

Corporate Risk Management Policy

November 2015

Contents

GLOSSARY	4
1 Introduction: Purpose and objectives	5
1.1 Purpose	5
1.2 Objectives	6
1.2.1 A tool to support decision-making	6
1.2.2 Embedding risk management in operational processes	6
2 Principles	8
3 Key concepts	9
3.1 Risk	9
3.1.1 Describing risks	9
3.1.2 Causes of risk	9
3.1.3 Risk indicators - examples	10
3.1.4 Risk level/"criticality"	10
3.2 Risk register	10
4 Methodology	11
4.1 Risk assessment	11
4.1.1 Identification	11
4.1.2 Prioritization	11
4.2 Risk response	11
4.2.1 Key concepts: risk acceptance, risk response and approval authority	11
4.2.2 Taking action: validation, escalation and implementation of response	14
5 Roles and responsibilities	15
6 Monitoring	16
6.1 An iterative monitoring process	16
6.2 Annual reports	17
7 WHO associated entities and hosted partnerships	17
8 Strengthening risk culture	17
8.1 Communication	18
8.2 Training	18
8.3 Review of this policy	18

Please contact the Office of Compliance, Risk Management and Ethics should you have any questions.

Annexes:

Annex 1 – Risk Register Template

Annex 2 – WHO Risk Framework (EB133/10)

WHO shall have the lowest tolerance for risks related to compliance (with administrative, financial and other rules, regulations, policies and procedures). Its appetite¹ for strategic, programmatic and operational risks shall be higher in order to meet the challenges faced in public health worldwide with the mix of caution, agility and innovation required to manage risk or exploit opportunities as appropriate. This implies that while sustaining its operations and meeting legal obligations shall be the highest priority for the Secretariat, WHO will demonstrate an informed risk taking readiness to promote technical excellence.

¹ Risk appetite is defined as the amount of risk an organization is willing to take on in pursuit of its objectives, based on risk criticality and proportionality (i.e. effort invested in risk treatment must be proportional to criticality and expected benefit).

GLOSSARY

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.

Risk is a potential event or occurrence beyond the control of the responsible Budget Centre, which could affect the achievement of the Organization's stated results. It is an expression of the likelihood that such a potential event or occurrence may happen and of the impact it may have.

Impact is the consequence of a risk event materializing

Probability is the likelihood that a risk will occur (per year)

Risk criticality is a function of risk impact and probability (impact * probability)

Risk appetite is the amount of risk WHO as an Organization is willing to take on in pursuit of its mission and objectives, based on risk criticality and proportionality (i.e. effort invested in risk treatment must be proportional to criticality and expected benefit). It varies for different types of risk.

Risk acceptance is the amount of risk that a Budget Centre is willing to take at the individual risk level, within the risk appetite of the Organization. Risk acceptance thresholds are determined for the most critical risks for which action is required.

Risk response includes the decisions made to bring the level of criticality of a given risk within the risk acceptance level. The Organization can make the decision to respond to a risk by either tolerating it, treating it (mitigating, transferring, or terminating), or exploiting it.

Approval authority is the organizational entity with the level of delegated authority required to make a decision on the risk response required for a given risk

Risk Register is a repository or risk log of identified risks by Budget Centre/Country Office, which includes priority ratings, escalation level and risk response strategy

This policy is based on the framework presented to WHO governing bodies in 2013². Risk is not a new concept in WHO, and has been practiced notably with the introduction of results-based management and of the Programme Budget (PB) since 2002-2003, the Medium Term Strategic Plan (MTSP) 2008-2013, the 2006 accountability framework and its 2015 revision³, and the consideration of business continuity plans in the management and administration of Budget Centres (BCs). There has however thus far not been a systematic corporate risk management process that goes beyond the risks connected to PB outputs to encompass all aspects of WHO operations. The Office of Compliance, Risk Management and Ethics (CRE) was established with a clear mandate to develop such a mechanism. This policy builds upon and integrates WHO's existing risk management practices into a consistent corporate policy. It also leverages on leading current risk practices in other organizations, particularly within the UN system.

1 Introduction: Purpose and objectives

Risks arise out of uncertainty in all aspects of operations and management: they are a matter of fact in all spheres of human activity. While some risks must be avoided, others may need to be taken in order to effect change. In some cases, not taking a risk may even be the highest risk. To enable WHO to make forward-looking rather than reactive decisions, this corporate risk management policy provides a mechanism to identify and differentiate between these very different types of risk and to better respond to change by addressing threats and embracing opportunities, while avoiding underestimating risk or overreacting. Accordingly, the intent is not to avoid all risks, but to ensure that WHO understands the risks that are inherent to its operations and chooses the appropriate strategy to manage them.

