INTERNATIONAL MARITIME ORGANIZATION

E

COUNCIL
120th session
Agenda item 4

C 120/4
18 May 2018
Original: ENGLISH

STRATEGY, PLANNING AND REFORM

Risk Management Exercise for the 2018-2019 biennium

Note by the Secretary-General

SUMMARY

Executive summary:	This document reports on the outcome of the risk management exercise 2018-2019, carried out by the Secretariat, as well as a summary of the final assessment of the 2016-2017 exercise
Strategic direction, if applicable:	Other work
Output:	OW 26
Action to be taken:	Paragraph 38
Related documents:	C 113/3/3, C 113/D; C 116/4 and C 116/D

Introduction

1 The Secretariat carried out the 2018-2019 risk management exercise in accordance with the Risk Management Framework approved by the Council, at its 113th session (C 113/3/3) at the beginning of 2016. The 2018-2019 risk management exercise covers risk events potentially affecting the delivery of the Secretariat's Business Plan for the 2018-2019 biennium.

2 The purpose of the 2018-2019 exercise is to implement the agreed risk management process (C 113/3/3), taking into account lessons learned from the 2016-2017 risk management exercise, as well as the comments provided by Council at its 116th session (C 116/D) and to identify any issues or areas for further improvement.

3 The 2018-2019 exercise was conducted involving:

.1 a review of the risk events identified, analysed and reported on in the 2016-2017 exercise;

.2 a reassessment of the impact and probability of each risk event to further harmonize the risk assessment; and

.3 the application of the risk management process to the Secretariat's Divisional Business Plan for the 2018-2019 biennium, identifying possible new risk events.

Final assessment of the risk events identified in the 2016-2017 risk management exercise

4 The first phase of the biennial risk management exercise consisted of updating the 2016-2017 risk events in order to:

.1 identify developments that influenced the assessment of the risk events in 2017.[1] These developments mostly consisted of changes to the scope of the risk events or the introduction of additional risk controls;

.2 identify risk events that were no longer relevant because they have been overtaken by developments or successfully mitigated; and

.3 carry over the remaining 2016-2017 risk events to the 2018-2019 risk management exercise.

5 The 2016-2017 risk event exercise identified 26 risk events. At the end of 2017, six risk events were no longer relevant, as they were successfully mitigated or overtaken by events. Those risk events have strikethroughs in table 1 below and are:

.1 risk event 3 "absence of examples or best practice around the UN system on accounting for services-in-kind";

.2 risk event 10 "failure of ICT systems and ability to provide Helpdesk support";

.3 risk event 13 "failure to migrate to a new Library Management System (LMS)";

.4 risk event 17 "inadequate conduct, and absence, of performance appraisal of staff";

.5 risk event 19 "inadequate preparation for the implementation of the new ICSC compensation package"; and

.6 risk event 23 "lack of logistical and technical support to REMPEITC".

6 Of the 26 risk events, 3 risk events did occur during 2017. Those risk events are highlighted in bold in table 1 below and are the following:

.1 risk event 16 "inability to attract staff";

.2 risk event 17 "inadequate internal justice system"; and

.3 risk event 20 "delays in the implementation or cancellation of planned technical cooperation activities".

[1] A similar exercise of updating the 2016-2017 risk events was conducted at the beginning of 2017, capturing the developments in 2016. Those developments were reported to the Senior Management Committee.

7 In addition, the assessment of two risk events was adjusted. The impact of risk events 1 "Budget shortfall" was reduced from 5 to 4 and the overall assessment of risk event 7 "ICT meeting support" was increased, as discussed by the Senior Management Committee (SMC) of the Secretariat last year, to match risk event 4 "IMO meeting support" (the newly assessed risk events are underlined in the matrix below).

8 At the end of 2017, the risk events were therefore distributed across the following risk levels of the risk matrix:

	Impact	Very Low	Low	Medium	High	Very High
Probability		1	2	3	4	5
Very High	5			4 consequences of Brexit (added in 2017)		
High	4					
Medium	3		~~17 Staff appraisal~~ 22 GBS implementation ~~23 REMPEITC support~~	2 Treasury placements ~~10 ICT system/support~~ 12 SI/AV equipment 24 GESAMP support		
Low	2		~~3 Services-in-kind~~ 8 Bravery award nomination 9 NGO/IGO participation **18 Internal justice system**	~~13 LMS migration~~ 14 SAP system 15 Staff absence (to be renamed "succession planning") **20 TC implementation** 21 TC funding 25 IMSAS implementation	1 Budget shortfall 5 IMO meeting support 7 ICT meeting support ~~19 ICSC compensation package implementation~~	
Very Low	1			11 ICT upgrades **16 Attracting staff**	6 IMO meeting participation	26 HQ safety/ security

Table 1: End of 2017 Risk Matrix, all risk events

9 The 26 risk events are categorized in seven risk categories based on their characteristics. The major developments in these seven risk categories are presented below.

RISK CATEGORY 1: Finance and budget

10 A major risk event that did occur, was the possible "**shortfall of the approved budgets for outputs" (risk event 1)** owing to lack of sufficient financial resources. In 2017, for the regular budget, the exchange rate loss was absorbed by using the Working Capital Fund (WCF) in accordance with the relevant Assembly resolution. As an additional control, a measure is in place to absorb exchange rate fluctuations in the Working Capital Fund, and to use a Special Contingency Account within the General Fund to absorb staff cost increases. Where additional funds are required, the Council is informed and a funding source proposed.

11 **Risk event 2 "inappropriate treasury placements or lack of capital to invest"** did not occur, but remains relevant. In 2017, the timely and regular monitoring of collection of Member States assessments and enhanced cash management process, particularly cash inflows and outflows forecasting, were improved.

12 **Risk event 2 "absence of examples or best practice around the UN system on accounting for services in kind"** was successfully mitigated and is no longer relevant. IMO implemented a process for services in kind during the 2016-2017 biennium.

13 A new risk event, **risk event 4 "consequences of Brexit"** was added to this risk category, as the United Kingdom exit from the European Union ("Brexit") has caused significant exchange-rate volatility and general economic uncertainty, leading to unpredictable movements in interest rates/inflation, as well as uncertainty for European Union citizens residing in the United Kingdom. Controls for this risk event are already in place. To mitigate the risk event, as per the Organization's financial rules and regulations, a reserve fund of £2 million is allocated both in the Working Capital Fund and the Special Contingency Fund.

RISK CATEGORY 2: Organization, preparation, running and support of IMO meetings

14 The "**timely organization, preparation, running and support of IMO meetings" (including ICT services) (risk events 5, 6, 7 and 9)** did not occur and are sufficiently mitigated.

15 With regard to **risk event 7 "unavailability of ICT services during meetings"**, additional measures were implemented to further mitigate the risk event. In particular, the Local Area Network (LAN) and Wi-Fi infrastructure were updated. The updates include the replacement of core and edge switches and wireless access points to cover all areas of the Secretariat in a more secured way. Firewalls and mobile device management systems were enhanced for improved security from cyber-attacks. Servers and desktop software were updated to the latest versions and patch levels. The telephone system was changed to a Unified Communication System for improved productivity and more secure communication with Member States and stakeholders. IMOWeb accounts, a secure mechanism for accessing IMO web resources by Member States, was enhanced for a more secure access to IMODOCS, GISIS and OMRS.

16 **Risk event 8 "failure to receive nominations for the IMO Award for Exceptional Bravery at Sea"** did not occur, but additional control measures were implemented, in particular promotional material that is being displayed at IMO headquarters.

