INTERNATIONAL MARITIME ORGANIZATION

E

COUNCIL
113th session
Agenda item 3

C 113/3/3
6 October 2014
Original: ENGLISH

STRATEGY, PLANNING AND REFORM

Risk Management Framework

Note by the Secretary-General

SUMMARY

Executive summary:	This document contains the updated Risk Management Framework following the Council's request for the Secretary-General to review the Risk Management Framework and identify any changes necessary to apply the Risk Management Framework to the Secretariat's Business Plan only
Strategic direction:	4
High-level action:	4.0.4
Planned output:	4.0.4.1
Action to be taken:	Paragraph 7
Related documents:	C 112/D; C110/WP.3 and C 110/3/5

Introduction

1 At its 112th session, the Council reconsidered its decision to apply the Risk Management Framework to the Organization's Strategic Plan and High-level Action Plan and consequently, the Council decided that the Risk Management Framework should only be applied to the Secretariat's Business Plan (C 112/D, paragraph 3.3).

Risk Management Framework

2 The current Risk Management Framework was adopted by the Council at its 110th session. At its 112th session in June 2014, the Council requested the Secretary-General to review the Risk Management Framework and identify any changes necessary following its decision on the application of the Risk Management Framework to the Secretariat's Business Plan only. The updated Risk Management Framework includes the following main changes:

.1 alignment of the terminology, firstly, to reflect the changes needed to apply the risk management to the Secretariat's Business Plan and secondly, to improve the consistency of the terms used across the Risk Management Framework;

.2 deletion of paragraphs recalling the development of the risk management process and procedures used in previous risk management iterations, with the aim of streamlining the Risk Management Framework (part C of the annex) into a tool that only includes the necessary steps to carry out the risk management process that covers the Secretariat's Business Plan;

.3 text on assessment of present controls was moved to the risk identification section of the Risk Management Framework from the section on development of risk management options. This corresponds with the actual procedures applied in the latest risk management iteration. As the initial risk assessment should be performed taking the existing controls into account, it is more appropriate to refer to them prior to the risk assessment; and

.4 adjustment of the probability assessment scale based on lessons learned of the previous risk management iteration showed that the previous probability assessment was considered difficult to apply.

Context Document required by the Risk Management Framework

3 Furthermore, paragraph 6 of part C of the annex to document C 110/3/5 states that the periodic review of the Context Document required by the Risk Management Process should be developed by the Secretary-General for approval by the Council.

4 The Context Document firstly, describes the aims and objectives that are already introduced in the risk management policy. Secondly, it aims to focus the exercise on the relevant biennium, however, the objectives in the Secretariat's Business Plan provide that focus for the biennial exercise.

5 Therefore, the standalone Context Document is deemed to only create an additional layer of paperwork and the essential paragraphs in the Context Document have been transferred to the Risk Management Framework. As a consequential amendment, the paragraphs relating to the development of the Context Document were removed in the risk management process.

6 The updated Risk Management Framework is attached in the annex for the approval of the Council.

Action requested of the Council

7 The Council is requested to approve the Risk Management Framework in the annex, to facilitate the application of risk management to the Secretariat's Business Plan for future risk management iterations.

***

ANNEX

RISK MANAGEMENT FRAMEWORK

PART A – DEFINITIONS

1 For the purposes of the Secretariat's Risk Management Framework, the following definitions apply.

Risk event

2 Any event which may adversely affect the ability of the Secretariat to meet its objectives as set out in the Secretariat's Business Plan.

Risk

3 A combination of the probability and impact of any risk event.

Risk tolerance

4 A measurement of the Secretariat's willingness to accept a risk. The risk tolerance is comprised of three levels:

.1 High tolerance level indicates that the risk is tolerable at its existing assessed risk level.

.2 Moderate tolerance level indicates that the risk is tolerable but further mitigating actions could be implemented to increase the risk tolerance to high.

.3 Low tolerance level indicates that the risk is not tolerable at the assessed risk level and further mitigating actions must be implemented.

Risk management

5 The process of identifying, assessing, communicating and mitigating risk events affecting the Secretariat's ability to meet its objectives.

