INTERNATIONAL MARITIME ORGANIZATION

IMO

E

COUNCIL
24th extraordinary session
Agenda item 3(b)

C/ES.24/3(b)
24 October 2007
Original: ENGLISH

STRATEGY AND PLANNING

(b) Risk Management

Note by the Secretary-General

SUMMARY

Executive summary:	This document reports on the outcome of the second session of the Council Working Group on Risk Review, Management and Reporting (CWGRM 2), held in the General Committee Room of Lloyd's Register, London, from 27 to 28 September 2007
Action to be taken:	Paragraph 4
Related documents:	C 98/D (paragraphs 3(b).1 to 3(b). 4), C 98/3(b)

Introduction

1 The Council, at its ninety-eighth session, in June 2007, considered the report of the first session of its Working Group on Risk Review, Management and Reporting (CWGRM) and, in particular, the draft Risk Management Framework prepared by the Group, which contained three elements: a definition of terms; a risk management policy; and an outline risk management process. The Council approved the definitions and the risk management policy, in principle, and instructed the Secretariat to further develop the risk management process for submission to, and consideration by, the second session of the Working Group.

2 The Council also approved the work programme for completion of the Risk Management Framework, which included a second session of the Group, in September 2007, to consider further the draft risk management process, followed by the reconvening of an Intersessional Correspondence Group to further develop that process prior to a third meeting of the Group, with a view to submitting the finalized Risk Management Framework to the Council's one hundredth session for approval.

3 The Working Group met for its second session on 27 to 28 September 2007, under the chairmanship of the Vice-Chairman of the Council, Mr. D. Ntuli (South Africa), and its report is set out at annex.

Action requested of the Council

4 The Council is invited to consider the outcome of the second session of its Working Group on Risk Review, Management and Reporting and, in particular, to:

.1 note the updated draft risk management process for the Organization, as set out at appendix 1 of the annex to this document;

.2 note the Working Group's future work programme, which was previously agreed by the Council, and, in particular:

.1 the terms of reference for the reconvened Intersessional Correspondence Group, to further develop the Risk Management Framework; and

.2 the proposed holding of the third session of the Working Group, possibly in April 2008, to finalize the Risk Management Framework;

.3 approve the report in general; and

.4 express appreciation to Lloyd's Register of Shipping for making available its General Committee Room for the meeting and for its generous hospitality throughout the session.

***

ANNEX

COUNCIL WORKING GROUP ON RISK REVIEW, MANAGEMENT AND REPORTING 27 to 28 September 2007

REPORT OF THE SECOND SESSION

GENERAL

1 The Council Working Group on Risk Review, Management and Reporting met from 27 to 28 September 2007 under the chairmanship of Mr. D. Ntuli (South Africa).

2 The meeting was attended by representatives from the following Member Governments:

AUSTRALIA
BAHAMAS
BELGIUM
BRAZIL
CHILE
DENMARK
FRANCE
GREECE
IRAN (ISLAMIC REPUBLIC OF)
ITALY
JAPAN
LIBERIA
MARSHALL ISLANDS
NETHERLANDS
NIGERIA
PANAMA
POLAND
RUSSIAN FEDERATION
SINGAPORE
SOUTH AFRICA
SPAIN
SWEDEN
TURKEY
UNITED KINGDOM
UNITED STATES

ADOPTION OF THE AGENDA

3 The Working Group adopted the agenda set out in document CWGRM 2/1, noting that, in line with the decisions of the ninety-eighth session of the Council on its future work programme, there was a single substantive item on the agenda for this session, namely the further development of the risk management process. In adopting the agenda, the Working Group also agreed that a record of decisions should be prepared by the Secretariat as the meeting progressed, with the final report of the session being compiled by the Secretariat, in consultation with the Chairman, after the session. This report includes those decisions agreed by the Working Group.

OUTCOME OF THE NINETY-EIGHTH SESSON OF THE COUNCIL

4 The Working Group noted the decisions of the ninety-eighth session of Council and the comments made by some delegations with regard to the definitions included in the draft Risk Management Framework. The Working Group noted that the definitions provided were working definitions and, whilst they may require minor updating in the future, agreed that no changes were required at present.

