

APPROVED

11.07.2024. BIA Senate meeting

(Protocol No. 165)

RISK MANAGEMENT POLICY of the Baltic International Academy

I. General issues

1.1. The Risk management policy has been developed in accordance with the development strategy of the Baltic International Academy (hereinafter - BIA) and is a component of the BIA quality assurance system.

1.2. Risk management is applied in all areas of BIA activity. The principles set out in the risk management policy are binding on all BIA employees.

1.3. The purpose of the Risk management policy is to determine a unified approach to the risk management process in BIA, to determine the basic principles of BIA Risk management, the framework of the system, as well as the division of responsibility in the implementation of the risk management process, the parties involved in Risk management and the monitoring of management processes.

1.4. Terms used in the BIA Risk management policy:

Risk – the possibility of an event or circumstance that may negatively affect the implementation of BIA activities and/or the achievement of strategic goals;

Risk management – a systematic process of identifying and controlling risks, which is implemented with the aim of minimizing and eliminating shortcomings and non-compliances in the activities of the BIA;

Risk identification – the process of monitoring risks, their identification, recognition and description;

Risk analysis – the collection and evaluation of data and information, with the aim of determining the impact of the risk and determining its level;

Risk assessment – the process of comparing the results of risk analysis and risk appetite criteria to determine whether the risk is acceptable or changeable;

Risk owner – a designated responsible personnel person responsible for analyzing, assessing

the specific risk, determining control measures and deadlines, as well as implementing risk mitigation measures.

II. Risk management objectives and tasks

2.1. Effective Risk management ensures timely prediction, identification and prevention of: risks in the implementation of BIA activities and/or in achieving strategic goals, potential damage to BIA's reputation, financial situation and operational activities, as well as allows ensuring compliance with legal requirements.

2.2. The Risk management process identifies, determines and controls those risks that are essential for the high-quality performance of BIA functions and the achievement of strategic goals.

2.3. Risk management objectives:

2.3.1. To promote the achievement of the overall goals set by BIA and/or the goals set for the specified period;

2.3.2. To facilitate decision-making under conditions of uncertainty;

2.3.3. To prevent inefficient use of financial and other resources;

2.3.4. To identify the negative consequences of possible events that may potentially affect the achievement of the goals set by BIA, the implementation of processes and projects;

2.3.5. To achieve an acceptable risk value by implementing risk mitigation measures, and after achieving an acceptable risk value, to ensure an acceptable risk value through controls;

2.3.6. To take measures to reduce future losses from undesirable events and to increase benefits at the existing risk level in the BIA.

2.4. Risk management tasks:

2.4.1. To identify, assess and analyse risks, their probability of occurrence and possible consequences;

2.4.2. To plan and manage risk mitigation and supervision (control and monitoring) measures.

III. Basic principles and categories of Risk Management

3.1. Risk management is a cyclical and regular process of strategic importance, which is implemented in a timely manner in response to external and internal changes and/or events.

3.2. Systematic and regular Risk management contributes to the achievement of BIA's goals, implementation and management of processes, reducing adverse impacts and ensuring timely response, preventing excessive risks in BIA's areas of activity and taking risks only in known

areas of activity.

3.3. The Risk management process includes risk identification, analysis and assessment, determination of the risk owner, reporting and informing, determination and implementation of risk mitigation and/or control measures, and risk monitoring.

3.4. BIA personnel and other involved parties participate in risk management. Every BIA employee is involved in identifying risk events, but BIA structural unit managers are involved in identifying risks.

3.5. BIA manages the following categories of risks:

3.5.1. strategic risks: global trends, political influence, economic situation, reputational risks, etc.;

3.5.2. *financial risks*: availability of funding, inadequate funding planning, etc.;

3.5.3. *operational risks*: personnel errors, inconsistencies of information technology and systems, inconsistencies and/or shortcomings of internal processes, risks with an impact on the work environment;

3.5.4. *legal and compliance risks*: non-compliance with or improper interpretation of regulatory requirements, personal data protection risks, etc.;

3.5.5. *corruption risks*: the likelihood that one of the staff representatives will act in their own or another person's material interests, obtaining for themselves or others undue benefits and causing harm to the BIA;

3.5.6. *risks of violations of ethical norms*: risks related to violations of the BIA Academic Honesty and Ethics Code;

3.5.7. *project risks*: risks related to project application, implementation and ensuring their sustainability.

3.6. The impact of risks shall be assessed in relation to the possible:

3.6.1. financial consequences that the risk may cause;

3.6.2. damage to reputation;

3.6.3. compliance violations.

3.7. The requirements and principles set out in the Risk management policy are binding on all BIA personnel.

3.8. In order to ensure a uniform and harmonised approach to the implementation of Risk management, the division of responsibilities for BIA risk management and their implementation are determined in internal regulatory enactments related to the Risk management policy.