



*LeiningerCPA, Ltd.*  
**RISK MANAGEMENT POLICY STATEMENT**

This policy provides an overview of the bank's risk management process and defines the broad responsibilities for overseeing corporate governance and risk management activities.

***Enterprise Risk Management Principles***

The Board of Directors recognize that managing risk is not an end in itself, and embrace a broader concept of guiding bank activities known as enterprise risk management, which recognizes the bank's responsibility to maximize opportunity as well as minimize risk.

*Risk* is defined as the potential that events, expected or unanticipated, have an adverse impact on the bank's capital and earnings. Similarly, *Opportunity* is defined as the potential that those events will have a positive impact; or stated more broadly, positively affect the achievement of bank objectives, supporting value creation or preservation.

The existence of risk is not necessarily a problem; even the existence of high risk is not necessarily a concern, so long as management effectively manages that level of risk. To put risks in perspective, management and the Board should decide whether the risks are warranted.

Generally, a risk is warranted when it is identified, understood, measured, monitored, and controlled as part of a deliberate risk reward strategy. It should be in the bank's capacity to readily withstand the financial distress that such risk could cause; the primary regulatory objective is to ensure that the bank does not assume more risk than it can effectively manage.

Enterprise risk management takes an approach that aligns risk appetite and strategy, while seizing opportunity and enhancing stakeholder value. This facilitates efficient allocation of the bank's personnel and resources according to the risk reward relationship. In this context, risk management systems should effectively act as performance management systems.

***Summary of Risk Management Responsibilities***

The directors and senior management are responsible for providing oversight of the bank's risk management activities, including (each step is further described in the following section):

1. *Recognizing and understanding the overall risk profile* and the levels and types of risk to bank earnings and capital, including on-going monitoring of changes to existing risks and risks that may arise from new activities (while ensuring that capital levels are maintained commensurate with the overall level of risk);

2. *Overseeing corporate governance processes*, including risk management/operating systems, internal control systems and internal/external audit programs, and ensuring they are maintained at levels of effectiveness commensurate with the bank's overall risk profile;
3. *Ensuring the capability of risk management systems* to pro-actively identify, measure, monitor and control risks to an acceptable level;
4. *Assessing the adequacy of senior management and board oversight* of the risk management process, and the related policies, procedures and limits.

### ***Description of Risk Management Responsibilities***

#### **1. Recognizing and Understanding the Overall Risk Profile**

Senior management and the Board may generally be kept apprised of the bank's activities and better understand the overall risk profile by:

- Actively participating in meetings, asking probing questions about risks and critically reviewing reports, and approving exceptions to policy statements and understanding the rationale for the exceptions and the resultant impact on the bank's risk profile.
- Reviewing internal/external audit and examination reports, covering all material areas of risk within the bank, and periodically meeting with the auditors and examiners.
- Holding management accountable for resolution of audit and examination findings and recommendations, and especially following-up on repeat criticisms.
- Providing a forum for employee or other forms of feedback regarding the effectiveness of the accounting and control environment.
- Providing comprehensive documentation of Board activities in the minutes, including individual votes or positions taken by Board members where appropriate.

The bottom line is that the Board must be able to detect/take action when management materially fails their responsibilities, and risks are no longer minimized to an acceptable level. The Board should place reliance on management, but not blind faith.

#### **2. Overseeing Corporate Governance Processes**

Senior management and the directors are responsible for ensuring the following objectives are met (each area is described below, and in separate policy and procedure statements). The overall responsibility for achievement of these objectives remains with senior management and the Board; the responsibility cannot be delegated to others within the bank or to outside parties.

- The bank's corporate governance process is supportive of a strong risk management culture (referred to as "inherent risk").
- Risk management and operating systems are pro-active and effective ("operating risk").
- The system of internal control operates effectively ("control risk").
- An effective internal audit and external audit program is in place ("audit/detection risk").

**Corporate governance objectives** – Senior management and the Board must ensure that the importance of internal control is understood and respected throughout the organization, often referred to as the “tone at the top.” They should also foster an environment of forthright communication and critical examination of issues.

**Risk management/operating system objectives** – In order to avoid uncontrolled or unacceptable exposure to risk, it is essential that any changes in the risk profile of the bank be pro-actively matched by commensurate changes in the bank’s risk management, operating and control systems. To help accomplish this, management and the directors should oversee material new, expanded, or modified products or services through an effective risk management process, including:

- Performing adequate due diligence prior to introducing the product or service, including those obtained through third party providers, including identification of potential risks;
- Developing and implementing controls, operating processes and management information systems to ensure risks are properly measured, monitored, and controlled; and
- Developing and implementing appropriate performance monitoring and review systems, including key performance targets and indicators, and status reports to management/Board.

