

APPROVED
by the Board of Directors
of Air Astana JSC
Minutes No.196 dated 05 September 2019

Policy on Internal Control System of Air Astana JSC

Almaty 2019

Contents

1. General Provisions	3
2. Main Terms	4
3. Goals and objectives of the Internal Control System	6
4. Control Environment	7
5. Risk Assessment	10
6. Control Activities.....	12
7. Information and Communication.....	15
8. Monitoring Activities.....	17
9. Report of the Board of Directors on Internal Control.....	19
Appendix 1. Matrix of Risks and Controls	20

1. General Provisions

- 1.1. The Policy on Internal Control System of “Air Astana” JSC (hereinafter referred to as the "Policy") has been developed in accordance with the recommendations of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the legal and regulatory acts governing the activities of “Air Astana” JSC (hereinafter referred to as the "Company"), as well as with the Company's internal documents approved by the Company's Board of Directors.
- 1.2. The purpose of this Policy is to establish principles, guidelines and responsibilities to be observed for the strengthening and effective functioning of Company’s Internal Control System (ICS), with a view to mitigating risks, and to disseminate the controls culture in order to assure compliance with the laws, regulations and other norms established by the regulatory authorities and by the Company.
- 1.3. Additionally, Policy is aimed at enhancing the efficiency of ICS and implementing documented and monitoring of Control Procedures.
- 1.4. Company’s Internal Control System is based on “COSO Internal Control—Integrated Framework”, which consists of five components and 17 principles relating to each component. Internal control is focused on achievement of operational goals, reporting goals and on compliance with legislation and internal regulations.

2. Main Terms

In the framework hereof, the following main terms and definitions shall mean as follows:

- **Application Controls** – programmed procedures in application software and related manual procedures designed to help ensure the completeness and accuracy of information processing.
- **Automated Controls** – control activities mostly or wholly performed through technology (e.g., automated control functions programmed into computer software; contrast with Manual Controls).
- **Business process risk owner** – the owner of business-process.
- **Category** – one of three groupings of objectives of internal control. The categories relate to operations, reporting, and compliance.
- **Compliance** – having to do with conforming with laws and regulations applicable to an entity.
- **Control** – policy or procedure that is part of internal control.
- **Control Activity** – action established through policies and procedures that help ensure that management’s directives to mitigate risks to the achievement of objectives are carried out.
- **Control Deficiency** – synonym for Internal Control Deficiency. A control deficiency may also describe a deficiency with respect to a particular control or control activity.
- **Design** – (1) intent; as used in the definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of objectives; when the intent is realised, the system can be deemed effective. (2) Plan; the way a system is supposed to work, contrasted with how it actually works.
- **Detective Control** – control designed to discover an unintended event or result after the initial processing has occurred but before the ultimate objective has concluded (contrast with Preventive Control).
- **External Environment** – anything outside of the Company that influences the ability to achieve strategy and business objectives.
- **Inherent Limitations** – those limitations of all internal control systems. The limitations relate to the preconditions of internal control, external events beyond the entity’s control, limits of human judgment, the reality that breakdowns can occur, and the possibility of management override and collusion.
- **Internal Control Deficiency** – shortcoming in a component or components and relevant principle(s) that reduces the likelihood that the Company can achieve its objectives.
- **Internal Environment** – anything inside of the Company that influences its ability to achieve strategy and business objectives.
- **Major Deficiency** – internal control deficiency or combination of deficiencies that severely reduces the likelihood that the Company can achieve its objectives.
- **Management Intervention** – management’s overruling of prescribed policies or procedures for legitimate purposes when dealing with non-recurring or non-standard transactions or events that otherwise might be handled inappropriately.

