GENERAL PROVISION

The risk management process in the Astana Financial Services Authority (the "AFSA") is designed to identify the risks to which the AFSA is exposed and ensure that these risks are appropriately managed, and the Risk Management Policy (the "Policy") helps to achieve these goals.

The Policy provides objectives, principles, and guidelines on the Enterprise Risk Management process in the AFSA (the "ERM").

The Enterprise Risk Management represents coordinated activities to direct and control the AFSA regarding risks including the culture, capabilities, and practices that the AFSA integrates with its strategy-setting to manage risks in creating, preserving, and realizing value.

PRINCIPLES

The effective ERM must meet the following principles:

- *Integrated* – the ERM is an integral part of all AFSA activities.
- *Structured and comprehensive* – a structured and comprehensive approach to the ERM contributes to consistent and comparable results.
- *Inclusive* – appropriate and timely involvement of all AFSA employees enables their knowledge, views, and perceptions to be considered and results in improved awareness and informed risk-taking.
- *Dynamic* – risks can emerge, change, or disappear as the AFSA's external and internal context changes. The ERM anticipates, detects, acknowledges, and responds to those changes in an appropriate and timely manner.
- *Best available information* – the inputs to the ERM are based on current and historical data, as well as on future expectations. The ERM explicitly considers any uncertainties and limitations associated with such information and expectations. Information should be clear, timely, and available to relevant stakeholders.
- *Human and cultural factors* – human behavior and culture significantly influence all aspects of the ERM at each level and stage.
- *Continual improvement* – the ERM is continuously improved through learning and experience.

RISK CULTURE

The ERM is an integral part of the AFSA culture and decision-making and is integrated into the organizational structure, operations, and processes related to the AFSA's mandate, strategic goals, and objectives.

The AFSA is committed to developing the ERM and risk-based decision-making competencies and awareness throughout the organization.

Risk culture begins with an understanding of the essence of risk, its types, and the importance of the ERM process at all levels of the AFSA.

The presence of a risk culture in the AFSA implies:

- encouraging employees to participate in decision-making and to discuss risks to the AFSA's strategic goals;
- having open and honest discussions about risks that the AFSA faces;
- encouraging risk-awareness across the AFSA;
- support from the AFSA Management on the ERM continuous improvement;
- the competence of the AFSA employees on risk management issues.

ROLES AND RESPONSIBILITIES

The Board of Directors of the AFSA

The Board through the Audit and Risk Committee of the Board:

- approves the manner of managing risks in the system of internal control;
- sets appropriate policies to manage risks to the AFSA's operations and the achievement of its objectives;
- provides oversight of the AFSA's the risk appetite and risk tolerance levels.

The Audit and Risk Committee of the Board

- assists the Board in the identification, assessment, management, and monitoring of the significant risks to the AFSA's objectives and activities by review and oversight.

The Executive Body of the AFSA

- oversees the establishment of effective risk management and control systems.

The Risk Committee of the Executive Body of the AFSA

- provides operational oversight of the AFSA existing risks;
- identifies and assesses any new risks that the AFSA needs to consider;
- facilitates the safe delivery of the performance targets to the stakeholders.

The Chief Executive Officer

- ensures the operational effectiveness of the ERM;
- provides leadership and direction to the AFSA Management, together with them shapes the values, principles, and policies that form the foundation of the ERM;
- sets broad-based policies and develops the AFSA's risk management philosophy and risk culture;
- monitors activities and risks in relation to the AFSA's risk appetite and risk tolerance levels.

The Risk Manager

- establishes the ERM policy and ensures its implementation;
- promotes the ERM competence throughout the AFSA, including facilitating development of the ERM expertise and helping align risk responses with the AFSA's risk appetite and risk tolerance levels, and developing appropriate controls;
- guides integration of the ERM with other management activities.

The Internal Audit

- provides the independent assessment of the effectiveness and recommends improvements to the ERM.

The AFSA Management including the Risk Owners

- have responsibility for managing risks related to their divisions' objectives;
- identify risks and ensure that the relevant risk treatment is adequate and effective;
- guide application of the ERM components within their areas of responsibility, ensuring application is consistent with risk tolerance levels;
- assign responsibility for the ERM procedures to the Risk Coordinator.

