing the efforts needed to implement the programme for change. For that reason, where relevant, the 10 actions will be implemented with the following prioritization criteria:

   i) **Prioritizing a subset of Principal Risks:** Annex iii represents a subset of Principal Risks (as defined in 2022, and will be updated annually) which are recognized to critically affect WHO’s work at country level. By prioritizing these Principal Risks, we can achieve maximum impact at country level, whilst prioritizing scarce resources.

   ii) **Focus on high-risk environments first:** With regards to the establishment of a surge capacity for gaps identified in the first line and second lines of assurance, due consideration of the following will be given for prioritization of resources:

      (1) **Countries**: Countries prioritized for support, countries with fragile health systems, and countries with high-risk indices relevant to Prioritized Principal Risks.

      (2) **Programmes/awards**: Emergencies Graded 2 and 3, programmes with an impact on Polio reduction and for those donors with specific or formalized risk management requirements.

      (3) **Service Delivery Activities**: with the aim to ensure minimum capacity is in place in WHO Country Offices to implement such activities in the following areas: Procurement and supply chain, Human Resources, Monitoring & Evaluation, Financial oversight, Security, PSEAH, Compliance and Risk Management and assurance.

c) **Finalizing the building blocks required to drive the ERM Strategy:** To implement the Risk Management Strategy, the following building blocks are currently being finalized, to steer the risk conversation, across all stakeholders, with a consistent language and in a comprehensive manner. They include:

   i) **Risk Taxonomy**. The risk taxonomy is a comprehensive, common, and stable set of risk categories that is used within an organisation to identify risks that could affect its objectives. The risk taxonomy is a fundamental building block of an ERM framework, and is used to correctly classify types of risk, aggregate them, and report on them in a consistent and meaningful way.

ii) **Risk Scoring Criteria**. Most organizations define scales for rating risks in terms of impact, and likelihood. Some form of measurement of risk is necessary to measure risks in a consistent way. Without a standard of comparison, it’s simply not possible to compare and aggregate risks across the Organization, and to know which risks to prioritize.

iii) **Key Risk Indicators**. Key Risk Indicators (KRIs) are critical for the purpose of risk tracking. When they are defined by the risk owner to take into account useful and available data sources within their processes, they provide early warning of increasing risk and/or control failures and act as a mechanism for continuous risk monitoring.

These building blocks are integrated through the end-to-end risk management process, which will be codified in the updated Corporate Risk Policy.

VII. What investments are needed?

Key investments in the areas of People, Process and Technology are needed to create the momentum for change, and then embed the change, to drive a truly risk-aware culture.

Investment type	Reason for Investment	Drivers of Cost
Additional Full-Time Equivalent (FTE) People costs[7] (agile model with experienced workforce supported by contractors and consultants to minimize FTE costs and allow flexibility)	• Delivery of specialized training to Key Stakeholders • Additional capacity at HQ level to drive the ERM Strategy • Additional capacity at the regional level to drive implementation at regional and country levels • Experienced risk advisors at country level in high-risk environments	• Number of additional HQ resources for the Global compliance, risk & assurance function • Number of additional resources for the compliance, risk & assurance function in the region and high risk environments (selected countries and programmes) • Number of additional resources for the gaps identified in the first line (including 1.5 where needed)
Individual Contractors and Consultants	• Burst capacity to proactively manage prioritized Principal Risks, • Burst capacity to respond to high impact risks which materialize • Specialized expertise around topics like: ○ Development of leading practice policies, processes, and tools ○ Change management around the implementation of the ERM Strategy (e.g., communication) ○ Development and delivery of specialized Training to Key Stakeholders	• Number of high-priority principal risks to be managed • Number of processes that need to be formalized and managed as per practice • Number of interventions that require a change programme to effect change (e.g., Risk awareness week, fraud & corruption awareness week). • Number of Training Workshops (consider number of regions, and countries)
Professional Association Memberships, Certifications and Training	• Building additional risk management expertise within the 2nd Line functions, to be less reliant on Individual Consultants, over time. • Increase the ability to Challenge, based on leading practice expertise.	• Number of FTE Staff Members • Number of Professional Associations held • Number of Certifications or training interventions embarked on.
Updating and redesigning digital risk management tools	*Development* • Development costs associated with the development or configuration of existing or new tools. *Licensing* • Software Licenses to specialized Risk and Compliance software and tools	• Development time (hours) required by the developer / development team. • Number of specialized software tools, and number of users.
Dashboard Development (Risks and Key Risk Indicators)	• Developer time to automate information pulling from the BMS ERP system or Risk	• Complexity of development requirements and number of hours

[7] An indication of cost was performed when a capabilities & resources requirements exercise was performed in the Compliance Review, concluded in February 2022.

Investment type	Reason for Investment	Drivers of Cost
	Management Tool (RMT) into near-real-time Dashboards	required by the developer / development team. - Could be external costs, or cross-charges from an in-house WHO team
Ancillary costs, including Travel and Training	*Travel* - In-person training to regions and countries to embed Risk Management Strategy, Risk Appetite Framework and updated ERM Building Blocks (e.g., the risk scoring criteria used for rating risks has changed in line with the updated Risk Appetite Framework) - Deployment of burst capacity to regions and countries to assess residual risks on Prioritized Principal Risk or High-impact risks which have materialized. *Training* - Strengthening capacity building at HQ, Regional and Country level - Train the trainer to build capacity - Potential expenses related to venue hire and related costs.	- Number of training interventions per annum, and number of CRE staff to deliver each training intervention. - Number of deployments to regions or countries per annum. - Number of verification missions included in the annual compliance, risk & assurance plans