- **Management Override** – management’s overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an Company’s financial condition or compliance status.
- **Management Process** – the series of actions taken by management to run the Company. An internal control system is a part of an integrated management process.
- **Manual Controls** – Controls performed manually, not through technology (contrast with Automated Controls).
- **Preventive Control** – control designed to avoid an unintended event or result at the time of initial occurrence (contrast with Detective Control).
- **Procedure** – action that implements a policy.
- **Process risk** – risk of the business process.
- **Reasonable Assurance** – the concept that internal control, no matter how well designed and operated, cannot guarantee that an Company’s objectives will be met. This is because of Inherent Limitations in all internal control systems.
- **Technology General Controls** – control activities that help ensure the continued, proper operation of technology. They include controls over the technology infrastructure, security management, and technology acquisition, development, and maintenance. Other terms sometimes used to describe technology general controls are “general computer controls” and “information technology controls.”
- **Transaction Controls** – control activities that directly support the actions to mitigate transaction-processing risks in Company’s business processes. Transaction controls can be manual or automated and will likely cover the information-processing objectives of completeness, accuracy, and validity.
- **Risk Management unit of Management Accounts and Risk Management Department** – the Company's structural unit responsible for risk management and internal controls issues.

3. Goals and objectives of the Internal Control System

- 3.1. Internal control is a process, affected by the Company's board of directors, senior management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance:
- Operations Objectives – effectiveness and efficiency of the Company's operations, including operational and financial performance goals, and safeguarding assets against loss.
 - Reporting Objectives – internal and external financial and non-financial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, standard setters, or the Company's policies.
 - Compliance Objectives – adherence to laws and regulations to which the Company is subject.
- 3.2. The internal controls are aimed at providing reasonable assurance that Company's objectives relating to external reporting and compliance with laws and regulations will be achieved and is implemented by organising the Internal Control System (ICS). The main goals of the ICS are as follows:
- Enhancing the operational efficiency.
 - Safeguarding of assets and the efficient use of resources.
 - Ensuring the completeness, reliability and accuracy of financial and management reporting.
 - Ensuring the compliance with legal requirements and internal regulations.
 - Decreasing the probability of risk and the potential loss from its realisation.
 - Controlling over the efficient functioning business processes.
- 3.3. ICS of the Company is integral part of the corporate governance and covers all levels of management, all internal processes and operations of the Company.
- 3.4. ICS ensures the building of a management system that is capable of rapid responding to risks, exercising control over business processes and daily operations of the Company, as well as immediately informing of management on any significant shortcomings and areas for improvement.
- 3.5. Engagement and constant cooperation of all employees of the Company is needed for reliable and efficient functioning of the ICS.
- 3.6. ICS of the Company is based on the "COSO Internal Control—Integrated Framework" and consists of five interrelated components:
- Control Environment
 - Risk Assessment
 - Control Activities
 - Information and Communication
 - Monitoring Activities.
- 3.7. The Policy is aimed at improvement of the efficiency of ICS of the Company by means of implementing the order of documenting and monitoring of Control activities.
- 3.8. The objectives of the Policy:
- Defining the roles and responsibilities within ICS of employees of the Company.
 - Description of the process of developing of the Matrix of risks and controls.
 - Description of the monitoring of control activities.

4. Control Environment

- 4.1. The control environment is the set of standards, processes, and structures that provide the basis for execution of internal controls across the Company. It is the foundation of other components of the ICS and it provides a clear structure to participants of the system.
- 4.2. The Board of Directors and senior management establish the tone at the top regarding the importance of internal controls including expected standards of conduct.
- 4.3. Board of Directors and senior management of the Company ensure the establishment of control environment, which demonstrates the significance, importance and necessity of internal controls and compliance with the business ethics norms on all the levels of operations.
- 4.4. Control environment includes:
 - Organisational structure and assignment of authority and responsibility
 - Ethical standards and integrity of the Company
 - Philosophy and management style
 - Personnel policy: the process for attracting, developing, and retaining competent individuals
 - Competence of employees: around performance measures, incentives, and rewards to drive accountability for performance.
- 4.5. The Policy defines the competence of the participants of the system depending on their role in the development, approval, implementation and evaluation of effectiveness of ICS.
- 4.6. Organisational structure of the Company is in line with the international best practices regarding the internal controls where all the participants have clear responsibilities.
- 4.7. **Board of Directors** is responsible for organisation of effective ICS of the Company:
 - approves the Policy on ICS, its updates and changes;
 - takes measures on improvement of the effectiveness of internal controls;
 - regularly reviews the evaluation of the efficiency of ICS.
- 4.8. **Audit Committee** of the Board of Directors is oversight body for effectiveness of Internal Control System with the following responsibilities:
 - analyses reports of external and internal auditors on status of internal control system;
 - analyses efficiency of the tools of the Company's internal control system and give proposals regarding these and other related issues;
 - controls observance of recommendations of the internal and external auditors of the Company regarding the internal control system;
 - analyses results and quality of the measures (remedial steps) elaborated by the Company for the enhancement of the system of internal control.
- 4.9. **Risk Committee**, which is comprised from senior management of the Company, is responsible for implementation of the Policy, reliable and efficient performance of the ICS and the following actions:
 - preliminary approves the Policy, its changes and updates;
 - provides the implementation of the Policy;
 - approves the scope of Action Plan on ICS;