High-level risk event categories

6 Categories that cover actions that are considered to be critical for the achievement of the Secretariat's objectives. Risk events must be attributed to at least one of these categories in order to be considered to affect the Secretariat as a whole. The high-level risk event categories are as follows:

.1 **Organizational status and effectiveness:** risk events that directly affect the achievement of the Secretariat's objectives as defined in the Secretariat's Business Plan (e.g. damage to the Organization's reputation amongst a group or groups of stakeholders through, for example, failure to meet the expectations of Member States; regionalization or unilateralism in the regulation of shipping; changing stakeholder needs (rate of change and scope); demographic and social/cultural trends; failure to keep pace with technological innovation; capital availability for major programmes; external regulatory and political trends, including wider United Nations developments; and non-adoption or non-compliance with the Organization's standards).

.2 **Financial:** risk events that directly affect the effective management and control of financial resources (e.g. liquidity (cash flow, non-payment of assessments, inability to meet obligations as they fall due); inflation and the associated effect on purchasing power; unfunded or inadequately funded commitments; budget management and control; and treasury management).

.3 **Operational:** risk events that affect the day-to-day running and safe operation of the Secretariat (e.g. business operations (human resources, capacity, meeting delivery, efficiency, service failure, ITCP delivery, meeting new requirements); empowerment (leadership, change readiness); information technology (relevance, availability, stability); information/business reporting (budgeting and planning, accounting information, pension funds, After Service Health Insurance (ASHI) liability, investment evaluation); fire and property damage; theft, fraud and other crime; personal injury; business continuity; disease and disability; and liability claims).

"What if …?" exercises

7 The consideration of possible future scenarios, characterized by the question "what if …?".

PART B – RISK MANAGEMENT POLICY

1 The Secretariat while working to achieve its objectives, faces many challenges with the potential to hinder its ability to achieve these objectives. Therefore, a systematic approach aimed at managing these risks events has been agreed on. The Council has defined the scope of the risk management as covering the risk events affecting the delivery of the Secretariat's Business Plan.

Policy aim and objective

2 The aim of risk management is to facilitate the achievement of the Secretariat's divisional objectives as set out in the Secretariat's Business Plan. Risk management in the Secretariat must, therefore, be explicitly linked to the Secretariat's Business Plan in two ways:

- **explicit link between risk events and objectives** – risk events are only relevant in the context of their ability to affect the achievement of objectives. Since the Secretariat's Business Plan defines the Secretariat's objectives, all risk events identified during the risk management process must be explicitly linked to one or more divisional objectives; and

- **provision of context for "horizon-scanning"** – it is a necessary part of any risk event identification to consider not only short-term and immediate areas of risk, but to also look forward and identify the future risk events arising from developments in the Secretariat's work and the relationship with its stakeholders. Such a long-sighted view has already been taken, partly, through the identification of the trends, developments and challenges facing the Organization.

3 Therefore, when conducting the risk management process, there should be an awareness of the risks inherent in the trends, developments and challenges, the outcome and approved recommendations of earlier iterations, and also the key features of the broader risk environment in which the Secretariat is operating. The following elements particularly affect the operations of the Secretariat:

- **current financial climate** – the global financial climate continues to present challenges to all organizations, both public and private. The effect is potentially both broad and deep, from the increased risk around the management and secure investment of the Organization's financial deposits, to the effective and timely resourcing of those parts of the Organization's work funded outside of the regular budget. Delivery of all objectives requires appropriate resourcing and the risks raised by the ongoing economic environment cannot be ignored in any consideration of risk to the Secretariat;

- **safety and security** – events over the past years highlight the fact that, across the world, United Nations personnel continue to face violence and threats from armed conflict, terrorism, kidnapping, banditry, harassment and intimidation. As a result, the United Nations Chief Executives Board for Coordination (CEB) recognized that the safety and security of United Nations system staff is an integral part of the activities undertaken by the United Nations system, should be included in the earliest planning stages and should be strengthened and enhanced. While the threat level at the Organization's Headquarters is permanently assessed in coordination with the host Government authorities, day-to-day operations may be affected by external threats and incidents (whether or not they may be aimed at the United Nations system or its component bodies) and by the consequential need to introduce heightened measures, at short or no notice, to ensure the safety and security of staff and delegates as well as business continuity. Similarly, staff travel and the implementation of activities (for example, technical cooperation training events) may be severely affected by safety and security considerations, with consequential negative effects on programme delivery and the need for appropriate security training for staff, experts and consultants;

