ภาคผนวก ก

Internal Control - Integrated Framework

Executive Summary

COSO Definition of Internal Control

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Key Concepts

- Internal control is a *process*. It is a means to an end, not an end in itself.
- Internal control is effected by *people*. It's not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

Executive Summary

Senior executives have long sought ways to better control the enterprises they run. Internal controls are put in place to keep the company on course toward profitability goals and achievement of its mission, and to minimize surprises along the way. They enable management to deal with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations.

Because internal control serves many important purposes, there are increasing calls for better internal control systems and report cards on them. Internal control is looked upon more and more as a solution to a variety of potential problems.

What Internal Control Is

Internal control means different things to different people. This causes confusion among businesspeople, legislators, regulators and others. Resulting miscommunication and different expectations cause problems within an enterprise. Problems are compounded when the term, if not clearly defined, is written into law, regulation or rule.

This report deals with the needs and expectations of management and others. It defines and describes internal control to:

- Establish a common definition serving the needs of different parties.
- Provide a standard against which business and other entities--large or small, in the public or private sector, for profit or not--can assess their control systems and determine how to improve them.

Internal control is broadly defined as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

The first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs.

Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Published financial statements are being prepared reliably.
- Applicable laws and regulations are being complied with.

While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time.

Internal control consists of five interrelated components. These are derived from the way management runs a business, and are integrated with the management process. Although the components apply to all entities, small and mid-size companies may implement them differently

than large ones. Its controls may be less formal and less structured, yet a small company can still have effective internal control. The components are:

Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors.

Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Control Activities

Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

Information and Communication

Pertinent information must be identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities and conditions necessary to informed business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders.

Monitoring

Internal control systems need to be monitored--a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities, and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board.

There is synergy and linkage among these components, forming an integrated system that reacts dynamically to changing conditions. The internal control system is intertwined with the entity's operating activities and exists for fundamental business reasons. Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise. "Built in" controls support quality and empowerment initiatives, avoid unnecessary costs and enable quick response to changing conditions.

There is a direct relationship between the three categories of objectives, which are what an entity strives to achieve, and components, which represent what is needed to achieve the objectives. All components are relevant to each objectives category. When looking at any one category--the effectiveness and efficiency of operations, for instance--all five components must be present and functioning effectively to conclude that internal control over operations is effective.

The internal control definition--with its underlying fundamental concepts of a process, effected by people, providing reasonable assurance--together with the categorization of objectives and the components and criteria for effectiveness, and the associated discussions, constitute this internal control framework.

What Internal Control Can Do

Internal control can help an entity achieve its performance and profitability targets, and prevent loss of resources. It can help ensure reliable financial reporting. And it can help ensure that the enterprise complies with laws and regulations, avoiding damage to its reputation and other consequences. In sum, it can help an entity get to where it wants to go, and avoid pitfalls and surprises along the way.

What Internal Control Cannot Do

Unfortunately, some people have greater, and unrealistic, expectations. They look for absolutes, believing that:

- Internal control can ensure an entity's success--that is, it will ensure achievement of basic business objectives or will, at the least, ensure survival.

Even effective internal control can only help an entity achieve these objectives. It can provide management information about the entity's progress, or lack of it, toward their achievement. But internal control cannot change an inherently poor manager into a good one. And, shifts in government policy or programs, competitors' actions or economic conditions can be beyond management's control. Internal control cannot ensure success, or even survival.

- Internal control can ensure the reliability of financial reporting and compliance with laws and regulations.

This belief is also unwarranted. An internal control system, no matter how well conceived and operated, can provide only reasonable--not absolute--assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs.

Thus, while internal control can help an entity achieve its objectives, it is not a panacea.

Roles and Responsibilities

Everyone in an organization has responsibility for internal control.

Management

The chief executive officer is ultimately responsible and should assume "ownership" of the system. More than any other individual, the chief executive sets the "tone at the top" that affects integrity and ethics and other factors of a positive control environment. In a large company, the chief executive fulfills this duty by providing leadership and direction to senior managers and reviewing the way they're controlling the business. Senior managers, in turn, assign responsibility for establishment of more specific internal control policies and procedures to personnel responsible for the unit's functions. In a smaller entity, the influence of the chief executive, often an owner-manager, is usually more direct. In any event, in a cascading responsibility, a manager is effectively a chief executive of his or her sphere of responsibility. Of particular significance are financial officers and their staffs, whose control activities cut across, as well as up and down, the operating and other units of an enterprise.