5 The Working Group expressed appreciation for the level of support and input to its work provided by the Council, and to all Member States for the level of interest and participation shown to date, whilst also encouraging participation in the future that is as broad as possible.

DEVELOPMENT OF A RISK MANAGEMENT PROCESS

General

6 The Working Group noted the two substantive documents received under this agenda item, namely a document prepared by the Secretariat, as instructed by the Council, which provided a draft risk management process, based on the outline developed by the first session of the Group (CWGRM 2/3) and a document submitted by the United Kingdom (CWGRM 2/3/1) which outlined further thoughts on the development of quantitative and qualitative risk assessments and of a risk appetite statement.

7 Following an introduction to both documents, the Group agreed to follow the structure of document CWGRM 2/3, whilst using the paper submitted by the United Kingdom to inform the discussion at each stage. The outcome of the Working Group's discussions, in the form of an updated risk management process, is attached as appendix 1 to this annex, while appendix 2, which sets out Terms of Reference for a reconvened Intersessional Correspondence Group, identifies the areas requiring particular focus and further development, prior to a third session of the Working Group.

Baseline concepts

8 There was a clear agreement from the Group that simplicity should be the principle underpinning the further development of the risk management process, with a recognition that, whilst there are many different approaches to risk management, the appropriate approach for the Organization's size and type should be guided by concerns of practicality and pragmatism in order to avoid an overly-complex risk management process becoming a diversion and a risk in itself. The Group, in particular, noted that the process would be iterative and that there would be the opportunity to use the feedback from the first iteration to further refine the process for the future.

9 The Working Group considered at some length the importance of the linkage between the risk management process and the Organization's Strategic Plan and High-level Action Plan (HLAP) and, as a consequence, the scope of the risk management exercise it was undertaking and the limits of the Organization's role within the overall chain of responsibility for maritime safety and security, the protection of the marine environment, the efficiency of shipping and legal matters related thereto. The Group recalled that the draft Risk Management Framework contained definitions of three high-level risk categories – namely, organizational status and effectiveness; financial; and operational – and noted that document CWGRM 2/3 had been based on a synthesis of the considerations of the first session of the Working Group, submissions to the earlier Intersessional Correspondence Group and publicly-available 'best practice' information. Consequently, it was primarily targeted at good 'corporate governance' and had been so developed by the Secretariat.

10 There was a clear understanding by the Group that this approach, subject to detailed consideration and any required improvements, would adequately address the Organization's financial and operational risks, but it was initially less clear how it might be applied to risks associated with organizational status and effectiveness.

11 In order to consider this point further, the Group discussed examples of what such operational status and effectiveness risks might be. As a starting point, it considered the risk event of a maritime accident, such as a ship sinking, it being further clarified that the risk event for the Organization, in this case, was not actually the ship sinking, but rather the ship sinking *because the Organization had failed in some way*. In very simple terms, this might happen in any of three ways, alone or in combination:

.1 the ship sinking because of a gap in the regulatory environment;

.2 the ship sinking because the regulatory environment, although complete, is not yet in force; or

.3 the ship sinking because the regulatory environment, although complete and in force, has not been effectively implemented and enforced.

12 To take the first scenario further, this might occur either because a relevant planned output on the Organization's HLAP was not produced, or because there was a gap in the HLAP itself. In terms of risk event and risk assessment structure this may lead to:

.1 a risk that the HLAP is incomplete in some specific respect; and

.2 the need for an assessment, for each planned output on the HLAP, of the risk to the Organization of an incident occurring because that output has not been produced (the result of which exercise may, in turn, lead towards some level of prioritization of the HLAP).

13 With regard to the second scenario, and with reference to Strategic Direction 2 in the Strategic Plan relating to global compliance with IMO instruments, performance indicator 2 (Entry into force) provides a list of those conventions adopted, but which have not yet entered into force. It would be possible, within the framework of the risk management process outlined in document CWGRM 2/3, to review this list and assess, for each convention, the impact and likelihood of an incident occurring because it had not yet come into force. The mitigations to address this gap could then be considered.