- **travel disruption** – extreme weather conditions or other factors such as airline strikes can have direct effects on the ability of the Organization to deliver its meetings' programme (e.g. through the inability of delegates and staff to reach the United Kingdom or other meeting venues), implement technical cooperation activities and to be represented at external meetings; and

- **commitments within the United Nations system** – can result in ambitious and complex goals that can expose the Secretariat to risks. As the United Nations moves towards climate neutrality, the Organization needs to be aware of reducing its carbon footprint. As the Organization complies with the objective of carbon neutrality as its contribution to the efforts within the United Nations system, certain risks might evolve which could affect the delivery mechanism of the Organization. This might require estimation of the Organization's greenhouse gas emissions, the efforts to be undertaken by them to reduce greenhouse gas emissions to the greatest extent possible, and finally, to analyse the cost implications and explore budgetary modalities of purchasing carbon offsets.

4 The objective of the Secretariat's risk management policy is to mitigate and/or prevent an adverse effect of foreseeable risk events on the achievement of its objectives.

- **mitigate and/or prevent** – the Secretariat recognizes that not all risks are avoidable, nor, even where such risks are avoidable, is it always in the Secretariat's best interests to do so. Effective and coherent risk management across an organization is a matter of professional judgement and it is frequently the case that a mitigation approach for one risk may increase a risk elsewhere, either directly or through a consequent lack of adequate resources for its own

mitigation. Similarly, each mitigation is likely to have a cost and it is necessary, in each case, to determine that the benefit, through the reduction in risk, outweighs the cost of the mitigation. Risk events and their associated risks and mitigations cannot be seen in isolation, either of the resources required for mitigation or of each other, and the Organization does not have an infinite pool of resources – the price of an increase in control is often a reduction in efficiency – and a delicate balance must be struck. It is, therefore, not the Secretariat's goal to eliminate risk, but to mitigate and/or prevent its effects;

- **foreseeable risks** – not all risk events can be foreseen and, for those that can, the risk associated with them cannot always be accurately predicted. However, the Secretariat seeks, through the establishment of a methodical approach to the identification and documentation of risk events to increase the Secretariat's institutional capability to foresee risk and, through the repeated experience of this process, to refine its skills in assessing the probability and impact of risk; and

- **achievement of objectives** – a risk event is only relevant in the context of an objective which it affects and for the Secretariat the objectives are those set out in the Secretariat's Business Plan. Therefore, it is an important principle that a risk event which does not affect the achievement of an objective of the Secretariat is not a risk to the Secretariat.

Methodology

5 The Secretariat is committed to reduce risk to a level that is as low as reasonably practicable, through the implementation of a risk management process comprised of:

Risk event identification
Risk assessment
Risk management options
Risk control selection
Implementation
Monitoring and review

Roles and responsibilities

6 The Secretary-General has the leading role in the risk management process. The internal audit activity assists the Secretariat in the identification and evaluation of significant exposures to risks and contributes to the improvement of the risk management systems.

7 The Secretary-General has the responsibility for the implementation and maintenance of the Secretariat's Risk Management Framework, the results of which are reported to the Council.

PART C – RISK MANAGEMENT PROCESS

Overview

1 The Secretariat's risk management process consists of the following elements:

- Risk event identification – On the basis of the Secretariat's Business Plan and the high-level risk event categories, specific risk events will be identified. For each risk event identified, controls that are already in place will be described;

- Risk assessment – For each risk event identified, its impact and probability will be determined taking into account the existing controls;

- Risk management options – Subsequently, available options to improve existing controls or to implement additional controls to further reduce risk will be determined, taking into account the agreed level of risk tolerance, which may include risk acceptance, risk avoidance, risk control, risk financing and risk transfer, while simultaneously considering their adequacy and cost-effectiveness;