**Internal control objectives** – Effective internal control is a foundation for safe and sound operations. The overall objective of the internal control process is to provide reasonable, but not absolute, assurance that the bank will achieve:

- Effective and efficient operations, including safeguarding of assets;
- Reliable financial reporting; and,
- Compliance with applicable laws and regulations.

Management is responsible for ensuring the effectiveness of internal control. Management self-assessments and on-going monitoring are an important first layer in ensuring the effectiveness of controls, but they are not impartial. Therefore, an important element in assessing the effectiveness of the internal control system is an internal/external audit function.

**Internal and external audit objectives** – The board is responsible for ensuring that the bank has an internal audit function, as supplemented by an external audit program as needed or required, that is appropriate to the size and the nature and scope of its activities.

The overall objective of the internal audit function is to independently and objectively evaluate and report on the effectiveness of the bank’s risk management, internal control, and governance processes, and the quality of performance in carrying out assigned responsibilities. This objective includes promoting effective control at reasonable cost.

The directors and senior management should be confident that the internal audit function addresses the risks and meets the demands posed by the bank’s current and planned activities. When properly structured and conducted, internal audit provides vital information about weaknesses in the internal control system so that management can take prompt, remedial action.

### **3. Ensuring the Capability of Risk Management Systems**

The bank's risk management systems should be effective in pro-actively managing and minimizing risk to an acceptable level, including the ability to:

**Identify risk** – To properly identify risks, the bank must recognize and understand existing risks or risks that may arise from new business initiatives. Risk identification should be a continuing process, and risks should be understood at the transaction and portfolio levels.

**Measure risk** – Accurate and timely measurement of risk is essential to effective risk management systems. The measurement systems will vary depending on the type and complexity of the products and services. Management should periodically test the measurement tools to make sure they are accurate. Sound risk measurement systems assess the risks individually (transaction level) and in aggregate (portfolio level).

**Monitor risk** – The bank must monitor risk levels to ensure timely review of risk positions and exceptions. Monitoring reports should be timely, accurate, and informative and should be distributed to appropriate individuals to ensure action, when needed.

**Control risk** – The bank must establish and communicate risk limits through policies, standards, and procedures that define responsibility and authority. These limits should serve as a means to control exposures to the various risks associated with the bank's activities. The limits should be tools that management can adjust when conditions or risk tolerances change. The bank shall also have a process to authorize and document exceptions or changes to risk limits when warranted.

### **4. Assessing the Adequacy of Senior Management and Board Oversight**

Management is responsible for the implementation, integrity, and maintenance of risk management systems. Management must keep the Board adequately informed about risk-taking activities through relevant and reliable board reports and other communications. Management should:

- Implement the bank's strategies, as part of a deliberate risk reward strategy;
- Develop policies that define the bank's risk tolerance and ensure that they are compatible with strategic goals;
- Ensure that strategic direction and risk tolerances are effectively communicated and adhered to throughout the bank; and
- Oversee the development and maintenance of management information systems to ensure that information is timely, accurate, and pertinent.

Senior management and the Board should consider the bank's policies, processes, personnel, and control systems, as further described below:

**Policies** – are statements, either written or verbal, of the bank's commitment to pursue certain results. Policies often set standards (e.g., on risk tolerances) and may recommend courses of action. Policies should express the bank's underlying mission, values and principles. A policy review should be triggered when the bank's activities or risk tolerances change.

**Processes** – are the procedures, programs, and practices that impose order on the bank's pursuit of its objectives. Processes define how daily activities are carried out. Effective processes are consistent with the

underlying policies and are governed by appropriate checks and balances. As a smaller bank, the regulators point out that our processes may be effective even when less formal in nature.

**Personnel** – are the staff and managers that execute or oversee processes. They should be qualified and competent; perform as expected; and understand the bank’s mission, values, policies, and processes.

**Control systems** – including the tools and information systems (and internal/external audit programs) that bank managers use to measure performance, make decisions about risk, and assess the effectiveness of processes. Feedback should be timely, accurate, and pertinent – appropriate to the level and complexity of risk taking.

### ***Categories of Risk***

The bank’s regulators have defined the following broad categories of risk:

- credit risk;
- market, interest rate and liquidity risk;
- transaction and operational risk;
- compliance and legal risk;
- strategic and reputation risks, including regulatory risk.

For each area or activity, the bank should assess the quantity of risk, quality of risk management, aggregate risk, and the direction or trend of the risk profile.

\* \* \* \* \*