INTERNATIONAL MARITIME ORGANIZATION

E

COUNCIL
110th session
Agenda item 3

C 110/3/5
30 April 2013
Original: ENGLISH

STRATEGY, PLANNING AND REFORM

Risk Management

Submitted by the Secretary-General

SUMMARY

Executive summary:	This document consolidates the Risk Management Framework following previous Council decisions, presents a Context Document and updates the Terms of Reference for the Council Risk Review, Management and Reporting Working Group
Strategic direction:	4
High-level action:	4.0.4
Planned output:	4.0.4.2
Action to be taken:	Paragraph 10
Related documents:	C 109/D; C 106/D, C106/3(b); C 100/D and C 100/3(b), appendix 1 of the annex

Background

1 At its 109th session, the Council decided to refer document C 109/3/2 (Germany) to the sixth session of the Council Risk Review, Management and Reporting Working Group (CWGRM), which should be held early in the 2014-2015 biennium, for detailed consideration, in conjunction with the entire Risk Management Framework (RMF), including consideration of the impact of the workload on the Secretariat.

Risk Management Framework

2 The Risk Management Framework was adopted by the Council at its 100th session in June 2008 (see C 100/3(b), appendix 1 of the annex).

3 At its 106th session in June 2011, the Council agreed to a number of changes to the Risk Management Framework in order to reflect recommendations of the Joint Inspection Unit's report entitled "Review of enterprise risk management (ERM) in the United Nations System: benchmarking framework" (see C 106/3(b), annex 1).

4 Furthermore, C 106 agreed with the decision of the fifth session of CWGRM that the periodic review of the Context Document required by the Risk Management Framework should be developed by the Secretary-General for approval by the Council and, as a consequence, paragraph 6 of part C of the Risk Management Process should be amended accordingly.

5 To consolidate the changes referred to under paragraphs 3 and 4, the Risk Management Framework is set out at annex 1. As the changes merely reflect decisions taken previously by the Council, annex 1 is reproduced in English only.

Context Document required by the Risk Management Framework

6 As stated above, C 106 clarified that the periodic review of the Context Document should be developed by the Secretary-General for approval by the Council and further recommended that, to ensure a chronological sequence, an amended Context Document should be approved by the Council prior to the conduct of each risk management exercise.

7 The Secretariat's risk management exercise is to be reviewed by the CWGRM and, in order to enable this review and ensure the early timing of the sixth session of the CWGRM in line with the decision of C 109 (paragraph 1 above), the updated context document is attached at annex 2 for the approval of the Council.

8 The only substantial change since the last context document (see C 106/3(b), annex 2) is the amalgamation of the section on "energy position" into a broader "sustainable development" section in point 3.3 on "Key factors to consider".

Terms of Reference for the Council Risk Review, Management and Reporting Working Group

9 Taking into account the Council's decisions above, the terms of reference for the CWGRM have been amended and are attached in annex 3.

Action requested of the Council

10 The Council is requested to:

.1 note the consolidated Risk Management Framework in annex 1, reflecting the Council's earlier approval of the changes thereto;

.2 approve the updated Context Document in annex 2; and

.3 approve the Terms of Reference for the Council Risk Review, Management and Reporting Working Group.

***

ANNEX 1
(English only)

RISK MANAGEMENT FRAMEWORK

PART A – DEFINITIONS

1 For the purposes of the IMO Risk Management Framework, the following definitions apply.

Risk event

2 Any event which may adversely impact on the ability of the Organization to meet its objectives.

Risk

3 A combination of the probability of any risk event and its consequences.

Risk tolerance

4 A measurement of the Organization's willingness to accept risk, being the highest level of risk at which additional mitigating controls are not required.

Unacceptable risk

5 A risk which falls outside the assessed risk tolerance level.

Risk management

6 The process of identifying, assessing, communicating and mitigating risks impacting on the Organization's ability to meet its objectives.

High-level risk event categories

7 **Organizational status and effectiveness:** those that directly impact on the achievement of the Organization's aims and objectives as defined in the Strategic Plan (e.g. Damage to the Organization's reputation amongst a group or groups of stakeholders through, for example, failure to meet expectation or "capture" by a narrow group of interests; Over-regulation; Regionalization or unilateralism in the regulation of shipping; Changing stakeholder needs (rate of change and scope); Public perception; 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).

8 **Financial:** those that directly impact on 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 associated impact on purchasing power; unfunded or inadequately funded commitments; budget management and control; and treasury management).

9 **Operational:** those that affect the day-to-day running and safe operation of the Organization (e.g. Business operations (human resources, capacity, meetings delivery, efficiency, service failure; ITCP delivery, meeting new requirements (e.g. Voluntary Member State Audit Scheme)); 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

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

PART B – RISK MANAGEMENT POLICY

1 In its work to achieve its mission in an ever-changing world, the Organization faces many challenges with the potential to hinder its ability to achieve its strategic aims and objectives. The Organization's response to this risk environment has been to adopt a systematic approach aimed at addressing and managing the risks to all of its activities.

