Global Peak Corp
Anti-Money Laundering (AML) Program
Compliance and Supervisory Procedures

1. Policy

It is the policy of Global Peak Corp (hereinafter: GPC) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the Money Laundering and Terrorist Financing Prevention Act (MLTFPA) and its implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable MLTFPA and associated regulations and rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

GPC will designate its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for the GPC's AML program. By the time such designation takes place, the Member of the Management Board shall perform the duties of the AML Compliance Person. The AML Compliance Person must have a working knowledge of the MLTFPA and its implementing regulations and must be qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the GPC´s compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that GPC keeps and maintains all of the required AML records. The AML Compliance Person is vested with full responsibility and authority to enforce the GPC's AML program.

GPC will provide the Financial Intelligence Unit of Estonia with contact information for the AML Compliance Person, including: (1) name; (2) title; (3) email address; (4) and telephone number and other necessary information proving the competence of the AML Compliance Person.

3. Voluntary Information Sharing with Financial Institutions

We will share information with financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions. We understand that this requirement applies even to financial institutions *with which we are affiliated*, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from GPC's other books and records.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist financing activities;

- determining whether to establish or maintain business relations, or to engage in a transaction; or

- assisting the financial institution in complying with performing such activities.

4. Checking the Office of International Sanctions and Politically Exposed Persons Listings

Before establishing business relations or engaging in a transaction, and on an ongoing basis, the GPC will check to ensure that a customer does not appear on the foreign sanctions list, politically exposed persons' list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes published by Financial Intelligence Unit (FIU) in its webpage. Because the International sanctions list, politically exposed persons' list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the international sanctions and politically exposed persons' list, we may also access that list through various software programs to ensure speed and accuracy. GPC will also review existing accounts against the international sanctions list, politically exposed persons' list and listings of current sanctions and embargoes when they are updated and will document the review.

If we determine that a customer is on the international sanctions list or is engaging in transactions that are prohibited by the economic sanctions and embargoes published by FIU, we will reject the transaction and/or block the customer's assets inform FIU immediately.

If we determine that a customer is on politically exposed persons' list we will apply enhanced due diligence measures according to the present procedures.

Our review will include customer accounts, transactions involving customers (including activity that passes through GPC such as wires) and the review of customer transactions.

5. Customer Identification Program

In addition to the information we must collect under § 21 and 22 of MLTFPA we follow the following rules and regulations in respect of custormer identification, where applicable: FINRA Rule 2010 (Standards of Commercial Honor and Principles of Trade), NASD Rules 2310 (Recommendations to Customers - Suitability) and 3110 (Books and Records) and Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3(a)(9) (Beneficial Ownership regarding Cash and Margin Accounts) and 17a-3(a)(17) (Customer Accounts). GPC documents and maintains a written Customer Identification Program (CIP). We will collect certain minimum customer identification information from each customer with whom GPC establishes business relations or engages in transactions; utilize risk-based measures to verify the identity of each customer with whom we establish business relations or engage in transactions; record customer identification information and the verification methods and results; provide the required adequate CIP notice to customers that we will seek identification information to verify their identities; and compare customer identification information with government-provided lists of suspected terrorists and international sanctions, once such lists have been issued by the government. *See* Section 5.g. (Notice to Customers) for additional information.

a. Required Customer Information

Prior to engaging in transactions, GPC will collect the following information, if applicable, for any person, entity or organization that is a party to the transactions:

(1) the name;

(2) date of birth (for an individual);

(3) an address, which will be a residential or business street address (for an individual) or a principal place of business, local office, or other physical location (for a person other than an individual); and

(4) an identification number, taxpayer identification number, or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

When establishing business ralations or endaging in transactions with a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, GPC will not engage in transactions and, after considering the risks involved, consider discontinuing existing business relations.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to

verify and document the accuracy of the information we get about our customers. We will analyze the obtained information to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and personal identification number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (*e.g.*, whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.
We will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source.

- Checking references with other financial institutions; or

- Obtaining a financial statement.

We will use non-documentary methods of verification when:

(1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;

(2) GPC is unfamiliar with the documents the customer presents for identification verification;

(3) the customer and GPC do not have face-to-face contact; and

(4) there are other circumstances that increase the risk that GPC will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the business relations are established. Depending on the nature of the relations and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the GPC's AML Compliance Person, file a notice to FIU in accordance with § 49 and 50 of MLTFPA.

We recognize that the risk that we may not know the customer's true identity may be heightened for certain types of business relations, such as an transaction made in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by FATF as a high risk and other monitored jurisdiction. We will identify customers that pose a heightened risk of not being properly identified.

