Adopted by the Directors

of GLOBALTRANS INVESTMENT LTD

Resolution of 24 January 2008

GLOBALTRANS INVESTMENT LTD

RISK MANAGEMENT STANDARD

TABLE OF CONTENTS

1 PURPOSE

The Risk Management Standard (hereinafter *the Standard*) of Globaltrans Investment Ltd (hereinafter *GTI or the Company*) has been developed in compliance with generally accepted principles of corporate governance and enterprise risk management (hereinafter *ERM*).

The main purpose of this Standard is to deliver integrated approach to risk management and provide overall understanding of structure elements of risk management system within the companies of GTI Group (GTI and its subsidiaries, hereinafter *the Group*).

2 APPLICATION

This Standard applies to all employees and all companies within the Group.

3 GENERAL PROVISIONS

ERM is a process, effected by the Boards of Directors, management and other employees of the Group companies, applied in strategy setting and across the companies, designed to identify potential events that may affect the companies and the Group in general, and manage risk to be within predefined risk appetite, to provide reasonable assurance regarding the achievement of the Group's objectives.

The main objectives of ERM are the following:

- increase the Group companies ability to achieve their objectives;
- increase value of the Group companies;
- guarantee the continuity and stability of the Group's business;
- increase effectiveness of the corporate governance system.

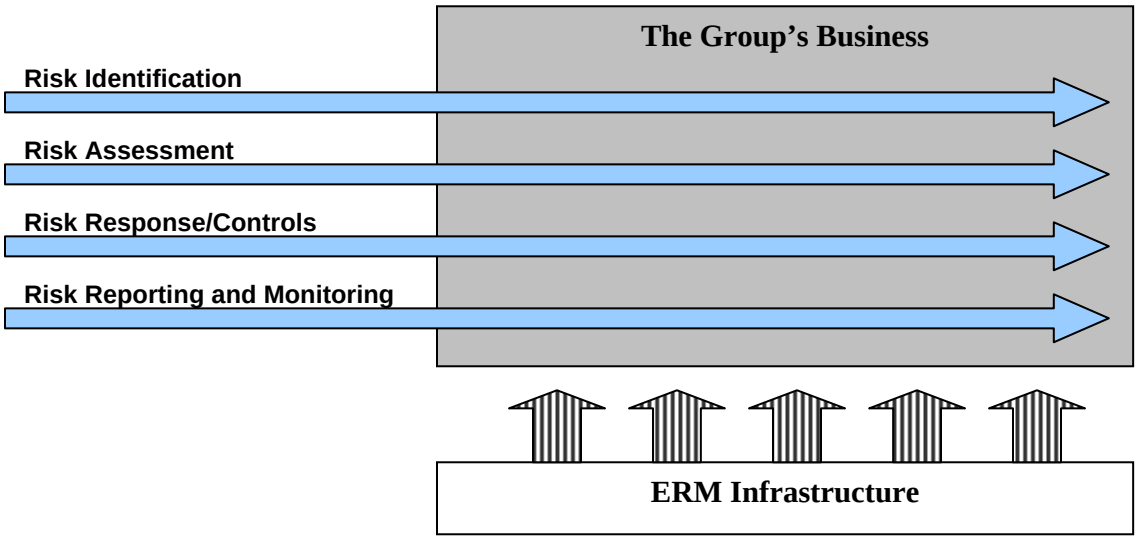
ERM in the Company's subsidiaries shall be based on the same principles as in the Company (please, refer to Risk Management Policy). Each subsidiary of the Company is required to:

- monitor and review its environment;
- state clear objectives;
- identify risks which interfere with achievement of its objectives;
- assess the impact and likelihood of the risks;
- implement effective actions designed to:
  - a achieve business objectives;
  - b safeguard subsidiary assets from inappropriate use, loss or fraud;
  - c facilitate economic, effective, efficient and safe operations;
- assess the effectiveness of existing controls/ risk responses.

The Company also requires every subsidiary to monitor, communicate and report changes in the risk environment and the effectiveness of actions taken to manage identified risks on an ongoing basis as well as report on the effectiveness of their risk management and internal control systems in general.