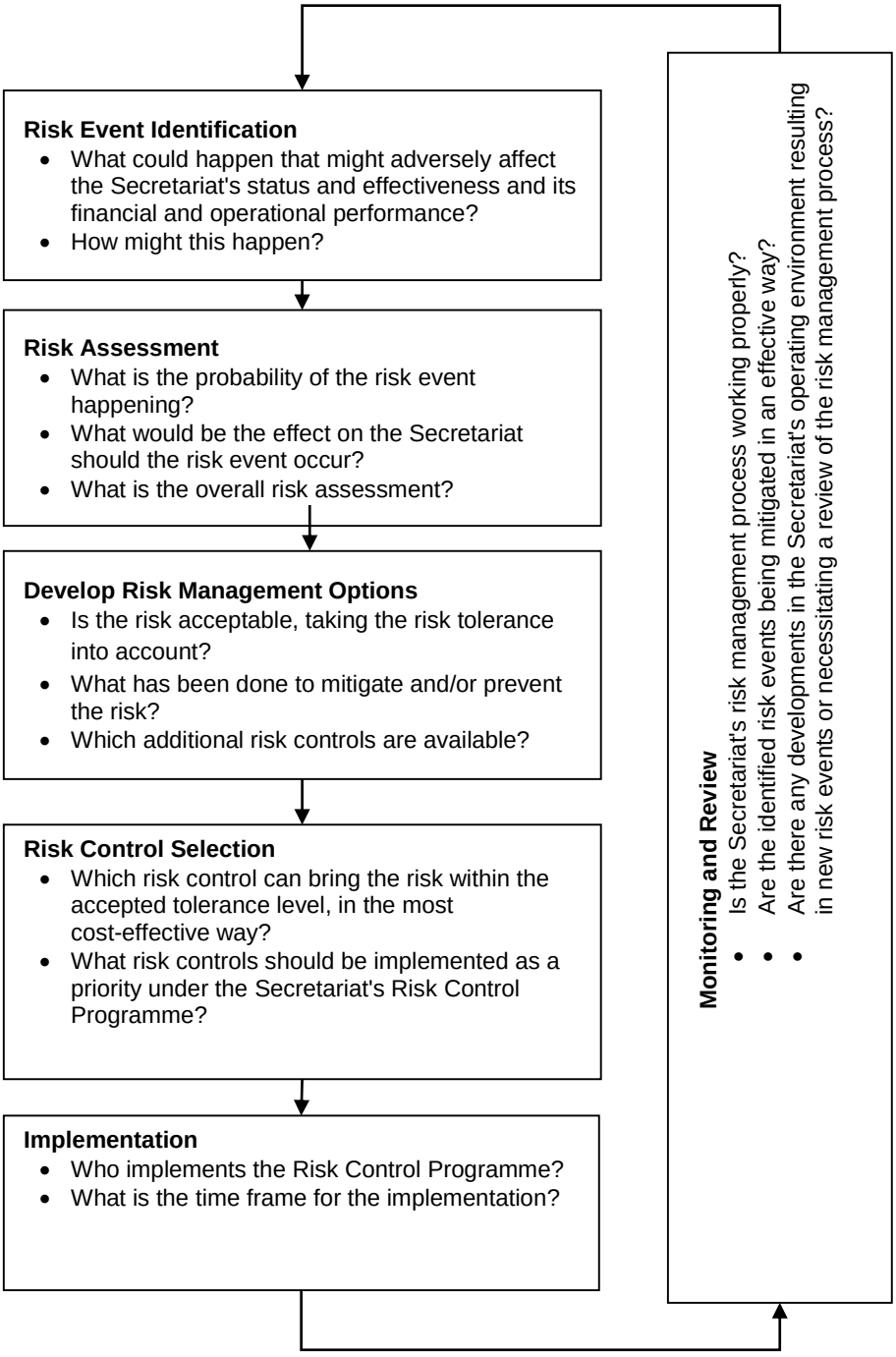
- Risk control selection – The risk management options for all identified risk events will be consolidated and prioritized on the basis of the risk tolerance levels and the available resources and develop a risk control programme indicating timelines, actions, responsibilities, etc.;

- Implementation – The risk control programme will be implemented; and

- Monitoring and review – The implementation of the risk control programme will be monitored and key changes in the risk environment will be reported to the Council for its review and action, as appropriate.