- reviews the reports on deviations and shortcomings within ICS;
 - supports improvements to the internal control environment, always seeking a balance among the effectiveness of the processes, controls and costs, as well as the alignment with the Company's strategic objectives.
- 4.10. **Internal Audit Services** conducts the evaluation of effectiveness of the ICS and provides reports to the Audit Committee and Board of Directors.
- 4.11. **Risk management unit** of Management Accounts and Risk Management department is responsible for organisation and functioning of ICS:
- develops the Policy, regularly reviews and updates the Policy, if necessary;
 - organises and coordinates the activity of the ICS;
 - provides methodological support to business process owners in constant improvement of business processes;
 - provides methodological support to business process owners in the development, documenting, implementation, monitoring and improvement of control procedures;
 - provides methodological support to business process owners in development and update of matrix of risks and controls;
 - identifies the need to implement new controls and/or the need for improvement in existing controls when the absence and/or insufficiency of these result in significant deficiencies;
 - reviews/evaluates the action plans indicated by the business process owners in relation to meeting the objectives of internal controls and mitigation of risks;
 - reviews the new internal regulations for their practicability and their coherency with existent internal regulations;
- 4.12. **Business process owner** is responsible for the following but not limited to:
- ensures that employees of their structural units comply with the Policy;
 - develops, documents, implements, monitors and improves control activities;
 - ensures efficient functioning of their business processes and control activities;
 - ensures the integration of business processes;
 - ensures the inclusion of control activities in to the relevant job descriptions;
 - self-assesses the control activities that are under their responsibility;
 - ensures the execution of existing control activities;
 - develops and implements new internal controls and improves existing control activities;
 - provides information on realisation of process risks to Risk management unit immediately upon identification;
 - provides all the documents regulating the business process (internal regulations, job descriptions and etc.) to Risk management unit as per request;
 - reports any changes in the internal controls (processes, people, and systems) in a timely manner.
- 4.13. **Compliance function** is responsible for ensuring the efficiency and effectiveness of design and implementation of actions in business processes aimed at managing the compliance risks, which include

risks of corruption and fraud as well as non-compliance with the applicable legislations and/or internal regulations.