RISK CATEGORY 3: ICT and SAP systems and services

17 The risk event **"failure of ICT systems and ability to provide Helpdesk support" (risk event 10)** was mitigated and is no longer relevant. The **"inability to implement the progressive upgrade/enhancement plans for ICT" (risk event 11)** did not occur and existing controls have been retained to mitigate the risk event.

18 With regard to **risk event 12 "failure of SI/AV equipment"**, the risk event was further mitigated by implementing additional controls. In 2017, the new equipment was continuously subject to statutory warranty provided by the installer and a high-level service agreement is in place. In addition, a support maintenance contract has been awarded to the existing providers.

19 The risk event associated with the implementation of a new "**Library Management System" (risk event 13)** is no longer relevant, as the implementation process was finalized in 2016.

20 With regard to **risk event 14 "SAP system failure, system design faults and inadequate SAP support**", in 2017, the SAP Quality Assurance service was employed to ensure the implementation of the ICSC compensation package project and setting up of a project steering group for the ICSC project to ensure the required direction, guidance and support was provided for the successful completion of the project.

RISK CATEGORY 4: Human resource measures

21 The risk events "**sudden absences of staff members"** and **"inability to attract new staff members" (risk events 15 and 16)** did not occur and existing controls have been retained to mitigate the risk events.

22 With regard to the **"inadequate conduct, and absence, of performance appraisal of staff" (risk event 17)** , as a new policy and new procedures are being developed in order to facilitate the process therefore increasing compliance levels, this risk event has been overtaken by developments and is no longer relevant.

23 Concerning **risk event 18 "inadequate internal justice system"**, the risk events occurred, as some procedural discrepancies were identified in a recent tribunal case. The risk event was further mitigated through the introduction of "lesson learned" sessions and documents after each case in order to constantly improve the quality of handling appeals and tribunal cases.

24 **Risk event 19 "inadequate preparation for the Implementation of the New ICSC Compensation Package approved by the UNGA"**, was no longer relevant as the new ICSC compensation package was implemented successfully.

RISK CATEGORY 5: Planning and delivery of technical cooperation activities

25 The risk event "**delays in the implementation or cancellation of activities" (risk event 20)** occurred as activities were postponed or cancelled mainly at the request of the host country. This risk was mitigated by reassigning the funds to other activities as well as continued communication with the recipient countries, donors and partners. The risk event "**lack of sufficient funding for planned activities" (risk event 21)** did not occur, nevertheless, the depreciation of the GBP significantly reduced the available funding for the delivery of planned outputs.

RISK CATEGORY 6: Delivery of IMO initiatives

26 **Risk event 22 "delays in the delivery of the Secretariat's obligations under the Goal Based Standards (GBS)" (risk event 22)"**, did not occur and the existing controls have been retained.

27 **Risk event 23 "lack of logistical and technical support to the Regional Marine Pollution Emergency, Information and Training Centre (REMPEITC)"** is no longer relevant, as it was successfully mitigated. IMO, UNEP and the United States Coast Guard consultant have undertaken different measures to secure the staffing of the Centre and therefore guarantee its continuity. This includes facilitating an agreement between the Centre and the Government of Jamaica to deploy a secondee, establishing an agreement with the Oil and Gas Industry to provide a consultant and to request assistance from the Government of Curacao, which has now agreed to fund the positions of Director and of Operations Manager, in addition to securing funding for additional posts for the 2018-2019 biennium. In light of these events, the United States Coast Guard has decided to continue its support for the Centre through the continuation of the provision of secondees.

28 With regard to **risk event 24 "lack of coordination and support of all the GESAMP activities"**, the risk event did not occur, however to further mitigate the risk event, meetings with relevant donors and stakeholders to provide longer term funding support to activities of GESAMP took place.

29 **Risk event 25 "implementation of the audit programme under the IMO Member State Audit Scheme (IMSAS)"** did not occur and existing controls have been retained to mitigate the risk events.

RISK CATEGORY 7: Safety and security at IMO Headquarters

30 The risk of **"health, security and safety incidents at IMO HQ" (risk event 26)** remains sufficiently mitigated.

End-of biennium analysis

31 At the end of the biennium, a final assessment of the risk events was conducted to assess the final status of each risk event and to identify if the risk events that remained would be relevant for the next biennium. This end-of-biennium assessment has shown that 17 of the 26 risk events did not occur due to a successful mitigation, but remain relevant. Three risk events occurred and remain relevant. Six risk events are no longer relevant due to mitigation or because they have been overtaken by developments. Following the final assessment, 20 of the 26 risk event have been carried over to the 2018-2019 biennium.

2018-2019 Risk Management Exercise

32 Following the finalization of the 2017 assessment of the risk events, potential changes to improve the risks event coverage as well as the assessment (changes in impact or probability) of risk events were considered in a meeting with the risk management focal points, taking into account comments made during C 116 and senior management in 2017, when the risk events were last presented, as well as the development of the new divisional business plans for the 2018-2019 biennium.

33 In addition, it was decided to separate risk event 26 "HQ safety/security" into two risk events, as while safety is a stable risk mitigated mainly by an insurance, the risk on security might change more often depending on the security situation in the United Kingdom.

34 Besides, the specific risk on the long-term funding agreement for the Organization's ASHI liabilities has been added. MED also proposed the addition of a risk event on the major projects, while MSD added a new risk on the delay of the Secretariat in responding to issues related to LRIT provisions.

35 In addition, considerations on new risk events, mainly concerned with the implementation of internal processes, resulted in the proposal of the following new risk events that should be added to the already existing Secretariat-wide risk events (e.g. meeting support, implementation of TC activities etc.):

.1 inadequate information and knowledge management;

.2 sharing of confidential information; and

.3 lack of compliance with the Organization's policies.

36 The results of the 2017 risk management assessment and the discussion of the focal points and divisions resulted in the following risk events and risk levels on the risk matrix (new risk events are marked bold):

	Impact	Very Low	Low	Medium	High	Very High
Probability		1	2	3	4	5
Very High	5			4 Consequences of Brexit		
High	4					
Medium	3			2 Treasury placements 11 SI/AV equipment **15 Policy compliance** 24 GESAMP support	**13 Knowledge management** **22 LRIT**	
Low	2		8 Bravery award nomination 18 Internal justice system	12 SAP system 16 Succession planning 19 TC implementation 20 TC funding 21 GBS implementation **23 Major projects** 25 IMSAS implementation	1 Budget shortfall 5 IMO meeting support 7 ICT meeting support **14 Sharing of confidential information**	**3 ASHI liability**
Very Low	1		9 NGO/IGO participation	10 ICT upgrades 17 Attracting/ retaining staff	6 IMO meeting participation	26 HQ safety 27 HQ security

Table 2: 2018 Risk Matrix, all risk events

37 The 27 risk events are distributed across the risk matrix as follows: 8 risk events are of a small risk level, 16 risk events are of a moderate risk level, 3 risk events are of a significant risk level and no risk event is of a critical risk level. The 27 risk events are grouped in eight risk categories based on their characteristics and a detailed description of all risk events for the 2018-2019 risk management exercise can be found in the annex.