Board of Directors

Management is accountable to the board of directors, which provides governance, guidance and oversight. Effective board members are objective, capable and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal and internal audit functions, is often best able to identify and correct such a problem.

Internal Auditors

Internal auditors play an important role in evaluating the effectiveness of control systems, and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role.

Other Personnel

Internal control is, to some degree, the responsibility of everyone in an organization and therefore should be an explicit or implicit part of everyone's job description. Virtually all employees produce information used in the internal control system or take other actions needed to effect control. Also, all personnel should be responsible for communicating upward problems in operations, noncompliance with the code of conduct, or other policy violations or illegal actions.

A number of external parties often contribute to achievement of an entity's objectives. External auditors, bringing an independent and objective view, contribute directly through the financial statement audit and indirectly by providing information useful to management and the board in carrying out their responsibilities. Others providing information to the entity useful in effecting internal control are legislators and regulators, customers and others transacting business with the enterprise, financial analysts, bond raters and the news media. External parties, however, are not responsible for, nor are they a part of, the entity's internal control system.

Organization of this Report

This report is in four volumes. The first is this Executive Summary, a high-level overview of the internal control framework directed to the chief executive and other senior executives, board members, legislators and regulators.

The second volume, the Framework, defines internal control, describes its components and provides criteria against which managements, boards or others can assess their control systems. The Executive Summary is included.

The third volume, Reporting to External Parties, is a supplemental document providing guidance to those entities that report publicly on internal control over preparation of their published financial statements, or are contemplating doing so.

The fourth volume, Evaluation Tools, provides materials that may be useful in conducting an evaluation of an internal control system.

What to Do

Actions that might be taken as a result of this report depend on the position and role of the parties involved:

Senior Management

Most senior executives who contributed to this study believe they are basically "in control" of their organizations. Many said, however, that there are areas of their company--a division, a department or a control component that cuts across activities--where controls are in early stages of development or otherwise need to be strengthened. They do not like surprises. This study suggests that the chief executive initiate a self-assessment of the control system. Using this framework, a CEO, together with key operating and financial executives, can focus attention where needed. Under one approach, the chief executive could proceed by bringing together business unit heads and key functional staff to discuss an initial assessment of control. Directives would be provided for those individuals to discuss this report's concepts with their lead personnel, provide oversight of the initial assessment process in their areas of responsibility and report back

findings. Another approach might involve an initial review of corporate and business unit policies and internal audit programs. Whatever its form, an initial self-assessment should determine whether there is a need for, and how to proceed with, a broader, more in-depth evaluation. It should also ensure that ongoing monitoring processes are in place. Time spent in evaluating internal control represents an investment, but one with a high return.

Board Members

Members of the board of directors should discuss with senior management the state of the entity's internal control system and provide oversight as needed. They should seek input from the internal and external auditors.

Other Personnel

Managers and other personnel should consider how their control responsibilities are being conducted in light of this framework, and discuss with more senior personnel ideas for strengthening control. Internal auditors should consider the breadth of their focus on the internal control system, and may wish to compare their evaluation materials to the evaluation tools.

Legislators and Regulators

Government officials who write or enforce laws recognize that there can be misconceptions and different expectations about virtually any issue. Expectations for internal control vary widely in two respects. First, they differ regarding what control systems can accomplish. As noted, some observers believe internal control systems will, or should, prevent economic loss, or at least prevent companies from going out of business. Second, even when there is agreement about what internal control systems can and can't do, and about the validity of the "reasonable assurance" concept, there can be disparate views of what that concept means and how it will be applied. Corporate executives have expressed concern regarding how regulators might construe public reports asserting "reasonable assurance" in hindsight after an alleged control failure has occurred. Before legislation or regulation dealing with management reporting on internal control is acted upon, there should be agreement on a common internal control

framework, including limitations of internal control. This framework should be helpful in reaching such agreement.

Professional Organizations

Rule-making and other professional organizations providing guidance on financial management, auditing and related topics should consider their standards and guidance in light of this framework. To the extent diversity in concept and terminology is eliminated, all parties will benefit.

Educators

This framework should be the subject of academic research and analysis, to see where future enhancements can be made. With the presumption that this report becomes accepted as a common ground for understanding, its concepts and terms should find their way into university curricula.