- 4.14. **Financial controller** is responsible for development and ensuring of control activities in business processes relating to financial management, financial and accounting reporting.
- 4.15. Senior management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- 4.16. Senior management of the Company is responsible for implementation of transparent, reliable and efficient organisational structure of the Company, and its further optimisation and update if necessary in case of change of strategy of the Company, and considering the changes in external factors that affect the Company.
- 4.17. Organisational structure of the Company must be aligned with the strategic goals and objectives and supports:
 - Identification of related and consistent goals and objectives at different levels of the Company;
 - Segregation and delegation of key authorities and responsibilities within the Company;
 - Explicit regulation of employees responsibility and criteria for performance assessment;
 - Proper internal reporting system;
 - Provision of efficient cooperation between structural units and employees of the Company.
- 4.18. Organisational structure of the Company must be regulated by internal regulatory documents with inclusion of goals and objectives, functions, responsibilities, rights, competencies, authority of bodies, structural units and employees of the Company.
- 4.19. Values and Code of Conduct are in place in the Company and reflect vision and understanding of business ethics by the participants of the ICS.
- 4.20. Board of Directors and senior management of the Company undertake necessary actions to decrease and eliminate possibility of unethical and unlawful actions by the employees.
- 4.21. Familiarisation of all new employees with the Code of Conduct shall be performed at the hiring stage. All employees pass training on knowledge of Code of Conduct on annual basis.
- 4.22. All employees are familiarised with the HEART values of the Company, adherence to which is evaluated in accordance with the Company's performance appraisal system.
- 4.23. The Company is committed to attract, develop, and retain competent individuals in alignment with objectives.
- 4.24. Senior management is responsible for development and implementation of human resource policy of the Company, approval of the total number of staff and ensures the compliance with the approved recruitment standards and procedures, transparent appraisal system, training of employees, and other procedures on human resource management.
- 4.25. Senior management is responsible for development and implementation of job descriptions with indication of functions and necessary competences.
- 4.26. Senior management is responsible for development and implementation of procedures on delegation of duties within the organisational structure that define the procedures for monitoring the implementation of assigned tasks and providing feedback to employees.
- 4.27. Business process owners are responsible for monitoring of performance of functional duties by employees as per job descriptions, providing feedback to employees and conducting of performance appraisal.

5. Risk Assessment

- 5.1. Risk assessment involves a dynamic and iterative process for identifying and analysing risks to achieving the Company's objectives, forming a basis for determining how risks should be managed. Precondition to risk assessment is the establishment of objectives, linked at different levels of the Company.
- 5.2. Senior management specifies objectives within categories relating to operations, reporting, and compliance with sufficient clarity to be able to identify and analyse risks to those objectives.
- 5.3. Risk assessment also requires senior management to consider the impact of possible changes in the external environment and within its own business model that may render internal control ineffective.
- 5.4. Board of Directors is responsible for the reliable, transparent and effective functioning of Corporate Risk Management System (CRMS) and the process of risk assessment in the Company.
- 5.5. Business process owner and the participants of ICS together with Risk management unit, conducts identification and assessment of process level risks.
- 5.6. Process risks are identified as per Rules of Identification and Assessment of Risks of Air Astana JSC, additionally the following could be conducted to identify risks:
 - Analysis of the existing control activities to identify the risks they are preventing;
 - Analysis of the block diagram to identify what could go wrong;
 - Collection and analysis of statistical data on realised process risks.
- 5.7. Identified significant process risks are documented and included in the matrix of risks and controls when it is required, and reviewed at least annually.
- 5.8. Risk management unit provides methodological support in the process of identification and assessment of risks and controls for the compliance of provided information with the Policy and international standards on ICS.
- 5.9. As part of regular risk assessment, senior management identifies changes in the below factors that could significantly impact the Company's ICS and responds as necessary:
 - Changing of External Environment, which is represented by regulatory, economic, and physical environments;
 - Changing of Internal Environment, which can be caused by organisational structure changes, new business lines, significant changes of existing business lines, acquired or divested business operations, rapid growth, changing reliance on foreign geographies, and new technologies;
 - Significant Personnel Changes, which are represented by changes in management and respective attitudes and philosophies on the system of internal control.
- 5.10. In assessing risks to the achievement of objectives the business process risk owners shall always consider compliance risks, which include risks of corruption and fraud as well as non-compliance with the applicable legislations and/or internal regulations.
- 5.11. Risk assessment includes, but is not limited to, management's assessment of the risks relating to the
 - Fraudulent reporting;
 - Possible loss (theft) of assets;

- Corruption resulting from the various ways that fraud and misconduct can occur.
- 5.12. As part of assessing fraud risk, management assesses (includes but is not limited to) the risk of management override of internal control. Management override describes action taken to override Company's controls for an illegitimate purpose including personal gain or an enhanced presentation of the Company's financial condition or compliance status.
- 5.13. As soon as significant changes are identified business process owners notifies Risk management unit and updates internal departmental documents and matrix of risks and controls.