1.1 Purpose

The purpose of this policy is to establish a robust risk management system that supports decision making when setting objectives, prioritizing strategic alternatives, selecting and managing the appropriate course of action, and evaluating results. This policy also serves to improve the quality of management and to calibrate WHO internal controls in the context of continuous improvement of operational processes, instructions, guidance, tools, and management information systems.

This policy is rooted in a systematic and consistent approach to risk management across WHO, fostering a culture that encourages open dialog about risk, based on a common language that articulates how staff are expected to approach risk, and strike an adequate balance between treating, tolerating and exploiting risk. To this end, this policy outlines a structured and transparent process that will ensure a coherent and complete risk reporting to inform decision-making. The premise is (i) to build a regular, systematic and iterative process that includes all Budget Centres, that is (ii) approved and supported by senior management in order (iii) to inform decision making adequately. Consequently, this policy:

- Outlines the objectives of WHO's risk management process;
- States the principles of WHO risk management;
- Provides common definitions across the Organization;
- Establishes a clear, coherent and inclusive methodological approach designed to support decision-making, composed of a bottom up phase of risk identification/assessment/proposed response, and a top down phase to validate risks and determine a risk response;
- Defines roles and responsibilities;
- Spells out monitoring and reporting requirements; and
- Lays out an approach to communication and training.

² EB 133/10 "Corporate risk register – organization-wide management in WHO"

³ The identification of risks and assumptions is a key element of results based management.

1.2 Objectives

The key high level objectives of WHO's risk management process are twofold:

- Inform effective decision-making to improve delivery of results; and
- Embed risk management in operational processes: in the results-based management cycle (planning, performance assessment, budgeting), and the accountability and internal control frameworks.

1.2.1 A tool to support decision-making

The ultimate aim of risk management is to inform and support more effective decision-making. To this end, this policy has been drafted to:

- Introduce a systematic and planned approach to risks
- Determine accountability for risk management
- Clarify governance in matters of risk management whereby:
 - Budget Centre Heads
 - identify and assess the risks they see in their routine operations, propose ways to respond to them and identify the authority level to which risks beyond their responsibility need escalating on a subjective basis;
 - manage risks related to their activities by implementing the approved risk response strategy;
 - update the risk register on a regular basis.
 - Approval authorities define responses to risk and make decisions on risks based on their criticality and the "proportionality" principle (i.e. the effort invested to respond to a risk must be in proportion to its criticality and to expected benefits);
 - CRE supports entities throughout the risk management processes, oversees the appropriate application of the risk policy, monitors the risk register, escalates systematically the most critical risks for decision on a risk response, monitors the implementation of mitigation plans and reports on the most critical corporate risks to the DG and WHO governing bodies.
 - All staff members support the identification and management of risks, in particular the risks that affect their direct activities and responsibilities. Staff members are invited to inform CRE of any additional risks they identify in their daily operations, or to supplement the data provided by their Budget Centre in the risk register.
- Provide management with appropriate information about risks and ensure an effective reporting process is in place to support decision-making

1.2.2 Embedding risk management in operational processes

To ensure that risk enables operational decision-making, risk management must be fully integrated into operations. WHO's risk management mechanism is therefore embedded into the results-based management process (strategic and operational planning, budgeting and performance assessment) and the accountability and internal control frameworks.

1.2.2.1 Results-based management: planning, budgeting and performance monitoring

Risk management is closely embedded in WHO's results-based management cycle. Both processes feed into and build on each other in order to ensure that risks are addressed consistently at the appropriate level and mitigation strategies are implemented to respond to risks. To this end, the risk management process has been designed to identify risks at the PB output level in order to provide inputs into the planning cycle.

Risks of an operational or administrative nature also feed back into the budgeting cycle to ensure that decisions regarding risk responses can be implemented in upcoming budget exercises. Implementation of risk response measures is integrated into Budget Centres' workplans as appropriate, in order to identify and plan for the resources that may be required to implement a risk response action.

CRE's monitoring of the risk register is timed in order to provide inputs to the mid-term review (MTR) of the implementation of the PB in the assessment of progress towards the achievement of outputs by BCs. It serves to update the status of the risks associated with PB outputs with particular attention to the expected results that are judged "not on track", and any decisions to be made on required re-programming. The risk monitoring process also provides inputs to the PB performance assessment (PBPA) undertaken at the end of the biennium to document the actual achievements of BCs towards expected results.

