Beyond Investment Risk

NOVEMBER 3, 2010 • ELAINE SPANG

As managers of the complex issues facing affluent investors, wealth management offices provide highly specialized services. That means they need sound internal controls to safeguard their clients' assets and information.

Small wealth management offices are particularly challenged in this area. These offices often have to rely on custom solutions to meet diverse client needs, resulting in technology and operations that are not as efficient or effective as they could be. Small operations can also lack the resources needed for sufficient internal controls.

The benefits of good internal controls include:

Minimizing error potential and safeguarding against specific risks.
Increasing your clients' confidence in the overall operations of the office and safety of confidential information.
Preventing errors or irregularities from occurring, and promoting early detection when they do happen.
Protecting employees by providing checks and balances and defining responsibilities and authorities.
Improved quality and timing of reliable information to support financial decisions.
Streamlined operations.

What Are The Risks?
Many of the risks faced by wealth managers and their clients are obviously finance related, revolving around cash and investment activities, such as misappropriation of funds, errors and delays in record keeping or improper allocation of funds. There are other more subtle risks, such as poor reporting and redundant activities, which can adversely affect decision-making and increase costs. Both technology and operations are sources of risk. Poorly implemented or managed systems and inadequate operational infrastructure can expose the office to significant communication and information risks.

What Are Internal Controls?
Internal controls are the systems and practices that are built into a wealth management office's core functions to safeguard clients' wealth and privacy. Internal controls are not a guarantee against risk. They are meant to provide reasonable assurance that an office can meet its goals and objectives, protect client assets and generate accurate information. Controls apply across the organization and are both tactical-addressing daily transactional activity-or strategic, such as policies and performance metrics related to employment. An effective internal control system begins with policies designed to encourage favorable actions and behavior-a set of governance standards that deal with ethics, hiring and work standards. These policies should signal senior management's desire to have values drive the office's decisions.

There are two types of internal controls, each with a different impact and cost:

Preventive controls are proactive measures designed to deter undesirable actions. They are the best type of controls, but often the most expensive to implement. Examples of preventive controls include: Segregation of duties to prevent one individual from having the ability to initiate, approve, record and reconcile a transaction.

Strong passwords to limit access to systems, programs and data.
Required authorizations.
Physical control over assets.
Adequate documentation to support all actions.

Detective controls are aimed at identifying a problem or undesirable action after it has happened. Detective controls are like a burglar alarm. They trigger an alarm after the event and provide evidence of the activity, but they do not prevent a loss or action from happening. Although detective controls are essential to a good internal control system, they are secondary to preventive controls. Examples of detective controls include:

Reviews and analyses.
Reconciliations.
Physical inventories.
Access log monitoring and review.
File integrity checks.
Motion detection in restricted areas.

Creating The Tight Controls
An effective internal control program is a continuous process of assessing risk, determining how to avoid those risks, detecting unwanted actions as soon as possible and correcting problems. It is a balancing act to ensure that the cost of control does not exceed the benefit. What follows are the basic elements of an internal control program. The approach to designing them will vary based on an office's complexity, staffing, and services.

Separation of duties (Preventive): Divide functions so that no one person has the opportunity to compromise a key process by having control over all parts of a transaction. For example, have different people initiate, approve and record cash movements. In a small office, this may be a challenge. If duties cannot be sufficiently separated, management review and oversight should be increased. Trusting a long-time employee with signing checks and moving funds is acceptable provided that same employee doesn't also record the activity, reconcile the bank accounts and prepare the reports.
Authorization, approval, verification (Preventive): Clearly define lines of responsibility and expectations with written job descriptions. Set limits for staff authorization and require supervisory approvals. For example, require dual signatures for disbursements in excess of a specified limit, control access to information through passwords and program permissions, and require a senior level individual to review supporting documents to verify that actions are appropriate, valid and in agreement with the company's policies.

Reconciliation (Detective): Require the regular, independent comparison of different sets of data to identify and investigate any discrepancies.
Asset security and information systems controls (Preventive and Detective): Protect physical assets by limiting access to equipment, cash and securities. Perform periodic physical counts and review and analyze written records or logs.
Ensure the security of information systems by restricting access to systems through passwords, access codes, firewalls and physical constraints.
Perform background and credit checks on employees, and make sure staff are properly trained.
Monitoring and performance reviews (Detective): Regularly compare reported results to budgets, forecasts, prior periods and other benchmarks to identify unexpected results or unusual conditions that require additional follow-up. Establish reporting deadlines.

Creating A Risk Management System

Risks change as an office matures and the interests and needs of its clients expand. Creating a risk management and internal control system is not a one-time event, but rather a continuing and evolving process. The best way for a wealth management office to evaluate its need for internal controls is to perform a risk assessment.

A risk assessment performed by an independent professional can identify potential risks and cost-effective controls. The report can help an office realign responsibilities to obtain a greater level of transparency and oversight.

The risk assessment documents the business and risk tolerance environment, evaluates current operations and controls, and identifies potential gaps in risk management.
It is a good idea to have a risk assessment at least every two years.

In challenging economic times like these, private wealth management offices need to be more vigilant about potential risks. This is the right time to revisit controls all across the organization, eliminating silos and creating connected activities, thus reducing risk and enabling management to make informed strategic and tactical decisions.

Elaine Spang, CPA (elaine.spang@windwardadvisory.com), is a partner at Windward Advisory Group (www.windwardadvisory.com), a private wealth management operations and technology consultancy offices in Princeton, N.J., Phoenix and Carlsbad, Calif.

About GreenHills Ventures

GreenHills Ventures, LLC., established in 2001 as a private investment holding company and General Partners for GHV Fund I and GHV Fund II, (GHV Fund), an early stage venture fund and GHV Wealth Management Holding, LLC. (GHVWMH), a wealth management firm focused on alternative investments for its single and multi-family offices and institutions. For more information visit www.greenhillsventures.com.