6. Control Activities

- 6.1. Control activities are the actions established through policies and procedures that help to ensure that senior management's directives to mitigate risks to the achievement of objectives are performed.
- 6.2. Control activities are developed by business process owners for each process risks that are included to the matrix of risks and controls to mitigate the risks to the achievement of objectives to acceptable levels.
- 6.3. Control activities are performed at all levels of the Company, at various stages within business processes, and should be complied with by all the employees. Control activities may be preventive or detective in nature and may encompass a range of manual and automated activities such as authorisations and approvals, verifications, reconciliations, and business performance reviews.
- 6.4. Control activities are documented and included to the mitigation action plan for preventing process risks within the structural units of the Company.
- 6.5. It is recommended for business processes to have a mix of manual and automated controls, depending on the availability of technology in the Company.
- 6.6. Senior management shall consider whether duties are divided or segregated among different employees to reduce the risk of error or inappropriate or fraudulent actions. Segregation of duties is typically built into the selection and development of control activities. Where segregation of duties is not practical, senior management shall select and develop alternative control activities.
- 6.7. Management of departments shall conduct high level business performance review by comparing actual performance versus budgets, forecasts, previous periods, and competitor results.
- 6.8. Management of departments ensure the development, approval, formalisation and documenting of control activities relating to operations, reporting, and compliance and that are aimed at:
 - Decrease of probability of risk occurrence;
 - Prevention of errors and/or identification of errors after their occurrence;
 - Identification and elimination of duplicate and redundant operations;
 - Identification of deficiencies and areas for improvement;
 - And, further improvement of ICS.
- 6.9. Risk management unit provides methodological support to business process owners in terms of documenting and identifying of process risks and identification of controls to them in the matrix of risks and controls and block diagrams.
- 6.10. Business process owners ensure the communication with the Risk Management unit in terms of identification of process risks and controls to them, development and update of block diagrams and matrixes of risks and controls for business processes they are responsible for.
- 6.11. Control Activities, subject to compliance by the bodies and employees of the Company, represent the documented action system and measures on provision of effective internal control over fulfilment of objectives, tasks and plans of the Company, detection and settlement of non-standard transactions as well as prevention, restriction and exclusion of risks and possible unfair and illegal actions of the management and employees of the Company.
- 6.12. Control activities include the following, but not limited to:

- Setting the goals and objectives, authorities and responsibilities of structural units and employees throughout all the levels of the Company.
- Authorisation for operations approval: operations shall be approved and performed only by the respective authorised individuals.
- Segregation of duties and absence of conflict of interests of employees while performing their functions.
- Creating and ensuring the efficient functioning of information exchange channels within the Company.
- Ensuring that all employees are aware of their responsibilities within ICS.
- Determination and setting KRAs (Key Response Areas) according to the documents of the Company.
- Risk management of the Company.
- Monitoring the purchase/disposal, reorganisation of the Company's assets and observance of property rights (asset protection);
- Monitoring the effective use of the Company's resources;
- Monitoring the implementation of the long-term strategy, medium-term business plan and Budget of the Company;
- Control over the implementation of investment projects;
- Monitoring the compliance with the established accounting and tax accounting procedures, the preparation and timely submission of reports (accounting, management, financial, tax, etc.);
- Control over execution of the decisions made by the bodies of the Company and assignments given by the senior management of the Company;
- Monitoring the fulfilment of the recommendations of an audit organisation performing the audit of financial statements of the Company as well as recommendations of the Internal Audit Service;
- Monitoring the compliance with information disclosure procedures of the Company;
- Control over the compliance with the set procedures and rules.
- Proper documentation of the internal control procedures.
- Other procedures as per Company's internal documents and regulations.

6.13. The development of control activities requires the following:

- The goal of the control activity;
- Responsible employee (owner of the control activity with sufficient authority to perform the control activities);
- The order of the performing the control activity;
- Frequency and timeframes of the performing the control activity;
- Control measures (technical, IT systems, documents and reports);
- The documents that proof the implementation of control activity;
- The documents that regulate the controls;
- Results of the performing of control activity.