Policy aim and objective

2 The aim of risk management is to facilitate the achievement of the Organization's mission statement as set out in its Strategic Plan.

3 The objective of the Organization's risk management policy is to minimize and/or prevent adverse consequences emanating from foreseeable risks to the achievement of its aims and objectives.

Methodology

4 The Organization is committed to reducing 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 analysis
Risk management options
Risk treatment selection
Implementation
Monitoring and review

Roles and responsibilities

5 All IMO Member States and the Secretary-General have a role in the management of risk.

6 The internal audit activity assists the Organization in the identification and evaluation of significant exposures to risks and contributes to the improvement of risk management and control systems.

7 The Council and the Secretary-General have responsibility for the implementation and maintenance of the Organization's risk management framework.

PART C – RISK MANAGEMENT PROCESS

Overview

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

- Establish context – The purpose of the risk management process is to implement IMO's risk management policy in the context of the trends, developments and challenges identified in the Organization's Strategic Plan;

- Risk event identification – On the basis of the high-level risk event categories, the Secretary-General will identify specific risk events, for example, through "what if …?" scenarios. Member States, the Secretary-General and other relevant stakeholders will identify further risk events;

- Risk analysis – For each risk event identified, the Secretary-General will provisionally determine its impact and probability, using a methodology agreed by the Council;

- Risk management options – For each risk event identified, the Secretary-General will identify mitigating factors and controls already in place. Subsequently, the Secretary-General will determine available options to further reduce risk, taking into account the agreed level of risk tolerance, which may include risk acceptance, risk avoidance, risk control, risk financing and risk transfer, having regard for their suitability and cost effectiveness;

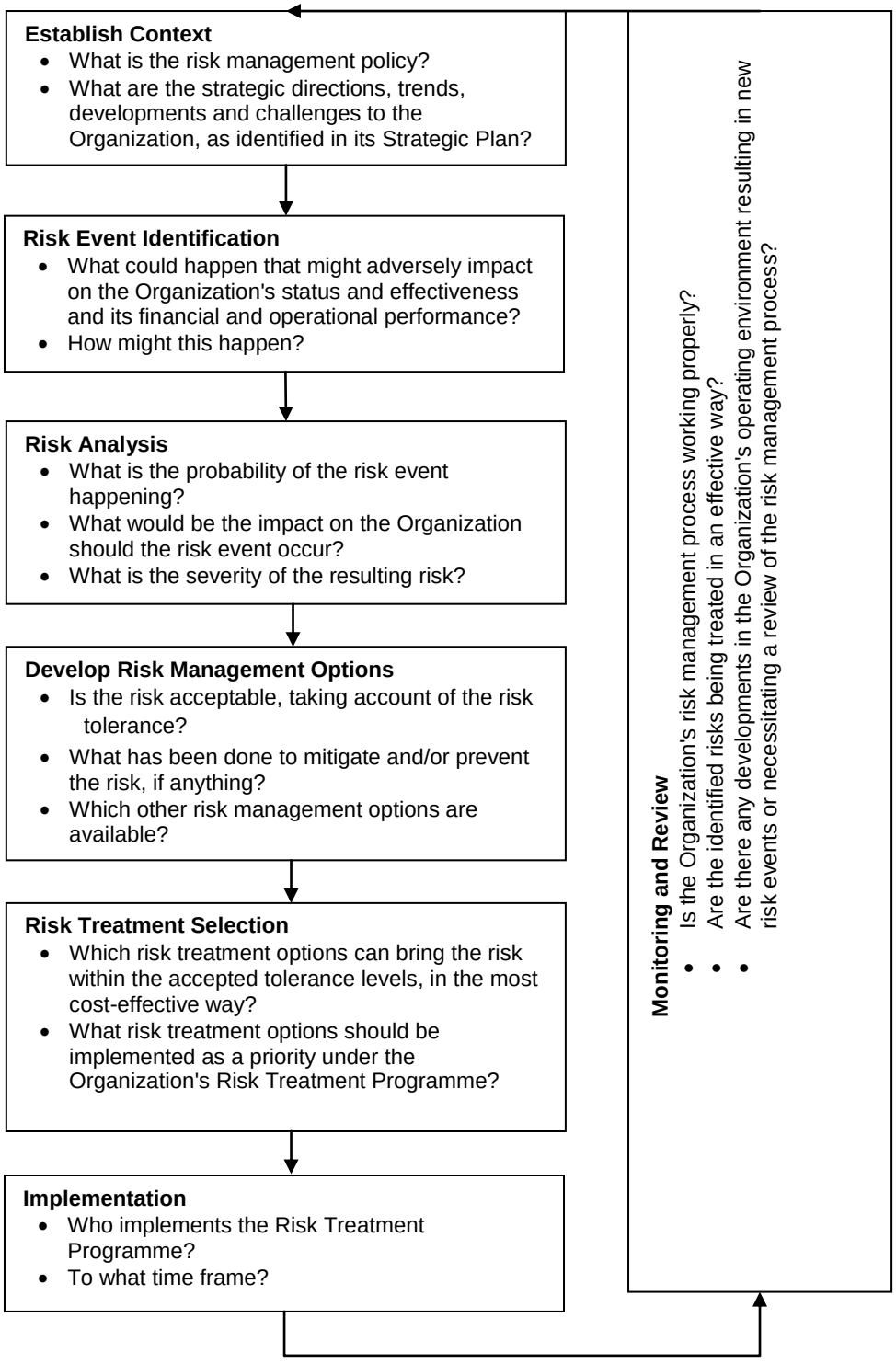
- Risk treatment selection – The Secretary-General will consolidate the risk management options for all identified risk events and prioritize them on the basis of the tolerance levels established by the Council and the available resources and develop a risk treatment programme indicating timelines, actions, responsibilities, etc.;