4 ERM FRAMEWORK

The Group's ERM Framework (hereinafter *the Framework*) has been designed to provide reasonable assurance of meeting the Group's business objectives and fulfilling its external obligations and commitments. The Framework consists of two types of components - risk management processes and risk management infrastructure (please refer to Picture 1. *ERM Framework* below).



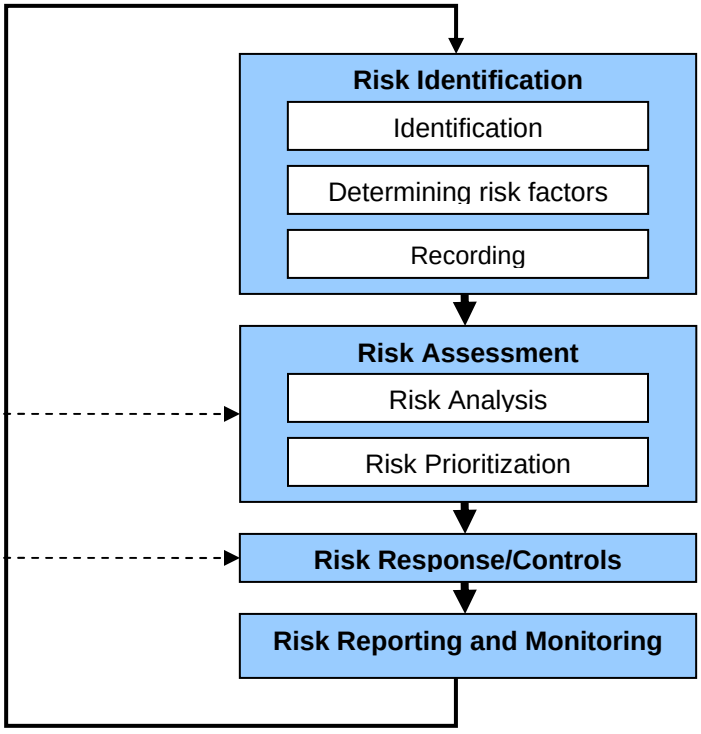
All risk management activities are performed on ongoing/regular basis, embrace the Group's business and are embedded into all key business processes. Mature ERM infrastructure is a sound basis for effective risk management activities.

5 RISK MANAGEMENT PROCESSES

Risk management includes the following activities:

- Risk Identification;
- Risk Assessment;
- Risk Response/Controls;
- Risk Reporting and Monitoring.

Cyclic nature of risk management is represented in the Picture 2. *Risk Management Processes* below:



5.1 Risk Identification

The Company recognizes that risks are inherent in the Group's business and can have both positive and negative impact. The identification of risks can only have value when explicitly linked to the Group's objectives.

Risk Identification includes the following activities: identification of risk, determining risk factors and recording information about risk and risk owner. Risk identification process ensures that, wherever possible:

- all significant sources of uncertainty are identified and recorded;
- both opportunities and threats are addressed as part of the process;
- the root cause is determined;
- interaction/conflict between stakeholders' interests and objectives, which can be a significant source of risk, is identified.

All risks, inherent to the Group's business, shall be considered on the following levels:

- Company level;
- Company's subsidiary level;
- Level of departments of the Company's subsidiary.

Risk identification process is based on both "top-down" and "bottom-up" approaches. "Top-down" approach means that risks are identified on a basis of the Group companies' strategies; in this case risk consequences are considered in the light of risk influence on the achievement of the strategic objectives. "Bottom-up" approach means that risk identification is based on analysis of the Company's business activities. Information about identified risks from all levels of the Group shall be accumulated and appropriately communicated to the Company level.

Integrated approach ("top-down" and "bottom-up" approaches) provides for completeness of coverage of risk identification and interrelation between risks and strategic goals as well as Group's business. Integrated approach allows to satisfy both shareholders interests and management interests and guarantee overall coverage of risks and detecting the deficiencies of risk communication.

When identifying risks, the Group companies shall use methods which enable to consider both existing and emerging risks, external and internal risks. Such methods include analysis of audit reports, previous risk registers, scenario scanning, interviewing the management, comparison with similar companies acting within the same market etc.