Action requested of the Council

38 The Council is requested to note the report on the outcome of the risk management exercise.

***

ANNEX

2018-2019 SECRETARIAT RISK MANAGEMENT EXERCISE

Risk event tables

Contents

1. Finance and budget

1. Risk event identification	
Name of risk event	Shortfall on the approved budget for outputs
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 13 & BP 14
Stakeholders and Responsibilities	
Internal and external stakeholders	Secretariat; Member States
Entity responsible	Administrative Division
Scope of risk event	
Qualitative description	Biennial budgets are approved by the Assembly. If external factors assumed in the budget formulation deviate greatly, then there is a risk of incurring overruns in the approved budgets; and the associated programmes may not be fully delivered as planned
Trigger of risk event	Higher UK inflation; unexpected changes in the cost-of-living index for London; changes in pay scales and benefits; significant currency fluctuations; adoption of additional work programmes
Nature of Risk Event	
Organizational	Damage to the Organization's reputation
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements)
Qualitative description of risk event outcome	The risk event outcome would be partial delivery, or non-delivery, of the programmes planned or mandated
Risk Controls	
Detailed description of current controls	Budget allotment notices by the Secretary-General and the budget release and availability check control in the SAP system. Close monitoring of the income and expenditure status and regular reporting to the management
Level of confidence in present control	Low
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	4
Probability	2
Assessment	7
Development of risk management options	
Risk tolerance level	Low – risk is not tolerable at the assessed risk level without further mitigating actions being implemented

Additional risk treatment and control mechanisms	Strengthen budgetary control procedures, provide monitoring advice at all levels of the organization, and devise strategies and policies, including austerity measures, to mitigate budgetary risks. If overruns are incurred by unexpected pay rises over and above the assumed increases reflected in the approved budget, the required additional funds can be secured from the Special Contingency Account. For other overruns, resource requirements should be justified with expected results, which are linked to outputs to be delivered and actual performance in achieving such results is measured by predefined performance indicators.

2. Risk event identification	
Name of risk event	Inappropriate treasury placements or lack of capital to invest
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 11
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States
Entity responsible	Administrative Division
Scope of risk event	
Qualitative description	One or more monthly treasury placements agreed by the Treasury Committee fails to correctly balance capital retention with the need to generate an investment return in line with DBP targets and the need to have sufficient cash balance to meet cash requirements during the same period of placement, either by investing for too long with a risky counterparty and suffering capital loss or through excessive caution in a desire to maintain capital and so failing to generate an adequate revenue stream.
Trigger of risk event	Urgent or unexpected payments of substantial amount were required during the period of placement and expected revenue from MS contributions was not received on time and one or more of the counterparties is suffering financial problem.
Nature of risk event	
Organizational	Not applicable
Financial	Unfunded or inadequately funded commitments
Operational	Not applicable
Qualitative description of risk event outcome	Cash on hand insufficient to meet payment needs, loss of funds through investment in appropriate counterparty, or failure to meet performance targets
Risk controls	
Detailed description of current controls	There is a robust process in place for informing and reminding Member States of their outstanding contributions through direct communication and regular Council documents. Further, there are sanctions in place for late payees under Article 61 of the IMO Convention, and early payment is incentivized through the Contributions Incentive Scheme. The Organization has a Treasury Policy which defines the amount and duration of any placements which can be made depending on the credit rating of the counterparty, and the Treasury Committee is charged with ensuring that any agreed investments are in line with the policy. All investment placements are reviewed monthly, and the Treasury Committee includes an external financial advisor who comments on counterparties and more general financial matters. The performance targets set in the DBPs are deliberately conservative to avoid creating a situation where significantly riskier investments are required.
Level of confidence in present control	High

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	3
Assessment	6
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Treasury Committee should monitor performance against target on a quarterly basis and advise of any requirements to change the Organization's investment policy should that be necessary

3. Risk event identification	
Name of risk event	No long-term funding agreement for the Organization's After Service Health Insurance (ASHI) liability
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 17
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States
Entity responsible	Administrative Division
Scope of risk event	
Qualitative description	The Organization's ASHI liability has increased from £21m in 2010 to over £40m in 2017, and while there have been 2 one-off transfers of funds, there is no long-term funding mechanism in place. The Secretariat will submit proposals for the Council's consideration during 2018, for inclusion in the 2020-21 results-based budget.
Trigger of risk event	Council consideration of Secretariat funding proposals
Nature of risk event	
Organizational	Not applicable
Financial	Unfunded or inadequately funded commitments
Operational	Not applicable
Qualitative description of risk event outcome	As the ASHI liability continues to increase, a larger proportion of the annual budget will be taken up with its funding, unless a long-term solution is found
Risk controls	
Detailed description of current controls	The ASHI liability is monitored and reported in the annual financial statements, and funded on a pay-as-you-go basis
Level of confidence in present control	Low

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	5
Probability	2
Assessment	7
Development of risk management options	
Risk tolerance level	Low tolerance level indicates that the risk is not tolerable at the assessed risk level without further mitigating actions being implemented directly
Additional risk treatment and control mechanisms	Funding proposals to be presented to the Council during the current biennium

4. New risk event: Risk event identification	
Name of risk event	Consequences of "Brexit"
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 13 & BP 14
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States
Entity responsible	Administrative Division
Scope of Risk Event	
Qualitative description	UK exit from the European Union ("Brexit") causes (has already caused) significant exchange-rate volatility and general economic uncertainty, leading to unpredictable movements in interest rates/inflation, as well as difficulties for EU citizens residing in the UK
Trigger of risk event	Referendum of 23 June 2016
Nature of risk event	
Organizational	Capital available for major programmes
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements)
Qualitative description of risk event outcome	Consequences for IMO Secretariat may include higher USD costs, lower investment returns, difficulty recruiting/retaining EU staff (GS), enforced changes in banking arrangements. Consequences for Member States, in addition to the above, may include (for some) a reduction in the real cost of the assessment
Risk controls	
Detailed description of current controls	In general, funds are held in currency in which expenditure will be incurred (especially USD). There are some exceptions (notably UNJSPF contributions, TC Fund budget, some projects)
Level of confidence in present control	Moderate

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	5
Assessment	8
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	Updated investment policy, careful budgeting of non-GBP expenditures. Close liaison with the host government to minimize the impact for IMO staff and/or any impact for delegates of any new visa/border arrangements

2. Organization, preparation, running and support of IMO meetings

5. Risk event identification	
Name of risk event	Delays in the organization, preparation, support and running of IMO meetings
Strategic directions potentially impacted	All SDs
Secretariat's business plan output potentially impacted	BP 01 of all divisions
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs; public; industry, including seafarers
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Non-delivery or delay in preparing meetings and other meeting requirements, including documents (formal submissions, briefs, working papers, reports, IMO instruments, guidelines, circulars etc.) in a timely manner or inability to provide logistics services (conference rooms/facilities, audio/video, registration, interpretation services etc.)
Trigger of risk event	Lack of coordination, staff shortage or inadequate resources (due to budgetary restrictions or lack of supply) within the Secretariat; non-compliance with the guidelines of the organization and methods of work of the various IMO organs; Breakdown or non-availability of equipment and/or rooms due to technical problems or damages
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Information/business reporting (budgeting and planning, accounting information, pension funds, After Service Health Insurance liability, investment evaluation); Business continuity, Empowerment (leadership, change readiness)
Qualitative description of risk event outcome	Meetings cannot be organized and managed successfully in accordance with the IMO programme of meetings, relevant rules of procedures and IMO guidelines which in turn could lead to the failure to deliver the outputs in the Strategic Plan. Inadequate support and services to IMO meetings could result in non-delivery or delay in the preparation of meeting documentation, the management of the meeting itself and report writing in cooperation with documents and translation sections. This could mean that important decisions affecting, in particular, budget, finance, HR and ICT management issues might need to be postponed affecting the Secretariat's operations.
Risk controls	
Detailed description of current controls	With regard to the budgetary planning of the meeting programme, effective management and control mechanisms have been established with coordination at the internal level of the Conference Division and with other IMO Divisions, in particular with the Administrative Division/Financial Services. Monthly analysis of statistics and thorough consultation exercises are being undertaken in the preparation of budgetary proposals. Additionally, coordination meetings with technical divisions and preparatory meetings with internal staff in the CD Division take place regularly. With regard to the preparation of documents, deadlines are established for all relevant meeting documentation and monitoring is in place.