14 Finally, with regard to incidents arising where the regulatory environment is already complete and in force, the risks in question, as far as the Organization is concerned, may relate, for example, to the clarity of its implementation guidance and advice or the effectiveness of its technical co-operation programme in promoting global and uniform implementation and enforcement of IMO standards. Also as an example, if an incident relates to a Member State that has voluntarily submitted itself to audit under the Voluntary IMO Member State Audit Scheme, potentially, the risk may relate to the effectiveness of the work being done under the Scheme to identify non-conformities, observations and necessary corrective action. Such risks would then relate explicitly back to the achievement of the Strategic Directions set out in the Strategic Plan.

15 With this understanding of risks to organizational status and effectiveness in mind, and in particular the fact that perceived 'external' risks may be seen through the prism of the Organization's own actions or inactions and, consequently, fall within its responsibility to manage such actions, the Working Group agreed that such risks could be addressed following the same overall process as for financial and operational risks, but that there would necessarily be some differences in the details of the methodology, an issue which might be considered by the subsequent Intersessional Correspondence Group.

16 A consequence of this discussion was the Working Group's consideration of the role of other, external, stakeholders in the risk management process. The Group agreed that there was a clear need for external input to the process, particularly through the initial identification of risks, although, with the understanding of the organizational status and effectiveness risks outlined above, the Group considered that the role and responsibility of other stakeholders in managing such risks would inevitably be limited. The Working Group agreed to request that the Intersessional Correspondence Group address this matter in broad terms, that is, "the linkage of the risk management process with the Organization's Strategic Plan and High-level Action Plan", with the specific points discussed in mind.

Detailed discussion of documents

17 In considering documents CWGRM 2/3 and CWGRM 2/3/1 in detail, the Working Group examined each stage of the draft risk management process, namely: establishment of context; risk event identification; risk analysis; development of risk management options; risk treatment selection; implementation; and monitoring and review.

18 The Group began by clarifying that the 'Risk Management Context Document', to be produced from the first stage in the process, should be one with a broad audience, both within the Secretariat and amongst the Member States and other stakeholders, as appropriate, and emphasized its importance in setting the scene for all subsequent work.

19 The Working Group also considered the matter of 'inherent risk' and 'residual risk' and proposed amendments to the risk management process to clarify this, in order to focus on simplicity and practicability and in recognition of the difficulty in many situations of assessing the actual 'inherent risk' prior to considering existing controls. The Group also recognized, however, the importance of reviewing risk events themselves without considering existing controls wherever possible, in order to make an assessment of whether the existing controls were, in fact, excessive. The Working Group recognized that some associated amendments were required to the table under paragraph 8 of document CWGRM 2/3, setting out the required contents of a risk event table, and noted that, in order to assess the results of the work done to date on the development of the risk management process, a few completed examples, through the pilot use of that table, would have some value.

20 The Group also considered the question of the categorization of risk events and, in particular, how the three high-level risk event categories defined in the Risk Management Framework might be further sub-divided. The Group agreed that such sub-division would be required, possibly in the form of a 'risk tree' showing the hierarchical structure, and considered that this matter, along with any associated developments of the table under paragraph 8 of document CWGRM 2/3, should be referred to the subsequent Intersessional Correspondence Group for consideration.

21 Further, the Working Group, when considering possible methodologies for risk analysis, discussed a range of options available, based on the experience of the participants and broader good practice. The Group shared an understanding that whilst the process presented in document CWGRM 2/3 constituted a solid basis, further work would be required to refine the details of the methodology, beginning with a final view on whether a 3x3 or a 5x5 matrix to assess likelihood and impact appeared most appropriate for the Organization. Following on from this, the tables presented under paragraphs 18, 19 and 20 of the document would require detailed work to provide a common understanding of the terms in use during the analysis and provide comparability across the Organization. From their own experience, a number of members of the

Group raised the need to assess, for each risk event, the degree of confidence, or the degree of assumption, in the assessment itself, which adds another dimension to the risk analysis stage. The Working Group agreed that the subsequent Intersessional Correspondence Group would be the appropriate forum to deal with such matters of detail, taking the discussions in the Working Group as a starting point.