All risks identified fall into four groups:

- Strategic risks – risks that influence the Company's ability to achieve its mission/strategy;
- Operational risks – risks that influence the Company's operational efficiency and effectiveness;
- Financial risks – risks that influence the Company's financial performance;
- Compliance risks – risks that influence the Company's adherence to relevant laws and regulations.

All risks identified shall be recorded consistently and fully documented to allow subsequent stages of the process to be effective. The following information shall be recorded:

- group of the risk
- category of the risk;
- description of the uncertainty associated with a particular activity, process, objective;
- risk factors;

- link between an identified source of risk and the relevant performance objectives to ensure that they are always considered together and the context of the risk is maintained;
- risk owner.

5.2 Risk Assessment

Risk assessment activity allows the Group companies to consider the extent to which potential events have impact on achievement of their objectives/the Group's overall objectives. Risk assessment is a continuous and iterative set of actions taking place throughout the Group.

Risk assessment involves two stages:

- analysis of individual risks and evaluation; and
- risk prioritization.

The Group companies shall analyze events from two perspectives - likelihood and impact, - taking into account the existing controls and their adequacy and effectiveness.

The most pertinent information sources and methods shall be used when analyzing impact and likelihood. Sources of information may include the following:

- past records;
- practice and relevant experience;
- relevant published materials;
- market research;
- the results of public consultation;
- experiments and prototypes;
- economic, engineering or other models;
- specialist and expert judgments.

The following methods are used:

- structured interviews with experts in the area of interest;
- use of multi-disciplinary groups of experts;
- individual evaluations using questionnaires;
- use of models and simulations;
- combination of the above mentioned techniques.

The selected method shall be determined by considering various factors, including benefits and challenges of the methods.

The companies evaluate likelihood, impact, control/risk response effectiveness using pre-established assessment criteria.

Risk prioritization enables risks to be ranked so as to identify management priorities. All risks are ranked in accordance with risk rating (impact x likelihood). Further risk management actions are defined by matching up risk rating and control/risk response effectiveness.

5.3 Risk Response/Controls

The purpose of responding to risks is to manage them within the risk appetite.

Risk responses fall within the following categories:

- avoidance;
- reduction;
- sharing;
- acceptance.

In determining risk response/controls, management shall consider the following:

- effects of potential responses/controls on risk likelihood and impact – and which response/control options allow to reduce risk to acceptable level;
- costs versus benefits of potential responses/controls;
- possible opportunities to achieve the company's objectives going beyond dealing with the specific risk.

The Company recognizes that controls are key mechanism for modifying and managing risk. System of internal control shall provide reasonable assurance of decreasing of potential loses within the risk appetite.

There are following types of controls:

- preventive controls - these controls are designed to limit the possibility of an undesirable outcome being realized. There are three categories of preventative control:
    a Physical, e.g. perimeter security fence and guards;
    b Procedural, e.g. segregation of duties, whereby no person has authority to act without the consent of another person;
    c Circumstantial: reducing the likelihood of the risk occurring by reducing the exposure to the root cause of the risk;
- detective controls - these controls are designed to identify occasions of undesirable outcomes having been realized.

All GTI Group companies shall undertake a regular review and testing of controls to ensure:

- they have clear ownership;
- they are clearly defined, communicated and understood;
- they are operating as designed and collectively reduce the risk to an acceptable agreed level;
- they remain cost-effective;
- where deficiencies are identified:
    a the implications, if not remediated, are established and options for treatment are identified;
    b they are reported so that the impact on the risk profile can be assessed;
    c remedial plans are put in place to fix controls where necessary, and monitoring is implemented post-fix to provide assurance that the control is now operating as intended.

If controls are no longer considered necessary or cost-effective they are subject to revision and removal.

5.4 Risk Reporting and Monitoring

The Company recognizes that regularly reporting and monitoring activity is fundamental to:

- aggregate risk-related information;
- actively and effectively manage risk;
- monitor and respond to changes in risk profile at all levels of management and across the Group's business.

