Oxford Policy Management

Enterprise Risk Management Policy

Global

March 2024

About Oxford Policy Management

Our vision is for fair public policy that benefits both people and the planet. Our purpose is to improve lives through sustainable policy change in low- and middle-income countries.

Through our global network of offices, we work in partnership with national Stakeholders and decision makers to research, design, implement and evaluate impactful public policy. We work in all areas of economic and social policy and governance, including health, finance, education, climate change and public sector management. We have cross-cutting expertise in our dedicated teams of monitoring and evaluation, political economy analysis, statistics, and research methods specialists. We draw on our local and international sector experts to provide the very best evidence-based support.

Oxford Policy Management Limited
Registered in England: 3122495

Ground Floor
40-41 Park End Street
Oxford, OX1 1JD
United Kingdom

Tel: +44 (0) 1865 207 300
Fax: +44 (0) 1865 207 301
Email: admin@opml.co.uk
Website: www.opml.co.uk
Twitter: @OPMglobal
Facebook: @OPMglobal
YouTube: @OPMglobal
LinkedIn: @OPMglobal

Key Definitions

Term	Definition
Accountable	To be ultimately answerable to the organisation's Stakeholders for a decision, action or results. The accountable individual or body may take responsibility for completing the necessary actions, but more often will delegate it to another.
Assurance	The process by which you test or audit the controls and monitoring practices in place. This can be carried out internally or by third party external providers.
Board	The Board of Directors of Oxford Policy Management Limited.
Consequence	The outcome of an Event and has an effect on objectives. A single Event can generate a range of consequences which can have positive and negative effects on objectives. Initial consequences can also escalate through knock-on effects.
Contractors	Persons with an individual contractual relationship with OPM.
Event	One occurrence, several occurrences, or even a non-occurrence. An Event can also be a change in circumstances. Events are sometimes referred to as incidents or accidents. Events always have causes and usually have consequences. Events without consequences are sometimes referred to a near-misses, near-hits or close-calls.
FARCC	Finance, Audit, Risk and Compliance Committee: the sub-committee of the Board of Directors of Oxford Policy Management Limited responsible for matters relating to finance, audit, risk and compliance.
GRCO	Governance, Risk and Compliance Officer, a member of the OPM Legal and Business Governance Team.
OPM, the Organisation or us, we, our	Oxford Policy Management Limited, Oxford Policy Management Limited's subsidiaries and branch and representative offices, wherever located, and Oxford Policy Management Limited's subsidiary's branch and representative offices wherever located.
Probability	The chance that something might happen. It can be defined, determined, or measured objectively or subjectively and can be expressed either qualitatively or quantitatively.
Responsible	To be answerable to the accountable individual or body for ensuring that the action is completed. In most cases the responsible individual or body will complete the action themselves.
Risk	"The effect of uncertainty on objectives"[1]. An effect is a deviation from what is expected which can result in positive or negative consequences. A risk is measured in terms of a combination of the likelihood of a possible Event occurring and the magnitude of its impact on the achievement of objectives.
Risk Analysis	The process used to understand the nature, sources, and causes of the risks that you have identified and to estimate the level of risk. It is also used to study impacts, consequences and to examine the controls that currently exist.
Risk Assessment	The analysis of risk through: Risk Identification, Risk Analysis and Risk evaluation.

[1] ISO 30001

Term	Definition
Risk Appetite	The amount and type of risk that an organisation is willing to take in order to meet its strategic objectives.
Risk Evaluation	The process that is used to compare risk analysis results with risk criteria to determine whether or not a specified level of risk is acceptable or tolerable.
Risk Identification	The process that is used to find, recognise and describe the risks that could affect the achievement of objectives. It also includes the identification of possible causes and potential consequences. Historical data, theoretical analysis, informed opinions, expert advice, and Stakeholder input may be used for risk identification.
Risk Management	Reducing uncertainty by systematically identifying and implementing cost-effective approaches for minimising the effect of threat realisation and maximising the effect of opportunities to the organization.
Risk Management Framework	A set of components that support and sustain risk management through an organisation. It includes our risk management policy, as well as the accountabilities, resources, processes and activities used to manage organisational risk.
Risk Tolerance	The levels of variation the organisation is able to withstand in regard to its Risk Appetite.
SMT	Senior Management Team: OPM's executive leadership team
Staff	Employees at all levels, directors, officers, agency employees, seconded employees, volunteers and interns.
Stakeholder	A person or an organisation that can affect or be affected by a decision or an activity. Stakeholders also include those who have the perception that a decision or an activity can affect them.
you and your	Either Staff, Contractors or both Staff and Contractors as applicable.