Table 1: High-level indication of the types of costs we will incur, to deliver on this strategy

VIII. Conclusion and timeframes

1. **Endorsement of the ERM Strategy and Risk Appetite Framework**. The following next steps are recommended to achieve Member State endorsement, through a consultation process that affords key stakeholders the opportunity to give input over the next 6 months:

#	Action	Date
1	**Endorsement by the Global Risk Management Committee (GRMC)** *Having reviewed the draft ERM Strategy as pre-read to the committee meeting, the committee endorses the document for submission to the GPG, with further recommendations for implementation (November 2022).*	Endorsed
2	**Consultation with Independent Expert Oversight Advisory Committee (IEOAC)** *The CRE team consults with IEOAC to ensure alignment of the ERM strategy with other oversight functions within WHO and makes recommendations to ensure alignment where there are gaps. (March 2023)*	Consulted
3	**Presentation to and endorsement by the Global Policy Group (GPG)** *Following recommendations and endorsement by the GRMC and IEOAC, the GPG Endorses the ERM Strategy for implementation within WHO.*	May 2023
4	**Member State information session** *Member States are consulted on the updated ERM Strategy, as endorsed by the GPG. Any review comments or feedback is fed into the operationalization plan.*	May/ June 2023
5	**Presentation to and discussion/review by PBAC 38** *The PBAC will review, provide guidance and recommendations for possible adoption to EB153.*	May 2023
6	**EB 153 review and endorsement** *The EB will consider the strategy, taking note of the PBAC report.*	May/ June 2023

Table 2: An overview of the next steps to Socialize the ERM Strategy with Key Governing Bodies

2. Implementing this strategy across the three levels of the Organization, along with a proactive, practical, and systematic approach to enterprise risk management and the active engagement and ownership of Regional Offices and key business owners will deliver an enabling Risk Culture, where Risk Management informs daily decision-making across WHO, in an inclusive, transparent, and efficient manner, leading to an environment where:

i) **GPW results are maximized**, as risks are managed in timely manner, and by all partners (opportunities are seized and crises minimized),

ii) **Trust in WHO increases**, and leads to increased and sustainable funding, and

iii) **WHO is recognized as best-in-class for its risk & assurance frameworks**, and helps raise the bar for other UN Organizations.

IX. Annexes

i. Risk appetite statement

World Health Organization

Risk Appetite Statement

19-09-2022

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.

Supporting documentation and training will be made available, expanding on the contents of the Risk Appetite Statement, and will provide more detailed instructions on how to operationalize, and fully realize, the value of Risk Appetite.

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.

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

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***
Averse	**A high 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**
Minimal	**A high 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.
Cautious	**A moderate 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).
Open	**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 **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.

*These are baselines which generally apply when dealing with individual risks. When faced with dilemmas in managing risks affecting different success factors, please refer to “Operationalizing Risk appetite” in the risk appetite statement.

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 Exploitation, Abuse and Harassment (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.

Risk Acceptability – **Minimal** – **High** 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 – **Cautious** – A **moderate** amount of risk affecting the core principles underlying Partnerships **can be accepted**, only if there are no treatment strategies that can be **easily and economically implemented**. When possible, mitigation must be developed to bring the residual risk to **at least a moderate level** , taking into consideration the relative importance of internal and external factors and timelines driven by the availability of resources.

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 **moderate** amount of risk affecting the core principles underlying Financial Sustainability **can be accepted**, only if there are no treatment strategies that can be **easily and economically implemented**. When possible, mitigation must be developed to bring the residual risk to a **lower level**, taking into consideration the relative importance of internal and external factors and timelines driven by the availability of resources.

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** – **High** 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.

Examples of risks that impact this key success factor - Sexual Exploitation & Abuse, 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** – **High** levels of risk affecting the core principles underlying Compliance & Integrity 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 – Fraud and corruption; and Breach of WHO's rules and/or international regulations and professional standards.

Business Continuity and Operational Excellence

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 **moderate** amount of risk affecting the core principles underlying Business Continuity and Operational Excellence **can be accepted**, only if there are no treatment strategies that can be **easily and economically implemented**. When possible, mitigation must be developed to bring the residual risk a **lower level**, taking into consideration the relative importance of internal and external factors and timelines driven by the availability of resources.

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

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

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.

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

D. Operationalizing WHO’s Risk Appetite

i) Trade-offs/dilemmas and tensions between Key Success Factors:

Delivery on WHO's Mission is the “Raison d'être” of the Organization. When delivering its mission, WHO may face complex situations where the attitude to risks prescribed for one success factor may come into tension with that of other success factors. This may be the case when deciding to engage 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. ***Any deviation from the authorized levels will be escalated*** to the higher level of management level for approval and justification should be adequately documented.

In ***contexts requiring immediate action***, and where platforms to discuss dilemmas are not immediately available, ***rationale for decisions*** will be documented and ***revisited retroactively*** as needed.

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) Risk management governance and monitoring:

When dilemmas regarding WHO's risk appetite arise, WHO will discuss in its management structures (including risk management committees where relevant) the strategic direction needed to guide operational decision-making, in particular for defining risk acceptability levels in pursuits of impact.

Where relevant, risk owners and decision-makers should consult with donors at the outset of implementing donor funded activities, in an open and transparent way, briefing them on the risks associated with the activities and the related acceptance levels defined, to allow them to understand the level of risk involved, the extent of mitigation planned and the related resource implications.

