risk oversight solutions

A better response to risk.

Sample Corporate Risk Management Policy

This document provides a sample Risk Management policy which includes an overview of the key roles and responsibilities of the various stakeholders.

PURPOSE:

The purpose of this policy is to create, enhance and protect shareholder value by designing, implementing and maintaining an effective, structured, and enterprise-wide risk management approach. We believe that adopting this policy will result in both immediate and long-term benefits to all stakeholders, internal and external. Benefits foreseen are:

- Increase the likelihood of achieving the company's business objectives.
- Enhance XYZ's competitive advantage.
- Deal with market instability more effectively.
- Enable XYZ to better meet customers' expectations and contractual requirements.
- Establish a Board level mandate to implement an enterprise wide approach to risk management to meet emerging risk management and risk oversight expectations.
- Enhance shareholder and customer confidence.
- Respond to escalating institutional shareholder demands for effective risk management frameworks in companies they invest in.
- Meet emerging credit rating agency expectations related to risk management.

SCOPE:

This policy applies to employees, officers and directors of each of XYZ Energy Services Corp. and its Subsidiaries. References in this policy to the Corporation mean XYZ Energy Services Corp. and its subsidiaries.

POLICY:

1.1 Risk Management Principles

Risk management is a systematic, structured, transparent, inclusive, and timely way to manage uncertainty and create and protect shareholder value. It should be adaptive to XYZ's business needs and a dynamic process. It should evaluate risk/reward trade offs within the organization's appetite for risk tolerance.

It is intended to be an integral part of all organizational processes, including strategic planning and decision making, and is based on best available, "fit for purpose" risk information. It is dynamic, iterative and facilitates continuous improvement of the organization.

2.1 Corporate Risk Assessment Methodology

The risk assessment methodology the Corporation has selected focuses on end result business objectives that the company must achieve to be successful over the longer term and drive shareholder value. The key goal is identification and consensus agreement on the acceptability of the company's residual risk position (residual risk status is a composite snapshot the helps decision makers and the board better understand the level of uncertainty that exists that business objectives will be achieved).The risk management methods and tools used by the Corporation are expected to evolve and mature over time with an overriding goal that the amount of formal risk assessment applied (as opposed to informal risk management which happens every day in every part of the Corporation) will be determined by carefully considering the costs and benefits of the additional information.

3.1 Risk Management Roles and Responsibilities

The **Board of Directors** is responsible for:

a. Approving and authorizing this policy.
b. Assessing whether the risk appetite and tolerance implicit in the Corporation's business model, strategy, and execution is appropriate.
c. Assessing whether the expected risks in the Corporation's strategic plan are commensurate with the expected rewards.
d. Evaluating whether management has implemented an effective and fit for purpose process to manage, monitor, and mitigate risk that is appropriate given the Corporation's size, growth aspirations, business model, and strategy.
e. Assessing whether the Corporation's risk management processes are capable of providing reliable information to the board on the status major risks that are or could impact on the achievement of the Corporation's objectives, including significant risks to the Corporation's reputation.

The **CEO** is responsible for:

a. Appointing the members of the Corporation's Risk Oversight Committee.
b. Assessing whether the Corporation's current and expected risk status is appropriate given the Corporation's and board of directors' risk appetite and tolerance.
c. Ensuring that there are reliable processes in place to provide the board of directors with an annual report on the effectiveness of the Corporation's risk management processes; and a report on the Corporation's consolidated residual risk status, including any remediation actions underway to adjust the Corporation's retained risk position.

The **Risk Oversight Committee** is responsible for:

a. Determining where and when formal documented risk assessments should be completed recognizing that additional risk management rigour and formality should be cost/benefit justified.
b. Ensuring that business units are identifying and reliably reporting the material risks to the key objectives identified in their annual strategic plans.
c. Reviewing and assessing whether material risks being accepted across XYZ are consistent with the Corporation's risk appetite and tolerance.
d. Developing, implementing, and monitoring overall compliance with this policy.
e. Overseeing development, administration and periodic review of this policy for approval by the Board of Directors.
f. Reviewing and approving the annual external disclosures related to risk oversight processes required by Canadian security regulators.
g. Reporting periodically to the CEO and the Board on the Corporation's consolidated residual risk position.
h. Ensuring that an appropriate culture of risk-awareness and response exists throughout the organization

Business unit leaders are responsible for:

a. Managing risks to their business unit's business objectives within the Corporation's risk appetite/tolerance.
b. Identifying in their business unit's annual strategic plan the most significant internal risks and external risks that have the potential to impact on the business unit's key objectives together with their plans to address those risks.
c. Reporting to the Risk Management Support Services unit the current composite residual risk rating on key objectives identified in the business unit's strategic plan and other objectives that may have been assigned to them by the Risk Oversight Committee and/or the CEO.
d. Completing documented risk assessments when they believe the benefits of formal risk assessment exceed the costs, or when requested to by the CEO or Risk Oversight Committee.

Risk Management Support Services unit is responsible for:

a. Providing risk assessment training, facilitation and assessment services to senior management and business units upon request.
b. Annually preparing a consolidated report on XYZ's most significant residual risks and related residual risk status, and a report on the current effectiveness and maturity of the Corporation's risk management processes for review by the Risk Oversight Committee, senior management, and the Corporation's board of directors.

c. Completing risk assessments of specific objectives that have not been formally assessed and reported on by business units when asked to by the Risk Oversight Committee, senior management, or the board of directors; or if the Risk Management Support Services team leader believes that a formal risk assessment is warranted to provide a materially reliable risk status report to senior management and the board of directors.

d. Conducting independent quality assurance reviews on risk assessments completed by business units and providing feedback to enhance the quality and reliability of those assessments.

e. Participating in the drafting and review of the Corporation's annual disclosures in the Annual Information Form (AIF) related to risk management and oversight.

NOTE: The roles defined for "Risk Management Support Services" in larger companies could be split with responsibilities (a) to (c) done by an ERM support group. Responsibility (d) would be done by Internal Audit. Responsibility (e) could be shared by both groups.