Risk Management System

Version	Date	Nature of Changes	Approved By
V1.0	22 May 2023	Original issue	Andrew Kerr, Chairman

1 Purpose and scope

1.1 This system defines the risk policy and risk management tools that SEG uses for managing threats to achieving SEG's objectives.
1.2 The objective of SEG's Risk Management Plan is to minimise risk to SEG's objectives and values.
1.3 The SEG Risk Management System is an integral part of the SEG Management System, and relates directly to the SEG Theory of Change, SEG MEL System and SEG Assurance System.
1.4 In many ways SEG is implicitly designed to manage threats to the environment and to the livelihoods and health and safety of those who fish, process and trade in eels and eel products, those who depend on them, and those who choose to purchase certified products.

2 Definitions

2.1 a 'threat' is any event, action, potential action, or inaction that could impede BCI achieving its objectives. Threats may be reputational (e.g. fraud), organisational (e.g. unclear requirements) or external (e.g. climate change, or competition).
2.2 Threats have associated 'risks', which are a combination of the likelihood of a threat actually happening and the impact it has if it happens. So, a risk may be high or low.
2.3 'Vulnerability' exists where risk management does not adequately reduce a threat to an acceptable risk level.

3 Risk policy

3.1 SEG experiences diverse threats to its values, and its ability to reach its objectives. The risk management system will manage these threats, and ensure all stakeholder values are adequately taken into account.
3.2 Reducing risk to zero is not SEG's aim, even if it were achievable. SEG therefore seeks to:
3.2.1 determine optimum risk for each significant threat it faces, and
3.2.2 manage risk in a balanced, monitored way, consistent with SEGs's values and achieving SEG's objectives.
3.3 To achieve these aims threats will be identified, even if they may remain outside SEG's control, and risk will be managed to:

3.3.1 lower vulnerability,
3.3.2 lower the overall impact on SEG's objectives and values, and
3.3.3 optimise SEG's response to challenges and opportunities.

3.4 SEG's ongoing employment of quality staff, governance systems, stakeholder consultations, requirement of certification bodies, and ISEAL community membership, are all part of this risk management.

3.5 SEG is managing risk for a very wide range of stakeholders. It is therefore important for SEG to consider:

3.5.1 where does the impact fall if a threat is not adequately responded to, and
3.5.2 how its stakeholders perceive risk, and their tolerance of risk.

3.6 A good risk management system helps SEG maximise opportunities, target resources effectively, and engage stakeholders effectively.

3.7 SEG's Risk Management System also facilitates identification and wise responses to external and organisational threats that may be difficult to determine from within.

4 Responsibility

4.1 Responsibility for implementing SEG's risk policy is shared across all parts of SEG.

4.2 Oversight of the policy, guidance on risk targets and annual review of risk management is a Board responsibility, with a named position responsible for reporting to the Board on implementation, including on revisions to the Risk Register and Management Plan.

4.3 SEG personnel are responsible for regularly reviewing the Threat Register, implementing appropriate parts of the Risk Management Plan and reporting on progress, challenges and opportunities.

4.4 Co-ordination of the Threat Register and Risk Management plan is the responsibility of named position, who is also responsible for ensuring sufficient inclusion and consideration of organisational and external threats.

4.5 SEG will use the following tools as part of implementing this Risk Policy.

4.5.1 A co-ordinated, annually-reviewed Threat Register.
4.5.2 A co-ordinated, annually-reviewed Risk Management Plan that categorises the identified threats, assigns each a risk rating and target risk rating, and sets out mitigation and monitoring responsibilities and schedules.
4.5.3 A root cause analysis of threats to inform the Risk Management Plan
4.5.4 An annual Board review of the Threat Register and Risk Management Plan.

5 Threat Register

5.1 SEG maintains a Threat Register of all the significant real and potential threats to SEG achieving its objectives.

5.2 The Threat Register relates to all parts of SEG's work, i.e.is not solely related to assurance.

6 Risk Management Plan

6.1 For each entry in the SEG Threat Register, SEG assesses the likelihood over five years and the impact, combing the two into a risk rating.

6.2 For each entry in the SEG Threat Register, SEG determines the target risk level. The extent of the gap between the risk rating and the target risk level (the vulnerability) is used to determine where further mitigation is required and prioritize action.

6.3 For each prioritized threat, SEG determines the necessary additional mitigation, and where responsibilities lie for necessary actions including gathering data to monitor and evaluate the success or otherwise of the mitigation.

6.4 For each prioritized threat SEG also sets a review schedule proportionate to the risk rating and risk vulnerability.

7 Root cause analysis

7.1 SEG uses Risk Root Cause Analysis to help highlight the underlying threats that may be in common across much of the Threat Register, and the mitigation of which may simultaneously and efficiently tackle many of the identified treats.

8 Risk review

8.1 The SEG Board reviews the Threat Register and Risk Management Plan on at least an annual basis. Selected prioritized risks may be reviewed more frequently. Such reviews consider, as a minimum:

8.1.1 whether any threats need to be added to the register,

8.1.2 whether any risk assessments need to be added or updated,

8.1.3 whether any risk target levels and associated vulnerabilities need to be added or updated,

8.1.4 whether mitigation metrics and indicators, schedules, responsibilities, and communications need to be added or updated, and

8.1.5 whether the schedule and responsibility for the review itself can be improved.