Table of contents

1. Introduction

1.1. Document Purpose

"Risk" is commonly regarded as a negative term, however, risk management is as much about exploiting potential opportunities as preventing potential problems. The aim of Risk Management at OPM is to both minimise risk and maximise opportunities in all OPM activities. OPM takes an holistic approach to the management of risks and business opportunities to improve the likelihood of meeting all our organizational aims. Through our Risk Management Policy and Framework, OPM seeks to:

- manage risk effectively;
- evaluate courses of action to support decision-making;
- safeguard Stakeholders and the organisation from harm;
- protect assets and the environment; and
- protect the OPM's public image.

2. Whom does this policy apply to?

This policy applies to the whole of OPM including branches and subsidiaries. It applies to all OPM Staff and Contractors and to all activities and processes associated with the operation of OPM. It is the responsibility of all OPM Staff and Contractors to understand and respond to risk through the following practices associated with any activity, function or process within the scope of their responsibility and authority:

- Timely Risk Assessment;
- identification and implementation of proportionate responses; and
- ongoing monitoring and communication of risks.

The policy impacts across all OPM policies, operating procedures and training programmes. Its contents will be applied in daily activities by SMT, Staff and Contractors.

3. Policy Statement

3.1. Principles

OPM will manage **Risk** effectively and in a consistent manner in all aspects of its business. All management levels will develop and encourage a culture of well-informed risk-based decision making.

This Enterprise Risk Management policy is based on three key principles:

- Honesty and Transparency
- Proportionality
- Accountability

Effective **Risk Management** relies upon open and effective communication, proportionate and timely responses, combined with clear accountabilities including named ownership of individual risks. To this end **OPM** will foster a culture of openness around **Risk** to support informed decision-making.

3.2. OPM's Commitment

OPM commits to:

- Make Risk Management a core factor in our decision making, so that, proportional resources are deployed to manage risks or opportunities that may affect our business objectives.
- Encourage and support our Staff in positive risk taking, within our stated Risk Appetite, particularly where it leads to growth and / or market innovation
- Maintain a clear Risk Appetite statement, to communicate it across the organisation, and encourage all Staff and Contractors to make decisions consistent with that statement, escalating risks promptly as necessary.
- Establish and maintain organisation-wide procedures and processes to ensure compliance with this policy, and remain consistent with other organisations facing similar risks.
- Provide clearly defined and documented roles and responsibilities for Risk Management, with risks being managed at the lowest level at which the manager has the authority and resources to take effective action.
- Ensure risks and opportunities are managed in an integrated way across all levels of the organisation covering the key interdependencies i.e. strategic, function-level, and project-level risks.
- Develop and maintain a robust continuous improvement and learning culture, which learns from internal and external experience, ensuring that OPM manages risks within our stated Appetite and exploits opportunities as fully as possible.
- Ensure effective assurance arrangements are in place to monitor risk management processes on a routine basis.

4. OPM's Appetite for Risk

OPM's Risk Appetite is set and approved by the Board. OPM maintains Risk Appetite Statement by assessing the organisation's openness to taking risks across key areas of our

business using the four-point scale, ‘Averse’, ‘Cautious’, ‘Open’, and ‘Eager’. The Statement conveys the amount and type of risk OPM is willing to take in order to meet its strategic objectives.

The Risk Appetite assessment is undertaken annually and the Risk Appetite Statement adjusted accordingly.

“OPM’s appetite for risk is CAUTIOUS in many areas, but with a strong appetite for growth our approach is more OPEN in regard to our business development strategy, and the technical capability required to hit our growth targets.

Being CAUTIOUS means OPM generally has a centralised approach to decision-making and is always willing to consider low risk actions which support delivery of our priorities / objectives.

As OPM aspires to decentralise and empower our teams to take more risks over time we expect our appetite to become increasingly OPEN to risk-taking. To ensure this shift is undertaken in a controlled manner we plan to develop frameworks to enable a greater level of devolved decision-making in the medium-term.”

OPM’s full Risk Appetite Statement is available in the Enterprise Risk Management Framework.

All risk identified as outside OPM’s Risk Appetite must be escalated to senior management for review.

5. Assessment and Categorisation of Risks

5.1. Risk Assessment

OPM’s approach to Risk Assessment requires first systematic Identification, then Analysis and finally Evaluation of its risks. We measure our risks using a five-point scale which combines the likelihood of a possible Event occurring and the magnitude of its impact on the achievement of objectives. The tables below define the terms used in measurement.

Please note that the Impact definitions should be used in the first instance, the possible quantitative effect has been given as supplementary guidance, and the thresholds given refer to corporate risks. Thresholds must be adjusted for Function- and project-level risks.