- 6.14. The combination of control activities that are aimed at mitigation of one risk shall provide the reduction of residual risk to the acceptable level to ensure the achievement of the objective.
- 6.15. Business process owners ensure the proper documentation of the control activities and their inclusion to the internal documents and regulations.
- 6.16. Control activities must be periodically reviewed for their relevancy, updated and improved with consideration of changes in business processes, organisational structure and emergence of new process risks.

7. Information and Communication

- 7.1. Information and its communication is the process of identification, documenting and timely bringing of necessary and relevant information to relevant employees and require the information support system in the Company.
- 7.2. The Policy regulates responsibility of employees and participants of the ICS on the documenting of control activities and exchange of relevant information.
- 7.3. Board of Directors is responsible for approval of Information Security Policy, Regulation on Confidential Information. Additionally, Board of Directors approves the order of disclosure of information, the list of publicly accessible documents.
- 7.4. Senior management is responsible for forming and maintaining of information support system and exchange of information, which includes the following:
 - Organising of system of collection, processing, and exchange of information, including the forming the report and messages, containing the information on three key areas (operations, preparation of financial report and compliance with laws and regulations.
 - Organising effective channels and means of communication that ensure the information flow both vertically and horizontally within the Company.
 - Access and safety of information from internal and external sources.
 - Bringing to the attention of employees of the current policies and procedures applied in the Company.
- 7.5. Board of Directors and senior management ensure the direct access of employees to the relevant documents of ICS.
- 7.6. Risk management unit ensures continuous and transparent cooperation with IAS, methodological support to business process owners within the ICS framework and ensures the exchange of necessary information.
- 7.7. Business process owners are responsible for development and update of matrix of risks and controls, forming the mitigation action plans for further improvement of ICS, as well as monitoring of actions on ICS within the business processes they are responsible for.
- 7.8. Matrix of risks and controls shall contain the following information and the template is given in Appendix #1:
 - Business process
 - Business process owner
 - Risk ID
 - Risk name
 - Code of control activity
 - Control activity
 - Owner of the control activity
 - Frequency of control activity
 - Type of control
 - Preventive/detective control

- Document, regulating the control activity
 - Assessment of design effectiveness
 - Justification of assessment.
- 7.9. Matrix of risks and controls shall be developed in all departments and shall be approved by the heads of the departments.
- 7.10. Structural units of the Company ensure the full and transparent cooperation and timely provision of requested information to the Risk management unit on:
- Matrix of risks and controls
 - Testing of effectiveness of design of control activities
 - Identification of deficiencies and areas for improvement on main and supporting business processes.
- 7.11. Business process owners shall inform Risk management unit on realisation of process risks in a timely manner. Risk Management unit in turn informs Compliance and Sustainability Department in case of risks related to compliance and sustainability.
- 7.12. Risk Management unit ensures timely notification and provision of information to the Risk Committee, which consists of the senior management, on deficiencies and realisation of process risks.
- 7.13. The Company obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.
- 7.14. The Company internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of other components of internal control.
- 7.15. Communication of information conveyed across the Company and its departments include:
- Policies and procedures that support personnel in performing their internal control responsibilities;
 - Specified objectives;
 - Importance, relevance, and benefits of effective internal control;
 - Roles and responsibilities of senior management and other personnel in performing controls;
 - Expectations of the Company to communicate up, down, and across the entity any matters of significance relating to internal control including instances of weakness, deterioration, or non-adherence.
- 7.16. The Policy is communicated to employees of the Company.
- 7.17. Communication exists between management and the board of directors so that both have information needed to fulfil their roles with respect to the Company's objectives.
- 7.18. Separate communication channel, such as internal whistle-blower hotline, is in place and serves as independent mechanism to enable anonymous and/or confidential communication in addition to normal channels.
- 7.19. The Company communicates with external parties regarding matters affecting the functioning of other components of internal control.