All AFSA employees

- understand that the ERM and risk awareness are a key part of the AFSA's culture;

- be aware of risks, which fall into their area of responsibility, the possible impacts these may have on other areas and the impact other areas may have on them.

THE ENTERPRISE RISK MANAGEMENT PROCESS

The Framework of the AFSA combines a top-down strategic view with a bottom-up operational assessment conducted by each division.

This combined approach ensures that all the significant risks which need to be considered are identified and managed properly.

The ERM is an iterative process with clearly defined steps, which must be systematically applied and integrated into the AFSA's organizational structure, operations, and processes:

Setting risk appetite and risk tolerance levels

The ERM cycle begins with the setting risk appetite and risk tolerance levels.

Risk appetite and risk tolerance levels are set and approved annually, but the CEO with the Board oversight continually monitors them at all levels and accommodates change when needed.

Following the Board's approval risk appetite and risk tolerance levels are communicated throughout the AFSA as they are intended to support decision-making being within the set appetite and tolerances.

Communication and consultation

Communication promotes awareness and understanding of risk and how to deal with it.

Consultation involves obtaining feedback and information to support informed decision-making.

Communication and consultation with appropriate external and internal stakeholders are the continual and iterative process and takes place within and throughout all steps of the ERM.

The AFSA demonstrates open communication and transparency and encourages employees to communicate upward any issues and concerns without fear of retribution.

Scope, context, criteria

The purpose of establishing the scope, the context, and criteria is to customize the ERM, enabling effective risk assessment and appropriate risk treatment.

Scope, context, and criteria involve defining the scope of the process, and understanding the external and internal context:

- *external context* - understanding of external stakeholders and hence the extent to which this external environment will impact the AFSA's ability to achieve its objectives;
- *internal context* - understanding organizational elements and the way they interact.

The ERM shall be applied at all levels of the AFSA activities using criteria set up by the Framework and the Policy.

Risk assessment

The purpose of risk assessment is to find, recognize, and address the risks that may affect the decision or the likelihood of achieving the AFSA's objectives.

Risk assessment is conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of stakeholders. It uses the best available information, supplemented by further inquiry, as necessary.

Risk assessment includes the following activities:

- *risk identification* – the purpose of risk identification is to find, recognize, and describe risks that might prevent the AFSA from achieving its objectives;

- *risk analysis* – the purpose of risk analysis is to comprehend the nature of risk and its characteristics including, where appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainties, risk factors, impact, likelihood, events, scenarios, controls, and their effectiveness. The likelihood and impact scores, as identified after consideration of existing controls, are combined to determine the **Inherent risk level**.
- *risk evaluation* – risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. Risk evaluation assists in the selection of risk treatment action for the risk to remain within the AFSA's risk appetite and risk tolerance levels.

Risk treatment

The purpose of risk treatment is to select and implement options for addressing and managing risks to the acceptable residual level. The **Residual risk level** is determined by the combination of the likelihood and impact scores, as identified after consideration of the effectiveness of the Risk treatment plan implementation.

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived with the achievement of the objectives against the costs, effort, or disadvantages of implementation.

The Risk Owners and other stakeholders should be aware of the nature and extent of the residual risk after the risk treatment. Monitoring and review need to be an integral part of the risk treatment implementation to give assurance that the different forms of treatment become and remain effective.

Risk treatments, even if carefully designed and implemented might not produce the expected outcomes and could produce unintended consequences.

The decision to retire the risk could be made if certain conditions are met. However, the Risk Owner must ensure that the established controlling and assurance mechanisms are continuous and effective.

Monitoring and review

The purpose of monitoring and review is to assure and improve the quality and effectiveness of the ERM design, implementation, and outcomes.

Monitoring and review should take place in all stages of the ERM. It includes planning, gathering, and analyzing information, recording results, and providing feedback.

The results of monitoring and review should be incorporated throughout the AFSA's performance management, measurement, and reporting activities.

Recording and reporting

The results of monitoring and review are incorporated in the AFSA's risk management reporting activities.

Reporting is an integral part of the AFSA's governance that helps enhance the quality of dialogue with stakeholders.

Risk management reports are designed to inform the Board promptly and regularly, the ARCo, and the Executive Body about the amount of risks accepted by the AFSA.