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not establish business relations or engage in transactions; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity; (3) close an account after attempts to verify customer's identity fail; and (4) determine whether it is necessary to file a notice to FIU in accordance with § 49 and 50 of MLTFPA.

e. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Comparison with Government-Provided Lists of International Sanctions

At such time as we receive notice that a government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purpose, we will, within a reasonable period of time after business relations have been established (or earlier, if required by law or regulation), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any government agency. We will follow all governmental directives issued in connection with such lists.

g. Notice to Customers

We will provide notice to customers that GPC is requesting information from them to verify their identities, as required by law. We will use the following method to provide notice to customers by email and phone call:

Important Information About Procedures for engaging in transactions

To help the government fight the funding of money laundering and terrorism activities, law requires providers of virtual currency exchange and virtual waalet services to obtain, verify, and record information that identifies each transacting person.

What this means for you: When you establish business relations with us, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your identifying documents.

h. Reliance on a Financial Institution for Identity Verification

We may, when all below conditions are fulfilled, rely on the performance by another person of some or all of the elements of our CIP with respect to any customer establishing business relations or who has established similar business relationship with the other person to provide or engage in services, dealings or other financial transactions:

- such reliance is reasonable under the circumstances;

- the other financial institution has entered into a contract with GPC requiring it to certify annually to us that it has implemented its anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the customer identification program;

- we gather from the other person at least information on who is the customer establishing the business relationship or making the transaction, their representative and the beneficial owner, as well as what is the purpose and nature of the business relationship or transaction;

- we have ensured that, where necessary, we are able to immediately obtain all the data and documents whereby it relied on data gathered by another person;

- we have established that the other person who is relied on is required to comply and actually complies with requirements equal to those established by Directive (EU) 2015/849 of the European Parliament and of the Council, including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and is under or is prepared to be under state supervision regarding compliance with the requirements;

- we take sufficient measures to ensure compliance with the following criteria:

1) the reliance on the other person does not impede the activities of GPC or performance of the duties and obligations provided in MLTFPA;

2) the other person performs all the duties of GPC relating to the CIP or its elements;

3) the reliance on the other person activities does not impede exercising supervision over GPC;

4) the competent authority can exercise supervision over the other person carrying out the CIP activity, including by way of an on-site inspection or another supervisory measure;

5) the other person has the required knowledge and skills and the ability to comply with the requirements provided for in this MLTFPA;

6) the GPC has the right to, without limitations, inspect compliance with the requirements provided for in MLTFPA;

7) documents and data gathered for compliance with the requirements arising from MLTFPA are retained and, at the request of GPC, copies of documents relating to the identification of a customer and its beneficial owner or copies of other relevant documents are handed over or submitted to the competent authority immediately.

6. General Customer Due Diligence

It is important to our AML reporting program that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we establish business relations with a customer, the due diligence we perform may be in addition to customer information obtained for purposes of our CIP.

For every business relation we will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. Such information should include:

- the customer's business;
- the customer's anticipated account activity (both volume and type);
- the source of the customer's funds.

7. Enhanced Due Diligence

For business relations that we have deemed to be higher risk, we will apply enhanced due diligence measures and obtain the following information:

- the purpose of the business relations;
- the source of funds and wealth;
- the beneficial owners of the accounts;
- the customer's (or beneficial owner's) occupation or type of business;
- financial statements;
- banking references;
- domicile (where the customer's business is organized);
- description of customer's primary trade area and whether international transactions are expected to be routine;
- escription of the business operations and anticipated volume of trading;
- explanations for any changes in account activity.

The enhanced due diligence measures will be applied in following cases:

- The customer is a politically exposed person

- Customer participating in the transaction is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that is considered to be a high risk jurisdiction according to the Financial Action Task Force or, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory.

- Red Flag situations as described below

- When, according GPC's Risk Assessment Model, the risk is high

8. Monitoring Accounts for Suspicious Activity, Risks Specific to GPC's Area of Activity

We will monitor customer activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business. AML Compliance Person will be responsible for this monitoring, he/she will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities. AML Compliance Person will conduct an appropriate investigation and review relevant information from internal or third-party sources before a notice to FIU is filed.

a. Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customers – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.

- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.

- Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.

- Background is questionable or differs from expectations based on business activities.

- Customer with no discernable reason for using the GPC's service.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.

- Tries to persuade an employee not to file required reports or not to maintain required records.

- "Structures" transactions below a certain amount to avoid reporting or recordkeeping requirements.

- Unusual concern with GPC's compliance with government reporting requirements and GPC´s AML policies.

Certain Funds Transfer Activities

- Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.

- Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer's business or history. May indicate a Ponzi scheme.

- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.

- Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.

Transactions Involving Penny Stock Companies

- Company has no business, no revenues and no product.

- Company has experienced frequent or continuous changes in its business structure.