8. Monitoring Activities

- 8.1. The goal of monitoring of ICS is to ensure the efficient functioning of ICS.
- 8.2. Monitoring represents the process of assessment if the internal controls components are in place and able to provide reasonable assurance that Company will achieve its objectives. Monitoring is conducted by responsible employees within their operational activities or by means of periodical testing.
- 8.3. Conducting of monitoring of ICS suggests the following:
 - Forming of control activities throughout all the levels of the Company;
 - Annual assessment of effectiveness of ICS;
 - Daily monitoring of important operations;
 - Bringing the necessary information to the attention of business process owners.
- 8.4. For the goal of effective and reliant functioning of ICS Board of Directors and senior management ensures the continuous monitoring and provision of feedback to all participants of ICS.
- 8.5. IAS conducts monitoring over the Company's ICS effectiveness by implementation of Annual Audit Plan, which include:
 - Review over effectiveness of ICS as a whole;
 - Audits aimed on assessment of ICS effectiveness within the separate departments and/or business processes.
- 8.6. As per results of audits IAS provides its recommendations on improvement of ICS. The results of such assessments shall be provided to Audit Committee and Board of Directors within the quarterly and annual reporting.
- 8.7. Ongoing evaluations, separate evaluations, or some combination of the two are used to ascertain whether each of the five components of internal control, including controls to affect the principles within each component, is present and functioning. Ongoing evaluations, built into business processes at different levels of the Company, provide timely information. Separate evaluations, conducted periodically, will vary in scope and frequency depending on assessment of risks, effectiveness of ongoing evaluations, and other management considerations. Findings are evaluated against criteria established by standard-setting bodies, or management and board of directors, and deficiencies are communicated to management and the board of directors as appropriate.
- 8.8. The Company selects, develops, and performs ongoing and/ or separate evaluations to ascertain whether the components of internal control are present and functioning.
- 8.9. Monitoring activities are selected, developed, and performed by management of departments to ascertain whether each component of ICS continues to be present and functioning or if change is needed.
- 8.10. Management selects, develops, and performs a mix of monitoring activities including both ongoing and separate evaluations.
- 8.11. Ongoing evaluations are generally performed by line operating or functional managers, who are competent and have sufficient knowledge to understand what is being evaluated, giving thoughtful consideration to implications of information they receive.
- 8.12. Company could conduct separate evaluations of the components of internal control to reconfirm ongoing

evaluation conclusions.

- 8.13. Separate evaluations are mainly conducted through the internal audit function or with attraction of external auditor.
- 8.14. The Company evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
- 8.15. Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
- 8.16. Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
- 8.17. Management tracks whether deficiencies are remediated on a timely basis.

9. Report of the Board of Directors on Internal Control

- 9.1. The Board of Directors shall be responsible for disclosing information on the ICS in the annual report submitted to the Shareholder, in which the Board of Directors shall:
- describe existing process of identification, assessment and management of essential risks that Company face;
 - specify that process was carried out during the year under review and realised (confirmed) before the date of approval of the annual report;
 - specify that process is assessed by the Board of Directors on a regular basis and complies with requirements of the present Regulations, i.e. to recognise the responsibility for ICS arrangement and assessment of its efficiency, including the explanation that such system represents only reasonable (not absolute) guarantee against essential distortions and losses.
- 9.2. The Board of Directors shall briefly describe in the annual report the process that it applies (if applicable, with the help of the Committees of the Board of Directors) for assessment of the ICS effectiveness. The Board of Directors shall also indicate measures taken to resolve significant issues related to internal control reflected in annual report.
- 9.3. The Board of Directors shall ensure that all information contained in the report is significant objective, adequate, reliable and up-to-date information of high level.
- 9.4. The Board of Directors may include into the annual report additional information to promote better understanding of risk management processes and internal control system of the Company.
- 9.5. If the Board of Directors cannot disclose information as provided by the items 9.1-9.3 of the Policy, and has not assessed the effectiveness of the internal control system, that shall be indicated with the relevant comments.

Appendix 1. Matrix of Risks and Controls

Business process		Risk		Control							
Business process name	Business process owner	Risk ID	Risk name	Description of the control	Owner of the control	Frequency, timeframe	Type of control	Preventive/ Detective control	Document regulating the control	Assessment of design effectiveness	Justification of assessment
1	2	3	4	5	6	7	8	9	10	11	12