2 This summary of the Secretariat's risk management process is presented in the following diagram, with each stage of the process analysed in detail in later sections.

THE RISK MANAGEMENT PROCESS



Risk event identification

Purpose:

3 The purpose of the risk event identification is to identify the Secretariat's exposure to potential risk by developing a comprehensive list of risk events which may adversely affect the achievement of the Secretariat's objectives, and for each risk event to regularly consider the existing controls in place and their effectiveness. Many of the risk events identified will subsequently be assessed as being unlikely, being already satisfactorily mitigated or having a low influence. In order to properly understand the risk environment in which the Secretariat operates, it is important to have a list of all risk events likely to be faced, before assessing them systematically.

Output:

4 The output of the risk event identification is a complete list of potential risk events the Secretariat is facing. To support a consistent assessment, risk events should be documented in a uniform format (through a database) as follows:

Risk Event Table		
Risk event identification	1. Name of risk event	*Name and brief description of the risk event*
	2. Scope of risk event	*Qualitative description of the events.*
	3. Nature of risk event	*High-level risk event category (and sub-category where identified)*
	4. Strategic Plan	*The strategic directions potentially affected by the risk event*
	5. Secretariat's Business Plan	*The divisional objectives potentially affected by the risk event*
	6. Stakeholders and responsibilities 6.1 6.2	 *Internal and external stakeholders affected by risk event* *Entity responsible for managing risk event*
	7. Risk Controls 7.1 7.2	 *Description of present controls* *Level of confidence placed in present controls*
Risk assessment	8. Risk assessment 7.1 7.2 7.3	*An assessment of the risk taking into account existing controls.* *Impact* *Probability* *Assessment*
Risk management options and Risk control selection	9. Risk tolerance	*A measurement of the Secretariat's willingness to accept a risk.*
	10. Potential action for improvement	*Recommendations to optimize the present controls or to implement additional controls to achieve the accepted risk tolerance.*

5 At this stage, boxes 1 to 7 in the table above should be completed for each risk event. It should be noted that when considering risk events, it is essential to place them in the context of the Secretariat's Business Plan by identifying specifically which objectives would be affected by a risk event. This requires a clear understanding of the Secretariat's Business Plan by those involved in the process.

6 This risk event identification should result in a consolidated and dynamic list of risk events covering the relevant Secretariat's divisional objectives. The results may be best consolidated depending on the area affected by the risk event. The risk events identified will be compiled in a database to support the management of the process.

Methodology:

7 The risk event identification is primarily a process of structuring and consolidating existing knowledge about potential risk events, including lessons learned from previous risk management exercises and of conducting "what if …?" exercises to examine scenarios for risks not previously considered. The risk event identification should also involve the assessment of the controls already in place for each risk event, and their likely effectiveness and possible financial impact. This should be done by those operationally responsible for managing the risk. This process should include the following elements:

- a workshop of the focal points in each Division to establish the purpose of the risk event identification and to identify significant high-level risks;

- a self-assessment exercise for key operational staff within each division, being asked to identify risk events within their area of operation; and

- follow-up interviews with key staff by the central risk team in the Office of the Secretary-General designed to validate the results and identify gaps, in particular through the use of "what if …?" exercises.

8 There will be an initial, comprehensive risk event identification at the start of a biennium in order to establish a risk register, with a periodic review for completeness on a biennial basis, and as required. For subsequent reviews, the existing risk register will be used as a starting point. Risk management is an iterative process and, in general, an important consideration when embarking on a subsequent iteration is the output of previous risk management iterations, key risks identified and necessary areas of focus. Nevertheless, it is still important to properly consider "what if …?" scenarios in each operational area on an ongoing basis, ensuring that the risk events on the risk register remain current.

Risk assessment

Purpose:

9 The purpose of risk assessment is to measure the risks associated with each identified risk event with the existing controls in place and, consequently, the Secretariat's exposure to risk in the delivery of the Secretariat's Business Plan.

