ENERGY CHARTER SECRETARIAT

CCDEC 2022

16 GEN

Brussels, 20 September 2022

Related documents:
CC 755, Message 2006/22

DECISION OF THE ENERGY CHARTER CONFERENCE

Subject: Adoption by correspondence – Risk Management Protocol

By CC 755 dated 30 August 2022, the delegations were invited to approve the Risk Management Protocol (attached) as recommended by the Budget Committee. As specified by Rule 19(b) of the Rules of Procedure concerning the adoption of decisions by correspondence, members of the Energy Charter Conference were informed that any delegation that was not in a position to approve the above decision was requested to notify the Secretariat of its position in writing by no later than 20 September 2022.

Having received no objections within the specified time limit, on 20 September 2022, the Conference **approved** the attached Risk Management Protocol with immediate effect.

Keywords: Risk Management Protocol

RISK MANAGEMENT PROTOCOL

I. OBJECTIVES

1. The Risk Management Protocol is designed in a systematic and organisation-wide approach, which supports the achievement of the goals of the International Energy Charter (the Organisation) by proactively assessing and managing risks across the Organisation. The objectives of the Risk Management Protocol are to ensure the sustainability of the Organisation as well as the adoption of risk-informed decisions across all levels of the Organisation.

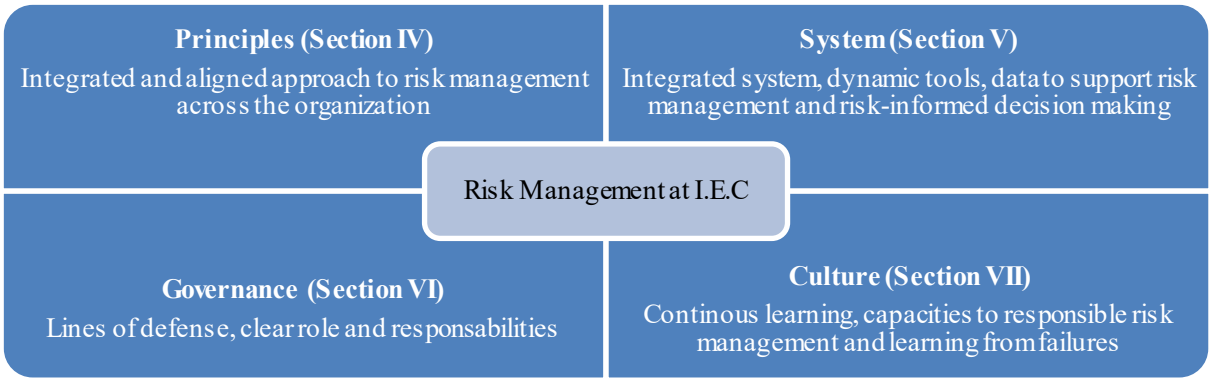
2. The framework provided by the Protocol does not replace any existing provisions of the Staff Regulations and Rules, Rules of Procedure of the Energy Charter Conference or decisions of the Conference and cannot contradict their application.

II. DEFINITIONS

3. For the purposes of the Protocol, the following terms and definitions apply:
   - **Risk:** the effect of uncertainty on the organisation's objectives, which could be either positive and/or negative. A risk, if realised, may enhance, prevent, degrade, accelerate or delay the achievement of objectives.
   - **Risk assessment:** the overall process of risk identification, analysis and evaluation. It aims at providing sufficient information at appropriate intervals for risk-informed management decisions.
   - **Risk management:** coordinated activities to direct and control the organisation with regard to risks.
   - **Risk criteria**: the factors against which the significance of a risk is determined
   - **Event:** an occurrence or change of a particular set of circumstances.
   - **A stakeholder:** a person or entity which can affect, be affected by, or perceive themselves to be affected by a decision or an activity.