Descriptor	Impact Definitions	Quantitative Effect (£)
Negligible	The consequences may result in negligible disruption to OPM’s operations, which should be easily recoverable.	<10k

Descriptor	Impact Definitions	Quantitative Effect (£)
Minor	The consequences may result in some minor injuries to OPM Staff and Representatives, possible damage to or loss of some equipment and facilities and limited delays to operations. Limited financial and/or reputational impact.	10k - 30k
Moderate	The consequences may result in injury to OPM Staff and Representatives which requires limited hospital treatment, significant loss of or damage to equipment and facilities, and delays to operations. Material (but manageable) financial impact. Reputational damage with local media coverage. Minor client relationship damage.	30k - 150k
Severe	The consequences result in severe injury to OPM Staff and Representatives, significant loss of or damage to equipment and facilities and major delays or cancellation of OPM projects. Major financial impact. Bribery or fraud committed on behalf of the company. Reputational damage with national media coverage. Significant client relationship damage.	150k - 750k
Critical	Consequences are catastrophic, resulting in the death or severe injury of OPM Staff or Representatives, major loss of equipment and facilities, and cancellation of OPM Projects. Financial impact which fundamentally undermines the continued existence of the company or has a fundamental effect on the relationship with the Company's shareholders or bank. Bribery or fraud committed by senior management. Reputational damage with worldwide coverage. Questionable whether recovery is possible.	750k+

5.2. Risk Categorisation

Following the identification and analysis of risks they are categorised to assist with our evaluation of risk exposure. All risks on the Corporate Risk Register are categorised using a the following schema which is aligned to OPM's strategic business plan.

Risk Type	Description
Strategic risk	Any risk to OPM arising from changes in its business, including the risk of the OPM business model or strategy proving inappropriate due to macroeconomic, geopolitical, industry, regulatory or other external factors. The risk that arises from significant investments or from changes to strategy and business direction for which there is a high uncertainty about success and profitability.

Financial risk	The risk that OPM, although solvent, may not have sufficient financial resources to enable it to continue to meet its obligations or may only secure such resources at excessive cost. The risk to earnings posed by falling or volatile income. Insolvency or default of client.
Operational risk	The risks resulting from inadequate or failed internal processes or systems, including business continuity risks. Risks related to the delivery of core business. Risks related to the effective management of business functions. The risk of a contractor failing to meet its contractual obligations, or the increased risk of default during the term of the transaction
Security risk	Risk affecting the security, health or wellbeing of Staff, Contractors and other Stakeholders.
Compliance risk	The risk that OPM may not act in accordance with legislative or client requirements whether purposefully or accidentally. People risks related to non-conformance with policy, process and procedures, including safeguarding. Risks related to OPM conducting business in a way that is inconsistent with its values, or that OPM is unable to demonstrate that it follows regulations and ethical practices.

6 Roles and responsibilities

5.3. Responsibilities for this policy

The Board is accountable for OPM's Enterprise Risk Management Policy as exercised through the oversight and approval of this document.

The table below details which bodies and individuals are Accountable or Responsible for various elements within this Enterprise Risk Management Policy and the Risk Management Framework that sits under it.

What	Who	Role
Risk Appetite & Culture	FARCC	Accountable for defining OPM's Risk Appetite in relation to strategic business plan and high-level objectives. Sets 'tone at the top'.
	SMT	Responsible for defining Risk Appetite. Responsible for promotion of a healthy Risk Culture through role-modelling to Staff and Contractors on behalf of Board.

What	Who	Role
	GRCO	Responsible for creating a risk-aware culture across Staff and Contractors, and ensuring widespread knowledge of OPM's Risk Appetite.
Risk Management Policy	FARCC	Responsible for scrutiny and quality assurance of OPM's Risk Management Policy on behalf of the Board. Responsible for verifying OPM's adherence to its Risk Management Policy through scrutiny and review.
	SMT	Responsible for establishment of OPM's Risk Management Policy and its integration with other business planning and management activities.
	GRCO	Responsible for maintaining and updating OPM's Risk Management Policy through periodic review and of this document, and as required by the SMT.
Risk Management Framework & Processes	SMT	Accountable for establishment of OPM's Risk Management Framework and processes.
	GRCO	Responsible for establishment of OPM's Risk Management Framework and processes therein. Responsible for overseeing Risk Management processes, both their design and effective implementation. Responsible for cross-functional coordination of risk management, including advising on specific aspects of Risk Management.
	Project Director	Accountable for Risk Management within the scope of their project(s).
Identification, Assessment & Recording of Risk	Board	Accountable for the Identification of strategic risks that impact on the sound financial and reputational standing of OPM in collaboration with the SMT.
	FARCC	Responsible for Analysing and recording strategic risks identified by Board Members.
	SMT	Responsible for timely Identification and Analysis of strategic risks that impact on the sound financial and reputational standing of OPM in collaboration with the Board, as well as other business risks which fall under their area of responsibility