At each level of the Organization, WHO will periodically compare the level of residual risk faced, with the levels of acceptability originally set, to identify situations needing escalation for approval or potential revaluation of the level of risk acceptability.

In contexts where the residual amount of risk remains outside of the targeted residual range for an extended period of time, Senior Management approval should be obtained, and rationale for remaining outside of target residual range will be documented.

The WHO risk appetite statement will be reviewed and adjusted as required by the changes affecting WHO’s environment and resources.

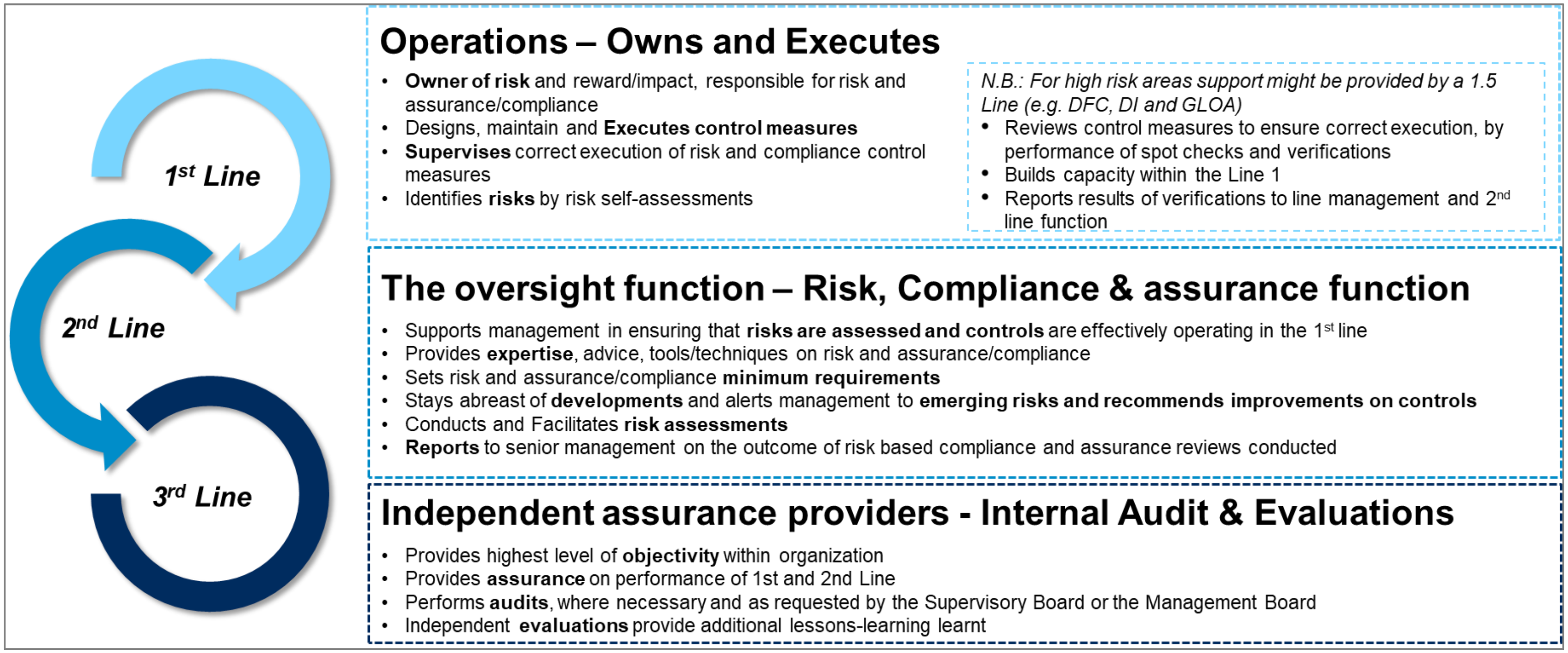
ii. The Three Lines of Assurance Model

Understanding the “Three Lines of Assurance” Model

Risk Management and Compliance are not solely the role of the Risk and Compliance functions in the Organization; compliance and risk management need to be embedded within day-to-day operations to be effective. Effective Risk Management and Compliance is a collaborative process that pulls together and leverages the various controls performed within WHO. While retaining overall responsibility for risk management and compliance in predefined areas, the risk & compliance function can therefore draw on the experience of the *first line* (incl. technical experts, and other control functions) where they exist. This collaboration approach can also help eliminate wasteful duplication of effort or obsolete procedures, as well as promoting information and knowledge sharing. Having clarity of individual roles and responsibilities for every actor in the process is helpful to advance operationalization of this strategy.

Reflected below is a proposed “Three Lines of Assurance Model” for WHO. It is based on a similar approach for broader accountability functions in an organization, the “Three lines model” as defined by the Chartered Institute of Internal Auditors guidelines. The latter reflects managerial responsibilities, oversight and external review/evaluation/audit where the majority of required responsibility is in the first line or level. This model was adapted for the WHO’s context, Organizational structure and capabilities for risk management outlining the primary managerial responsibilities and higher-level roles and responsibilities for each of the levels.

An overview of the proposed WHO 3 Lines Model. Defining the 3 Lines will bring clarity around roles and responsibilities for managing risks. Described in the bullet points below are the high-level roles & responsibilities.