III. PILLARS

4. The Risk Management Protocol is based on **four pillars**, summarised in the following diagram and detailed in subsequent sections:



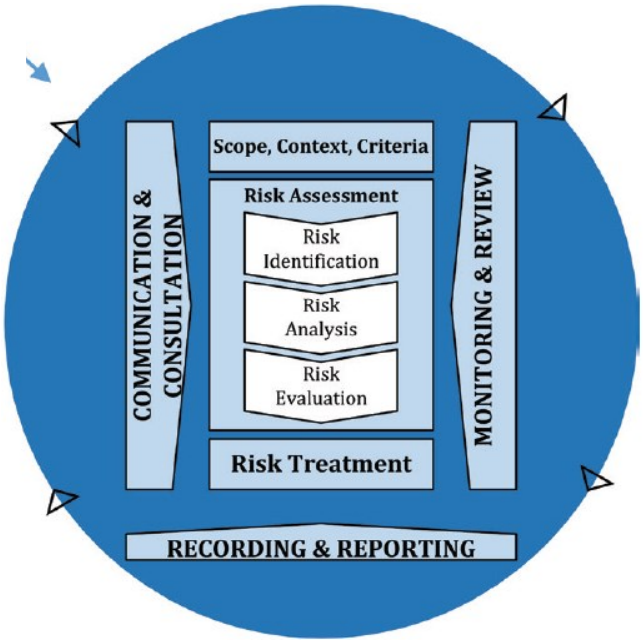
IV. PRINCIPLES

5. The principles below ensure the effectiveness of the Risk Management Protocol:

- Integrated and aligned: risk management is an integral part of all the activities of the Organisation.
- Structured and comprehensive: to facilitate consistent and comparable results.
- Inclusive: appropriate and timely involvement of stakeholders [via discussions in relevant working groups and consultations] enables their knowledge, views and perceptions to be considered.
- Dynamic: it should address changing risks and events in an appropriate and timely manner.
- Best available information: the inputs should also consider future expectations (not only current or historical information). Information should be timely, clear and available to the relevant stakeholders.
- Continual improvement: the organisation will consider its own experience, evolving international standards and best administrative practices.

V. RISK MANAGEMENT SYSTEM

6. In line with ISO 31000:2018, the Risk Management system refers to six key elements: communication and consultation (A); context (B); assessment (C); treatment (D); monitoring and review (E); recording and reporting (F).



Source: ISO 31000:2018

7. These elements are applied across the whole Organisation: at the Unit's level, at Secretariat's level and at the Organisation's level.

A) Communication and Consultation

8. An inclusive communication and consultation with all the relevant stakeholders, including staff, should take place at regular intervals to inform on risk identification, assessment, treatment, monitoring, reporting and review.

B) Context

9. The contextual analysis, identifying key trends and issues, hazards and opportunities, provides a key source of evidence to contribute to the identification of risks. Establishing the context requires understanding the external and internal context relevant for the realisation of objectives at each level.

10. **External context** includes but is not limited to social, cultural, environmental, political, legal, financial, technological, security and economic factors. It also implies understanding the external stakeholders and their relationships, perceptions, and expectations. Similarly, the **internal context** includes strategic objectives, values, standards, resources available, business processes, organisational culture, relationships with internal stakeholders, capacities, etc.

C) Risk Assessment

11. **Risk identification** considers 'future events', their causes and potential impacts. In the context of the International Energy Charter, the following risk categories could be identified:

1) **Financial**:

a) Deviation from the approved budget
In accordance with Article 19 of the Financial Rules, a system of budget control is established to periodically forecast budget results and unforeseen expenditure.

b) Reliability of accounting and reporting in accordance with International Public Sector Accounting Standards (IPSAS)
In accordance with Article 24 of the Financial Rules in conjunction with Instruction 14 of the Financial Rules, internal rules of procedure are established to permit financial reporting on all activities of the Secretariat to ensure that financial information provided is the most accurate and relevant.

c) Value for Money

d) Market risk

e) Foreign currency exchange risk

f) Interest rate risk

g) Credit risk

h) Liquidity risk

2) **Deliverables**:

a) impact on the expected deliverables

b) required unexpected deliverables

3) **Operational**:

a) Delay or acceleration of applicable operations

b) Inadequate project management

c) Lack of forward-planning

4) **Organisational**:

a) Governance

b) Accountability

c) Human resources: effect of the organisation's actions on the personnel

d) Internal control

5) **Compliance:**

a) Fraud and Corruption
In accordance with Instruction 14 of the Financial Rules, internal control procedures are established to ensure sound financial management, including preventive,

detective and corrective internal controls in relation to the legality and regularity of the operations, to the prevention of fraud and conflict of interests and to the safeguarding of the Organisation's interests.

b) Changes in the regulatory framework within the country of operation;

c) Changes in the international regulatory framework, including principles of international civil service

d) Deviation from rules and regulations applicable within the Organisation

e) Privacy breaches

f) Compliance with the Manual on Data Protection and international best practices.

g) Process risk

h) Compliance with established procedure and standard process.