	With regard to the provision of meeting services, regular maintenance patterns have been introduced and plans have been drawn up well in advance and confirmed at the earliest possible opportunity to better utilize existing human resource. With regard to the provision of interpretation services, efforts to expand the pool of qualified interpreters are being made, occasional support is sourced from the Translation Services.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	4
Probability	2
Assessment	6
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	Continuous good communication among the stakeholders and effective budgetary planning, management and control mechanisms. Close monitoring and modernization of document processes, agenda prioritization and exact time management. Continued development of the Document Management System and SAP reporting capabilities which will improve reporting systems. Installation of new equipment to ensure sufficient back-up. Implementation of efficiency measures. Greater use of technology (PaperSmart meetings) in day to day practices. Introduction of formal training for all staff from technical divisions who are responsible for preparing IMO documentation to ensure that good IMO standard practice is achieved. Adjustments in the meeting agenda to ensure critical agenda items are completed without delay allowing full interpretation of the discussion.

6. Risk event identification	
Name of risk event	Inadequate participation in IMO meetings/ conferences
Strategic directions potentially impacted	All SDs
Secretariat's business plan output potentially impacted	BP 01 of all divisions
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs; public; industry, including seafarers
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Disruption/ cancellation of IMO meetings/conferences or the failure to achieve an adequate participation due to the absence of relevant delegates

Trigger of risk event	Significant disruption of international travel e.g. due to natural disaster, terrorist threats or major outbreak of infectious diseases as well as measures taken by Governments and the Organization due to safety, security or health considerations, leading to decisions by delegations to not participate in certain IMO meetings
Nature of risk event	
Organizational	Damage to the Organization's reputation; Regionalization or unilaterism in the regulation of shipping; Public perception
Financial	Budget management and control
Operational	Business continuity
Qualitative description of risk event outcome	Delegates might not be able to get to the IMO HQ which might lead to disruption/ cancellation of IMO meetings. This may disrupt the IMO Meeting Programme and delay important decisions by the IMO organs affected.
Risk controls	
Detailed description of current controls	The Secretariat monitors relevant information regarding the outbreak of infectious diseases, especially from WHO and the UK Government's authorities, as well as information from other sources related to disruption of international travel. In the event of an incident, a deadline would be established for cancelling the meeting in question.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	4
Probability	1
Assessment	5
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Contingency plans should be developed to address the possibility of IMO having to cancel a programmed meeting shortly before its scheduled start. Should the specified incidents occur more often, alternative means of ensuring participation by delegates affected will need to be explored, i.e. technologies for remote participation.

7. Risk event identification	
Name of risk event	Unavailability of ICT services during Meetings
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 01
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; NGOs and IGOs
Entity responsible	Administrative Division

Scope of risk event	
Qualitative description	Risk event affects the ability of the Secretariat to successfully conduct a meeting (including disruptions of translation/word processing work, the distribution of documents through IMODOCS and provision of terminology/referencing work), and of the Organization to deliver its work regulatory programme
Trigger of risk event	Failure of network or other computing systems
Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Not applicable
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Information technology (relevance, availability, stability); Business continuity
Qualitative description of risk event outcome	Failure of IMO bodies to successfully conclude their work in a timely manner
Risk controls	
Detailed description of current controls	Reliable provision of sufficient hardware systems including redundant setup. Upgrade and enhancement of IT systems, ensuring more robust backup, greater capacity, speedier response to emergencies and adequate level of helpdesk support
Level of confidence in present control	High
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	4
Probability	2
Assessment	6
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Ensure back-up systems are in place to minimize risks. Ensure the presence of an IT officer on site. Additional controls can be developed and introduced following examination of reasons for disruptions and success, or weaknesses, of existing controls in resolving observed problems.

8. Risk event identification	
Name of risk event	Failure to receive nominations for the IMO Award for Exceptional Bravery at Sea
Strategic directions potentially impacted	All SDs
Secretariat's business plan output potentially impacted	LED BP 01 & BP 02

Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; NGOs and IGOs
Entity responsible	Legal Affairs and External Relations Division
Scope of risk event	
Qualitative description	Failure to receive nominations, or nominations that are worthy of the Award, by the deadline would seriously jeopardize the annual exercise and the longevity of the Award scheme itself
Trigger of risk event	Failure to receive nominations
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception
Financial	Not applicable
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Business continuity
Qualitative description of risk event outcome	Possible development of solutions on national or regional level, which would be undermining the Organization's authority. Increased scrutiny by Member States if the Secretariat is not able to deliver the agreed outputs, possibly leading to less effectiveness and initiatives elsewhere.
Risk controls	
Detailed description of current controls	1. Display of pull-ups calling for nominations in the IMO building (lobby, Main Hall and restaurant). 2. Preparation of an electronic flyer in the three official working languages with links to the Awards guidelines and the nomination form to provide quick access to the relevant information. The electronic flyer has been shared in social media, uploaded on the IMO website and emailed to IMO Member States, IGOs and NGOs. 3. Display of a "calling for nominations" PowerPoint slide on the screens of the Main Hall before the start of IMO meetings and during coffee breaks. 4. Drafting of a few paragraphs to be included in the Secretary-General's opening briefs for the following meetings: PPR 5, NCSR 4, SSE 5 and MEPC 72. 5. Online survey for delegates (Member States, IGOs and NGOs) to identify core issues within the nomination process that might hinder the submission of nominations.
Level of confidence in present control	High
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	2
Probability	2
Assessment	4

Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Further to the results of the above-mentioned online survey, and pending approval, the following measures are being considered to be implemented in 2018 or 2019: 1. Find new opportunities to promote the Award on social media and online advertising in maritime e-magazines. 2. Enclose a list of all the previous recipients of the Award with the usual circular letter inviting nominations for the Award. 3. Enclose the nomination form of the last Award winner with the above-mentioned circular letter. 4. Explore options to create an online form in order to facilitate the submission of nominations.

9. Risk event identification	
Name of risk event	Provision of inaccurate/incomplete information on the participation of NGOs in consultative status in IMO meetings
Strategic directions potentially impacted	All SDs
Secretariat's business plan output potentially impacted	LED BP 02 & BP 03
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs
Entity responsible	Legal Affairs and External Relations Division
Scope of risk event	
Qualitative description	The Council has to review periodically (once every two years) the contribution to IMO's work of non-governmental organizations in consultative status, in part on the basis of their attendance at and submission of documents to IMO meetings
Trigger of risk event	The information may be inaccurate because complete information is not available and/or human error when compiling the data
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception
Financial	Not applicable
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Information technology (relevance, availability, stability); Business continuity
Qualitative description of risk event outcome	Decreased trust by Member States in the Secretariat's work and perceiving it as unable to deliver, possibly leading to increased scrutiny on initiatives elsewhere

Risk controls	
Detailed description of current controls	A manual system is in place to record NGO participation in IMO's work, with double-checking
Level of confidence in present control	High
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	2
Probability	1
Assessment	3
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Potentially improve the information recording system by designing a computerized system linked to the registration and IMODOCS databases