Operations – Owns and Executes

- **Owner of risk** and reward/impact, responsible for risk and assurance/compliance
- Designs, maintain and **Executes control measures**
- **Supervises** correct execution of risk and compliance control measures
- Identifies **risks** by risk self-assessments

N.B.: For high risk areas support might be provided by a 1.5 Line (e.g. DFC, DI and GLOA)

- Reviews control measures to ensure correct execution, by performance of spot checks and verifications
- Builds capacity within the Line 1
- Reports results of verifications to line management and 2nd line function

The oversight function – Risk, Compliance & assurance function

- Supports management in ensuring that **risks are assessed and controls** are effectively operating in the 1st line
- Provides **expertise**, advice, tools/techniques on risk and assurance/compliance
- Sets risk and assurance/compliance **minimum requirements**
- Stays abreast of **developments** and alerts management to **emerging risks and recommends improvements on controls**
- Conducts and Facilitates **risk assessments**
- **Reports** to senior management on the outcome of risk based compliance and assurance reviews conducted

Independent assurance providers - Internal Audit & Evaluations

- Provides highest level of **objectivity** within organization
- Provides **assurance** on performance of 1st and 2nd Line
- Performs **audits**, where necessary and as requested by the Supervisory Board or the Management Board
- Independent **evaluations** provide additional lessons-learning learnt

Figure 3: Defining the high-level roles and responsibilities for each of the 3 lines of assurance.

Practical application of the 3 Lines of Assurance Model to the WHO Governance Structures and Organizational Layers

To allow for easier adoption of the 3 Lines of Assurance Model, it might be useful to illustrate how the 3 Lines Model is practically applied to the existing Governance Structures within WHO.

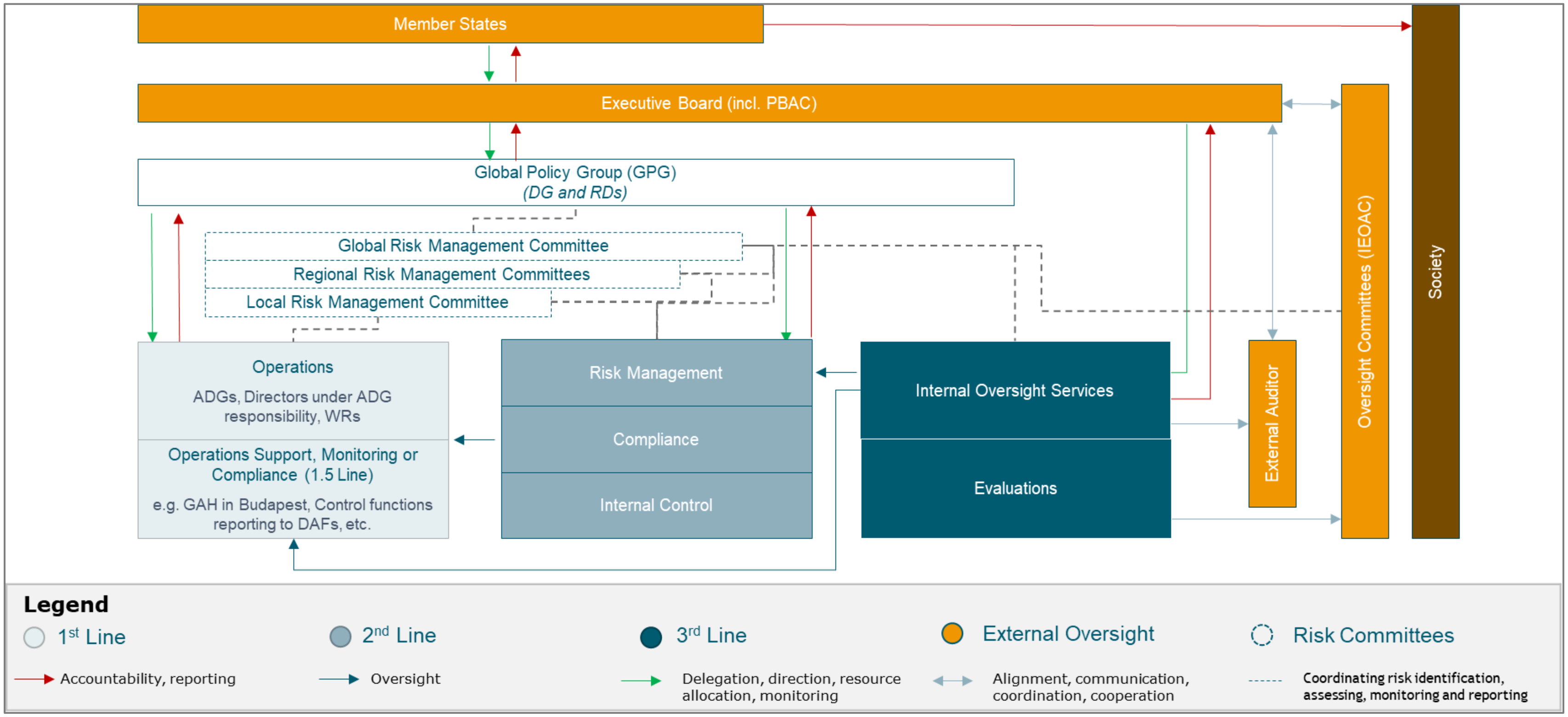
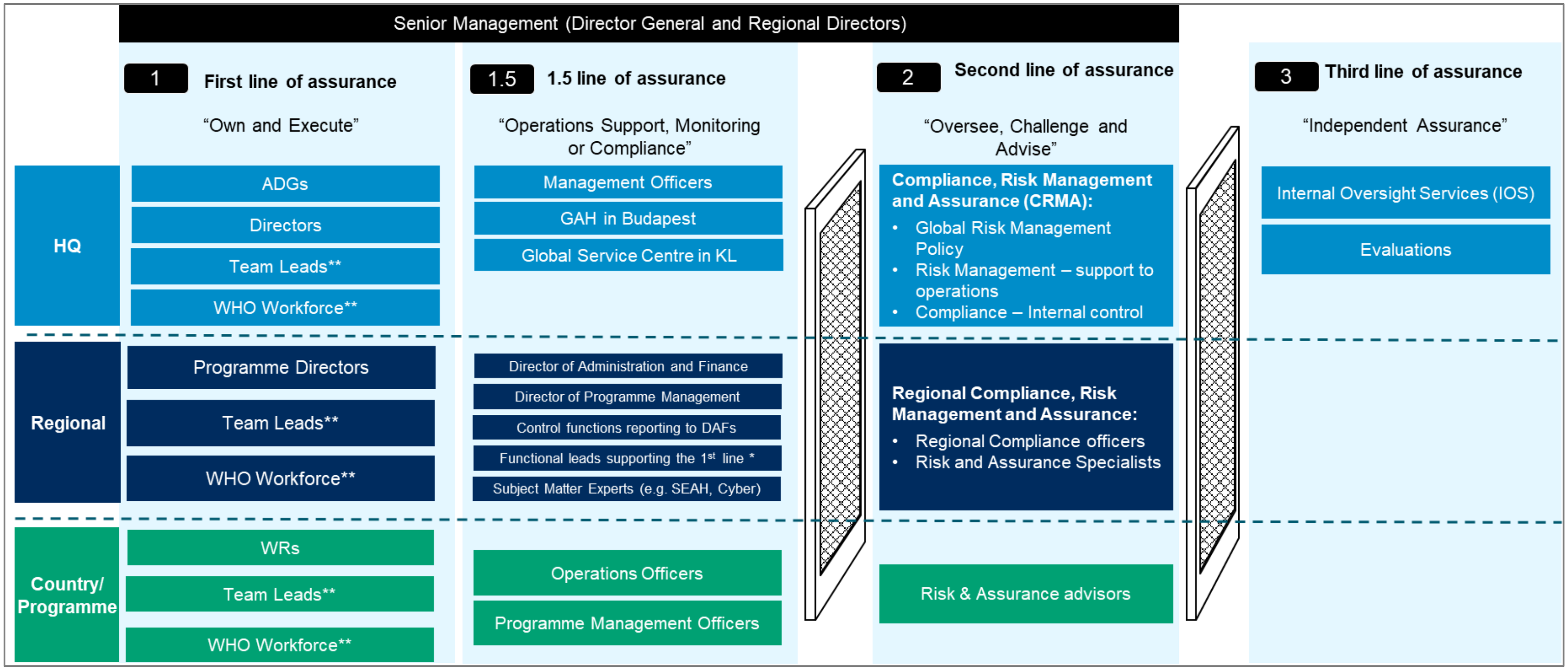