- Implementation – The Council and Secretary-General, as appropriate, will implement the risk treatment programme;

- Monitoring and review – The Secretary-General will monitor implementation of the programme and report key changes in the risk environment to the Council for its review and action, as appropriate.

2 This summary is represented in diagrammatic form on the following page, with each stage of the process being analysed in detail in the later sections.

DIAGRAMMATIC REPRESENTATION OF THE RISK MANAGEMENT PROCESS



Establish Context

Purpose:

3 The risk management process must take place in an appropriate context, aware of the objectives of the process, as defined in the risk management policy and through the Strategic Plan. The setting of context establishes the scope and focus of the risk management process.

Output:

4 The output of this part of the process should be a brief risk management context document which summarizes:

- the purposes of risk management;
- the key issues to be addressed through risk management, including those associated with the delivery of the Organization's Strategic and High-level Action Plans;
- areas of focus identified through previous risk management reviews, and changes in operational situation or strategic directions.

5 The document should identify the roles and responsibilities of those involved in the process, including the roles and responsibilities of Member States and observer organizations.

Methodology:

6 The risk management context document will be developed by the Secretary-General, drawing on the Strategic Plan and the Risk Management Policy, for approval by the Council. It should be communicated throughout the Organization in order to provide background and support a consistency in approach and prioritization.

7 The context document should be reviewed on a regular basis based on feedback from the risk management process, the output of the *Ad Hoc* Council Working Group on the Organization's Strategic Plan, and the output of the Council Risk Review, Management and Reporting Working Group.

Risk event identification

Purpose:

8 The purpose of the risk event identification is to identify the Organization's exposure to uncertainty by developing a comprehensive list of future risk events which may adversely impact on the achievement of the Organization's strategic directions. At this stage, the emphasis is on the completeness of the list in order to build a full risk profile. Many of the risk events identified will subsequently be assessed as being unlikely, low impact, or already satisfactorily mitigated through controls, but in order to properly understand the risk environment in which the Organization operates, it is important to have a list, as complete as possible, of all risk events likely to be faced, before methodically analysing and treating them.

Output:

9 The output of risk event identification is a complete list of potential risk events facing the Organization, structured according to the high-level risk event categories as set out in the risk management policy, that is: organizational status and effectiveness; financial; and operational. Risk events (and the associated risks) should be documented in a common format to support consistent analysis 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, their size, type, number and nature*
	3. Nature of risk event	*High-level risk event category (and sub-category where identified)*
	4. Strategic Plan	*The strategic directions potentially impacted by the risk event*
	5. High-level Action Plan	*The high-level actions potentially impacted by the risk event*
	6. Stakeholders and responsibilities	*Those impacted by the risk event and those responsible for assessing and managing it*
	6.1	*Internal and external stakeholders*
	6.2	*Entity responsible*
Risk analysis	7. Risk analysis	*An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls and mitigations, if any, at the time of the assessment*
	7.1	*Impact*
	7.2	*Probability*
	7.3	*Assessment*
	7.4	*Comment*
Development of risk management options and Risk treatment selection	8. Risk tolerance	*Objectives for control of the risk and accepted level of risk*
	9. Risk treatment & control mechanisms	*An assessment of the present controls and the level of confidence placed in them.* *Identification of means for monitoring and review*
	10. Potential action for improvement	*Recommendations to optimize the controls and mitigations to achieve the accepted risk tolerance*

10 At this stage, boxes 1 to 6 in the table above could 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 strategic directions of the Organization, by identifying specifically which directions would be impacted through the occurrence of the risk event. This requires a clear understanding of the Strategic Plan by those involved in the process.

11 This risk event identification should result in a consolidated and dynamic list of risk events covering the Organization and its strategic directions. The results may be best segregated depending on the nature of the risk event. The high-level risk event categories identified will necessarily require further sub-categorization in order to produce a meaningful list, and to group similar risk events together. Such sub-categories are likely to emerge during the course of the identification process. The risk events identified may be held in document or database format, or the possibility exists of using specific risk management software to support the management of the process.