22 In considering the risk analysis methodology, the Group emphasized the role of the party responsible for managing the risk in making an initial assessment, prior to peer or expert review of that assessment, which was an approach used by many Group members in their own administrations. The Working Group also noted, in particular, the emphasis placed in document CWGRM 2/3/1 on risk tolerance and the detail provided in how a risk tolerance policy might be established. The Working Group invited comments for consideration by the Intersessional Correspondence Group on how such an approach might be integrated with the risk management process being developed.

23 The Working Group also considered whether the goal of the risk management process should be to capture all risk events, or simply to identify and capture the most significant risks facing the Organization. The Group concluded that while it was desirable to capture all risk events, those assessed at the lowest level of risk should be excluded from the main risk register and consequently receive a significantly lower level of consideration, improving the overall efficiency of the process. Risk events so excluded should, nevertheless, be adequately documented elsewhere.

24 Finally, the Working Group considered the mechanisms for monitoring and review, noting that this would likely run throughout the risk management process, rather than constituting a stand-alone exercise, and that this stage of the process would be crucial in determining how the Council might discharge its oversight responsibility for corporate governance. The Group emphasized that the risk management process was a tool to support the Council and the Secretary-General in discharging their responsibilities in this area and should not be so prescriptive as to hamper the effective operation of the Organization or the Secretariat in practice. The Group further considered that, whilst document CWGRM 2/3 provided a useful starting point from the point of view of monitoring and review, many participants would have much to share from their own experiences and, consequently, this stage of the process should be referred to the Intersessional Correspondence Group for further development, taking into account also that it would be subject to further review following implementation of the first iteration of the risk management process.

FUTURE WORK PROGRAMME

25 The Working Group noted that it had been charged, at this session, with developing the risk management process further, so that it might be subsequently progressed by the Intersessional Correspondence Group (as previously agreed by C 98), and that this task had been completed. Additionally, the Working Group had identified specific areas where the Intersessional Correspondence Group should focus its efforts, in order to improve the efficiency of its work.

26 With this in mind, the Working Group developed outline Terms of Reference for the Intersessional Correspondence Group, which were subsequently finalized by the Chairman, in conjunction with the Secretariat, and are attached as appendix 2 to this report. The Group reconfirmed the work programme to complete the Risk Management Framework developed by its first session and subsequently approved by the Council (document C 98/D, paragraph 3(b).3).

In this regard, the Working Group confirmed that a third session of the Group should be held in early April 2008, with a view to finalizing the Risk Management Framework for submission to the one hundredth session of the Council in June 2008.

27 The Working Group further requested that, in the meantime, the Secretariat produce some worked examples or pilot studies based on the preliminary risk management process attached at appendix 1 to this report, for consideration by the third session of the Group.

ANY OTHER BUSINESS

28 The Working Group formally thanked Lloyd's Register of Shipping for hosting the meeting and for the excellent facilities and generous hospitality provided throughout the session.

ACTION REQUESTED OF THE COUNCIL

29 The Council is invited to consider the outcome of the second session of its Working Group on Risk Review, Management and Reporting and to:

.1 note the updated draft risk management process for the Organization, as set out at appendix 1 of this report;

.2 note the Working Group's future work programme, which was previously agreed by the Council, and, in particular:

.1 the terms of reference for the reconvened Intersessional Correspondence Group, to further develop the Risk Management Framework; and

.2 the proposed holding of the third session of the Working Group, possibly in April 2008, to finalize the Risk Management Framework;

.3 approve the report in general; and

.4 express appreciation to Lloyd's Register of Shipping for hosting the meeting and for its generous hospitality throughout the session.