Member States
Executive Board (incl. PBAC)
Global Policy Group (GPG)
(DG and RDs)
Global Risk Management Committee
Regional Risk Management Committees
Local Risk Management Committee
Operations
ADGs, Directors under ADG responsibility, WRs
Operations Support, Monitoring or Compliance (1.5 Line)
e.g. GAH in Budapest, Control functions reporting to DAFs, etc.
Risk Management
Compliance
Internal Control
Internal Oversight Services
Evaluations
External Auditor
Oversight Committees (IEOAC)
Society
Legend
○ 1st Line
● 2nd Line
● 3rd Line
● External Oversight
◌ Risk Committees
Accountability, reporting
Oversight
Delegation, direction, resource allocation, monitoring
Alignment, communication, coordination, cooperation
Coordinating risk identification, assessing, monitoring and reporting

Figure 4: Articulating the future-state Governance Model for WHO using the 3 Lines of Assurance lens

Categorising new and existing roles across the three layers of WHO, using the 3 Lines lens

Further, WHO colleagues might be interested in understanding how their existing roles and responsibilities can be mapped or understood in terms of the 3 Lines of Assurance Model. Illustrated below is an indicative mapping, which although not exhaustive, highlights how key existing roles and potential new roles in terms of the ERM Strategy can be mapped across the 3 Lines, but also where assurance sits across the three levels of the Organization.



	Senior Management (Director General and Regional Directors)			
	1 First line of assurance "Own and Execute"	1.5 1.5 line of assurance "Operations Support, Monitoring or Compliance"	2 Second line of assurance "Oversee, Challenge and Advise"	3 Third line of assurance "Independent Assurance"
HQ	ADGs Directors Team Leads** WHO Workforce**	Management Officers GAH in Budapest Global Service Centre in KL	**Compliance, Risk Management and Assurance (CRMA):** • Global Risk Management Policy • Risk Management – support to operations • Compliance – Internal control	Internal Oversight Services (IOS) Evaluations
Regional	Programme Directors Team Leads** WHO Workforce**	Director of Administration and Finance Director of Programme Management Control functions reporting to DAFs Functional leads supporting the 1st line * Subject Matter Experts (e.g. SEAH, Cyber)	**Regional Compliance, Risk Management and Assurance:** • Regional Compliance officers • Risk and Assurance Specialists	
Country/ Programme	WRs Team Leads** WHO Workforce**	Operations Officers Programme Management Officers	Risk & Assurance advisors	

Figure 5: Categorizing new and existing roles across the three layers of WHO, using the 3 Lines lens[12]

[12] Footnotes to the figure 4:
* Examples of Functional Leads supporting the first line (e.g., Programmatic Divisions, Communicable Diseases, NCDs)
** WHO Workforce and Team Leads are present across Country, Regional and HQ Levels