Methodology:

12 The risk event identification is primarily an exercise in consolidating and structuring existing knowledge about potential risk events, including lessons learned from previous experience (see also paragraph 48), and in conducting "what if …?" exercises to examine possible scenarios for possible risk events not previously considered. With this in mind, the process should include the following elements:

- senior management workshop to establish the purpose of the risk event identification and to identify significant top-level risks;
- a self-assessment exercise for key operational staff within each division, being asked to identify risk events within their area of operation;
- follow-up interviews with key staff by a central risk team designed to validate the results and identify gaps in the identification, in particular through the use of "what if …?" analysis;
- seek the input of all stakeholders through a review of the risk event identification by Committees and Sub-Committees;
- the continued role of the Council Risk Review, Management and Reporting Working Group as a forum to provide input from the Member States into the risk management process and, in particular, with regard to risks relating to organizational status and effectiveness. This might involve: identification of scenarios for "what if …?" analysis; review and commentary on such analysis; identification of specific risk events.

13 There will be an initial, comprehensive risk event identification 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 can be used as a starting point, but it is still important to properly consider possible "what if …?" scenarios and "horizon-scanning" in each operational area on an ongoing basis, ensuring that risks on the risk register remain current.

Risk analysis

Purpose:

14 The purpose of risk analysis is to measure the risks associated with each identified risk event and, consequently, the Organization's exposure to risk in the delivery of the relevant sections of its Strategic and High-level Action Plans.

Output:

15 The outcome of the risk analysis will be, for each identified risk event, the information contained in box 7 of the risk event table. It will then be possible to rank risks based on their probability and impact, and consequently identify those areas where greatest focus is required.

Methodology:

16 The analysis of risk events to arrive at a view of the risk involved requires an assessment of the "probability" of the risk event occurring, and the "impact" should the risk event occur. In view of the size, nature of the Organization and the functions it performs, and the need to focus on practical risk management without an elaborate bureaucratic process, a simple assessment of risk is the most appropriate.

17 A 3-category "Low, Medium, High" approach to assessment is the most simple, but can have the effect of over-simplification, with too many risks being assessed as being "Medium" in impact and probability. With this in mind, a five-category approach provides further refinement, and greater scope for comparative ranking and assessment of risks.

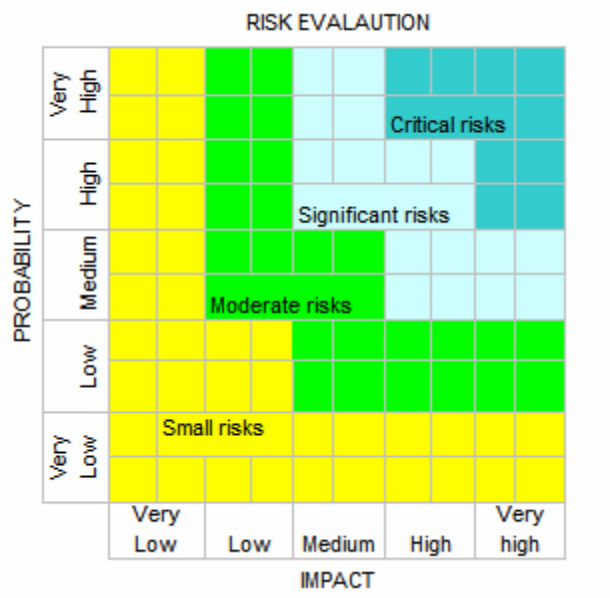
18 The Organization has, therefore, determined to use a five-category approach. Under such an approach, it is important that there is a clear understanding of the terminology being used in order to arrive at a consistent assessment of risks across the Organization – what might be considered "critical" to a treasury clerk, for example, may not, in fact, be critical to the Organization as a whole. A table setting out indicative risk impact descriptions is shown below and will be used in the risk management process:

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.	Injury to an individual.
2 – Low	Between £10,001 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 several people.
3 – Medium	Between £100,001 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.	Serious injury to one or more people.
4 – High	Between £1,000,001 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.	Loss of 1-9 lives.
5 – Very High	£10,000,001 or more	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 10 or more lives.

19 Similarly, when assessing probability, it is important that there is a clear understanding of the time frame in question and the meaning of the terms used. While the time frame would typically be a year, in view of the biennial nature of the Organization, a standard period of two years is more appropriate. Any time frame chosen should correspond with a review of the Strategic and High-level Action Plans of the Organization.

Probability	**Chance of occurring in time frame**
1 – Very low	1%
2 – Low	3%
3 – Medium	10%
4 – High	30%
5 – Very high	99%

20 Combining the two leads to a simple classification of risks in four categories as shown in the chart below:



While this categorization will allow the Organization to compare the overall risk of two events, it is important not to lose the probability and impact categories, as mitigation strategies are developed based on this information.