1.2.2.2 Accountability, and the internal control framework

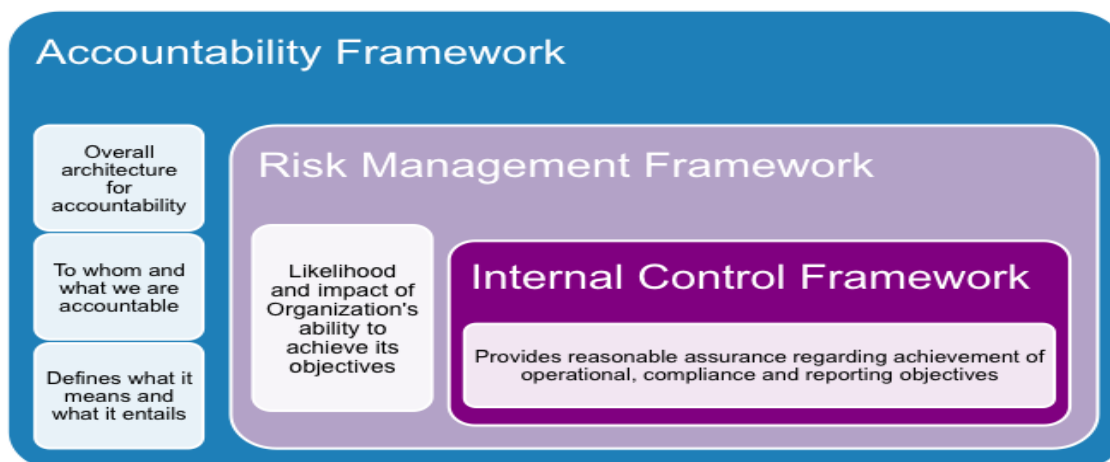
WHO's Accountability Framework provides the conceptual structure that defines from whom authority flows, to whom, for what purpose, and how it is carried out. It underlines WHO's commitment to the shared values and culture of accountability and transparency. This policy is a tool to enable the Organization to internalize risk management as one of the pillars to improve accountability by facilitating cultural and behavioural change towards owning and being responsible for the risks involved in working to achieve results.

The accountability framework operates in tandem with risk management, which identifies and manages the likelihood or impact of a risk, in order to improve the probability of achieving the Organization's objectives; and the Internal Control Framework, which provides the critical systems and structures necessary to ensure that WHO's operational, compliance, and reporting objectives are met.

As illustrated in Figure 1, these elements, together, are critical to accomplishing established organizational objectives and goals as expressed in the WHO General Programme of Work (GPW), and the PB with enhanced accountability and greater transparency⁴.

⁴ Risk management can be seen as the *raison d'être* or the "engine" behind the internal control system: while a risk can generate the need to establish one or more control means, no control would be necessary without risks. If risk management is a decision-making supporting tool, internal control can be seen as a steering tool. Accordingly, risk management and the internal control framework are part of ultimately the same process, and the activities and documentation elaborated within the risk management and internal control areas constitute a unique set having the same purpose. In concrete terms, this entails close links between the risk management process and the internal control framework, ensuring that both processes simultaneously inform and feedback on each other.

Figure 1: WHO's accountability framework



Controls are established to address risks, and the risk management and internal control frameworks provide feedback to each other. Internal control checklists are updated based on information provided by the risk register to provide guidance to Budget Centre managers.

Identification of and response to risk is part of WHO's accountability framework and the responsibility of all BCs. Risks are identified in relation to organizational objectives, as defined through strategic planning process, programme planning, office plan development, and any ad hoc objective setting exercise (i.e. emergency response situations).

Risk management is integrated into staff performance management. While managers are not and will not be held accountable to prevent all risks, they are responsible for identifying, assessing risk and implementing effective risk management strategies in the areas under their responsibility. The response strategies decided upon to address any given risk are expected to be fully implemented and become an integral component of departmental/country offices workplans.