There shall be specific, timely, accurate and reliable reporting, and an appropriate flow of risk information. Risk reporting allows to communicate key outputs from existing ERM process to key stakeholders.

Each company of the Group shall perform external and internal risk reporting. Internal risk reporting shall be provided to management of their area of responsibility, and escalated in accordance with the

Group hierarchy. External risk reporting shall be provided to the company's external stakeholders on a regular basis in compliance with corporate and regulatory disclosure requirements. Thus, there are three levels of risk reporting in the Group: the overall Group's level, subsidiaries' level and individual level.

The objectives of the Group's level of risk reporting are:

- to provide assurance to shareholders that existing systems of internal control and risk management perform in the best way to safeguard the shareholders' investment and the Company's assets;
- to inform the internal and external stakeholders of the Company about the Group's risks and how the Group manages its risks.

The objectives of the subsidiaries' level of risk reporting are:

- to provide assurance that the subsidiaries' risk management process is operating effectively and risks are being managed, thereby increasing confidence in their ability to achieve objectives and inform decision making;
- to enable key risks and issues to be aggregated, prioritized and addressed appropriately.

Individual level of risk reporting shall cover:

- the status of key risks surfaced through the process, highlighting:
    a any material changes that could modify their likelihood of occurring and/ or their impact; and
    b any breach of risk appetite (tolerance or limit);
- the status of mitigating actions for key risks, where progress is behind agreed target or is significantly threatened; and
- any significant emerging risks that shall be raised and monitored.

Risk monitoring provides reasonable assurance that the management plan remains relevant. The companies shall give the priority to monitoring:

- high risks;
- credible failure of treatment strategies;
- risk-related activities that feature high incidence of change;
- risk tolerances especially where application of risk tolerances results in high levels of residual risk;
- technological advances that may offer more efficient alternatives to current risk treatment.

There are three types of monitoring activity:

- continuous (or at least frequent) monitoring through routinely measuring or checking particular parameters (for example cash flows).
- review of risks and risk response by line management (sometimes called 'control self assessments') which are often selective in scope but typically routine and regular and which shall be selected on risk-assessment criteria.
- auditing, using both internal and external audit staff. As far as possible these audits shall test systems rather than conditions. They shall be more selective in scope and less frequent than the above mentioned measures.

6 RISK MANAGEMENT INFRASTRUCTURE

The Company recognizes that there should be a specific internal environment, risk management infrastructure, which provides an appropriate foundation for enterprise risk management.

The internal environment is the basis for all other components of ERM, providing discipline and structure. It influences the way strategies and objectives are established, business activities are structured, risks are identified, assessed, and acted upon, and reporting and monitoring activities are performed.

Risk management infrastructure includes:

- ERM strategy and methodology;
- ERM culture and philosophy, including integrity, ethical values and competence of the employees;
- ERM organizational infrastructure, including responsibilities in the area of ERM;
- Tools and technology, IT and other systems supporting effective risk management.

6.1 ERM methodology

The Company recognizes that the Group needs clear guidance and direction on what risk management activities should be carried out, how and by whom these are taken and with what overall objectives. With this purpose the Company develops, implements, timely updates ERM methodology package which includes risk management strategy, policy, standard and more detailed guidelines, policies and procedures to ensure that all Group companies take their risk management activities in a coordinated manner.

Establishing a sound risk management strategy is very important for effective and efficient risk management, it helps to determine priorities and resource allocation.

Risk management policies and procedures set out the basis on which decisions are taken through determination of the companies' appetite for risk, which is formalized in risk assessment criteria. Policies and procedures may be stand alone documents or may be embedded within existing policies and procedures covering business activity.

6.2 ERM culture and philosophy

ERM culture and philosophy are the fundamental for the performance of risk management. A well developed and clear risk management philosophy allows to effectively recognize and manage risk through the Group's business.

The Company recognizes that effective risk management can not be sustainable without being aligned with the culture of the organization. To improve the performance of risk management, changes in culture may be required, which are performed through appropriate "tone at the top", training programs, incentives and measurement mechanisms etc.

Establishing employee integrity and ethics is essential to the success of the ERM Framework. Integrity and ethical values are established by senior executives of the Group companies (i.e., tone at the top) and are reflected in the corporate culture of the Group.

