UKRAINE
NGO «INTERNATIONAL ANTI-CORRUPTION ASSEMBLY»
Legal entity identification code 40030266,
15/3, E. Konovalets str., Kyiv, 03150
tel. num.: +38 068 843 65 93; +38 050 843 90 83
e-mail: info@iacassembly.org, http://www.iacassembly.org

RISK MANAGEMENT POLICY

Document	Risk Management Policy
Organization	Non-Governmental Organization "International Anti-Corruption Assembly" (NGO "IACA")
Version	7.0
Approved	February 25, 2026
Approved by	Secretary General of the Central Committee of NGO "IACA"
Contact for reports	iaca@iacassembly.org

Legal Entity Identification Code (EDRPOU): 40030266
Registration Certificate No. 1448234 dated 24 September 2015

12-A Zhylianska Street, Office 101, Kyiv 01033, Ukraine
www.iacassembly.org/en/ | info@iacassembly.org

1. General Provisions

The Non-Governmental Organization "International Anti-Corruption Assembly" (hereinafter referred to as the "Organization" or "IACA") implements a systematic approach to risk management as an integral part of ensuring the integrity, resilience, and effectiveness of its activities.

This Risk Management Policy establishes a unified framework for the identification, assessment, treatment, monitoring, and review of risks across all areas of the Organization's activities, regardless of the country in which projects are implemented.

This Policy has been developed in accordance with:
- The Charter of the Organization (2019 revised edition approved by the General Assembly);
- The legislation of Ukraine (including the Law of Ukraine "On Prevention of Corruption", the Law of Ukraine "On Public Associations", and other applicable legislation);
- The United Nations Convention against Corruption (UNCAC), particularly Articles 5, 7, and 13;
- ISO 31000:2018 "Risk Management — Guidelines";
- The COSO Enterprise Risk Management (ERM) Framework, adapted for non-profit organizations;
- Recommendations of Transparency International, OECD, USAID, and other international donors regarding risk management for non-governmental organizations;
- The Independence-First Principle, ensuring the Organization's independence while receiving external funding.

2. Purpose of the Policy

- To ensure the systematic identification, assessment, and management of risks of all types;
- To minimize the adverse impact of risks on the achievement of the Organization's statutory objectives;
- To ensure organizational resilience, stability, and the capacity to withstand external challenges;
- To improve decision-making through risk-based analysis;
- To protect the reputation, resources, members, participants, and beneficiaries of the Organization;
- To support the Organization's hybrid operating model while preserving its independence.

3. Scope of Application

This Policy applies to all areas of the Organization's activities, including:
- Programmatic, project, and international activities;
- Financial and administrative operations, including grant management;
- International cooperation and the activities of Separate Subdivisions and Representative Offices (Clause 1.16 of the Charter);
- Work involving employees, volunteers, partners, and beneficiaries;
- Information security and communications.

This Policy is mandatory for:
- The General Secretary;
- Members of the General Assembly, the Central Committee, and the Audit Commission;
- Employees (both staff and non-staff personnel), volunteers, and interns;
- Heads of Separate Subdivisions and Representative Offices;
- Contractors and partners participating in joint projects.

4. Types of Risks

The Organization recognizes the following principal categories of risks, taking into account ISO 31000 and anti-corruption best practices:
- Strategic risks (failure to achieve the mission, loss of influence or relevance);
- Operational risks (process failures, project implementation risks);
- Financial and fraud risks (misuse of funds, misappropriation of assets);
- Reputational risks (loss of trust among donors, partners, beneficiaries, or the public);

- Legal and compliance risks (violations of laws, regulations, contracts, or donor requirements);
- Safeguarding risks (including Child Safeguarding and Protection from Sexual Exploitation and Abuse (PSEA));
- Information security and data protection risks;
- External risks (political, geopolitical, military, economic, regulatory, or other external factors).

5. Core Principles of Risk Management

- Proactivity, systematic implementation, and integration into all organizational processes in accordance with ISO 31000;
- Proportionality of risk management measures to the Organization's scale, resources, and operating model;
- Transparency, accountability, and proper documentation;
- Continuous learning and awareness-building among personnel and volunteers;
- Priority of preventive measures and adherence to the Independence-First Principle;
- Integration with anti-corruption, ethical, and governance policies.

6. Risk Management Process (in accordance with ISO 31000)

6.1. Risk Identification

Regular collection of information from management, members, employees, volunteers, and partners to identify existing and emerging risks.

6.2 Risk Analysis and Assessment

Assessment of the likelihood, potential impact, and overall level of identified risks.

6.3 Risk Treatment

Selection of an appropriate response strategy, including risk avoidance, risk reduction, risk transfer (through insurance, contractual arrangements, or other mechanisms), or risk acceptance.

6.4 Monitoring, Review, and Communication

Regular monitoring of the effectiveness of risk management measures, communication with relevant stakeholders, and periodic updates to the Risk Register.

7. Responsibilities

7.1 General Secretary

The General Secretary is responsible for implementing the risk management system, coordinating risk management activities, and reporting significant risks to the Central Committee.

7.2 Central Committee

The Central Committee approves key organizational risks, the Risk Register, and strategies for risk mitigation and management.

7.3 Audit Commission

The Audit Commission provides independent oversight of financial, operational, and fraud-related risks in accordance with Clause 5.2 of the Charter.

7.4 All Employees and Volunteers

All employees and volunteers are responsible for identifying risks within their areas of activity, reporting them promptly, and complying with established control measures.

8. Related Documents

This Policy forms part of the Organization's integrated internal governance framework and is linked to:

- Anti-Corruption Policy;
- Anti-Fraud Policy;
- Conflict of Interest Policy;
- Code of Conduct;
- Data Protection and Privacy Policy;
- Financial Procedures and Procurement Policy;

- Whistleblowing and Whistleblower Protection Policy.

9. Final Provisions

The Policy shall be reviewed at least once annually, or whenever significant changes occur in the external environment, applicable legislation, international standards, donor requirements, or the Organization's activities, to ensure its continued relevance and effectiveness.

Approved by:

General Secretary of the Central Committee
NGO "International Anti-Corruption Assembly" _____ Viacheslav Sayenko