2 Principles

WHO's risk management approach is guided by the following principles:

- Integration into relevant corporate processes: risk management is not a stand-alone activity but a part of the responsibilities of WHO management as well as of relevant operational processes, specifically strategic planning, programme development, budgeting, work planning and internal control to ensure consistent consideration of risk in all decision making and resource allocation.
- Transparent and inclusive process: risks are inherent to all operations and decisions. All stakeholders and decision makers must be involved to identify, assess, validate and manage risks in a two tiered process from the bottom up in a first instance, and then from the top down.
- Systematic and structured process: risk management must be a systematic iterative process that remains responsive to change, continuously sensing and reporting changes related to both external and internal events that shape the context of WHO operations. Risk monitoring and review must report the dynamics of risk as new risks emerge, while some change, and others disappear.
- Anticipating and managing risk: risks to the achievement of an expected result and measures to mitigate them must be included in strategy development and planning (i.e. the PB).

- Recognizing opportunities: opportunities arising from the normal course of work to deliver results need recognition and related emerging risks are assessed in their own right.
- Timely decision-making: avoiding or delaying making a decision amounts to making a decision to maintain status quo. This may only exacerbate existing problems. This policy establishes an affirmative process to manage risk.
- Decision-making at the right level of authority: decisions on risk must be made at the level of delegated authority. Where the authority needed to address a risk has not been given, the risk must be escalated to a higher management level.
- Two-tiered risk analysis, individually and concurrently as they relate to the same overall objective: each risk must be assessed in its own right as well as in combination with other risks relating to the same objective to ensure the best strategic response is selected. Cross cutting risks are identified and escalated to the level of authority where they can be addressed.

3 Key concepts

3.1 Risk

Risk is a potential event or occurrence beyond the control of the responsible Budget Centre, which could affect the achievement of the Organization's stated results. It is an expression of the likelihood that such a potential event or occurrence may happen and its impact. If it materializes, the event may have an impact on the achievement of the Organization's political, strategic and operational objectives.

3.1.1 Describing risks

A risk must be clearly described for WHO to assess adequately its exposure and develop an appropriate response. A risk description must:

- Relate to the objective(s) whose achievement is at risk – one or more key objectives may be affected. The best way to address a risk may differ for different objectives and the same risk may impact differently on different objectives; and
- State both the cause and effect – not simply stating the opposite of the objective.

3.1.2 Causes of risk

Risks can originate from either external or internal causes:

- External causes relate to outside events or circumstances usually beyond WHO's control. They can include threats such as emergency situations or humanitarian crisis or opportunities such as sudden changes in governmental policy, or the emergence of new scientific evidence. The effects of such risks can be managed for instance through contingency plans;
- Internal causes can be linked to organizational strategy, programme management capacities, human resources issues or the effectiveness of internal controls. Such risks can pose threats that WHO must mitigate or opportunities which WHO needs to exploit to further the achievement of results.

3.1.3 Risk indicators - examples

- Risks whose likelihood and financial impact are high,
- Complete lack of reliability of financial statements;
- Reputational impact potentially having an echo outside WHO;
- Risks whose realization might induce direct harm to one or more people following a decision, activity, action or lack of decision/action of WHO;
- Operations interruption or delay, related to an activity perceived as vital for more than a specific time duration;
- Decision or activity derived from a decision taken by WHO potentially to be cancelled due to a lack of compliance with rules and regulations;
- Exception: low probability risks whose impact is disproportioned.

3.1.4 Risk level/"criticality"

The risk level is defined by its characteristics IMPACT* PROBABILITY, also referred to as "criticality" of the risk. A risk may have a major impact when it occurs although the probability that it may happen can be very remote. Conversely, a risk with a minor impact may turn into a major risk for the Organization if it occurs repeatedly or is not managed. Therefore, when discussing the criticality of a risk, there should be clarity about the impact and probability of each risk on the relevant objective(s).

3.1.4.1 Risk Impact

Impact is the consequence of a risk event materializing. Impact categories can be distinguished based on the nature of the risk:

- External impact: on WHO, based on exogenous factors or related to action/lack of action of an entity;
- Financial impact: unforeseen/unbudgeted costs, loss of asset value, reliability of financial statements;
- Safety impact: security implications, physical integrity of people, psychological integrity of staff;
- Impact related to operations delivery: number and importance of affected services, type and duration of delays, number of affected projects;
- Compliance and legal impact: violations related to the legal framework or other compliance issues;
- Reputational impact: Echo in media, reputation of people and institutions, stakeholders' perception, trust, staff motivation.

3.1.4.2 Risk Probability

Probability is defined as the likelihood of a risk event occurring (per year). Some types of risks, in particular financial ones, can be expressed relatively precisely in terms of probability and impact. Often, for example for reputational risks, exactitude is not possible, and a measure of judgment is required.