Risk management training programs should be explicitly linked to risk management activities, roles and responsibilities. To promote the "right" risk-related behavior, incentives and performance measurement mechanisms shall consider the risk-related performance. Conversely negative behaviors in relation to risk should be subject to appropriate consideration and follow-up actions.

The Company is aware of the necessity of a common language which should be developed to support effective risk management activities. A common language will help to ensure common understanding of risk and risk management activities and provide clarity of communication and action.

6.3 ERM organizational infrastructure

Governance and organization is a fundamental part of the Group companies' ERM Framework. It includes both the authorities within the companies having a broader responsibility for risk management, such as the Boards of Directors, the Company's Audit Committee, Internal Audit function, local risk managers, and the way that risk is assigned throughout the Group companies, including how ownership and accountability for risk is expressed and carried out. Clear assignment of roles and responsibilities helps to reduce any gaps, inefficiencies and overlaps in risk coverage, and facilitate communication.

6.4 Tools and technology

Tools and technology may be required to leverage and support risk management activities. Such tools may include information gathering surveys, workshop and facilitation tools, self assessment and reporting tools, early warning indicators systems, information management and work flow tools as well as risk aggregation and reporting systems which can be based on information technology (depending on business needs and the level of risk management system development).

IT systems are crucial for mature risk management. IT systems store, process, and transmit information and enable management to make well-informed risk management decisions. Data repositories are used for administration of data relating to risk management. Early warning systems can be used to identify potential issues early enough for appropriate action to be taken. Such systems provide key information on risk and controls to key people in a timely manner. The Group companies can use analytical and modeling tools to provide greater insight into specific areas of significant risk.

7 RESPONSIBILITIES

7.1 GTI Board of Directors

The Board of Directors' risk management and control responsibilities include:

- promoting a culture that emphasizes integrity;
- embedding sound risk management in all aspects of the Group's activities;
- approving the Group's risk appetite;
- reviewing the Group's risks profile;
- setting the overall policies for risk management and control;
- adopting the most appropriate scheme of delegation of the Board's responsibilities;
- receiving regular reports on the management of key risks and taking appropriate follow-up action;
- receiving annual reports on the effectiveness of the ERM system;
- integrating risk management into the Board's own decision-making;
- reporting to shareholders on the Group's risks and the effectiveness of ERM system.

7.2 GTI Audit Committee

The Audit Committee is responsible for:

- reviewing and monitoring the ERM's design and implementation effectiveness within the Company/Group;
- providing an opinion on the effectiveness of the ERM in the Company/Group and reporting it to the Board of Directors.

7.3 GTI Internal Audit

Internal Audit is responsible for:

- performing independent assessment of enterprise risk management and internal control systems effectiveness and reporting the results to the Audit Committee;
- receiving regular reports on the management of key risks and taking appropriate follow-up actions;
- advising management and local risk managers on performing activities in the area of risk management.

7.4 GTI subsidiaries Boards of Directors

Risk management and control responsibilities of the GTI subsidiaries' Boards of Directors are similar to the responsibilities of the GTI Board of Directors but only in the area of their competence (only subsidiary level). The subsidiaries' Boards of Directors should ensure that subsidiaries ERM systems are developed, implemented and performed on the basis of overall risk management principles defined at the Group level.

7.5 Risk Managers

Risk managers (risk managers in the Company and its subsidiaries) are responsible for:

- receiving reports containing risk-related information;
- consolidating and analyzing information about risks identified, including their description, assessment and risk management actions;
- reporting results of analysis to the appropriate Board of Directors;
- reporting results of analysis to the Company Risk managers (applicable only for subsidiaries' Risk managers);
- communicating with all internal stakeholders regarding risk-related issues;
- advising management on performing activities in the area of risk management, including explanation of risk management guidelines provisions;
- monitoring of new risk management standards, best practices and changes in regulatory requirements; and
- initiating changes in existing ERM system.

7.6 Management

Management is responsible for:

- performing risk identification, assessment, treatment and monitoring;
- reporting to local risk managers all risk-related information;
- integrating risk management into the day-to-day activities in the sphere of their responsibilities.