High-level roles and responsibilities for the functions that together will form the Compliance, Risk Management and Assurance (CRMA) team

Role Description	High Level Responsibilities	Present at HQ	Present in Regions	Present in Countries
Risk and Assurance Team *Support to Operations*	• Provide complementary expertise and support on high-risk areas and key processes (e.g. Prioritized risks, Programme Budget, etc.), implementation and monitoring of effective risk management practices (including fit for purpose design of internal control) in their geographical remit. • Design specific risk management tools for high-risk areas (e.g., Prioritized Risks, namely PSEAH, Fraud and Corruption, etc.), • Provides training and share best practices. • Assist management in performing and documenting risk assessments and operationalizing the risk appetite framework. • Design the process for maintaining risk register(s) and mechanisms for escalating emerging risks and risks exceeding risk acceptability levels. • Promote the use of documented risk-assessment in management decision-making process. • Conduct awareness risk management raising and communication activities with business owners of high-risk areas and key processes. • Provide consolidated analysis and contribute to organizational reporting on risk and assurance activities. Escalate significant risks to the relevant risk management committees.	Y	Y	Y
Compliance Team *Internal Control Testing & Monitoring*	• Provide methodological guidance to maintain an effective internal control framework (e.g., Risk & Control Matrices (RACMs) developed by business owners). • Develop, implement, and maintain risk-based test plans to assess the operating effectiveness of controls using various testing and monitoring techniques (including remote testing, walkthroughs and on-site field visits as required by the level of residual risk). • Contribute to organizational reporting on risk and assurance activities: Report on their work and communicate identified trends using global metrics and reporting tools to guide the decision-making and risk assessment and communicate findings (errors, risks or process inefficiencies) with recommendations and follow-up on corrective actions for remediation. • Escalate significant risks related to detected control failures and delays in the implementation of corrective actions to the Global Risk Management Committee.	Y	Y	
Global ERM Team	• Develop and maintain policies, procedures and tools related to Global risk management, compliance and assurance. • Responsible for alignment, communication, collaboration and coordination among the Compliance, Risk Management and Assurance teams. • Review emerging key corporate risks and coordinates the activities of the Global Risk Management Committee. • Consolidates all activities of the Compliance, Risk Management and Assurance teams (including regions) and report on integrated assurance to Senior Management.	Y		

Table 3: High level responsibilities for each of the reconfigured function within the new (future state) Compliance, Risk Management and Assurance (CRMA) Team

iii. Prioritized Principal Risks

To facilitate the implementation of the risk strategy, in a resource constrained environment, the actions proposed will primarily focus on a subset of Principal Risks which bear the highest level of exposures at country level, thus threatening the Organization's goal of creating impact at country level. This list will be used for prioritization of funding (people, capacity), and development of additional risk and control guidance and tools. A list of Prioritized Principal risks is established based on the following principles and will be updated annually:

- Those risks that affect impact at a country level (i.e., the lowest delivery point).
- Those risks that are inherent to delivery of services, and which carry the most operational risks.
- Those risks that, if they materialize, have a high impact on the following key enablers: technical excellence, people's health and safety, compliance & integrity, as defined in WHO's 2023 Risk appetite statement.

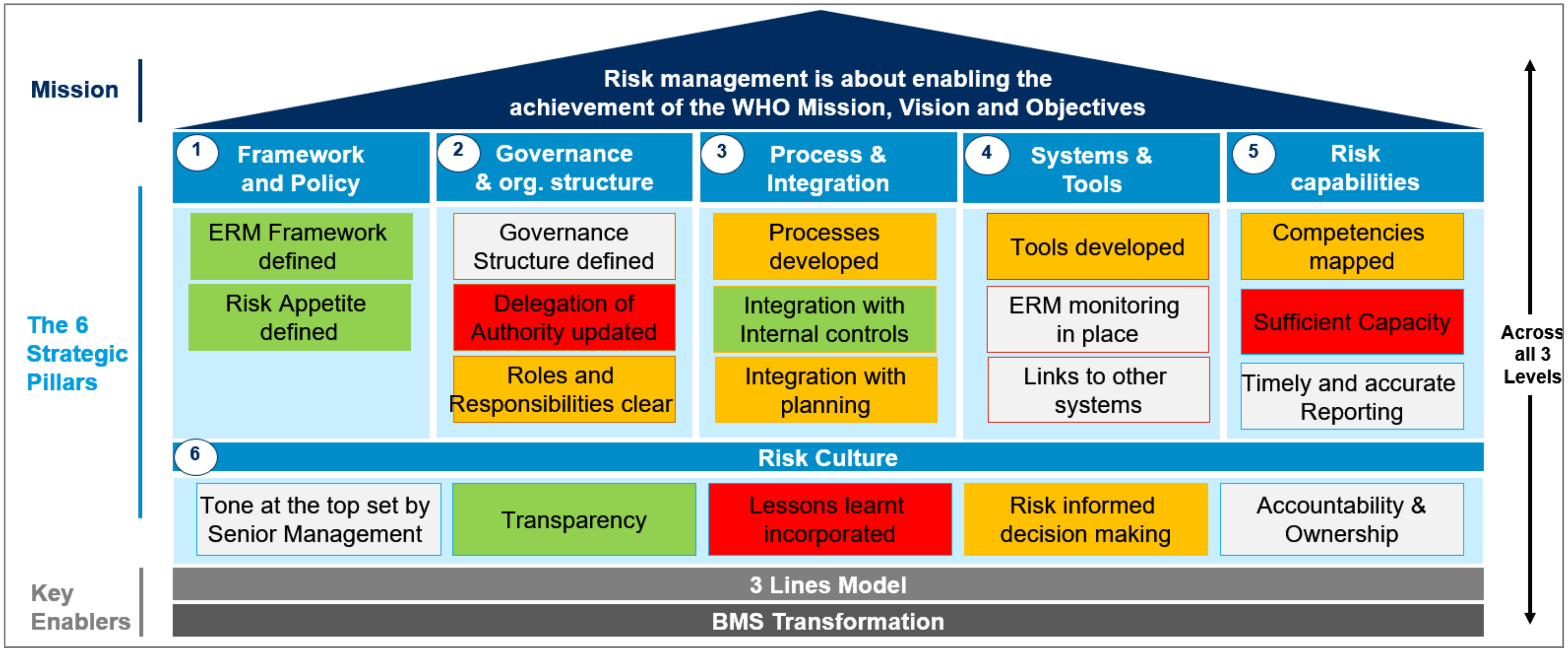
Defined below are the Prioritized Principal Risks for 2023 to 2024, in the context of our current risk management maturity:

Short Risk Name	Link to Principal Risk Register (published May 2023)	Definition
Supply chain	ID 18: Vulnerable Supply Chain Operations	Failure to deliver quality health products timely to address country needs. Increasing costs due to inefficient and siloed operations.
Delivery of Results (M&E)	ID 8: Inability to measure impact	Poor data or unavailability of data in health may affect the ability of the WHO and its partners to identify public health needs, respond to them effectively and demonstrate impact against the triple billion goals.
Security	ID 2: Business Service Disruptions / Security Incidents	Disruption to business continuity, including arising from security and safety incidents, that affect the efficient performance of WHO operations (e.g. by interrupting activities, financial loss, harm to staff, damaged reputation, loss of data).
Fraud & corruption	ID 6: Fraud and Corruption	Due to weak or inappropriate internal controls or vulnerable external business environments fraud and corruption may be committed by staff and non-staff, potentially leading to inability to implement WHO activities in an effective, efficient and economical manner
PSEAH	ID 14: Sexual Exploitation, abuse, and harassment or misconduct	Inability to prevent, detect and manage cases of sexual exploitation, abuse and harassment and other forms of misconduct thereby harming people and affects the reputation of the Organization.
Incoherent communication	ID 5: Misinformation / disinformation and mistrust in science	Risk of inability to manage misinformation and/or disinformation campaigns targeted at science, medicine, WHO and its Member States
Cybersecurity	ID 4: Cybersecurity Breach	Risk of a large 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 proceedings, or damaged reputation.
Quality of publications	ID 12: Quality and Excellence of WHO's Normative work compromised	The technical excellence of WHO's normative and technical work is compromised, negatively affecting WHO's reputation, leadership and the effectiveness of technical support for Member States.

Table 4: Prioritized Principal Risks for the period 2023 to 2024

iv. The Reference Maturity Model for Risk Management in the UN System

Building Resilience within WHO will be guided by the JIU benchmark [13]UN Reference Maturity Model for Risk Management[14] i.e., the 6 Pillars, as summarized in the image below, and further detailed in Annex v below:



Mission

Risk management is about enabling the achievement of the WHO Mission, Vision and Objectives

The 6 Strategic Pillars

1 Framework and Policy
- ERM Framework defined
- Risk Appetite defined

2 Governance & org. structure
- Governance Structure defined
- Delegation of Authority updated
- Roles and Responsibilities clear

3 Process & Integration
- Processes developed
- Integration with Internal controls
- Integration with planning

4 Systems & Tools
- Tools developed
- ERM monitoring in place
- Links to other systems

5 Risk capabilities
- Competencies mapped
- Sufficient Capacity
- Timely and accurate Reporting

6 Risk Culture
- Tone at the top set by Senior Management
- Transparency
- Lessons learnt incorporated
- Risk informed decision making
- Accountability & Ownership