3.2 Risk register

The Risk Register is a repository or risk log of identified risks by Budget Centres (Headquarters or regional office departments and Country Offices). It has been designed to match the provisions of the EB 133/10 document. It provides for a definition of risks including by PB outputs, and enables Budget Centres to rank risks in light of their impact and probability (See Annex 1).

4 Methodology

This policy proposes a two-tiered approach based on (i) a bottom-up risk assessment process (carried out by Budget Centres), coupled with (ii) a mechanism to escalate risks to the adequate approval authority (with the right delegation of authority) to decide on the risk response from the top down.

4.1 Risk assessment

Risk assessment is understood as the systematic process of identifying and prioritizing (i.e. "ranking") risks.

4.1.1 Identification

The identification of risks is conducted from the bottom up, whereby Budget Centres are required to formulate and describe the risks they see in their daily operations on an intuitive basis. As outlined in WHO's risk framework document EB133/10, potential risks are structured in six categories (financial, political/governance, reputational, staff/systems and structures, strategic and technical/public health), and are documented in the risk register (Annex 1).

4.1.2 Prioritization

As part of the risk assessment, Budget Centres also prioritize, or rate the risk level (or criticality) of identified risks based on the combination between their impact and probability scores. They allocate an impact and probability score ranging from 1 to 5 to each risk. Figure 2 shows how the risk criticality level is calculated. It is based on probability and impact scores and ranges from 1 (low) to 4 (severe). The criticality level of low probability risks that have a high impact (i.e. 4 or 5) is rated as moderate to significant.

Figure 2: Risk scores

			Impact				
			Very low	Low	Medium	High	Very high
			1	2	3	4	5
Probability	Very low	1	1	2	3	4	5
	Low	2	2	4	6	8	10
	Medium	3	3	6	9	12	15
	High	4	4	8	12	16	20
	Very high	5	5	10	15	20	25
			1	2	3	4	
			Low	Moderate	Significant	Severe	
			Criticality				

The criticality level determines the level to which decision on a response to address a risk needs to be escalated. Risks which are scored high (i.e. severe or significant criticality level) are systematically escalated by CRE to the approval authority retained for approval of a risk response (see Figure 4 below).

4.2 Risk response

4.2.1 Key concepts: risk acceptance, risk response and approval authority

Budget Centres Heads are requested to complete the risk register by proposing a risk response to address the risks they have identified. The process of defining a risk response is twofold: it requires (i) determining a risk acceptance level, (ii) selecting the appropriate action and (iii) selecting an escalation level with the authority to act on a risk.

4.2.1.1 Risk acceptance

Risk acceptance levels are determined for the most severe and significant risks of the Organization that require escalation and action (See Figure 4 below). Determining the acceptability of an individual risk in order to decide on an adequate risk response requires considering the following two elements simultaneously:

- The hierarchical level having to approve the risk response strategy of a risk (approval authority): based upon its criticality. Although, generally, an effort should be done to limit the criticality of any risk, the acceptability of a risk with or without risk mitigation measures is determined on a case by case basis by the BC, subject to validation by the next level of authority.
- The effort invested in treating a risk: must be proportioned to its criticality and to expected benefits (proportionality principle)

4.2.1.2 Risk response actions

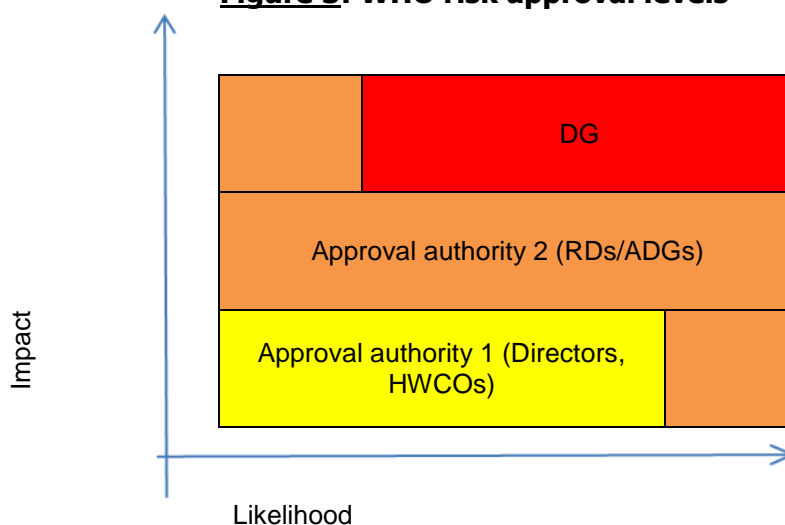
Defining a risk response is selecting the action that will bring the criticality level of a risk into line with its acceptance level. Risk responses can include:

- Tolerate: accept the risk if the opportunities outweigh the threat and the existing controls are adequate to contain the risk. This option may be applied when exposure is tolerable, control is impossible or the cost of control exceeds potential benefit. It may be supplemented by contingency planning for handling the potential impact. The question of whether a particular risk can be tolerated is a key management decision.
- Treat by either:
 - Mitigating: reducing the risk's impact, probability and/or strengthen existing controls to develop new controls to reduce risk to acceptable levels.
 - Transferring: sharing risk with a third party. Transferring risk works well with financial risk or risks to assets, by for example taking conventional insurance or engaging a third party to bear the risk. The relationship with the third party needs to be carefully managed. This option is not possible for reputational risks.
 - Terminating: avoiding the risk either by not undertaking associated activities or changing the scope of related activities, the procurement process, supplier, or activity sequencing.
- Exploit: seek to exploit the event/circumstance(s) that can generate a risk to the benefit of WHO and its objectives or the circumstances of which also present opportunities which could add value to the Secretariat.

4.2.1.3 Systematic approval authority level

There are three approval authority levels in WHO that carry the responsibility to make decisions regarding risk (Figure 3):

Figure 3: WHO risk approval levels



The criticality level determines the action required to manage a risk as shown in Figure 4:

Figure 4: determination of risk acceptance and response

Criticality		Acceptance	Action required to respond to risk	Approval authority role	CRE role
Severe	4	Requires appropriate action to manage risk	The risk is unacceptable and is escalated to the highest Approval authority, i.e. reported to the DG, and monitored by CRE. An action plan to implement response action is mandatory,	DG makes decision on mitigation strategy and requests an action plan, prepared by the risk owner to implement response action.	CRE oversees implementation of action plan. CRE monitors the evolution of the risk.
Significant	3	Requires appropriate action to manage risk	The risk is undesirable. It is escalated to the approval authority and reported to the ADGs and/or RDs as applicable.	ADGs at HQ and RDs in the regional offices make a decision on the response action to address risk.	CRE monitors the implementation of the response action.
Moderate	2	Requires action but may be tolerated. The risk must be monitored continuously	The risk requires a response and is escalated to the approval authority as appropriate. The responsible BC may accept the risk in agreement with the approval authority where applicable.	Where applicable the ADGs at HQ and RDs in the regional offices may decide to tolerate the risk, or decide on response action.	CRE monitors risk through normal annual exercise
Low	1	Can be tolerated and can be managed through appropriate controls	The responsible BC keeps the risk register up-to-date to follow up on the risk	The BC head monitors the risk in the next iterations of the risk register.	CRE carries out annual monitoring exercise

Some risks may present specificities which call for de-linking criticality/acceptance and approval authority levels. Such specific risks, typically because they are beyond the control of a BC, are escalated to the relevant approval authority (see below "specific escalation to other approval level").

4.2.1.4 Specific escalation to other approval level

When proposing a risk response, BCs are also required, where applicable, to indicate in the risk register the level of management ("approval" authority) to which a risk presumably needs to be escalated to be addressed effectively⁵. Risks should be escalated if BCs consider that the risk meets one or more of the following criteria:

- Addressing the risk requires decisions/actions that exceed the authority levels of the BC Head;
- The risk cuts across or may impact multiple BCs and/or addressing the risks requires action by multiple BCs; or
- Addressing the risk requires corporate changes (e.g. changes to corporate policies).

Where BCs have indicated that a risk requires a response sanctioned by a higher level approval authority, and this has been validated as per the process described below ("validation"), it is understood that their assessment is that the named approval authority is responsible for determining an adequate risk response.

4.2.2 Taking action: validation, escalation and implementation of response

For a risk response action to be implemented effectively, it is critical that the decision on the risk response be made and validated at the right level of authority. This policy therefore provides a validation mechanism coupled with a systematic escalation process for the most critical risks.

4.2.2.1 Validation

All risks identified and prioritized by the BCs, as well as the proposed responses and approval authority level, are validated by the next hierarchical level (RDs/ADGs). This validation stage is designed to provide a top-down review of the risks identified by the BCs, and, specifically, to:

- Quality review the risks identified, amend as appropriate to reformulate and/or add other risks;
- Confirm the level of risk ("criticality") rated by the BC;
- Confirm the risk owner (person responsible to manage the risk, and take required actions);
- Validate the escalation level in line with delegation of authority – or "de-escalate" the risk if it considers that the risk does not warrant escalation;
- Review and finalize risk acceptance level (see below); and
- Review and finalize a risk response in consultation with the BC.