Output:

10 The outcome of the risk assessment will be, for each identified risk event, the information contained in box 8 of the risk event table. The risk assessment enables the ranking of risk events based on their probability and impact, and consequently, the identification of risk events on which to focus when deciding on risk management options.

Methodology:

11 The risk assessment requires an evaluation of the probability and the impact of a risk event occurring with the existing controls in place. A five-category approach is used for the assessment of risks. The time frame of each risk management iteration should correspond with the time frame of the Secretariat's Business Plan. In view of the biennial nature of the Secretariat's Business Plan, a standard period of two years is adopted.

12 When assessing probability, a clear understanding of the time frame in question and the meaning of the terms used is important. The following terms describe the probability assessment:

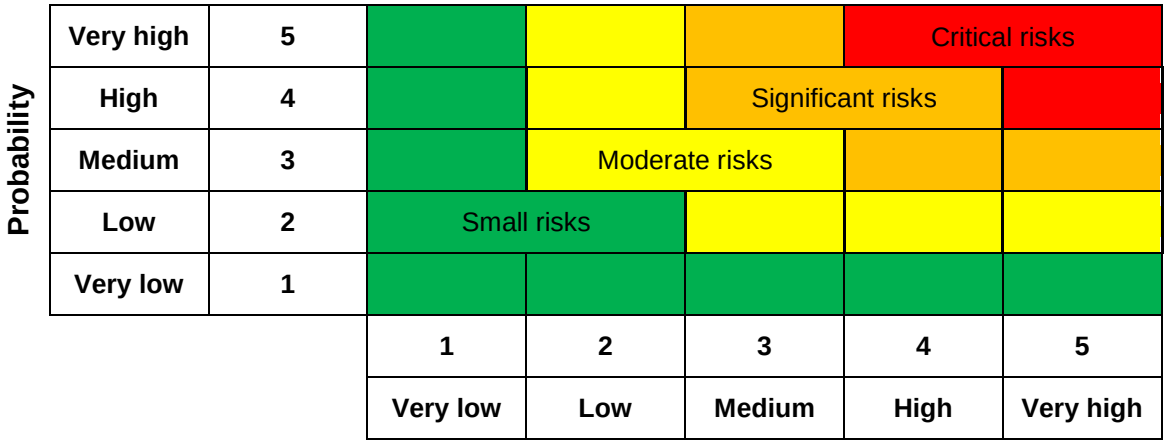
Chance of occurring in time frame	**Probability**
1 – Very low	1%
2 – Low	25%
3 – Medium	50%
4 – High	75%
5 – Very high	99%

13 Similarly, when considering the impact of a risk event, a clear understanding of the time frame and the terminology is important, in order to achieve a consistent assessment of risks across the Secretariat. The following table sets out the risk impact descriptions for the risk assessment:

Impact	**Financial impact**	**Information**	**Political impact**	**Occupational health & safety**
1 – Very low	≤£10,000	Information that would not cause undue harm, such as unclassified, routine policy information.	The embarrassment is restricted to within the Organization, the public remain unaware.	Danger to one or more individuals.
2 – Low	> £10,000 and ≤ £100,000	Information that could cause some harm to individuals, such as in confidence information or personal information.	Industry and public made aware of embarrassment' through specialized media.	Injury to an individual.
3 – Medium	> £100,000 and ≤ £1,000,000	Information that could cause some harm to a Member State, such as confidential information, for example commercial or Member State information.	Complaints raised with Member State or a political representative of that Member State.	Injury to several individuals.
4 – High	> £1,000,000 and ≤ £10,000,000	Information that could cause substantial political or security implications to a Member State or other UN body.	Widespread adverse publicity reaching national press, radio and television. Questions likely to be raised in Member State or other UN body.	Serious injury to one or more individuals.
5 – Very high	> £10,000,000	Information that could have extreme security or political implications or other information that would threaten the ongoing operations of IMO.	Widespread adverse publicity with calls for the Secretary-General to resign or Organization to be reviewed.	Loss of one or more lives.

14 Combining probability and impact leads to a simple assessment of risks in four categories as shown in the chart below:

Risk Assessment



15 While this categorization will allow the Secretariat to compare the overall risk of risk events, it is important not to lose sight of the separate probability and impact assessment, as mitigation strategies are developed based on this information.