Key Enablers

3 Lines Model

BMS Transformation

Across all 3 Levels

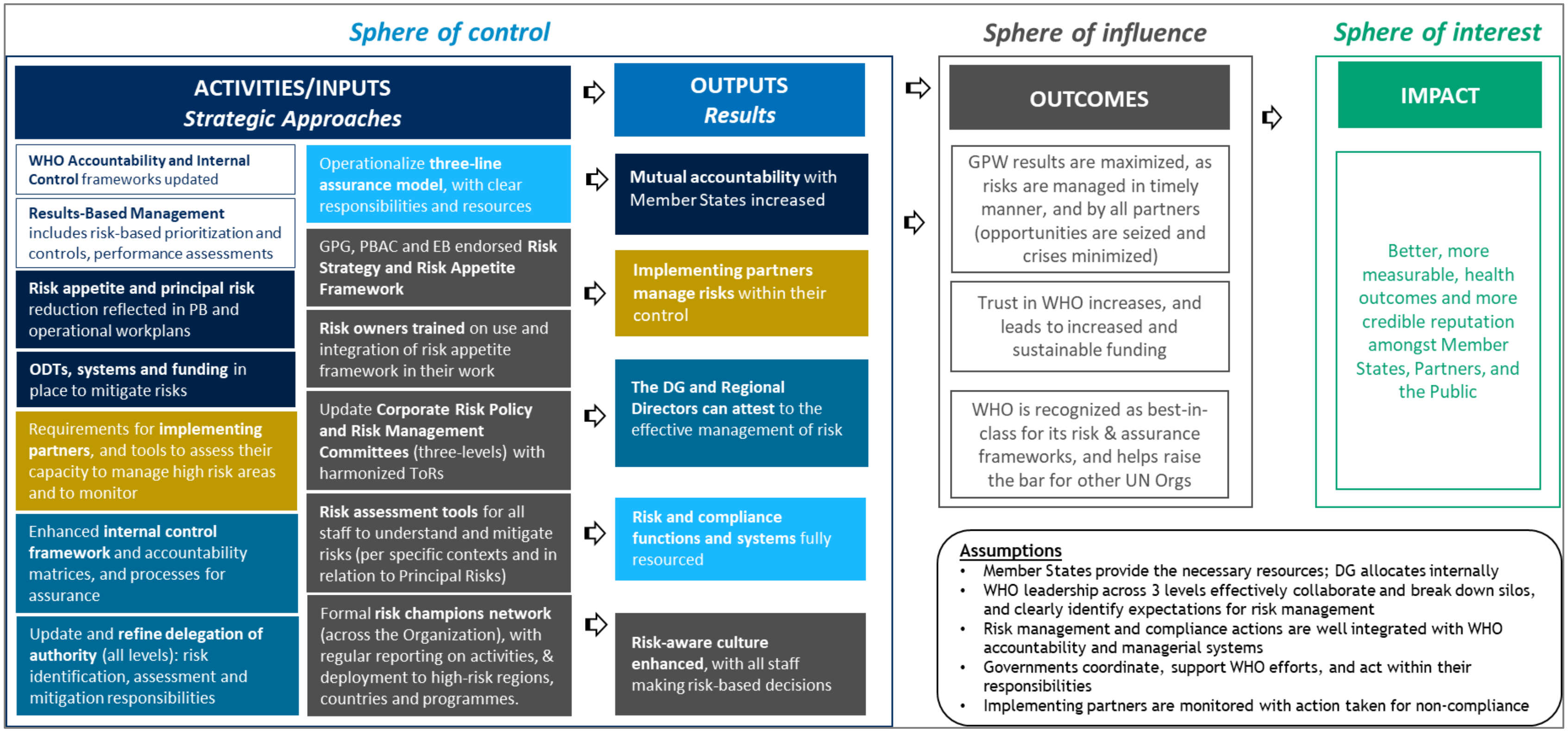
Figure 6: Illustrating how the 6 pillars of the JIU Reference Maturity Model has been translated into a target future state for Risk Management within WHO

[13] https://www.unjiu.org/news/jiurep20205-enterprise-risk-management-approaches-and-uses-united-nations-system-organizations

[14] The High-Level Committee on Management (HLCM) issued the Reference Maturity Model (RMM) for Risk Management in the UN System in September 2019 and is how we have benchmarked our own ERM (CRE) Function, and will function as an action plan for us, as specialists, to mature the ERM function over time.

v. The Theory Of Change supporting the Risk Management Strategy

The Risk Management Strategy is supported by the Theory of Change, linking Activities to Outputs, and then to outcomes, to really achieve impact. Outlined below are the activities, outputs, outcomes, and impact driving our organizational goal: **"An enabling Risk Culture, where Risk Management informs daily decision-making across WHO, in an inclusive, transparent and efficient manner."**



Sphere of control

ACTIVITIES/INPUTS
Strategic Approaches

- **WHO Accountability and Internal Control** frameworks updated
- **Results-Based Management** includes risk-based prioritization and controls, performance assessments
- **Risk appetite and principal risk** reduction reflected in PB and operational workplans
- **ODTs, systems and funding** in place to mitigate risks
- Requirements for **implementing partners**, and tools to assess their capacity to manage high risk areas and to monitor
- Enhanced **internal control framework** and accountability matrices, and processes for assurance
- Update and **refine delegation of authority** (all levels): risk identification, assessment and mitigation responsibilities
- Operationalize **three-line assurance model**, with clear responsibilities and resources
- GPG, PBAC and EB endorsed **Risk Strategy and Risk Appetite Framework**
- **Risk owners trained** on use and integration of risk appetite framework in their work
- Update **Corporate Risk Policy and Risk Management Committees** (three-levels) with harmonized ToRs
- **Risk assessment tools** for all staff to understand and mitigate risks (per specific contexts and in relation to Principal Risks)
- Formal **risk champions network** (across the Organization), with regular reporting on activities, & deployment to high-risk regions, countries and programmes.

OUTPUTS
Results

- **Mutual accountability** with Member States increased
- **Implementing partners manage risks** within their control
- **The DG and Regional Directors can attest** to the effective management of risk
- **Risk and compliance functions and systems** fully resourced
- **Risk-aware culture enhanced**, with all staff making risk-based decisions

Sphere of influence

OUTCOMES

- GPW results are maximized, as risks are managed in timely manner, and by all partners (opportunities are seized and crises minimized)
- Trust in WHO increases, and leads to increased and sustainable funding
- WHO is recognized as best-in-class for its risk & assurance frameworks, and helps raise the bar for other UN Orgs

Sphere of interest

IMPACT

Better, more measurable, health outcomes and more credible reputation amongst Member States, Partners, and the Public

Assumptions

- Member States provide the necessary resources; DG allocates internally
- WHO leadership across 3 levels effectively collaborate and break down silos, and clearly identify expectations for risk management
- Risk management and compliance actions are well integrated with WHO accountability and managerial systems
- Governments coordinate, support WHO efforts, and act within their responsibilities
- Implementing partners are monitored with action taken for non-compliance

Figure 7: Illustrating the inter-related activities or inputs, outputs, outcomes, and impact, in the context of the spheres of control, influence and interest.