CRE notes and monitors decisions to change an approval authority or de-escalate a risk in the risk register where BCs previously named a different approval authority. Where the approval authority confirms that they are the right level to address a given risk, the decision on the appropriate risk response measure is the responsibility of the relevant approval authority. The implementation of the risk response is the responsibility of the relevant BC(s) once the risk response has been communicated to them.

4.2.2.2 Systematic escalation of the most critical risks

As validation takes place, CRE simultaneously reports severe and significant risks systematically to the relevant approval authority. As shown in Figure 4:

- Severe risks are considered as requiring action and are systematically reported by CRE to the DG. The DG makes the final decision to approve or amend the response action proposed to address a

⁵ EB 133/10, paragraph 15.

severe risk. The DG consults with approval level 2 as appropriate. CRE monitors the implementation of related action plans to implement risk responses in conjunction with the responsible BCs.

- Significant risks and/or the risks identified by BCs as requiring a higher approval authority level are escalated to the approval authority level 2 (i.e. at HQ, ADGs, and in the regions, the RDs) who monitor progress on action taken. CRE monitors implementation of the risk response.
- Low and moderate risks, after validation by the appropriate hierarchical level, are either escalated to a higher level if they require a higher approval authority, or are managed by the respective BCs that report progress on actions to address the risks in the risk register.

The risks that escalate beyond acceptable limits despite the actions of the responsible BCs are systematically included in the next iteration of the risk register as significant or severe risks for continuous monitoring by CRE.

4.2.2.3 Implementation of risk responses

In all cases, the monitoring of the risk register, updated on an annual basis, serves to record progress on actions taken to address the risks. The risk response is integrated into corporate planning documents and workplans for full implementation.

Implementing a risk response may require preparing an action plan. This is a requirement for WHO's most critical risks, and monitored by CRE. Action plans can either be of a preventive or reactive nature. The main objective of an action plan is to prepare and document specific management responses (actions), with timelines and indicators to monitor the risks and assign owners to the risks that are considered of unacceptable level. The risk owner is then responsible for the management of all activities to implement the risk response.

5 Roles and responsibilities

Roles and responsibilities in relation to WHO's risk management process are specified in Figure 5 below:

Figure 5: Roles and responsibilities

Responsible entity	Roles and responsibilities
CRE	<ul style="list-style-type: none"> • Ensure that the overall risk management framework is effective and relevant and applied organization-wide • Monitor quality of risk assessment • Escalate the most critical risks for action: (i) report severe risks (criticality level 4) to the DG for decision on an action plan and monitors implementation of mitigation strategy; (ii) report significant risks (Criticality level 3) to the ADG and / or RD concerned as applicable • Monitor implementation of the action plans designed to mitigate severe and significant risks. • Analyse risk data, identifying trends and patterns and presenting information to the DG • Report annually to the Executive Board
Approval authority 1: Budget Centre Heads (departmental Directors at Headquarters or in the	<p>Budget Centre Heads are responsible for the overall management of the risks that relate to their respective operations in relation to programmes and office management. Specifically, they:</p> <ul style="list-style-type: none"> • Identify the risks entailed in their operations (programmatic or office related) in consultation with their staff to ensure a broad ranging perspective;

regional offices, Heads of WHO Country Offices, Heads of WHO entities)	<ul style="list-style-type: none"> • Rate risk level i.e. "criticality", on a subjective basis; • Propose the acceptance level of risks; • Propose a response to address individual risks; • Escalate to the right approval authority level (entity which has the delegation of authority required to take the responsibility to respond to a risk) individual risks that (i) the budget centre does not have the capacity or authority to manage, (ii) require a coordinated or organization-wide response or (iii) would affect WHO as a whole; • Define risk management responsibilities within their office and ensure controls are in place and functioning to manage risks within defined acceptance levels; • Ensure that the risks identified are mapped against the Programme Budget; • Ensure that risks responses are aligned with risk acceptance levels; • Implement risk responses and integrate them into their workplans; • Continuously monitor their exposure to risk and update the risk register, when the status of risks changes or new risks develops.
Approval authority 2: RDs and ADGs	<ul style="list-style-type: none"> • Ensure that the risk management process is conducted in their area of authority, and support Budget Centres in the process • Review, validate and amend as appropriate the risks and related responses that are submitted to them as part of the validation stage • Review the risks escalated to them by the Budget Centre Heads either because (i) they require decisions/actions exceeding the Budget Centre authority level, or (ii) they cut across multiple Budget Centres or require action by multiple Budget Centres, or (iii) they require corporate changes. • Review significant risks (criticality level 3) reported by CRE and design an action plan to address them • Provide support to the DG in addressing severe risks (Criticality level 4) • Ensure that the actions decided to mitigate risks are implemented • Ensure that risks that cannot be adequately managed at their level of authority are escalated to the DG
Approval authority 3: DG	<ul style="list-style-type: none"> • Review the risks escalated either because (i) they require decisions/actions exceeding the Budget Centre authority level, or (ii) they cut across multiple Budget Centres or require action by multiple Budget Centres, or (iii) they require corporate changes. • Review severe risks (criticality level 4) reported by CRE and design an action plan to address them • Support the risk management process
All staff	Support the identification and management of risks, in particular the risks that affect the activities and responsibilities of the staff member. Staff members are invited to report or supplement the information provided by their Budget Centre directly to CRE.