16 It is the responsibility of line managers to make an initial assessment, which is then reviewed by the risk team in the Office of the Secretary-General to arrive at a consensus on the risk assessment. The individual risk assessment could involve steps similar to those described in paragraph 7 (on risk event identification). Such an assessment would be subject to a moderation process and a common approach to involve all relevant stakeholders, who independently assess each risk. The results, and in particular any views departing significantly, can then be discussed, and the view of the group agreed. This ensures that all perspectives are taken into account to produce a consistent assessment of each risk.

17 Following the individual assessment for each risk event, the results can be consolidated and reported, identifying the most significant risks to the Secretariat. Risks that are clearly negligible and do not require mitigations, should not be included in the main risk register.

Development of risk management options

Purpose:

18 The purpose of the development of risk management options is to regularly consider for each risk event, the level of risk that can be tolerated taking the existing controls into account and to develop and analyse options to reduce risks that are higher than the level of risk tolerated. When relating the risk tolerance level with the present controls outlined in the risk identification section, the possibility also exists that a particular risk will be "over-controlled", and that proper risk management can be maintained while lightening the present control systems in order to improve efficiency and effectiveness.

Output:

19 The outcome of the development of risk management options will be, for each risk event, the information contained in boxes 9 and 10 in the risk event table. For each risk event where the risk is presently outside of the tolerated risk levels a number of possible additional controls must be presented, along with the assignment of their estimated cost and effect on risk reduction in order to enable an assessment of the adequacy and cost-effectiveness of each risk event.

Methodology:

20 The first step of the development of risk management options is to determine the level of risk that can be tolerated for a particular risk event. Risk tolerance will not be uniform across the Secretariat – certain areas of the operation are more sensitive than others. The setting of the risk tolerance is a matter of professional judgement, and should be the responsibility of those managing the risk. In addition, through consolidation of all risk data, there should be an independent oversight, at a corporate level, of defined risk tolerances to ensure that they are consistent with the overall position of the Secretariat.

21 The Secretariat should never accept a risk that is critical. If a risk assessment identifies a risk as critical or significant, controls must be developed to reduce the risk to a level within the accepted risk tolerance. All risks should be reduced to a level at, or below, the highest level of risk at which additional controls are not required.

22 Having determined the current risk tolerance, the second step is to develop control options which target either a reduction in the probability of the event occurring, or in the impact should the risk event occur. The risk control options available are specific to the particular risk in question and may also influence other risk events, either positively or negatively. Each option available will also have costs, directly through financial expenditures or indirectly through staff time, and each will have an effect on the level of risk. The estimated cost and effect on the level of risk should be assessed for each risk event. This will enable a prioritization of risk controls and support the implementation of the risk control programme.

23 The risk management will typically follow one of five methods:

- risk acceptance – i.e. doing nothing about the risk;
- risk avoidance – i.e. avoiding the activity that creates the risk in the event that the risk cannot be mitigated to a satisfactory level and the activity is not essential to achieve the Secretariat's objectives;
- risk control – i.e. using a variety of methods to prevent or mitigate the risk. These might target the impact and/or the probability of the risk event;
- risk financing – i.e. assigning funds to cover all or part of losses that might be caused by the risk event; and
- risk transfer – i.e. transferring all or part of the risk to a third party by paying a financial compensation. This includes insurance as well as contractual arrangements whereby the counter party indemnifies the Secretariat against liabilities concerning specified circumstances.

24 The overall aim of such options should be to bring the controlled risk within the level of risk acceptable for the specific risk event. Consequently, the evaluation of each control option should include an analysis of the estimated risk assessment of each risk event, after putting the control in place as well as an estimation of the costs for implementation of each control.

25 The effort put into the development of additional controls should reflect the level of the risk assessment. That is, for risks which are assessed as "small", and to some extent "moderate", it is not appropriate to devote significant time and effort to develop further risk reducing controls. For significant objectives and major risks, falling into the significant and critical risk categories, a more rigorous approach is required that provides as detailed estimation of costs and effect on risk reduction of these risk events.