We believe this report offers a number of benefits. With this foundation for mutual understanding, all parties will be able to speak a common language and communicate more effectively. Business executives will be positioned to assess control systems against a standard, and strengthen the systems and move their enterprises toward established goals. Future research can be leveraged off an established base. Legislators and regulators will be able to gain an increased understanding of internal control, its benefits and limitations. With all parties utilizing a common internal control framework, these benefits will be realized.

Internal Control Issues in Derivatives Usage

Executive Summary

Problems surrounding the use of derivatives in recent years often revolved around difficulty in understanding their risks and their use for risk management purposes. These problems highlight the need for management to develop internal control systems for derivative activities.

The COSO report, *Internal Control--Integrated Framework,* issued by the Committee of Sponsoring Organizations of the Treadway Commission in 1992, is becoming a widely accepted basis for developing business control systems and assessing their effectiveness. This information tool was developed to help end-users of derivative products establish, assess, and improve internal control systems using the COSO Framework. Many of the control considerations discussed are also applicable to financial instruments other than derivatives.

This Executive Summary provides senior management and boards of directors with an overview of how the COSO Framework might be applied to risk management activities involving the use of derivatives. It can be used to help management design control processes, especially by providing direction for formulation of risk management policies. It also provides insights that enable those charged with oversight responsibilities to constructively examine existing policies and procedures. This information is augmented by the following supplements.

Supplement 1 -- Formulating Policies Governing Derivatives Used for Risk Management

Describes the process of developing a policy governing derivatives use in the context of the overall risk management policy of an entity. It recognizes that risk management policies encompass all aspects of control. It also recognizes the importance of establishing clear and carefully written policies to avoid confusion and miscommunication, and provides examples of various aspects of a risk management policy for derivatives. This supplement can be used as a reference to formalize such a policy.

Supplement 2 -- Illustrative Control Procedures Reference Tool

Provides examples of controls over derivative activities associated with each of the five components of control specified in the COSO Framework. It can be used as a reference for establishing, assessing, and improving controls relating to derivative activities, and can be useful for selecting controls considered to be appropriate in particular circumstances.

Overview of Derivatives and Their Environment

Derivatives are financial contracts that derive their value from the performance of underlying assets (such as a stock, bond, or physical commodity), interest or currency exchange rates, or a variety of indices (such as a composite stock index like the Standard & Poor's [S&P] 500).

Derivatives include a wide assortment of financial contracts, including swaps, futures, forwards, options, caps, floors, and collars, whose values are derived based on defined formulas that apply to notional amounts (hypothetical reference amounts). Derivatives can also include certain assets and liabilities whose value and cash flows are directly determined by an underlying instrument or index, such as collateralized mortgage obligations, interest-only and principal-only certificates, and structured notes. Other types of derivatives include contracts traded on organized exchanges standardized by regulation, as well as contracts that are traded in unregulated over-the-counter (OTC) markets, including individually tailored contracts negotiated between two parties for a specific purpose. A more detailed overview of various types of derivatives is included in Appendix A.

Risks associated with derivatives include market, credit, liquidity, as well as various other risks, described more fully in Appendix A. In addition to these technical risks, there is the fundamental risk that the use of these products may not be consistent with entity-wide objectives. Derivative use is sometimes misunderstood because, depending on the type of instrument and its terms, an instrument may be used to increase, modify, or decrease risk. As contract features increase in complexity, the value and effectiveness of a derivative in achieving objectives may become more difficult to ascertain before such positions are closed out or settled for cash. Derivative products and activities must be well understood in order for control systems to provide

adequate assurance that derivatives use will support achievement of entity-wide strategies and objectives.

Utilizing the COSO Framework Control Principles in Derivatives Management

This document relates to derivatives each of the five components of control specified in the COSO Framework, focusing primarily on derivatives that are used for risk management purposes. An environment that provides for appropriate control over derivative activities generally has certain characteristics.