6 Monitoring

6.1 An iterative monitoring process

CRE analyses risks and reports regularly to senior management. The annual risk register exercise is timed to provide inputs to both the Mid Term Review of the PB (MTR) and the PB Performance Assessment (PBPA) which report on achievement of results with consideration of underlying risks and assumptions. The iterative on-going risk monitoring process is designed to capture changes in risk levels, either due to associated factors or mitigating measures taken, on an annual basis:

- CRE oversees the development and implementation of action plans to respond to severe risks.

- CRE monitors the implementation of the response strategies developed to address significant organizational risks.
- For low and moderate risks, CRE analyses progress in the implementation of risk responses through the risk register updates.

All Budget Centres are asked to update the risk register on an annual basis, to reflect⁶:

- Any change in the assessment of the risk (i.e. risk level or criticality) after application of the risk response;
- Any suggested changes to the risk response;
- Progress made in the implementation of the risk treatment plan.

To guide its work and monitor risks effectively, key performance indicators provide the background to address the following:

- Action plans follow-up I = % action plans meeting deadlines or for which a new planning is validated before deadline expires
- Action plans follow-up II = % action plans whose planning has been revised twice or more
- Risk evolution = % existing risks whose evolution indicates a stable or decreasing criticality level
- Risk policy application rate = % risks documented and managed according to policy

6.2 Annual reports

CRE will produce an annual risk report outlining:

- The status of the most critical risks for the Organization and emerging risk patterns together with actions to reduce them;
- The repartition of the most critical risks by Major Office;
- Major risks by Major Office;
- Major risks by PB outputs; and
- The Organization's response to its most critical risks.

A detailed annual report presents the preliminary results of the status of the risk management exercise (i.e. an analysis of the risks catalogued by Budget Centre, as well as an assessment of cross cutting risks), overall compliance with the risk management policy, the initial lessons learned from the process and a way forward to strengthen the risk management process. CRE's annual report is submitted to the DG and reported to WHO's governing bodies through the Executive Board annually.

7 WHO associated entities and hosted partnerships

WHO associated entities and hosted partnerships whose financial statements are consolidated into WHO's financial statements communicate their main risks to CRE. Their main risks are included in CRE's annual report.

8 Strengthening risk culture

To foster a culture that encourages dialog about risks and an effective response to risk, both strategically and in daily operations, high importance is given to:

- Involving all staff, according to their role and competences, in risk management activities

⁶ EB 133/10. Paragraph 18. z

- Ensuring all entities speak the same language and use the same tools to discuss risk management
- Reinforcing training and awareness raising.

8.1 Communication

To this end, communication will aim to ensure that:

- The key components of this policy and the risk framework are communicated effectively to staff across the Organization.
- Internal reviews of the policy and framework are adequate.
- The information captured in the risk register is available to relevant staff at all times
- The risk register is completed by BCs in consultation with their staff

8.2 Training

Recognizing that risk awareness and training are vital elements for successful implementation of risk management, information activities are incorporated in WHO training programmes:

- Strengthening the capacity of the staff involved in the risk management process to interpret and implement the risk management policy, in order to contribute effectively to the corporate risk management process
- Enhancing staff awareness of the consequences of risks within their responsibility. Identification and management of risk is included in PMDS objectives.

8.3 Review of this policy

CRE will undertake a review and update of the risk management policy to draw from practice and lessons learned, as well as other relevant reviews and findings, after three years following its entry into force.