6) **Strategic**:

a) Code of conduct and ethics

b) Public opinion and media

c) Stakeholder relations

d) Reputation

7) **Safeguarding and valuation of assets**:

a) Ensure permanent inventory of the movable and immovable property constituting the assets of the Secretariat in accordance with Article 24(2)(d) of the Financial Rules;

b) Maintain detailed records of all assets and liabilities of the Secretariat in accordance with Article 25 of the Financial Rules.

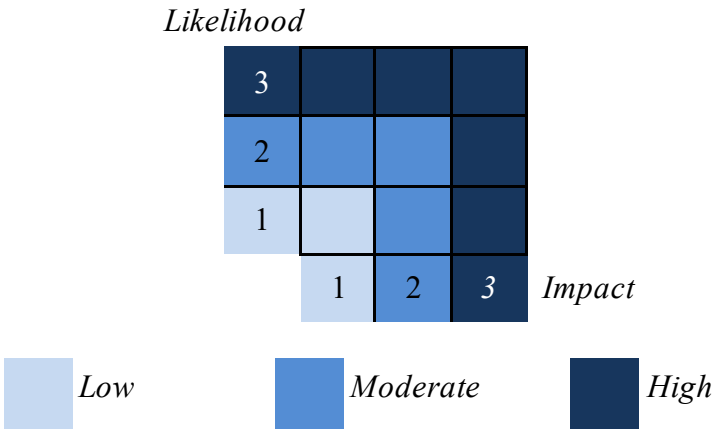
12. Each identified risk is assigned to a category and recorded in the **Risk Register** (the template of a risk register is presented in Annex 1).

13. **Risk analysis** requires an assessment of the **likelihood** of a risk and its potential **impact** on the objectives to be determined based on available information:

Likelihood	**1**	**2**	**3**
Description	Low chance of materialising (<30%)	Moderate chance of materialising (30% - 70%)	High chance of materialising (<70%)

Impact	1	2	3
Financial	<15% deviation from the approved budget	15-45% deviation from approved budget	>45% deviation from approved budget
Deliverables	<20% of expected deliverables were impacted negatively or positively **and/or** Negligible or no negative or positive impact of the expected deliverables	20-50% of expected deliverables were impacted negatively or positively **and/or** Moderate negative or positive impact on the expected deliverables	>50% of expected deliverables were impacted negatively or positively **and/or** Significant negative or positive impact on the expected deliverables
Operational	Delay or acceleration functioning by less than 2 weeks	Delay or acceleration of applicable operations by 2 to 6 weeks	Delay or acceleration of applicable operations by more than 6 weeks
Compliance	Negligible deviation from applicable rules and regulations	Moderate deviation from applicable rules and regulations	Significant deviation from applicable rules and regulations
Safety and Security	Almost none or little effect on the personnel	Moderately injurious or traumatic effect on the personnel **and/or** Moderately injurious or traumatic effect directly or indirectly caused by the organisation's actions	Severe psychological/physical effect on the personnel **and/or** severe psychological/physical effect caused by the organisation's actions
Reputation	Isolated and/or several negative or positive comments from external stakeholders	Negative or positive reports/articles in national, regional and/or international media	Negative or positive reports/articles in several national, regional and/or international media for a significant period, and/or criticism from key stakeholders

14. Based on the likelihood and impact as presented above, the **risk level** (high, moderate or low) is determined:



15. High-Level Risks: require further in-depth risk analysis, as well as analysis of treatment and monitoring measures, and of any necessary budget in case of its materialisation. The analysis needs to include the precautions to eliminate unnecessary damage on the Organisation, including its staff members.

16. Moderate-Level Risks: require analysis of treatment and monitoring measures, as well as appropriate budgeting in case of its materialisation.