The Control Environment consists of the integrity, ethical values, and competence of the entity's personnel, as well as management's philosophy and operating style. An active and effective board of directors should provide oversight. It should recognize that the "tone at the top" and the attitude toward controlling risk affect the nature and extent of derivative activities. The board should review management's planned decisions regarding the appropriateness and effectiveness of derivative strategies and positions. For example, the board should probe for explanations of past results to determine that derivative activities are effective in accomplishing objectives for which they were used. The audit committee should work with internal and external auditors to oversee implementation of risk management policies, procedures, and limits. Senior management should recognize that its philosophy and operating style have a pervasive effect on an entity. For this reason, senior managers should understand their control responsibilities, authorize use of derivatives only after risks and expected benefits have been carefully analyzed, and clearly communicate objectives and expectations for derivative activities. Senior managers should make a conscious decision about the extent of authority over derivatives delegated to management. Management should have the competence needed to understand derivative activities. Employees involved in such activities should possess the necessary skills and experience. The training process should develop and improve specific skills relating to responsibilities and expectations about derivative activities.

Risk Assessment is the identification and analysis of risks relevant to achieving objectives that form a basis for determining how risks should be managed. From a risk management perspective, entity-wide objectives relating to the use of derivatives should be consistent with risk management objectives. Mechanisms should exist for the identification and assessment of business risks relevant to the entity's unique circumstances. Use of derivatives should be based on a careful assessment of such business risks. Management should clearly link benefits of and support for derivative use with entity-wide objectives. Management also should obtain an understanding of personnel, management operating systems, valuation methodologies and assumptions, and documentation as a foundation for identifying and assessing the capability to manage risk exposures associated with derivative activities. Management should provide specific measurement criteria for achieving derivative activities objectives, such as value at risk. Risk analysis processes for derivative activities should include identifying risk, estimating its significance, and assessing the likelihood of its occurrence.

Control Activities are the policies and procedures to help ensure that management directives are carried out. Policies governing derivative use should be clearly defined and communicated throughout the organization. The risk management policy should include procedures for identifying, measuring, assessing, and limiting business risks as the foundation for using derivatives for risk management purposes. Aspects of the risk management policy for derivatives should include controls relating to managerial oversight and responsibilities; the nature and extent of derivative activities, including limitations on their use; and reporting processes and operational controls. The policy should provide for monitoring exposures against limits, and for the timely and accurate transmission of positions to the risk measurement systems. It also should provide for evaluation of controls within management information systems, including the evaluation of resources provided to maintain the integrity of the risk measurement system.

Information and Communication focus on the nature and quality of information needed for effective control, the systems used to develop such information, and reports necessary to communicate it effectively. Communications should ensure that duties and control responsibilities relating to derivative activities are understood across the organization. Adequate

systems for data capture, processing, settlement and management reporting should exist so that derivative transactions are conducted in an orderly and efficient manner. Mechanisms should be in place to obtain and communicate relevant information covering derivative activities. Directors and senior management should obtain sufficient and timely information to monitor achievement of objectives and strategies for using derivative instruments.

Monitoring is the component that assesses the quality and effectiveness of the system's performance over time. Control systems relating to derivative activities should be monitored to ensure the integrity of system-generated reports. The organizational structure should include an independent monitoring function over derivatives, providing senior management with an understanding of the risks of derivative activities, validating results, and assessing compliance with established policies.

Applying the COSO Framework Control Principles to Derivatives

This tool recognizes that the nature and extent of derivatives use are frequently found in the overall risk management processes of an organization. Such processes, as they relate to the use of derivatives for risk management purposes, should generally involve the following:

- Understanding operations and entity-wide objectives.
- Identifying, measuring, assessing, and modifying business risk.
- Evaluating the use of derivatives to control market risk and linking use to entity-wide and activity-level objectives.
- Defining risk management activities and terms relating to derivatives to provide a clear understanding of their intended use.
- Assessing the appropriateness of specified activities and strategies relating to the use of derivatives.
- Establishing procedures for obtaining and communicating information and analyzing and monitoring risk management activities and their results.

Management may consider evaluating the appropriateness of the risk management processes governing derivatives against each of the five components of control specified in the COSO Framework.

Policies that document the risk management processes and provide for the use of derivatives should be carefully constructed to recognize that risk management means different things to different people. Precise reasons for using derivatives are not always apparent, and risk relating to certain activities and uses may be interpreted differently. Since there are no standard definitions of what risk management activities entail, appropriate control means that entities must use very specific language to describe expectations for using derivatives for risk management purposes. Policies should identify objectives and expected results, clearly define terms and limits, and identify and classify activities and strategies that are permitted, prohibited, or require specific approval.

