CORPORATE POLICY

Risk Management and Internal Control Policy

POLICY NUMBER	OPES-POL-05
VERSION	IFC
POLICY OWNER	Managing Director
APPROVED BY	Board of Directors, 6 March 2025
EFFECTIVE DATE	6 March 2024
NEXT REVIEW	12 months after approval
APPLIES TO	All OPES activities, engagements and projects

1. Purpose

This policy sets out how OPES identifies, assesses, manages and reports risks to its people, clients, finances, reputation and the communities where it works. It also sets the minimum internal controls that protect OPES's assets and the integrity of its records.

2. Principles

OPES follows the principles of ISO 31000 (Risk management) and the COSO Internal Control framework. Risk management is:

- **Integrated** into strategy, business development, project delivery and financial decisions
- **Proportionate** to the size and complexity of each activity
- **Informed** by the best available information, including local knowledge
- **Continuous**, with risks reviewed as circumstances change

3. Risk categories

Category	Examples
Strategic	Market changes, loss of key clients, policy shifts in Ghana's energy and mining sectors
Financial	Currency movements (cedi, NOK, USD), late client payments, cash flow
Compliance and integrity	Bribery, sanctions, conflicts of interest, regulatory breaches
Operational and project	Delivery delays, quality failures, subcontractor performance

Category	Examples
Health, safety and environment	Site visits, offshore and mining environments, road travel
Environmental and social	Impacts on communities, land, labour conditions in client projects
Information and cyber	Data breaches, loss of confidential client information
Reputational	Association with controversial projects, partners or individuals

4. Risk appetite

The Board sets OPES's risk appetite and reviews it each year.

- **Zero tolerance:** bribery and corruption, sanctions breaches, fraud, SEAH, child or forced labour, and any knowing breach of law
- **Very low:** risks to health and safety, and serious environmental or social harm
- **Moderate:** commercial and financial risks taken in pursuit of growth, where they are understood and managed

5. The risk management process

1. **Identify** risks at company level, and for every new engagement, project or partner.
2. **Assess** each risk for likelihood and impact on a 5 × 5 matrix, giving a rating of Low, Medium, High or Critical.
3. **Treat** each risk by avoiding, reducing, transferring (for example through insurance or contract terms) or accepting it within appetite.
4. **Record** risks, owners, actions and deadlines in the Corporate Risk Register and in each project risk register.
5. **Monitor and report** risks regularly, and escalate those rated High or Critical.

Rating	Who must be informed	Review frequency
Critical	Managing Director and Board Chair immediately	Weekly until reduced
High	Managing Director within 48 hours	Monthly
Medium	Risk owner and line manager	Quarterly
Low	Risk owner	Annually

6. Engagement and partner screening

Before accepting any engagement, OPES completes an Engagement Risk Assessment covering the client, the project, the country and sector context, integrity and sanctions screening, conflicts of interest and environmental and social risks. Engagements with Critical risks that cannot be mitigated are declined.

7. Internal controls

OPES maintains the following minimum controls:

- **Segregation of duties:** no single person can initiate, approve and record the same payment
- **Delegation of authority:** a written schedule sets out who may approve contracts, payments and commitments, and up to what value
- **Dual authorisation:** for all payments above USD 5,000 and all payments to new suppliers

- **Bank controls:** all payments are made by bank transfer to accounts in the payee's name; cash is limited to a small, reconciled petty-cash float
- **Reconciliation:** bank accounts reconciled monthly and reviewed by a second person
- **Records:** financial and project records kept for at least seven years
- **Independent audit:** annual accounts audited by an independent external auditor
- **Insurance:** professional indemnity, public liability, employer's liability and travel insurance maintained at appropriate levels

8. Business continuity

OPES maintains a business continuity plan covering loss of key personnel, IT systems and office access, and security incidents affecting staff travelling in the field. The plan is tested at least once a year.

9. Roles and responsibilities

Role	Responsibility
Board of Directors	Sets risk appetite, approves this policy and reviews the Corporate Risk Register at least twice a year
Managing Director	Owns this policy, the Corporate Risk Register and the internal control environment
Compliance Officer	Supports risk assessments, integrity screening and control testing
Engagement and project leads	Maintain project risk registers and escalate risks
All personnel	Identify and report risks and follow controls

10. Monitoring and review

The effectiveness of risk management and internal controls is reviewed annually by the Board, informed by the external audit, any internal reviews and incident reports. This policy is reviewed at least every 12 months.