- Officers or insiders of the Company are associated with multiple penny stock companies.

- Company undergoes frequent material changes in business strategy or its line of business.

- Company has been the subject of a prior trading suspension.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.

- Unusual transfers of funds or journal entries among accounts without any apparent business purpose.

- Maintains multiple accounts or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.

- Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.

Other Suspicious Customer Activity

- Buying and selling currencies with no purpose or in unusual circumstances.

- Payment by third-party check or money transfer without an apparent connection to the customer.

- Payments to third-party without apparent connection to customer.

- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

b. Responding to Red Flags and Suspicious Activity

When an employee of GPC detects any red flag, or other activity that may be suspicious, he or she will notify our CEO. Under the direction of the AML Compliance Person, GPC will determine whether or not and how to further investigate the matter. This includes applying enhanced due diligence measures and may include gathering additional information internally or from third-party sources, contacting FIU, freezing the business relations and/or filing a notice to FIU.

8. AML Recordkeeping

a. Responsibility for Required AML Records and Filing Notices to FIU

Our AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly, and that notices to FIU are filed as required.

9. Training Programs

We will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. Our training will occur on at least an annual basis. It will be based on GPC's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of notices to FIU); (3) what employees' roles are in the GPC 's compliance efforts and how to perform them; (4) the GPC 's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the MLTFPA.

We will develop training in GPC, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. We will maintain records to show the persons trained, the dates of training and the subject matter of their training.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

10. Program to Independently Test AML Program

The testing of our AML program will be performed at least annually (on a calendar year basis) by personnel of GPC, none of whom are the AML Compliance Person nor do they perform the AML functions being tested nor do they report to any such persons. Their qualifications include a working knowledge of applicable requirements under the MLTFPA and its implementing regulations. To ensure that they remain independent, we will separate their functions from other AML activities. Independent testing will be performed more frequently if circumstances warrant.

a. Evaluation and Reporting

After we have completed the independent testing, staff will report its findings to senior management. We will promptly address each of the resulting recommendations and keep a record of how each noted deficiency was resolved.

11. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the GPC's AML compliance program to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report the CEO. Such reports will be confidential, and the employee will suffer no retaliation for making them.

Annex 1

RISK ASSESSMENT MODEL FOR THE APPLICATION OF CLIENT DUE DILIGENCE MEASURES

This Annex sets out the risk assessment model for the application of due diligence measures.

Four categories associated with the person participating in the transaction shall be taken into account upon risk assessment:

I. place of residence or seat of the person participating in the transaction – country and geographical risks shall be taken into account;

II. parameters characterising the person participating in the transaction – customer risk shall be taken into account;

III. economic activities of the person participating in the transaction – product and service risks shall be taken into account; and

IV. transaction partners of the person participating in the transaction and risks related to them – the CLIENT risk of the transaction partners of the person participating in the transaction, the country and geographical risks and the product and service risks shall be taken into account.

Upon assessment of these risks, each risk category shall be assessed on a scale of 3 points where:

The risk is low	There are no risk factors of impact in any risk category and the customer and the customer's operations are transparent and do not deviate from the operations of an average, reasonable person engaged in the same field of activity. Thereby there is no suspicion that the risk factors on the whole might cause the realisation of the threat of money laundering or terrorist financing.
The risk is medium	There is one risk factor or there are several risk factors in the risk category, which differ(s) from the operations of a person engaged in the same field of activity, but the operations are still transparent. Thereby there is no suspicion that the risk factors could, on the whole, cause realisation of the threat of money laundering or terrorist financing.
The risk is high	There is one feature or there are several features in the risk category which, on the whole, undermine the transparency of the person and the person's operations, as a result of which the person differs from a person operating in the same field. Thereby the realisation of the threat of money laundering or terrorist financing is at least possible

Next, the score should be totalled. Thereafter the total amount should be divided by 4. The average of the categories determines whether the risk category of the person participating in the transaction is high, medium or low.

Risk Level Risk Category	Low Score 1	Medium Score 2	High Score 3	Coefficient	Impact on risk level
1. Place of residence or seat of person participating in					

transaction					
2. Parameters characterising person participating in transaction					
3. Economic activities of person participating in transaction					
4. Transaction partners or person participating in transaction and persons related to them					
Average	N/A	N/A	N/A	N/A	1,25

If the average of the categories is under 2, it should be noted that the cutsomer cannot have a low risk category if at least one of the categories has a high risk. The customer's overall risk category is also high if a risk factor as such calls for this.