Roles and Responsibilities

Informed, involved senior-level governance is needed to ensure that risk management systems are in place and functioning as anticipated. The board of directors, its audit committee, and senior management have roles that represent critical checks and balances in the overall risk management system.

Board responsibilities--The board of directors is responsible for overseeing the business of the entity, including its policies for managing risk and using derivatives. Monitoring and other day-to-day operations of the entity, on the other hand, are the responsibility of senior management. The policy direction provided by the board is important in determining the nature and extent of the use of derivatives. The board of directors provides oversight, reviews and approves the broad objectives to be accomplished, and provides specific delegation of responsibility and authority. It typically authorizes and approves management's strategies, operating plans, and policies for accomplishing objectives. This approval helps to ensure that activity-level objectives are consistent with broad entity-level objectives.

The board of directors and senior management should carefully consider the resources required to use derivatives effectively. They should ensure that policies require employment of competent professionals to carry out risk management activities and strategies in accordance with its risk management policy and that such policy defines when reliance on outside advisors is appropriate. Further, compensation policies should be structured in a way that avoids incentives for excessive risk taking. The board should make a conscious decision about the amount of discretion that managers have in using derivatives.

Audit committee responsibilities--The audit committee should understand the scope of internal and external audit testing of compliance with approved risk management policies, procedures, and limits and become comfortable that such controls appear to be functioning as intended. The audit committee also should be alert to the risk that such controls could be circumvented.

CEO responsibilities--The CEO has overall responsibility for formulating derivatives policy and generally should be assisted in developing the policy and monitoring compliance by senior management who are not part of the day-to-day or derivatives management process. Senior management should formulate and implement approved policies, controls, and limits to ensure that the risks of derivative activities and the manner in which they are conducted are in accordance with the board's authorization.

CFO responsibilities --The CFO also should be active in formulating the entity's derivatives policy and overseeing its implementation.

Controller responsibilities--The controller is responsible for establishing the appropriate accounting treatment for all derivative activities. The corporate controller's department, not the individual business unit, should develop and document the accounting policies for derivatives. The corporate controller's department or other appropriate department independent of the business unit should also take an active role in applying the policies by assuming responsibility for documenting, assessing, and measuring compliance with appropriate accounting criteria.

Business unit responsibilities--The business unit is responsible for recommending, approving, and executing risk management strategies. Segregating transaction initiation by the business unit and

transaction review by the corporate controller or other appropriate independent department help establish necessary control over adherence to the entity's derivative policies and objectives.

What to Do

Actions that might be taken to better understand or apply the COSO Framework to derivatives will depend on the position and role of the parties involved. A board of directors, senior management, and others involved with derivatives may consider a number of actions, including:

- Initiating a self-assessment of entity-wide control systems, directing attention specifically to areas of derivative operations that are of primary importance.
- Fully integrating management of derivative activities into the enterprise's overall risk management system by developing and implementing a comprehensive risk management policy.
- Ensuring that policy objectives specifying the use of derivatives are clearly articulated and documented.
- Requiring that any use of derivatives be clearly linked with entity-wide and activity-level objectives.

Derivatives will continue to be an important business tool for managing an entity's risk management activities. Their significance is expected to increase with the development of new products and techniques that refine and improve the ability to achieve risk management and other objectives. Adequate understanding of the nature and risks of derivatives is essential to using these tools prudently. Improved awareness of how specific instruments behave under varying market conditions can only produce better informed management decision making. Effective control is critical to any well-managed derivative operation. Control systems serve as the infrastructure for accomplishing entity-wide objectives. Applying the COSO Framework can help ensure that the use of derivatives is carefully integrated into the overall organizational control system and that unforeseen and undesirable outcomes are minimized.

ประวัติผู้เขียน

ชื่อ - สกุล	นางสาวนพวรรณ ฟูติตระกูล
วัน เดือน ปี เกิด	6 ตุลาคม 2518
ประวัติการศึกษา	สำเร็จการศึกษามัธยมศึกษาตอนปลาย โรงเรียนบุญวาทย์วิทยาลัย จ.ลำปาง ปีการศึกษา 2536 สำเร็จการศึกษาปริญญาบัญชีบัณฑิต สาขาวิชาการบัญชี มหาวิทยาลัยเชียงใหม่ ปีการศึกษา 2540
ประวัติการทำงาน	
2541 – ปัจจุบัน	ธนาคารออมสินสาขาแจ้ห่ม จ.ลำปาง