3. ICT and SAP systems and services

10. Risk event identification	
Name of risk event	Inability to implement the progressive upgrade/enhancement plans for ICT
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 18, BP 19 & BP 20
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; Public
Entity responsible	Administrative Division
Scope of Risk Event	
Qualitative description	Risk event affects the ability to ensure that the computing capabilities of the Secretariat remain fit for purpose
Trigger of risk event	Changes in funding decisions
Nature of Risk Event	
Organizational	Failure to keep pace with technological innovation
Financial	Unfunded or inadequately funded commitments
Operational	Information technology (relevance, availability, stability)
Qualitative description of risk event outcome	Aging hardware facilities will result in deteriorating services for all users, in turn resulting in slower computer facilities and more frequent errors and failures
Risk Controls	
Detailed description of current controls	Good understanding at high level of the Secretariat of the need for adequate computing facilities. Enhancement/upgrade of ICT infrastructure and update of licenses. Operating an Information Security Management System (ISMS) and obtaining ISO 27001 Certification in Oct 2015.
Level of confidence in present control	High
Risk Analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	1
Assessment	4
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Adequate funding needs to be in place for regular upgrade and enhancement plans with prioritized and phased investments for these purposes

11. Risk event identification	
Name of risk event	Failure of SI/AV equipment
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	CD BP 01
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs
Entity responsible	Conference Division
Scope of risk event	
Qualitative description	Inability to be able to provide interpretation and audio/video services including recording of meeting proceedings
Trigger of risk event	Any failure of SI/AV equipment
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception
Financial	Unfunded or inadequately funded commitments
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements)
Qualitative description of risk event outcome	Meetings are disrupted or suspended because of the failure of SI/AV equipment. No recording of the proceedings can be made as required. Loss of outcome reporting facilities for meetings.
Risk controls	
Detailed description of current controls	Frequent checks and maintenance visits. Prompt solution to any identified problem. Provision of required stock of spare parts on site. The sound system in the Main Hall was replaced in the second half of 2015 and the sound systems in CRs 9 & 10 in summer of 2016.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	3
Assessment	6
Development of risk management options	
Risk tolerance level	Low – risk is not tolerable at the assessed risk level without further mitigating actions being implemented
Additional risk treatment and control mechanisms	Timely consultation with maintenance contractors and repair and/or replacement of the faulty parts. Increased periodic checks and enhanced maintenance level

12. Risk event identification	
Name of risk event	SAP System Failure, System Design Faults and Inadequate SAP Support
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 16
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States
Entity responsible	Administrative Division
Scope of risk event	
Qualitative description	Disruption of business operations due to unavailability or faulty SAP system. System faults and failures that jeopardize full functioning of SAP system to support administrative, budgetary, financial and non-financial operations of the organization.
Trigger of risk event	Incorrect system configuration, system design faults and gaps, missed requirements, hardware failures, lack of adequate SAP support, unsuitable SAP services supplier or SAP support contract
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception; Failure to keep pace with technological innovation
Financial	Unfunded or inadequately funded commitments; Budget management and control
Operational	Information technology (relevance, availability, stability); Information/business reporting (budgeting and planning, accounting information, pension funds, After Service Health Insurance liability, investment evaluation); Business continuity
Qualitative description of risk event outcome	Possible liability to the Organization due to wrong calculation of financial commitments. Risk of delay in processing payroll, procurement of goods and services and travel requests. Risk of use of manual system due to inadequate set-up of the SAP system, possibly leading to under-utilization of the SAP system.
Risk controls	
Detailed description of current controls	**SAP System Failure** • Proactive monitoring of hardware and software performance and timely update of relevant software releases • Set-up of real-time disaster recovery system and periodic tests and simulation of disaster recovery plans • Improvement of infrastructure resiliency, improvement of business continuity arrangement • Improvement of internal control through segregation of duties **System design faults** • Comprehensive requirements gathering • Integrated user acceptance and quality assurance testing • Avoidance of customization of the standard SAP system • Robust change control procedures **Inadequate SAP support** • Proactive monitoring and improvement of service delivery though agreed service level agreements • Proactive management of SAP knowledge in the organization
Level of confidence in present control	High

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	5
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	Increase in-house skills in outsource contract management, closely monitor the performance of SAP service providers, negotiate favourable and flexible SAP service delivery contract

4. Organizational management

13. Risk event identification	
Name of risk event	Inadequate information, data and knowledge management
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	All divisional outputs
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs; public; industry, including seafarers
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Due to the specialized functions and limited functional back-up, the sudden absence of staff members can limit the effectiveness of the Secretariat; lack of oversight of data systems, lack of overall strategy on knowledge management.
Trigger of risk event	Retirement or resignation of key staff; Disruption on information/ knowledge transfer and acquisition process
Nature of Risk Event	
Organizational	Damage to the Organization's reputation; public perception; failure to keep pace with technological innovation
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements (Member Audit Scheme)), information technology (relevance, availability, stability), information/business reporting (budgeting and planning, accounting information, pension funds, After Service Health Insurance liability, investment evaluation), business continuity
Qualitative description of risk event outcome	Operational disruption due to time spend on finding relevant information; difficulties providing evidence for actions and decisions; vital records not appropriately secured to ensure business continuity
Risk controls	
Detailed description of current controls	Information security management system related to the ICTS ISO certification, IMO policy on storage and disposal of documentation
Level of confidence in present control	Low
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls.	
Impact	4
Probability	3
Assessment	7

Development of risk management options	
Risk tolerance level	Low tolerance level indicates that the risk is not tolerable at the assessed risk level without further mitigating actions being implemented directly
Additional risk treatment and control mechanisms	Define information management strategies and processes; identify roles and responsibilities for information management. Incorporate mandatory recordkeeping requirements into all Secretariat operations, including in requirements for project planning, departmental management and reporting, and other essential business processes and workflows. Incorporate recordkeeping responsibilities for senior managers and staff job descriptions to identify clear and accountable roles and responsibilities for recordkeeping. Increase motivation of staff in order to ensure adequate knowledge-sharing and collaboration. Establishment of fora and processes for oversight and consultations on knowledge management.

14. Risk event identification	
Name of risk event	Sharing of confidential information
Strategic directions potentially impacted	SD7
Secretariat's business plan outputs potentially impacted	All divisional outputs
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Breach of the Organization's policies, regulations and rules concerning the sharing of information either due to a lack of knowledge of the Organization's policies or intentional unauthorized sharing of information
Trigger of risk event	Staff sharing confidential information with Member States or other external sources
Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements (Member Audit Scheme)), business continuity
Qualitative description of risk event outcome	Compromise the conduct of meetings; create unnecessary issues when discussing sensitive topics; damage the reputation of the Organization and in particular the Secretariat among Member States and possibly the general public
Risk controls	
Detailed description of current controls	Regulations, policies and guidelines are in place, in particular, Article I of the Staff Regulations and Staff Rules, the Code of Ethics and the ICT Information Security Manual
Level of confidence in present control	Low

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	4
Probability	2
Assessment	6
Development of risk management options	
Risk tolerance level	Low tolerance level indicates that the risk is not tolerable at the assessed risk level without further mitigating actions being implemented directly
Additional risk treatment and control mechanisms	Training for staff. Easily accessible information and clearly defined responsibilities as stewards and keepers of information in job descriptions and job reviews.

