CORPORATE RISK MANAGEMENT POLICY

GOAL

This policy aims to establish, at Bitcoin To You, principles, guidelines and responsibilities to be observed in the corporate risk management process, in order to enable the proper identification, assessment, treatment, monitoring and communication.

COVERAGE

This policy applies to all Bitcoin To You employees and service providers in managing the risks that impact their environment in a corporate manner.

GUIDELINES

Bitcoin To You is committed to maintaining a robust and integrated governance model in order to ensure, for the benefit of its stakeholders (customers, suppliers, employees, society, government, investors, etc.), the achievement of its business objectives while fulfilling their responsibilities with diligence and accountability.

Bitcoin To You understands corporate risk management to be a key component of that commitment. The management of corporate risks is a continuous, transparent and responsibility process for all employees of the organization at all levels. Each one is responsible for knowing the Risks in their area of operation and managing them according to the concepts, guidelines and directions contained in this policy and in its complementary documents.

Thus, Bitcoin To You seeks to establish the rules for risk management, based on existing best practices and regulations, through the segregation of lines of defense and the monitoring of internal controls.

Segregations of functions, roles, responsibilities, areas and practices are considered “lines of defense” in order to mitigate the materialization of risks that could cause losses to the Company.

1. First line of defense:

The first line of defense is directly responsible for managing, identifying, monitoring, eliminating and/or reducing the materialization of risks. Such defenses are commonly related to the functions, practices and areas that maintain the operational processes of Bitcoin To You. In this way, this line of defense has the objectives:

- Idto enlist, evaluate, control, eliminate and/or reduce risks;
- Create actions that allow better management and control for the treatment of risks;
- Maintain diligent internal controls; and
- Report potential losses of the organization.

2. Second line of defense

The second line of defense of Bitcoin To You is responsible for the control and monitoring of risk levels, in order to ensure that they are within the established permitted level. Thus, this line of defense has the objectives:

- Ensure the effectiveness and implementation of the risk management structure;
- Provide guidance on the practices to be adopted to ensure efficiency in risk management;
- Ensure that the establishment of limits and approval range will be followed and complied with;
- Manage and monitor operational risks and losses;
- Manage and monitor the efficiency obtained in internal controls and risk mitigation actions;

- Provide visibility to managers regarding the situation of the control and risk environment.
-

3. Third line of defense:

Bitcoin To You's third line of defense is responsible for independently evaluating internal controls and risks to the company's senior management. empresa In this way, this line of defense has the objectives:

- Audit and monitor internal processes and controls independently.
- Conduct and create assessments on how to measure the efficiency of risk management and internal controls.

RULES FOR RISK MANAGEMENT

The risk management structure should be segregated by defense lines, capable of periodically evaluating processes, practices and controls in order to identify and measure vulnerabilities that can cause losses and, consecutively, impact business objectives.

Processes must have control activities that ensure that their risks are known, controlled and mitigated appropriately.

Risk measurement should consider exposure to vulnerability and impact, based on the limits described below.

1. Vulnerability identification

The first step to risk management efficiency is identifying the level of risk vulnerability. For this,the risks must be controlled, subsequently identified, evaluated, documented and formalized according to the level of vulnerability so that they can be treated correctly..

2. Vulnerability measurement

To measure the vulnerability of risks, these should be controlled, later identified, evaluated, documented and formalized according to the level of vulnerability evidenced below so that they can be treated correctly..

- **Low:** andeffective internal controls for risk mitigation.
- **Medium:** predominance of effective internal controls to mitigate risks.
- **High:** effective controls for risk mitigation.
- **Extreme**: ino ineffective controls for risk mitigation.

3. Impact measurement

The quantification and control of risk shouldbe carried outbased onthe impact generated by it under the financial, operational, reputational and regulatory perspectives.

4. Reputational impact (financial perspective)

Another fact of risk measurement to be taken into account is the impact of it from a reputational perspective, as it directly affects the company and consequently financially impacts Bitcoin To You. In this sense, the scale of impact on the company's reputation for risk measurement is structured as follows::

- **Low:** Impacto irrelevant in reputation, in small group of customer and with rapid remediation.
- **Medium:** impacto minimum in reputation, local media attention and reversible in the short term.
- **High:** effectivecontrols for risk mitigation.
- **Extreme:** ino ineffective controls for risk mitigation.

5. Regulatory impact

The regulatory impact is evaluated in order to prevent risks of fines, penalties, penalties and other derivatives of regulatory rules of the activity. Although there are no specific rules for the activity developed by Bitcoin To You,it follows the best legalformatting guardianship by analogy the exercise of its activity. In this sense, the regulatory impact scale to be considered for risk measurement is::

- **Low:** nolegal charges that do not result in penalties or fines.
- **Medium:** Legal notifications that resulted in thecomplication of fines ornon-significant penalties.
- **High:** legal notifications that resulted in thecomplication of significant fines or sanctions that do not impact the continuity of businessoperations.
- **Extreme:** exposure and great tendency to legal notifications with the generation of penalties, due to iabsence orpredominance of ineffective controls for risk mitigation.

6. Treatment and monitoring

To treat therisks, attention should be paid to the level of exposure and priority. In this way, the following measures can be adopted as risk treatment:

- **Avoid:** discontinue activities, products, services, business, practices or processes that entail the identified risks.
- **Reduce:** adoptmeasures or actions to reduce and/or eliminate the vulnerability or impact of the identified risk.
- **Share:** Transfer the vulnerabilityor impact to third parties..
- **Accept:** there is nothing to do and/or no measure is adopted.

7. Treatment time

Risk controllers, managers of the first line of defense, must carry out the risk treatment according to the level of exposure and within the deadlines below:

- **Low:** within 360 days after identification.
- **Medium:** within 180 days after identification.
- **High:** within 60 days after identification.
- **Extreme:** immediately limited within 30 days after identification.

When it comes to risks that have regulatory impacts,these should be addressed within the time limits stipulated by regulatory agencies and law, for example: NOTIFICATIONS from the COAF, notifications from the Internal Revenue Service and others.

8. Approval spur

To ensure efficiency in the treatment of risks, they must be approved as set out below.

- **Low risk:** employee responsible for the process and/or activity;;
- **Medium risk:** sector coordinator and/ordepartment;
- **High risk:** industry coordinator and/or department in conjunction with directors.
- **Extreme risk:** managing partner..

GENERAL PROVISIONS

Considering the complexity in managing corporate risks, the particularities ofthe business and its operations, as well as its operational structure, this policy may be complemented by specific procedures (standards, procedures and work instructions) when applicable and required.