21 It is the responsibility of line managers to make an initial analysis, which is then reviewed and/or moderated by other layers of the Organization to arrive at a consensus of risk. The individual risk analysis could involve steps similar to those described in paragraph 12 (on risk event identification). Such analyses would be subject to a moderation process and a common approach to this is the use of a technique similar to "voting" in a workshop involving all relevant stakeholders or through questionnaire, all of whom independently assess each risk in turn. The results, and in particular any views departing significantly from the average, can then be discussed, and the view of the group agreed. This ensures that all perspectives are taken into account to produce a rounded analysis of each risk. The degree of assumption in assessing probability and impact should also be considered and may be recorded in box 7 of the risk event table.

22 Following the individual analysis, the results can be consolidated and reported on, identifying the most significant risks to the Organization, and in particular relating these back to the strategic directions impacted.

Develop risk management options

Purpose:

23 The purpose of the development of risk management options is to regularly consider, for each risk event: the existing mitigations in place and their effectiveness; the level of risk which can be tolerated in this area; and to develop and analyse options to reduce the risk where this is higher than the level of risk tolerated. The possibility also exists that a particular risk or risks 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:

24 The outcome of the development of risk management options will be, for each identified risk event, the information contained in boxes 8 and 9 in the risk event table. For each risk event where the risk is presently outside of the tolerated risk levels, there will also be a number of documented options to address it, along with an assessment of their cost and impact.

Methodology:

25 The first step in the development of risk management options is to document the mitigations already in place over the risk, and determine their likely effectiveness. This should be done by those operationally responsible for managing the risk, and would typically be done in parallel with the risk event identification. In order to determine the effectiveness of controls, a common technique is to re-assess the risk in terms of its probability and impact with the mitigations in place, thus giving a revised risk level.

26 The second step is to determine the level of risk that can be tolerated for a particular instance. Risk tolerance will not be uniform across the Organization – certain areas of the operation, and certain strategic directions are more sensitive than others. The setting of risk tolerances is a matter of professional judgement, and should be the responsibility of those with responsibility for 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 Organization. In particular, risk tolerances not established as "low" would require justification.

27 The Organization should never accept a risk that is critical. If a risk assessment identifies a risk as critical or significant, mitigation strategies 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 mitigating controls are not required.

28 Having determined the current risk level, and the risk level which can be tolerated, the third step in the process would be to develop mitigation options which target either a reduction in the probability of the event occurring, or the impact should it occur. The risk mitigation 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 a cost, directly in financial terms or in lost staff time, and each will have an impact on the level of risk.

29 The risk management options will typically follow one of five techniques:

- risk acceptance – i.e. doing nothing about the risk;
- risk avoidance – e.g. avoiding the activity that creates the risk in the event that the risk cannot be mitigated to a satisfactory level;
- risk control – e.g. using a variety of techniques to remove or reduce the risk. These might target either the impact or the probability of the risk, or both. For example, there is a risk to the Organization from disruption through terrorist activity. Contingency planning might reduce the impact of the risk event should it occur, while larger security barriers might reduce the probability of the risk event occurring;
- risk financing – e.g. assigning Organizational funds to cover all or part of losses using a variety of techniques; and
- risk transfer – e.g. transferring all or part of the risk to a third party for a financial consideration. This may be via insurance and also includes contractual arrangements where the counter party indemnifies the Organization against liability in specified circumstances.

30 The overall aim of such options should be to bring the mitigated risk within the level of risk tolerated in this area, and consequently a key part of the analysis of each management option should be an analysis of the estimated level of risk presented by the risk event, after putting in place the mitigation option.

31 The level of analysis put in to the development of options should reflect the level of the risk. 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 developing options to reduce such risks further and, in particular, the documentation should be kept light and pragmatic. Risks that are clearly negligible, requiring no mitigation, should not be included in the main risk register. For significant projects and for major risks outside of tolerance levels, a more rigorous approach is required. It is the responsibility of the relevant manager to determine the level of detail required.

Risk treatment selection

Purpose:

32 The purpose of the risk treatment selection is to develop a coherent, prioritized and cost-effective response to all unacceptable risks facing the Organization.

Output:

33 For the initial review of risks, the output of the risk treatment selection should be an Organization-wide risk treatment programme to address mitigation strategies where weaknesses or issues have been identified. This will necessarily require a consolidation and prioritization exercise, particularly where treatment options involve associated costs. It should contain information on the selected treatment option for each risk, the timescale for implementation, costs involved and responsibilities for delivery, in order to support subsequent monitoring of progress.

34 For interim risk management reviews in response to changing circumstances, a project- or initiative-specific risk management plan should be developed addressing all risks identified and assigning responsibilities. This will be incorporated in the next iteration of the risk management process, and should be reviewed as a part of the regular management of the project.