17. Low-Level Risks: do not require further analysis or treatment.

18. Based on the above analysis, an **evaluation** is made in order to determine which risks can be assumed and which risks require a priority response.

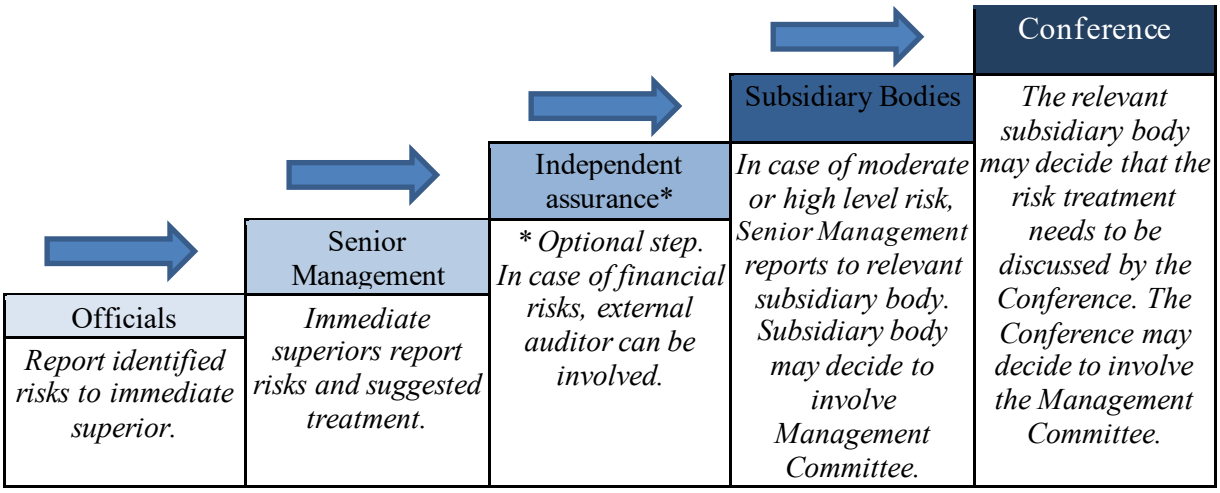
D) Treatment

19. Selecting the most appropriate treatment option(s) involves balancing the potential benefits derived from the achievement of the deliverables set in the Programme of Work against the disadvantages of implementing some measures.

20. For example, according to draft Article 19(3) of the Financial Rules, if the risk of budget over-expenditure is identified, the Deputy Secretary-General may suspend the use of appropriations or of specific commitments of appropriations for which no legal commitments exist.

21. Risks could be considered as potential threats, but also as opportunities. A low level of risk is usually tolerated (in order to achieve the mandate and strategic objectives) and doesn't require particular treatment. On the contrary, for each High or Moderate level risk, specific risk measures must be identified.
    - In case of threats to organisational objectives, risk treatment may be to:
        - **Terminate**: seeking to eliminate the activity that triggers such a risk
        - **Transfer**: passing the ownership and/or liability to a third party
        - **Mitigate**: reducing the likelihood and/or impact of the risk below the threshold of acceptability
        - **Tolerate:** enduring the risk
    - In case of opportunities, risk treatment may be to:
        - **Exploit:** making the opportunity happen to benefit from it
        - **Experiment:** testing new solutions in uncertain contexts
        - **Enhance:** increase the likelihood or impact through reinforcing the trigger condition or increasing the exposure
        - **Accept:** no proactive actions

22. Following the appropriate level of reporting, the identified risks could be escalated. Since not all risks could be managed at the level where they are identified, depending on the circumstances and the measures to be adopted, the discussion could be escalated to a higher decision-maker. In this case, management of risks shall be escalated in accordance with the table below:



E) Monitoring and Review

23. Regular risk **monitoring and review** should be conducted on all levels and categories of risk within the Organisation to inform management decisions and its results should be recorded in the risk register and reported as appropriate. The risk register needs to be updated if new information becomes available that affects the identification, analysis, evaluation and treatment measures. Real-time monitoring of opportunities and threats should be considered in rapidly changing contexts to provide an early-warning mechanism and enable proactive response. In addition, the status and effectiveness of the treatment measures adopted also need to be monitored.