* * *

APPENDIX 1

DRAFT RISK MANAGEMENT PROCESS

Overview

1 As developed at its first session, the CWGRM prepared a draft risk management process for the Organization consisting of the following:

- 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 likelihood, using a methodology determined by the Council which may be qualitative, quantitative or a combination of both;

- 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, which may include risk avoidance, risk control, risk retention, risk financing and risk transfer, having regard for their suitability and cost effectiveness;

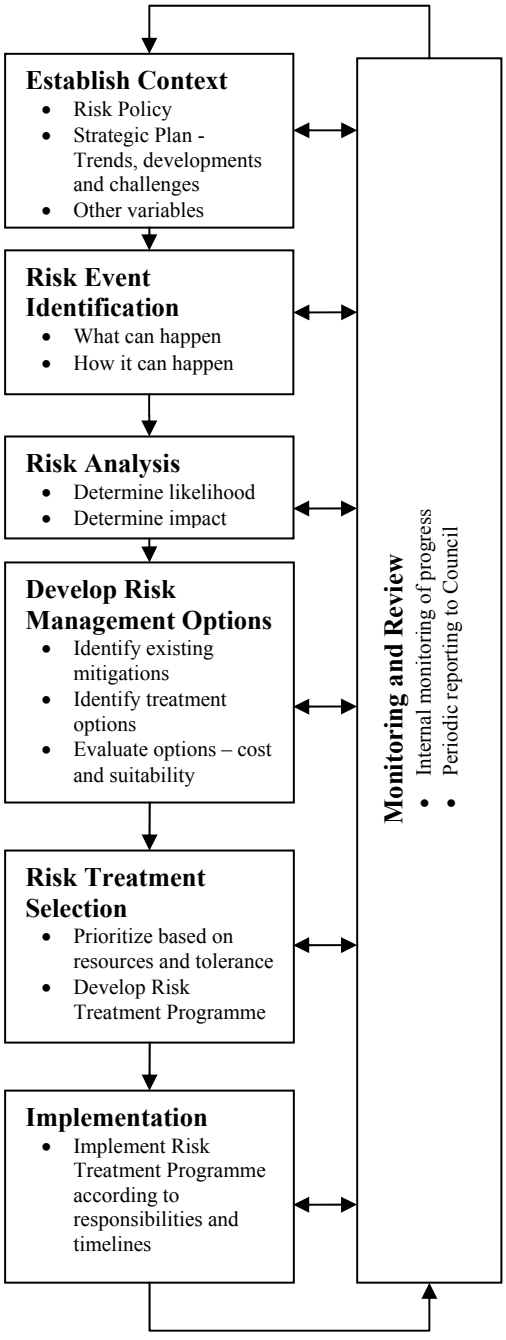
- Risk treatment selection – The Secretary-General will consolidate the risk management options for all identified risk events and prioritize them on the basis of the tolerance levels established by the Council and the available resources and develop a risk treatment programme indicating timelines, actions, 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 the establishment of context 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 defined by the Strategic Plan;
- areas of focus identified through previous risk management reviews, and changes in operational situation or strategic objectives.

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 and endorsed by the Assembly. 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 objectives. 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 the risk event identification exercise 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. An example format might be:

Risk Event Table	
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 objectives	*The strategic objectives potentially impacted by the risk event*
5. Stakeholders and responsibilities	*Those impacted by the risk event and those responsible for assessing and managing it*
6. Risk assessment	*An assessment of the residual risk, being the impact and likelihood of the risk event occurring before considering existing controls and mitigations*
7. Risk tolerance	*Objectives for control of the risk and desired level of residual risk, being the impact and likelihood of the risk event occurring after considering existing controls and mitigations*
8. 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*
9. Potential Action for Improvement	*Recommendations to optimize the risk*

10 At this stage, items 1 to 5 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 objectives of the Organization, by identifying specifically which objectives 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 exercise should result in a consolidated and dynamic list of risk events covering the Organization and its strategic objectives. 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 analysis is primarily an exercise in consolidating and structuring existing knowledge about potential risk events, including lessons learned from previous experience (see also paragraph 49), 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 exercise 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 Risk Management 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 exercise 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 event 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.

Risk analysis

Purpose:

14 The purpose of the risk analysis is to review each inherent risk event identified and arrive at an assessment of its importance to the Organization, based on a view of its likelihood and level of potential impact. For clarity, at this stage the assessment is on identifying the 'residual risk' of the risk event, that is, the risk after existing mitigating controls and other factors are taken into account.