15. Risk event identification	
Name of risk event	Lack of compliance with the Organization's policies (Governance, ethics and integrity of the Organization)
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	All divisional outputs
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs; public; industry, including seafarers
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Lack of compliance with established IMO policies
Trigger of risk event	Staff not completely aware of content of the Secretariat's policies or the lack of enforcement and consequences when policies are not being adhered to
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception; Non-adoption or non-compliance with the Organization's standards
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements (Member Audit Scheme)), empowerment (leadership, change readiness), business continuity, liability claims
Qualitative description of risk event outcome	Damage the reputation of the Organization and in particular the Secretariat among Member States and possibly the general public; claims due to breaches of policies by staff member (ethics violations or harassment); danger to the health and safety of staff members (i.e. non-completion of the UNDSS information before travel); claims due to breaches of policies by delegates (e.g. harassment of any kind)

Risk controls	
Detailed description of current controls	Some policies are accompanied by courses that have to be passed and certificates are issued; updates to policies and new policies are shared within the Organization
Level of confidence in present control	Low
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	3
Assessment	6
Development of risk management options	
Risk tolerance level	Low tolerance level indicates that the risk is not tolerable at the assessed risk level without further mitigating actions being implemented directly
Additional risk treatment and control mechanisms	Make all courses and tests mandatory, and introduce a timeframe in which the courses have to be refreshed; follow up on mandatory training completion; provide training and presentations on policies to staff; improve the enforcement of the policies

5. Human resource measures

16. Risk event identification	
Name of risk event	Inadequate succession planning
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	All divisional outputs
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs; public; industry, including seafarers
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Inadequate succession planning can limit the effectiveness of the Secretariat
Trigger of risk event	Lack of a succession planning policy, late advertisement of posts (cost saving strategy on recruitment policy), sudden staff departure, lack of knowledge management, poorly defined job descriptions and over-reliance on seconded staff
Nature of risk event	
Organizational	Damage to the Organization's reputation; Demographic and socio/cultural trends
Financial	Unfunded or inadequately funded commitments
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Business continuity, empowerment (leadership, change readiness)
Qualitative description of risk event outcome	Vacancies: key positions being vacant over a longer period of time. Staff training and development (talent management): Successors for posts are not prepared to fill the post internally. Loss of institutional knowledge: no formal knowledge transfer can lead to external successors not being able succeed in the position and organizational knowledge to be lost once senior staff retires (transition period); lack of mentoring programme Functional fit: posts continuously re-advertised without assessing the current strategic focus of the Organization.
Risk controls	
Detailed description of current controls	Resources management has been improved, budgetary provisions are in place to reinforce the teams when needed. At divisional level the restructuring of divisions now allows replacements to take over the day-to-day running of business and increases the sharing of knowledge and information within divisions.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	5

Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	Staff succession planning policies to be strengthened. A review of current practices is needed in order to identify areas for improvement, including an identification of cross-divisional responsibilities and synergies, with a view to identifying long-term human resource requirements to sustain the work load and deliver as requested. Develop and implement a succession plans and corresponding training needs; Ensure continuous review of posts and job descriptions and their fit with the Organization's strategy. Establish measures to ensure adequate knowledge transfer for Secondees, including JPOs, and temporary staff leaving the Organization.

17. Risk event identification	
Name of risk event	Inability to attract and retain suitably qualified staff
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	All divisional outputs
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; INGOs and NGOs; public; industry, including seafarers
Entity responsible	All divisions
Scope of risk event	
Qualitative description	Due to the specialized functions and length of recruitment process, delay in the recruitment of staff can limit the effectiveness of the Secretariat
Trigger of risk event	Failure to attract highly qualified permanent, temporary, contractual staff, Secondees, JPOs and consultants
Nature of risk event	
Organizational	Damage to the Organization's reputation; demographic and socio/cultural trends
Financial	Unfunded or inadequately funded commitments
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Business continuity, empowerment (leadership, change readiness)
Qualitative description of risk event outcome	Delays in recruitment processes lead to gaps where sufficient knowledge or competencies might be lacking have a direct impact on the Secretariat's delivery of the objectives specified in the Secretariat's Business Plan
Risk controls	
Detailed description of current controls	Continuous review and enhancement of working practices. Efforts are made to expand the pool of contractual translators, temporary staff and consultants. Reliance on seconded resources from Member States to meet the demands for the delivery of the work load.
Level of confidence in present control	Moderate

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	1
Assessment	4
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	Ensure that working conditions are attractive, especially for those working nights, and consider possible measures to promote staff or provide them with more financial incentives, possibly through the new Performance Recognition scheme; Expand the outreach of recruitment to be able to reach the target audience for the specific position, e.g. young professional, through promoting internship programmes. Motivate staff (without promotion or financial incentives) such as with better work/life balance, opportunities for further development, volunteering and outreach opportunities, etc.

18. Risk event identification	
Name of risk event	Ineffective handling of cases by IMO requiring use of the internal justice system
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 02, BP 03 & BP 04
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat
Entity responsible	Administrative Division
Scope of risk event	
Qualitative description	Effective and timely operation of the internal justice system
Trigger of risk event	Conflicts are not prevented or dealt with in a timely manner
Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Budget management and control
Operational	Not applicable
Qualitative description of risk event outcome	Internal conflicts that are not handled appropriately may lead to tribunal cases ruling against IMO. Such cases are labour intensive and may result in high payments for lost cases. It may result in poor staff morale, work disruption and potential financial liabilities for the Organization.

Risk controls	
Detailed description of current controls	The internal justice system was revamped to include a whole phase of informal resolution of disputes. Following this revamping of the system, a group of staff members was trained in mediation techniques and now act as mediators. In addition, a harassment prevention programme has been set up and training for managers is mandatory. In addition, a document was prepared to deal with cases of retaliation after staff members raise a concern. This will become an appendix to the Staff Regulations and Staff Rules.
Level of confidence in present control	High
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls.	
Impact	2
Probability	2
Assessment	4
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level.
Additional risk treatment and control mechanisms	The harassment prevention policy is being further strengthened to professionalize the investigation of allegations of harassment. The issue of personal accountability for decisions made should be further explored, combined with additional training on legal matters for managers.

6. Planning and delivery of technical cooperation activities

19. Risk event identification	
Name of risk event	Delays in the implementation or cancellation of planned technical cooperation activities
Strategic directions potentially impacted	SD1
Secretariat's business plan output potentially impacted	TCD BP 05, MSD BP 05, MED BP 04, LED BP 04, MSA&IS 04
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; INGOs and NGOs; public; industry, including seafarers
Entity responsible	TCD, MSD, MED, LED, MSA& IS, AD
Scope of risk event	
Qualitative description	Delays in the creation and implementation of technical assistance and outreach activities, workshops and training courses, including the development of training materials, as requested by Member States in order to fulfil their respective obligations, build capacity and implement/enforce IMO instruments
Trigger of risk event	Lack of resources, delays in finalization of training materials and changes in the planned activities (schedule and priority). One or more components of the activity failed or did not materialize (withdrawal of a consultant on short notice, beneficiary State(s) withdraws offer to host or request postponement). Measures put in place by Governments and by IMO's own risk mitigation plans to address the direct risk posed to staff/dependents/consultants due to safety, security or health considerations (political instability, terrorist threats, natural disasters, outbreak of disease etc.).
Nature of risk event	
Organizational	Damage to the Organization's reputation; regionalization or unilaterism in the regulation of shipping, failure to keep pace with technological innovation, Capital available for major programmes; non-adoption or non-compliance with the Organization's standards
Financial	Budget management and control, unfunded or inadequately funded commitments
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Empowerment (leadership, change readiness); Business continuity; Disease and disability; Information/business reporting (budgeting and planning, accounting information, pension funds, After Service Health Insurance liability, investment evaluation)
Qualitative description of risk event outcome	Inability of the Secretariat to proceed with the planning and/or delivery of TC activities as disruption impacts delivery of intended benefits, and on the approved budgets. Lack of standards and inadequately trained maritime personnel. Failure to assist a Member State or States to prepare for audits through a planned TC activity
Risk controls	
Detailed description of current controls	With regard to the delivery of TC activities, the technical co-operation activities are well planned and the pre-assessment of activities are well formulated. There is a mandatory evaluation of completed activities (workshops and training courses). Besides, partnership arrangements are updated regularly and a regular monitoring and reporting to IMO meetings takes place. Besides, the on-going communication with the recipient countries, donors, the Council and TC Committee is necessary. With regard to the planning of TC activities, the identification of key components are necessary for the delivery of the activity and development of milestones to monitor delivery progress, which are included in PID. In addition, contingency considerations are made by the implementing officer.
Level of confidence in present control	Moderate

Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	5
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	With regard to the delivery of TC activities, strengthening of oversight activities, augmenting technical staff, utilization of competent consultants and partnerships for the development of training materials and the delivery of technical co-operation activities, including increase of funding

20. Risk event identification	
Name of risk event	Lack of or insufficient funding to implement the technical cooperation activities
Strategic directions potentially impacted	3
Secretariat's business plan output potentially impacted	TCD BP 05, BP 06, BP 07, MSD BP 05, MED BP 04, LED BP 04, MSA&IS 04
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; INGOs and NGOs; public; industry, including seafarers
Entity responsible	TCD, MSD, MED, LED, MSA&IS, AD
Scope of risk event	
Qualitative description	Insufficient financial contribution from donors, the Trading Fund surpluses and/or in-kind support secured for TC activities
Trigger of risk event	Voluntary contributions from IGOs, NGOs and Member State donors decrease. Publishing income to the Trading Fund decreases or dries up completely
Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception; Capital available for major programmes
Financial	Budget management and control, unfunded or inadequately funded commitments
Operational	Business continuity
Qualitative description of risk event outcome	Subsidies to the TC fund of the Organization eliminated (funding must be replaced from other sources). Some TC activities of the Organization might be negatively affected. Identified needs of developing States, including emerging needs, might not be addressed.

Risk Controls	
Detailed description of current controls	Continuous listing of IMO on the Organization for Economic Cooperation and Development/ Development Assistance Committee (OECD/DAC) Statistical Reporting Directives list. Closer working relation with donors. Use of conservative estimates of the anticipated donors' contributions.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	5
Development of risk management options	
Risk tolerance level	Low – risk is not tolerable at the assessed risk level without further mitigating actions being implemented
Additional risk treatment and control mechanisms	Increase the overall resource mobilization for TC activities. Develop more strategic links with key donors through long term strategic agreements. Diversify the donor base by proactively seeking out new donors and donor groups. Develop a thematic funding strategy to enable donors to provide funds towards high-level strategic objectives providing IMO with flexible funding to meet strategic goals and rapidly respond to emerging needs.

7. Delivery of IMO initiatives

21. Risk event identification	
Name of risk event	Delay in delivery of the Secretariat's obligations under Goal-based Standards (GBS)
Strategic directions potentially impacted	SD2
Secretariat's business plan output potentially impacted	MSD BP 03
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; IGOs and NGOs; public; industry, including seafarers
Entity responsible	MSD
Scope of risk event	
Qualitative description	The International goal-based ship construction standards (GBS) for bulk carriers and oil tankers are mandatory under new SOLAS regulation II-1/3-10 from 1 January 2012 and became applicable from 1 July 2016
Trigger of risk event	Lack of Secretariat resources to deliver the GBS verification audit process and the possible lack of nominated auditors could cause delays in the submission of the outcome of the initial and/or maintenance audits
Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements)
Qualitative description of risk event outcome	The Secretariat has a GBS verification audit scheme in place, including a GBS Trust Fund, and established a roster of auditors. A maintenance audit is planned for 2018 as well as an initial verification audit for Turk Lloyd.
Risk controls	
Detailed description of current controls	Plans for the 2018 audits are underway and the Secretariat is dealing with the Scheme. The Secretariat is currently preparing and implementing the GBS maintenance audit scheme according to the agreed schedule by the Committee (MSC 98) as well as preparing for the new audit expected for Turk Lloyd.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	5

Development of risk management options	
Risk tolerance level	Low – risk is not tolerable at the assessed risk level without further mitigating actions being implemented
Additional risk treatment and control mechanisms	Recruitment of new auditors

22. Risk event identification	
Name of risk event	Delay of Secretariat in responding to the LRIT Data Distribution Plan (DDP) server, the Information Distribution Facility (IDF) and the Operational Governance Body (OGB), SOLAS Contracting Governments and Data Centre Operators requests
Strategic directions potentially impacted	Other work
Secretariat's business plan output potentially impacted	MSD BP 02
Stakeholders and responsibilities	
Internal and external stakeholders	Member States
Entity responsible	MSD
Scope of risk event	
Qualitative description	The Secretariat is responsible for the operation of the LRIT Data Distribution Plan (DDP) server and the Information Distribution Facility (IDF). In case of any malfunctions of the Data Distribution Plan (DDP) server, the LRIT provisions require immediate investigation and activating the Disaster recovery site if the issue cannot be resolved within four hours. There are also requirements for notification of the incident to all LRIT system components (MSC.1/Circ.1376/Rev.2 refers). The Secretariat also has responsibility for the overall functioning of the LRIT system and is one of the members of the LRIT Operational Governance Body (OGB). There are also many processes where the Secretariat is involved that require prompt action (usually within 24 hours), such as the establishment, testing and modification of LRIT Data Centres, the updating of information into the DDP, the issuance of Public Key Infrastructure (PKI) certificates and/or the integration of new SOLAS Contracting Governments into the system.
Trigger of risk event	Lack of Secretariat resources (only one officer in charge) to deliver its responsibilities under SOLAS regulation V/19-1, resolution MSC.263(84) on Revised Performance standards and functional requirements for the long-range identification and tracking of ships, MSC.1/Circ.1259/Rev.7 and MSC.1/Circ.1294/Rev.5 on LRIT Technical documentation (Parts I and II, respectively) and MSC.1/Circ.1376.Rev.2 on Continuity of service plan for the LRIT system
Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Not applicable
Operational	Business continuity
Qualitative description of risk event outcome	The unavailability of the DDP server has direct implications to the functioning of the LRIT system and the rights of SOLAS Contracting Governments to request LRIT information as a coastal State and to exclude others from receiving such information. The definition and activation of coastal State standing orders is done through the DDP web interface. If the DDP server is not available, SOLAS Contracting Governments are

	not able to activate coastal State requests. Moreover, the unavailability of the DDP server may have financial implications for SOLAS Contracting Governments in respect to active coastal State requests (as they will be unable to deactivate the request until the DDP services are restored). The unavailability of staff in MSD to process different requests may delay the establishment and testing of LRIT Data Centres, the integration of new SOLAS Contracting Governments into the system and/or the resolution of any issues with LRIT system components.
Risk controls	
Detailed description of current controls	There are many processes where prompt action by the Secretariat is required at many stages (usually action is taken within 24 hours for regular requests or two hours in case of a malfunction with the LRIT Data Distribution Plan server and/or the Information Distribution Facility). Most of these processes cannot continue without action by the Secretariat
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	4
Probability	3
Assessment	7
Development of risk management options	
Risk tolerance level	Low – risk is not tolerable at the assessed risk level without further mitigating actions being implemented
Additional risk treatment and control mechanisms	Review existing processes so as to reduce the level of actions required by the Secretariat. Assign LRIT responsibilities to existing staff in MSD to act as backup and/or recruit additional staff to support the necessary actions, especially during absence of the person in charge.