Parameters of determining CLIENT's risk level

the CLIENT's risk level is low – $x < 2$

the CLIENT's risk level is medium – $2 \leq x \leq 2.75$

the CLIENT's risk level is high – $x > 2.75$

Annex 2

INTERNAL CONTROL RULES

1. The Tasks of Internal Control

- to verify compliance of GPC and its managers and employees with the legislation, precepts of the FIU, decisions of the management bodies, GPC's CIP and other internal rules, contracts and good practices concluded by GPC.

- in co-operation with all the management levels of GPC, to identify and assess the risks that may affect the effectiveness of GPC's activities and its internal control system, determine the priorities of its activities and draw up work plans on the basis of the results of the risk assessment;

- to assess the management and control measures implemented to achieve GPC's objectives, their effectiveness, sustainability and effectiveness, and express an opinion on the adequacy, reliability and necessity of these measures;

- to inform the top management of its findings and conclusions and, if necessary, make recommendations for remedying the situation, modifying measures or implementing new ones;

- as a result of the aforementioned activities, to increase GPC's management's confidence that the management and control measures implemented are aimed at achieving the goals set by GPC are sufficient and not superfluous.

2. The Tasks of the Management Board

The management board shall perform the tasks and duties of the internal control or appoint a person responsible for the internal control of GPC (hereinafter: the internal auditor) and, if necessary, to set up a corresponding structural unit under the direction of that person, ensure the necessary conditions for the work of the internal auditor, access to the information necessary for work and the functional independence of GPC's other operations, and implement, as far as possible, proposals.

3. Independence of Internal Control

In order to ensure the independence of the internal control, the internal auditor shall not be involved in the duties that affect the outcome of an internal audit.

The person responsible for internal control shall be independent in the planning of his activities.

The internal auditor shall be independent in carrying out audits, making observations, conclusions and recommendations, and informing the results, and maintaining neutrality with regard to the auditee.

Internal auditor may not serve in the position and perform other duties which cause or may cause a conflict of interest.

4. Qualification of Internal Auditor

The internal auditor is guided by the rules of conduct contained in internationally accepted standards.

The internal auditor ensures that the audits are carried out professionally and with due diligence, in accordance with applicable legislation and internationally accepted standards.

5. Risk Assessment, Audit Planning and Audit:

The purpose of internal control is, among other purposes, to prevent the realization of risks, which will be achieved by fulfilling the work plan based on the results of the risk assessment.

Risk assessment for the purposes of these rules is a process aimed at identifying risks in GPC and prioritizing those changes that are necessary in the strategic audit plan, and preparing an annual work plan for an audit.

All the management levels of GPC and the person responsible for internal control must be involved in the risk assessment.

Risk assessment is carried out at least once a year before the audit work plans are drawn up.

An audit work plan is prepared for the planning of internal audit work.

GPC's audit work plan is prepared by the person responsible for internal control and approved by the CEO of GPC.

The audit work plan shall be prepared at the beginning of each year and shall state:

- the results of the risk assessment;
- audit objects and objectives;
- the planned deadline for completion of each audit by quarter;

The audit work plan shall be based on the results of the risk assessment, take account of the operational priorities set for them and the resources available for internal audit, and leave a reasonable reserve to perform one-off tasks coming from GPC's management board.

An audit plan is prepared by the internal auditor. The audit plan must contain the following information:

- the purpose of the audit;
- the name of the audited entity or sector;
- the scope of the audit and the period covered;
- the time of the audit;

The audit involves audit planning, audit activity, final report preparation and reporting of results and, if necessary, ex-post audits.

The audit object may be any of GPC's structural units, systems, processes, operations, functions and activities.

The internal auditor must be guaranteed access to the information necessary for conducting the entire audit in GPC.

The internal auditor shall be guaranteed all the rights and working conditions necessary for the performance of his duties, including the right to receive clarifications and information from the managers and employees of GPC, and to monitor the elimination of the deficiencies found and the implementation of the proposals made.

Internal audit is carried out at least 2 times a year.

6. Internal Audit Report

At the end of each audit, the internal auditor will draw up an audit report, which will outline the findings, conclusions and recommendations for modifying the situation based on evidence contained in the audit dossier made during the audit.

The internal auditor shall forward the final report to the CEO of GPC and, if necessary, to other management staff.

When reporting breaches of law, the internal auditor must comply with applicable laws and internationally accepted standards.

The Internal Auditor is required to promptly forward information to CEO about the information disclosed to him/her about the violation of the law, or to the detriment of the interests of the clients.

7. Audit Documentation and Procedures:

Any information obtained during the audit, which is the basis for making conclusions and making recommendations, assessing risks and planning future audits, must be documented.

In order to ensure the high quality of the audit and to enable a later understanding of the audit process, all documents obtained during the audit and the prepared working papers must be included in the audit file. The dossier must ensure that the documents are easily accessible by reference in the final report and elsewhere.