Output:

15 The outcome of the risk analysis exercise will be an updated risk register, as shown in the table under paragraph 8 above, with the completion of item 6, the risk assessment. It will then be possible to rank risks based on their likelihood and impact, and consequently identify those areas where greatest focus is required. The degree of assumption in ranking likelihood and impact has to be considered.

Methodology:

16 The analysis of risk events to arrive at a view of the risk involved requires an assessment of the 'likelihood' 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 likelihood. With this in mind, a five-category approach provides further refinement, and greater scope for comparative ranking and assessment of risks.

18 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 inherent 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, as an example, indicative risk impact descriptions is shown below:

Impact	Financial Impact	Information	Political Impact	Occupational health & safety
1 – Negligible	<£20,000	Unclassified, routine policy information.	The embarrassment is restricted to within the Organization, the public remain unaware	Minor injuries to an individual
2 – Low	Between £20,001 and £100,000	In confidence information or personal information.	Industry and public made aware of 'embarrassment' through specialized media.	Injury of more than a minor nature but expected to be restricted to a single individual.
3 – Medium	Between £100,001 and £1,000,000	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 people
4 – Very High	Between £1,000,001 and £10,000,000	Member State or other UN body information which, if provided, would have substantial political or security implications for that country or 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 people
5 – Extreme	£10,000,001 or more	Information which, if provided to other parties, might have extreme security or political implications or other information that would threaten the ongoing operations of the IMO.	Widespread adverse publicity with calls for Secretary-General to resign or Organization to be reviewed.	Loss of life(s)

[source: Australia submission to Intersessional Correspondence Group, minor amendments]

19 Similarly, when assessing likelihood, it is important that there is a clear understanding of the timeframe in question and the meaning of the terms used. While the timeframe would typically be a year, in view of the biennial nature of the Organization, a standard period of two years might be more appropriate. For major projects which will run for in excess of two years, the appropriate period might be the anticipated life of the project, or the life of the project for which funding has been secured:

Likelihood	**Chance of occurring in timeframe**
A – Almost Certain	95%
B – Likely	75%
C – Moderate	50%
D – Unlikely	25%
E – Rare	5%

20 Combining the two then gives an inherent risk assessment as shown in the chart below:

Likelihood	1	2	3	4	5
A	2	3	4	5	5
B	2	2	3	4	5
C	1	2	3	4	5
D	1	1	2	3	4
E	1	1	2	2	3

Impact

Risk Assessment
1 = Low
2 = Moderate
3 = Significant
4 = High
5 = Severe

[Source: Australia submission to the Intersessional Correspondence Group]

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 11 (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.

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 objectives 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 'residual risk' of the risk event where this is higher than the level of risk tolerated. The possibility also exists that a particular risk or risks will be 'overcontrolled', 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 an updated risk register, as shown in the table under paragraph 8 above, with, for each risk event, the completion of item 7, the risk tolerance, and item 8, the risk treatment and control mechanisms. For each risk event where the 'residual risk' is presently outside of the tolerated risk levels, there will also be a number of documented options to address the risk, along with an assessment of their cost and their impact on the 'residual risk'.

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 identification exercise. In order to determine the effectiveness of controls, a

common technique is to re-assess the risk in terms of its likelihood and impact with the mitigations in place, thus giving the 'residual risk' level.

26 The second step is to determine the level of risk which can be tolerated in this particular instance. Risk tolerance will not be uniform across the Organization – certain areas of the operation, and certain strategic objectives 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 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 likelihood 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 residual risk.

28 The risk management options will typically follow one of four 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 likelihood 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 likelihood 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.

29 The overall aim of such options should be to bring the mitigated residual 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.

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

31 The level of analysis put in to the development of options should reflect the level of the residual risk. That is, for risks which are inherently 'low', 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 inherently 'low/negligible', requiring no mitigation, should not be included in the main risk register. For significant projects and for major risks and remaining residual risks, 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 response to all significant risks facing the Organization, with defined objectives that allow for future assessments of the implementation.

Output:

33 For the initial review of risks, the output of the risk treatment selection should be an Organization-wide risk response initiative 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 response initiative, that is, through the submission of costed proposals for consolidation, evaluation and prioritization against limited resources.