What	Who	Role
	GRCO	Accountable for the standardisation of Assessment and recording of risks, through common terminology and methodology. Responsible for recording strategic risks identified by SMT Members.
	Project Boards	Accountable for the Identification, Analysis and recording of project-level risks.
Monitoring risks and OPM's responses to those risks	Board	Accountable for monitoring and overseeing strategic risks as captured in the Corporate Risk Register.
	FARCC	Accountable for scrutiny and challenge of OPM's responses to Risk through periodic risk reviews.
	SMT	Accountable for ensuring escalation processes are in place and working effectively. Responsible for monitoring and overseeing strategic risks as captured in the Corporate Risk Register.
	GRCO	Responsible for monitoring OPM's responses to strategic risks as captured in the Corporate Risk Register. Responsible for coordinating responses where risks impact more than one area.
	International Office Directors	Accountable for risk management processes in the relevant International Office. Responsible for monitoring and overseeing country-level risks as captured in the Office Risk Register.
	Project Boards	Accountable for ensuring that adequate responses to project-level risks are in place.
Reporting	SMT	Accountable for quarterly reporting to FARCC, providing updates on risks.
	GRCO	Responsible for maintaining quality within Risk Management. Responsible for reporting the status of escalated risks to the SMT and the FARCC, including recommended actions.
	Project Boards	Accountable for periodic highlight reporting of project-level risks to SMT via GRCO.

What	Who	Role
Learning & Training	SMT	Accountable for the development of risk management guidance and training, and ensuring appropriate Staff are adequately trained in risk management.
	GRCO	Responsible for promoting competence throughout the company, including development of risk management guidance and delivering risk management training.

5.4. Your Responsibilities: what we expect from you

You are Responsible for keeping yourself informed about OPM's Risk Management Policy; for adhering to OPM's Risk Management Framework and the processes within it. You are expected to maintain your own competence through attending OPM's mandatory Enterprise Risk Management training, to ensure You understand Risk Management terminology and OPM's measurement methodology.

You are Responsible for the identification, analysis and recording of risks within the scope of Your own role.

You are Responsible for communicating updates and risk mitigation/potential issues with Your line management.

You are Accountable for escalating risks which require a higher level of authority, when appropriate.

6. Quality, Improvement and Review

OPM's GRCO has overall responsibility for maintaining the quality of this Risk Management Policy (and the processes and procedures that flow from it) and for its ongoing improvement, on behalf of the Board and SMT. Quality will be maintained through the following procedures:

- Provision of regular Enterprise Risk Management Guidance & Training
- Annual Review of all Enterprise-level Risk Management Documentation
- Periodic Review of Function-level Risk Registers
- Liaison with OPM Project Management Office to ensure that they have appropriate governance structures in place to review project-level Risk Registers

6.1. Guidance & Training

OPM will ensure that that all Staff and Contractors are aware of this policy and that relevant Staff receive appropriate training in the implementation of this policy.

6.2. Risk Management Documentation Reviews

The Risk Management Policy, the Risk Management Framework and processes, OPM's Corporate Risk Register and any associated training materials will be reviewed bi-annually by the GRCO. The findings of the review will be reported to the SMT. The SMT may make recommendations for change to be considered, challenged and approved by the FARCC, on behalf of the Board.

6.3. Risk Register Reviews

Individuals responsible for receiving Highlights Reports will undertake reviews of individual Risk Registers as needed. When reviewing a Risk Register the individual should verify the integrity of the information recorded, and assess suitability of the responses proposed and their efficacy.

Risk Registers define current risks across the business and provide a graphic illustration of trends sufficient to enable senior management and the Board to appreciate the current and trending risk profile of OPM

Reviews of Highlight Reports and individual Risk Registers will allow for the identification of links between risks highlighted in different areas of the business or common risk responses adopted. At an enterprise level, common risks may be aggregated or considered together. Likewise risks that are addressed by a common response may be aggregated or grouped. The GRCO will have a view across the various Risk Registers.

Enterprise Risk Management Policy

Document Purpose:

The aim of Risk Management at OPM is to both minimise risk and maximise opportunities in all OPM activities. Through our Risk Management Policy OPM seeks to:

- manage risk effectively;
- evaluate courses of action to support decision-making;
- safeguard Stakeholders and the organisation from harm;
- protect assets and the environment; and
- protect the OPM's public image.

Policy Overview			
Policy Owner	Head of Legal		
Applies to	Employees at all levels, directors, officers, agency employees, seconded employees, volunteers and interns. Contractors.		
Global or local scope	Global		
Version Number	3.0	**Effective from**	01.03.2024
Approvals (Dates)		**Board**	23.02.2024
		Policy Authorisation Committee	16.02.2024
		Other (please state)	[Date]