8 REVISION OF THE STANDARD

This Standard is subject to periodical review. This will allow the Standard to take into account any changes in the risk management system, regulatory changes or changes in the Company operations.

APPENDIX 1: Glossary

Risk	The possibility that an event will occur and adversely affect the achievement of company's objectives.
Inherent risk	The risk associated with company's activities in the absence of any response actions, which may alter either the risk's likelihood or impact.
Residual risk	The remaining risk after management has taken action to alter the risks likelihood or impact.
Risk appetite	The amount and type of risk that company is prepared to accept, tolerate or be exposed to in achieving its business objectives.
Risk area	The indication of a generic risk, used as an overarching label for a cluster of associated (specific) risks.
Risk assessment	The set of tasks in which risk is measured and prioritized.
Risk aversion	The situation that someone is willing to give up something valuable (potential rewards) to reduce the risk exposure.
Risk awareness	The level of management's consciousness about the fact that a company faces risks and their understanding of the need to effectively address them.
Risk capability	The processes, people, reports, methodologies and systems needed to implement a particular risk management strategy.
Risk capacity	The aggregate financial ability of a company to absorb or withstand losses from risk incidents.
Risk criteria	The classification/scales for measuring and depicting risk impact (consistent with a company's value drivers) and likelihood (consistent with the planning horizon).
Risk exploitation	The choice to take the risks inherent in its strategy even to the point of increasing a company's exposure to risks.
Risk exposure	The level to which the assets (value sources) of a company are potentially affected by the occurrence of well-defined risk events.
Risk factor	The possible (internal or external) force or condition influencing the events that affect the achievement of a company's business objective.
Risk financing	The process by which a company pays for the outcome of an undesirable risk incident.
Risk identification	The process of defining what can happen that fundamentally affects the success of company's business. The set of tasks in which risk is identified, sourced and described.
Risk impact	The significance of risk to a company based on criteria selected by management/Board of Directors.
Risk indicator	A measure of the level of exposure to risk, used for monitoring (trends) and control purposes.
Risk likelihood	The probability that or frequency with which an event is expected to occur over a given time horizon.
Risk management	A process, affected by the company's Board of Directors, management and other employees, applied in strategy setting and across the company, designed to identify potential events that may affect the company, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of the company's objectives.
Risk maturity	The extent to which a robust risk management approach has been adopted and applied by management across a company.
Risk measurement	The methodologies and techniques used to determine the likelihood and consequences of events and to provide information for decision making.
Risk mitigation	The steps taken by management to reduce the pain or limit the adverse effects of risk incident.
Risk monitoring	The activities of management to oversee and review the effectiveness

	of the risk management process.
Risk philosophy	The set of shared believes and attitudes characterizing how a company considers risk in everything it does.
Risk map	The graphical depiction of risks, usually plotted on impact and probability axes, based on risk assessment criteria.
Risk reduction	The strategy to take action to decrease risk to an acceptable level, focused on diminishing likelihood and impact.
Risk register	The list of a company's specific risk (area) s including their definitions, intended to create a common risk management language within a company.
Risk response	The approach selected by management to bring residual risk within desired risk tolerances, based upon the assessment or likelihood and impact, as well as cost and benefits.
Risk retention	The conscious and rational decision to accept the consequences of the undesirable event.
Risk rating	The multiplication of risk impact and risk likelihood, used to prioritize risk(area)s.
Risk sharing	The reduction of risk likelihood or risk impact by transferring or otherwise sharing a portion of the risk.
Risk taking	The act of deliberately selecting and executing strategies, whose outcomes are subject to uncertainty and result in significant exposures.
Risk tolerance	The acceptable variation relative to the achievement of an objective.
Risk transfer	The risk response to pass a risk through to an independent financially capable third party at a reasonable economic cost under a legally enforceable arrangement.
Risk transparency	The level to which risks are adequately priced using consistent methodologies that enable comparison, aggregation and monitoring of outcomes.
Risk treatment	The specific strategy selected for managing risk; sometimes used to refer exclusively to risk reduction strategies.