36 Whilst such a process will require central coordination, it will require the co-operation, participation or contribution of all stakeholders, including Member States, where appropriate, in order to ensure that the risk response initiative 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 response initiative is presented for approval.

Implementation

Purpose:

37 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:

38 The output of the implementation will be the new controls in place, and an updated risk register reflecting, for each risk event, the new situation in items 6 'Risk assessment' and 8 'Risk Treatment and Control Mechanisms' in the table under paragraph 8, along with a re-assessment of the residual risk. This will also be the output from any subsequent iterations of the risk management process.

39 There should also be a post-implementation review across the Organization to re-assess the Organization's overall risk exposure, identify areas with significant residual risk, identify lessons learned from the exercise and plan for coming iterations.

Methodology:

40 It is appropriate to use standard project management methodologies in the course of the implementation of the risk response initiative. 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 response initiative, 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 significant risks are given the appropriate priority. Feedback in the form of monitoring and review, and reporting to senior management and the Council, are a key part of the Organization's effective governance arrangements.

Output:

43 At the completion of the risk management exercise, there should be a summary report to senior management, 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 In between risk management exercises, the output of the monitoring and review should be a series of periodic reports to senior management or to the Council, as appropriate, covering changes and actions, in particular:

- the present situation on all risk events with an inherent risk of 'severe', including information on mitigating controls, implementation status on selected treatments, inherent and residual risk levels;

- the present situation on all risk events with a residual risk of 'significant' or above, 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 where the residual risk cannot be brought within tolerance because of resource constraints on risk mitigation options;

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

Methodology:

45 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.

46 There is no one model for managing the risk management process. In some organizations, responsibility remains decentralized, and each director is directly responsible for their own area. While this leads to clear ownership and responsibility for risk management, it can lead to a non-uniform approach, to the establishment of risk tolerances at a lower level, which do not match the needs of the organization, and to a lack of coordination in response to risk-related issues.

47 In contrast, a number of organizations assign responsibility for the risk management process to a central team. Whilst this is frequently necessary in order to manage a complex process while supporting consistency of approach and action and, in particular, to support consolidated reporting to a senior level, it is important that a central function is not seen as being 'responsible for risk', which must remain the responsibility of Member States and the specified operational staff.

48 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 senior management and to the Council. There is also a role for internal audit review of the process.

49 Monitoring should also include a process to identify ‘loss events’ with a material effect, review why they occurred, where the failure in the control mechanisms lies and how this situation might be remedied. This information should then be captured in the risk register, along with planned action to address weaknesses.

* * *

APPENDIX 2

INTERNATIONAL MARITIME ORGANIZATION

**Intersessional Correspondence Group
of the
Council Risk Review, Management and Reporting Working Group (CWGRM)**

Terms of reference

1 As agreed by the IMO Council, the Intersessional Correspondence Group is hereby reconvened "to develop further the Risk Management Framework" (document C 98/D, paragraph 3(b).3(iii)).

2 Specifically, the Intersessional Correspondence Group will:

.1 develop further the risk management process (document CWGRM 2/3 (Secretariat)), as reviewed and amended by the second session of the CWGRM (27 and 28 September 2007); and

.2 in so doing, consider the following topics in particular:

- the tables contained in the document;
- the desirability of IMO using a 3 or 5 category matrix for risk assessment;
- the sub-categorization of the high-level risk event categories;
- the desirability of including in the risk management process a more detailed consideration of risk appetite, taking into account document CWGRM 2/3/1 (United Kingdom);
- the methodology for monitoring and review; and
- the linkage of the risk management process with the Organization's Strategic Plan and High-level Action Plan.

3 The Intersessional Correspondence Group should submit its report to the Secretariat by 29 February 2008, providing the output of its work, for consideration by the third session of the CWGRM, which is tentatively scheduled for April 2008.

Note: For the Intersessional Correspondence Group's information, the Secretariat will, in the meantime, carry out a pilot project aimed at providing worked examples of the risk management process, based on the version of the document agreed by the second session of the CWGRM.