F) Recording and Reporting

24. While all identified risks are recorded in a risk register**, risk reporting** ensures that relevant risk information is available across all levels of the organisation in a timely manner to provide the necessary basis for risk-informed decision making.

25. Risk reporting is organised in accordance with steps applicable to the escalation of risk treatment. Only Moderate and High level risks are to be reported to the Contracting Parties during a meeting of the subsidiary groups.

26. Any revision to the present Protocol is to be discussed by the Budget Committee.

VI. GOVERNANCE

27. The Organisation is governed in accordance with five lines of defence as presented below[1].

- **First line of defence**: Immediate superior's responsibility and daily control of risks

[1] Originally, three lines of defence: 2014 The Institute of Internal Auditors *The Three Lines of Defence in Effective Risk Management and Control, IIA Position Paper*.

28. All officials of the Organisation have a role to play in risk management.

29. Identified risks and breaches shall be immediately reported to the competent authority in line with the Staff Manual (in most of the cases, this would mean the immediate superior).

30. Consequently, immediate superiors oversee risk management by providing fair leadership, ensuring the effective operation of controls, proper communication of such risk and taking responsibility for the actions or inactions of their subordinates.

- **Second line of defence**: Hierarchical control and oversight

31. In line with the hierarchy of the Organisation, the Secretary-General is accountable for the adequacy of the Secretariat's risk management. In this task, the Secretary-General is assisted by the Deputy Secretary-General, Senior Management and different internal bodies of the Secretariat.

- **Third line of defence**: Independent assurance*

32. * Optional element. In case of financial risks, the external auditors could be involved in line with the existing provisions of the Organisation. The external auditor is responsible for providing the Conference with a reasonable assurance that the organisation is managed on a sound economic and efficient basis, as well as reasonable assurance standard that financial statements give a true and fair view of the Secretariat's net equity and financial position. The external auditor performs its statutory duties in accordance with the Financial Rules, Implementing instructions and Terms of Reference of the External Auditors.

- **Fourth line of defence**: Subsidiary Bodies of the Conference

33. In line with their Terms of Reference, the relevant subsidiary body of the Conference will address possible risks and their mitigation at one of its meetings. A subsidiary body may decide to discuss the issue with the Management Committee.

- **Fifth line of defence**: The Energy Charter Conference

34. As the governing and decision-making body of the Organisation, the Energy Charter Conference will receive, if needed, relevant reports from the subsidiary bodies with respect to Risk Management in the organisation. The Conference may decide to authorise the Management Committee to address specific risks, in line with the latter's Terms of Reference.

VII. CULTURE AND CAPACITY BUILDING

35. The Organisation recognises that the mindsets and behaviours of individuals and groups inside the organisation play a crucial role in the effective execution of Risk Management. A mature risk management culture is characterised by the following:
    - Risk-informed decision making at all levels, including flexibility for adaptive management and course correction.
    - Responsible risk-taking and innovation is rewarded.
    - 'Failures' are acknowledged and recognised as part of the learning curve, particularly while operating in complex contexts.
    - Continuous learning for strengthened risk management capacities.
    - Key stakeholders are involved in all stages of the risk management process.
    - Absence of approaching risk management purely as a compliance issue.
    - Open communication on all risk management issues and lessons learned and a culture of "working out loud."
    - Adequate budget allocations for risk management at all levels.
    - Secretariat's personnel are enabled to 'stay and deliver' at an acceptable level of security risk.

36. The Deputy Secretary-General is to consider annual training on risk management for officials of the Secretariat and officers of the Conference.

ANNEX 1 DRAFT RISK REGISTER – TEMPLATE

N°	Description	Category	Risk Level: Impact/Likelihood	Risk Treatment	Responsible
	Brief description of the risk	***Financial*** ***Deliverables*** ***Operational*** ***Organisational*** ***Regulatory*** ***Strategic***	*Potential effect if future event occurs.* *Risk Level (High, Moderate or Low) based on* ***Likelihood*** *(1-2-3) and* ***Impact*** *(1-2-3)*	*Action(s) taken*	*The person or organ in charge*