Risk control selection

Purpose:

26 The purpose of the risk control selection is to develop a coherent, prioritized and cost-effective response to all unacceptable risks faced by the Secretariat.

Output:

27 The output of the risk control selection should be a Secretariat-wide risk control programme to apply additional controls where an unacceptable risk was identified. This will necessarily require a consolidation and prioritization exercise, particularly where controls involve associated costs. For each risk event, the risk control programme should contain information on the selected control, the timescale for implementation, costs involved and responsibilities for delivery, in order to support the subsequent progress.

Methodology:

28 A process akin to a cost-benefit analysis should, where appropriate, be used to develop the risk control programme, for example, through the submission of costed proposals for risk controls intended for the consolidation, evaluation and prioritization of controls against limited resources.

29 All options should be considered, including the removal or modification of some of the existing controls in order to achieve the same risk at a lower cost or if they are not thought to have a significant effect on the risk.

30 Whilst such a process will require central coordination, it will also entail the cooperation of all relevant divisions, in order to ensure that the risk control programme will be delivered effectively. In some cases, it may be necessary to consider tolerating a higher risk than planned when resources required to further mitigate the risk are not available.

Implementation

Purpose:

31 The implementation is designed to ensure that the selected risk controls are implemented in a timely and cost-effective manner.

Output:

32 The output of the implementation will be the new controls in place and, consequently, an updating of the information contained in boxes 7 and 8 of the risk event table. This will also be the basis for the identification and assessment of risk events of any subsequent iterations of the risk management process.

Methodology:

33 As the objectives and responsibilities have already been identified, this part will primarily involve regular progress reporting, identification and resolution of implementation issues and, finally, a post-implementation review to determine the effectiveness of the new controls, including the examination of further improvements.

34 Whilst responsibility for implementation will be identified for each individual control of the risk control programme, a consolidated database will be maintained in order to provide a consistent approach across the Secretariat and to ensure the concentration on risk events that have priority for the Secretariat. Additionally, this ensures that the Secretariat's risk database is maintained between iterations of the risk management process and, consequently, that the Secretariat's exposure to risk can be reported at any stage.

Monitoring and Review

Purpose:

35 The purpose of monitoring and review is to ensure that the Secretariat's risk management process is working properly, that actions are being taken on a timely basis and that unacceptable risks are given the appropriate priority. Feedback in the form of monitoring, review, and reporting to the Senior Management Committee and the Council, are a key part of the Secretariat's effective governance arrangements.

Output:

36 On completion of each risk management iteration of the risk management process, a summary report should be prepared for the Senior Management Committee and the Council setting out key risk events, controls in place, plans for additional controls, responsibilities and time scales for implementation.

37 On completion of each risk management iteration, there should also be a review across the Secretariat to identify lessons learned from the exercise and plan for future iterations (see paragraph 34).

38 In between risk management iterations, periodic reports of the monitoring and review process should be prepared for the Senior Management Committee, as appropriate, covering interim developments, in particular:

- the present situation of all risk events determined to have an unacceptable level of risk, including information on controls and the implementation status on selected additional controls;

- information on all risk events which cannot be brought within an acceptable risk level because of resource constraints on the risk control options; and

- the implications of any significant changes to the risk environment.

Methodology:

39 The use of a comprehensive and properly-maintained risk database will support the monitoring and review process. It is essential that a system of regular monitoring is implemented to ensure the controls are continuously applied and effective. Therefore, the risk controls selected should be periodically reviewed to ensure they are still in place, effectively controlling the risk, within the assumed costs, while detected deficiencies need to be corrected to restore the implementation of controls as planned.

40 When preparing monitoring reports, the following should be considered and recorded:

.1 Developments – what has happened since the last update?

.2 Current status – what is the current status of each risk event?

.3 New risk events – what new risk events affecting the delivery of the Secretariat's Business Plan have arisen since the last review, and what risk events previously identified, but not mitigated, warrant additional controls now?

.4 New controls – what controls are to be developed to address the current or newly identified risk events?

.5 Effect on the risk management process – what is the effect of all these actions on the process?

.6 Is the risk management process being implemented effectively and within the envisaged costs?