Methodology:

35 A process akin to a cost-benefit analysis should, where appropriate, be used to develop the risk treatment programme, that is, through the submission of costed proposals for consolidation, evaluation and prioritization against limited resources.

36 All options should be considered, including the removal or modification of some of the existing controls in order to achieve the same level of risk at a lower cost or, indeed, to remove controls entirely if they are not thought to be having a significant impact on the risk level.

37 Whilst such a process will require central coordination, it will require the cooperation, participation or contribution of all stakeholders, including Member States, where appropriate, in order to ensure that the risk treatment programme will be delivered effectively and it will, necessarily, be an iterative process. In some cases, it may be necessary to consider tolerating a higher level of risk than had been planned because the resources required to mitigate it further are not available. This should be reported clearly when the risk is presented for approval.

Implementation

Purpose:

38 The implementation of the risk treatment selection is designed to ensure that the selected risk treatments are implemented in a timely and cost-effective manner.

Output:

39 The output of the implementation will be the new controls in place and, consequently, an updating of the information contained in boxes 7 and 9 of the risk event table. This will also be the output from any subsequent iterations of the risk management process.

Methodology:

40 It is appropriate to use standard project management methodologies in the course of the implementation of the risk treatment programme. The objectives and responsibilities having been identified earlier, this 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 arrangements, and where further improvements can be made.

41 Whilst responsibility for action will be identified for each element of the risk treatment programme, a consolidated reporting structure should be maintained in order to provide a consistent approach across the Organization and to ensure that focus is maintained on the basis of the prioritization of risks. This, along with input from specific reviews, ensures that the Organization's risk register is maintained between iterations of the risk management process and, consequently, that the Organization's exposure to risk can be reported on at any stage.

Monitoring and Review

Purpose:

42 The purpose of monitoring and review is to ensure that the Organization'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 and review, and reporting to the Senior Management Committee and the Council, are a key part of the Organization's effective governance arrangements.

Output:

43 At the completion of the initial risk management process, there should be a summary report to the Senior Management Committee, and to the Council, through the Working Group, setting out key areas of risk, mitigating controls in place, development plans, responsibilities and timescales. A similar report should be produced on completion of each biennial iteration of the risk management process.

44 On completion of the implementation phase, there should also be a review across the Organization to identify lessons learned from the exercise and plan for future iterations (see paragraph 40).

45 In between risk management processes, the output of the monitoring and review should be a series of periodic reports to the Senior Management Committee or to the Council, as appropriate, covering changes and actions, in particular:

- the present situation on all risk events determined to have an unacceptable level of risk, including information on mitigating controls and implementation status on selected treatments;
- those risk events which have been identified as being the responsibility of the Member States, through the Council and the technical committees, along with a progress report on actions taken;
- information on all risk events which cannot be brought within tolerance because of resource constraints on risk mitigation options; and
- the implications of any significant changes to the risk environment.

Methodology:

46 The use of a comprehensive and properly-maintained risk register will support the monitoring and review process. Whilst responsibility for each risk event and, consequently, for associated controls, mitigations and treatments should be clearly identified in the risk register, this responsibility is likely to be devolved through the Organization.

47 It is essential that, having established the risk treatment programme, a system of regular monitoring is implemented to ensure the treatments are continuously applied and effective. This may consist of monitoring loss events to ensure they are contained within acceptable limits. However, this has a basic flaw in that losses have to be incurred in order for the failure in the control mechanisms to be detected. Therefore, the risk treatments selected should be periodically reviewed to ensure they are still in place, effectively controlling or minimizing the risk, within the envisaged costs. Where defects are located, they need to be rectified to restore control.

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

.1 Developments – what has gone on since the last update?

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

.3 New risk events – what new risk events/issues affecting the delivery of the Strategic and High-level Action Plans have arisen since the last review, and what risk events previously identified, but not treated, warrant treatment now?

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

.5 Effect on the risk treatment programme – what is the effect of all these actions on the programme?

.6 Opportunities – what opportunities are seen in the course of this review?

.7 Is the risk treatment programme being implemented effectively and within the envisaged costs?

49 For the Organization, particularly for the first iterations of the risk management process, there is a clear need for Organization-level consolidated reporting in order to maintain consistency of approach and, consequently, for a central management of the risk management process. This strategic view of the risk management process will necessarily focus on higher levels of risk and areas of particular concern or sensitivity, and this will be the source of the regular reports to the Senior Management Committee and to the Council.