23. Risk event identification	
Name of risk event	Potential delays in implementation of major projects due to financial, human resources or political issues
Strategic directions potentially impacted	SD1, SD3
Secretariat's business plan output potentially impacted	MED BP 05
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States
Entity responsible	MED
Scope of risk event	
Qualitative description	Major projects is mostly subject to external factors and risk events. One major risk is the political risks associated with policy and legal reforms which are expected outputs of the project. Internal risks are associated with sudden loss of project staff or delays in recruitment of project staff, as the projects are on tight timelines.
Trigger of risk event	External political changes at project countries, more than one-month delay in staff recruitments

Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Business continuity
Qualitative description of risk event outcome	IMO reputation at stake, withdrawal of donor funds, lack of donor support in future
Risk controls	
Detailed description of current controls	Well-designed project monitoring and evaluation systems in place, close communications with donors, Project Coordination Units keep monitoring the projects and risk factors
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	6
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	More frequent monitoring of field activities, more presence in field, reduce staff recruitment time to minimum and prevent staff turnover

24. Risk event identification	
Name of risk event	Lack of coordination and support of all the GESAMP activities including IMO-led WGs and its Executive Committee
Strategic directions potentially impacted	SD1, SD3
Secretariat's business plan output potentially impacted	MED BP 06 & BP 07
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; NGOs and IGOs; Industry, including seafarers
Entity responsible	MED
Scope of risk event	
Qualitative description	Single donor support for GESAMP (i.e. SIDA) is no longer a sustainable financial mechanism resulting in cash flow difficulties, operational setback and protracted delivery of planned activities and outputs
Trigger of risk event	Diminution of funding support

Nature of risk event	
Organizational	Damage to the Organization's reputation; Public perception; Non-adoption or non-compliance with the Organization's standards
Financial	Unfunded or inadequately funded commitments; Budget management and control
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements); Information/business reporting (budgeting and planning, accounting information, pension funds, After Service Health Insurance liability, investment evaluation); Business continuity
Qualitative description of risk event outcome	Potential decrease in GESAMP's activities, limited personnel to administer and operate the GESAMP office, internal non-compliance with GESAMP standards and endangering the effective execution of GESAMP's Mission Statement
Risk controls	
Detailed description of current controls	Fund raising strategy revised, utilized limited sponsoring agencies (UN bodies) to support activities for GESAMP, particularly working group meetings
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	3
Assessment	6
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	Intensify fund raising through identification and selection of sponsors and donors; develop activities for medium to longer funding support.

25. Risk event identification	
Name of risk event	Delay in the implementation of audit programme under the IMO Member State Audit Scheme (IMSAS)
Strategic directions potentially impacted	SD1
Secretariat's business plan output potentially impacted	MSA&IS BP 03 & BP 03
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; public
Entity responsible	MSA&IS

Scope of risk event	
Qualitative description	From 1 January 2016 audits under the Scheme became mandatory, following entry into force of amendments to the mandatory IMO instruments included in the scope of the Scheme. Implementation of up to 25 audits in accordance with the annual timetable, based on the audit schedule (document C 112/INF.3), depends on availability of resources, both human (auditors nominated and made available by Member States and Secretariat staff) and financial (regular budget of the Organization).
Trigger of risk event	A shortfall in the number of auditors or Secretariat staff with the requisite language skills and/or experience to form the full complement of audit teams to carry out audits as per the annual timetable
Nature of risk event	
Organizational	Damage to the Organization's reputation
Financial	Not applicable
Operational	Business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements (Member Audit Scheme)), business operations (human resources, capacity, meetings delivery, efficiency, service failure, ITCP delivery, meeting new requirements (Member Audit Scheme))
Qualitative description of risk event outcome	The Secretariat has prepared for the implementation of audits under the Scheme, including funding of audits through the regular budget, maintaining an active roster of auditors and increasing the current staff complement in the Department in accordance with the decisions of the Council. Taking into account the volume of work, if the Secretariat experiences lack of or unavailability of human resources (qualified auditors from Member States and the Secretariat) due to various reasons, the conduct of audits in accordance with the annual timetable may not be achievable.
Risk controls	
Detailed description of current controls	The Assembly and Council have invited Member States to continue nominating qualified auditors who meet the criteria established in the Procedures and make them available for audits. Audit Officers from the Department are strategically allocated audit team duties to allow flexibility to be reassigned to other audits in case of a shortfall in the available auditors for a particular audit. For any possible shortfall in the available audit staff, all audit planning is followed by all staff, with the ability to for anyone to intervene as a stop gap measure if a shortfall in available staff were to occur.
Level of confidence in present control	Moderate
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	3
Probability	2
Assessment	5
Development of risk management options	
Risk tolerance level	Moderate – risk is tolerable but further mitigating actions should be implemented to increase the risk tolerance to high
Additional risk treatment and control mechanisms	Close monitoring of audit planning, its progression and the identification of any other factors that could increase the risk event with respect to each audit. Forward planning in order to identify potential lack of available auditors with specific competence and identify solutions and contingency measures to address the risk.

8. Health and safety at IMO Headquarters

26. Risk event identification	
Name of risk event	Health and safety incident at IMO HQ
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 08
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; public
Entity responsible	AD
Scope of risk event	
Qualitative description	Accident or natural disaster makes it impossible to use building for significant length of time and/or causes significant injuries/loss of life
Trigger of risk event	Accident (e.g. fire, catastrophic failure of lift) or natural disaster (e.g. flood)
Nature of risk event	
Organizational	Not applicable
Financial	Not applicable
Operational	Fire and property damage, personal injury, business continuity, liability claims
Qualitative description of risk event outcome	Effects range from injury or health consequences to death for occupant(s); from partial to complete destruction of building and resulting inability to use it for intended purposes; damage to building, infrastructure and equipment entailing repair/replacement. Direct cost of repairs and business continuity; indirect cost of liabilities (to staff or other occupants), capital available for major programmes; operations disrupted.
Risk controls	
Detailed description of current controls	Risk heavily insured, rigorous regime of inspection and maintenance, adherence to statutory and other guidelines (building), good local emergency services
Level of confidence in present control	High
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	5
Probability	1
Assessment	6
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	N/A

27. Risk event identification	
Name of risk event	Security incident at IMO HQ
Strategic directions potentially impacted	SD7
Secretariat's business plan output potentially impacted	AD BP 08
Stakeholders and responsibilities	
Internal and external stakeholders	Secretariat; Member States; public
Entity responsible	AD
Scope of risk event	
Qualitative description	Criminal attack or politically motivated act of violence makes it impossible to use building for significant length of time and/or causes significant injuries/loss of life
Trigger of risk event	Random criminal attack or politically motivated act of violence (bomb, "active shooter") causes significant injuries/loss of life or makes it impossible to use building for significant length of time
Nature of risk event	
Organizational	Not applicable
Financial	Not applicable
Operational	Fire and property damage, personal injury, business continuity, liability claims
Qualitative description of risk event outcome	Effects range from injury to death for as few as one or as many as all occupants; from partial to complete destruction of building and resulting inability to use it for intended purposes; plus cost and liabilities to the Organization and damage to building, infrastructure and equipment entailing repair/replacement. Direct cost of repairs and business continuity, indirect cost of liabilities (to staff or other occupants), capital available for major programmes; operations disrupted; significant staff distress.
Risk controls	
Detailed description of current controls	Security and advice provided by Host Government; UN security and safety framework provides information; risk heavily insured. Robust security procedures, regular liaison with host State and UN authorities.
Level of confidence in present control	High
Risk analysis	
An assessment of the risk, being the impact and probability of the risk event occurring, taking into account existing controls	
Impact	5
Probability	1
Assessment	6
Development of risk management options	
Risk tolerance level	High – risk is tolerable at its existing assessed risk level
Additional risk treatment and control mechanisms	N/A