***

ANNEX 2

CONTEXT DOCUMENT

REQUIRED BY

THE RISK MANAGEMENT FRAMEWORK

OF THE

INTERNATIONAL MARITIME ORGANIZATION

CONTENTS

1 Introduction

1.1 Purpose of this document
1.2 Structure of this document

2 Objectives of risk management and the Organization's risk management policy

2.1 Introduction
2.2 Objectives of risk management
2.3 Connection to the Strategic Plan

3 Scope and focus of the risk management process

3.1 Introduction
3.2 Scope of the 2014-2015 risk management exercise
3.3 Key factors to consider

1 INTRODUCTION

1.1 Purpose of this document

At its 100th session, in June 2008, the Council approved the Organization's Risk Management Framework containing risk management definitions, the Organization's risk management policy, and a risk management process to be followed in identifying, managing and reporting on the risks to the Organization. At its 106th session in June 2011, the Council revised the Risk Management Framework[1].

The Council has further agreed that this Risk Management Framework should, in the first instance, be applied to the strategic directions and high-level actions[2] under the responsibility of the Secretary-General as well as the Secretariat's related key objectives for a biennium.

This context document, therefore, seeks to set out:

- the objectives of risk management; and
- the scope and focus of the 2014-2015 iteration of the risk management process.

1.2 Structure of this document

This document is structured as follows:

- Section 2 – Objectives of risk management and the risk management policy. This section briefly sets out the objectives of risk management, linking this directly to the Organization's approved risk management policy and to the trends, developments and challenges identified in its Strategic Plan; and
- Section 3 – Scope and focus of the risk management process. This section establishes the scope of the 2014-2015 iteration of the risk management process, and identifies key factors to consider during the process.

2 OBJECTIVES OF RISK MANAGEMENT AND THE ORGANIZATION'S RISK MANAGEMENT POLICY

2.1 Introduction

This section briefly sets out the objectives of risk management, linking this directly to the Organization's approved risk management policy and to the trends, developments and challenges identified in its Strategic Plan.

2.2 Objectives of risk management

The Organization's risk management policy, see annex 1, part B, paragraphs 1 to 7 of this document, establishes that:

[1] See annex 1 of this document.

[2] Strategic directions will be derived from the Organization's Strategic Plan and High-level Actions from the High-level Action Plan of the Organization and priorities for the 2014-2015 biennium, to be adopted by the twenty-eighth regular session of the Assembly.

"*The objective of the Organization's risk management policy is to minimize and/or prevent adverse consequences emanating from foreseeable risks to the achievement of its aims and objectives.*"

This statement identifies three key aspects of risk management, which should be considered when applying the risk management process:

- **minimize and/or prevent** – the Organization recognizes that not all risks are avoidable, nor, even where such risks are avoidable, is it always in the Organization'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 Organization's goal to eliminate risk, but to minimize and/or prevent its effects, noting also that paragraph 4 of the risk management policy, in addressing methodology, notes that:

  "*The Organization is committed to reducing risk to a level that is as low as reasonably practicable …*"

- **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 Organization seeks, through the establishment of a methodical approach to the identification and documentation of risk events, and through a more formalized horizon-scanning exercise to be conducted on a regular basis, to increase the Organization's institutional capability to foresee risk and, through the repeated experience of this process, to refine its skills in assessing the likelihood and impact of risk. The introduction of a formalized risk management process is a first step in building risk assessments into all of the Organization's work, and the Organization's ability in this regard will increase with each iteration of the risk management process; and

- **achievement of aims and objectives** – a risk is only relevant in the context of an objective on which it impacts and, for the Organization, the objectives are those set out in its Strategic Plan and High-level Action Plan. The degree to which the Strategic Plan and the High-level Action Plan fall within the scope of this iteration of the risk management process is established in more detail in the next Section of this document; however, it is an important principle that a risk which does not impact on achieving an objective of the Organization is not a risk to the Organization.

2.3 Connection to the Strategic Plan

The Organization's Strategic Plan and the related High-level Action Plan form a comprehensive view of its long-term plans and short-term objectives, and it is the achievement of these objectives which provide the context for the risk management process. Risk management in the Organization must, therefore, be constantly and explicitly linked to the Strategic Plan and the High-level Action Plan in two ways:

- **explicit link between risks and objectives** – as noted above, risks are only relevant in the context of their ability to impact on the achievement of objectives. Since the Strategic Plan and the High-level Action Plan define the Organization's objectives, all risk events and risks identified during the risk management process must be explicitly linked to one or more strategic directions and/or planned outputs[3]. The scope of this process is discussed further in section 3; and

- **provision of context for "horizon-scanning"** – it is a necessary part of any risk event identification exercise to consider not only short-term and immediate areas of risk, but also to look forward and identify the potential for future risk events arising from developments in the Organization's work and its relationship with its stakeholders. Such a long-sighted view has already been taken in developing the Strategic Plan and, in particular, through the identification of the trends, developments and challenges facing the Organization. The relevant section of the Strategic Plan provides essential background for any consideration of future risk events undertaken as a part of this risk management process.

3 SCOPE AND FOCUS OF THE RISK MANAGEMENT PROCESS

3.1 Introduction

This section establishes the scope of the 2014-2015 iteration of the risk management process, and identifies key factors to consider during the process.

3.2 Scope of the 2014-2015 risk management exercise

For the purposes of this iteration of the risk management process established in the Risk Management Framework, the Council has defined the scope as covering the strategic directions and high-level actions under the Secretary-General's responsibility, as well as the Secretariat's related divisional objectives for the 2014-2015 biennium[4].

To integrate it more closely with the Organization's existing management processes, the scope of this exercise will, therefore, be the risk events impacting on the delivery of the Secretariat's Divisional objectives for 2014-2015.

These naturally include the high-level actions and planned outputs, which are the direct responsibility of the Secretary-General, as well as the key support and delivery activities of the Secretariat, which may be outside those defined in the High-level Action Plan but which are a necessary part of delivering the strategic directions set out in the Strategic Plan.

[3] Planned outputs will be derived from the High-level Action Plan to be adopted by the twenty-eighth regular session of the Assembly.

[4] These will be found in the Divisional Business Plans to be annexed to the Secretary-General's proposal for Results-based Budget 2014-2015.

All Divisional objectives will be cross-referenced directly to the Strategic Plan, providing the necessary linkage identified in section 2.

3.3 Key factors to consider

Risk management is an iterative process and, in general, an important consideration when embarking on a particular iteration is the output of previous risk management iterations, key risks identified and necessary areas of focus.

Accordingly, when conducting the 2014-2015 iteration of the risk management process, Secretariat staff should be conscious of the risks inherent in the trends, developments and challenges identified in the Strategic Plan, the outcome and approved recommendations of earlier iterations, and also the key features of the broader risk environment in which the Organization is presently operating.

While some of the foregoing elements may have a deeper impact on the Organization's regulatory functions, the following 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 impact 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 Organization;

- **safety and security** – events over the past two 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 co-operation training events) may be severely affected by safety and security considerations, with consequential negative impact on programme delivery and the need for appropriate security training for staff, experts and consultants;

- **travel disruption** – due to extreme weather conditions or other factors such as airline strikes can have direct impacts 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 co-operation activities, be they organized by Headquarters or field staff or through delegation to other entities; and be represented at external meetings;

- **the impact of climate change** – an ongoing priority for the Organization's work to find appropriate solutions that will ensure the reduction or limitation of greenhouse gas emissions from international shipping, climate change is an area with a high public profile where there is a need to act, and be seen to act, in a timely and effective manner for the benefit of all of the Organization's stakeholders. Through the Organization's regulatory process, its impact is already being felt by the shipping industry and climate change certainly has the potential to be felt directly by the Organization's day-to-day operations – particularly in terms of their effect on the local environment and its relationship with staff and delegate health and well-being, but also, for example, because of continuing efforts, within the Organization, to comply with the objective of carbon neutrality throughout the United Nations system and, in the longer term, because of the risks to its Headquarters and field premises of rising sea levels; and

- **sustainable development** – the rise in global population and increased economic activity in the last decade has significantly increased pressure on the world's natural resources to a level that threatens sustainable development. Increasing global demand for energy with sudden rises in the price of the main energy sources have been prevalent, highlighting the global reliance on cheap energy to maintain the baseline operating costs for industry and the public sector and thereby current standards of living. In order to ensure sustainability, there is increased urgency in the search for new technology including alternative sources of energy, in particular non-fossil fuels, which will, in turn, have an effect on the work of IMO, from environmental concerns, through trading patterns, to ship design and technology.

***

ANNEX 3

DRAFT REVISED TERMS OF REFERENCE FOR THE COUNCIL RISK REVIEW, MANAGEMENT AND REPORTING WORKING GROUP

1 The Council Risk Review, Management and Reporting Working Group is a key part of the Organization's risk management and control framework, with a remit to provide an independent report to the Council on all matters related to risk and governance. It plays a companion role to the Ad Hoc Council Working Group on the Organization's Strategic Plan, but with a different focus.

2 Specifically, its remit is to:

.1 receive and review risk management reports submitted by the Secretary-General, following each biennial application of the risk management process, and make observations and recommendations to the Council, as appropriate, on:

.1 the key areas of risk;

.2 mitigating controls in place;

.3 development plans;

.4 responsibilities; and

.5 timescales;

.2 review, during the course of a biennium, interim reports submitted by the Secretary-General to the Council on any changes and actions taken, and make observations and recommendations to the Council, as appropriate, on:

.1 the present situation on all risk events determined to have an unacceptable level of risk, including information on mitigating controls and implementation status on selected treatments;

.2 information on all risk events which cannot be brought within tolerance because of resource constraints on risk mitigation options; and

.3 the implications of any significant changes to the risk environment;

.3 in general, monitor the effectiveness of the Risk Management Framework and recommend to the Council any changes which may be considered necessary; and

.4 consider how to apply the Risk Management Framework across all the elements of the Organization's Strategic Plan and High-level Action Plan, and the mechanism by which this might be achieved, taking into consideration the impact of the workload on the Secretariat as well as relevant discussions in the Council.