THE EXCELLENT FIDUCIARY

A Model for Managing Fiduciary Risk

Ronald E. Hagan[*]

A critical legal duty accompanies the responsibility of employers to manage employee benefit plans fairly and safely. Tactics for managing the associated risks are not intuitive and pose a significant challenge for the typical executives who populate a plan management committee. Risk management is often left for others in an enterprise to consider, but current events mandate a change in thinking and action. A framework of standardized procedures is needed.

INTRODUCTION

As enterprises look to acquire and keep qualified workers, the labor, talent, and human capital market remains highly competitive. Many firms give various employee benefits, such as health and welfare, disability, retirement, and profit-sharing programs, to recruit and retain talent. Managing the risks connected to such benefit programs is challenging, especially if the tactics used fail to align with the enterprise's risk culture. Sponsoring and administering various employee benefit plans (EBPs) triggers the acquisition of severe potential liability, exposing the enterprise and the EBP oversight committee to risks that fall inside the purview of the Employee Retirement Income Security Act of 1974 (ERISA). Regulatory, litigation, data security, service providers, and internal systems represent significant sources of risks for EBP fiduciaries. Inextricably linked with governance and compliance, risk management depends on critical decision-making criteria that are proven to produce safer and better-performing EBPs.

THREE CRITERIA FOR CRITICAL DECISION-MAKING

Risk management is ongoing and ubiquitous. Whether discussing daily risk management for an EBP committee or enterprise risk management, neither are "one and done" activities or tasks. It necessitates ongoing learning about how dangers and opportunities change, which may require realigning risk decisions, objectives, or tactics. It also calls for management measures and controls to ensure that policies and procedures for activities that affect risk are understood, followed, and evaluated for effectiveness.

Many EBP fiduciaries are not risk compliance officers,

[*]*RONALD E. HAGAN* is chairman of RolandlCriss' Risk Standards Committee, and his firm is the premier risk manager for employee benefit plan sponsors. Mr. Hagan has a lengthy career in employee benefit plan risk management. He has pioneered many certifications, standards practices, and fiduciary risk management strategies preferred by boards of directors and human resources executives. Reach him by e-mail at ronhagan@rolandcriss.com.

and as a result, they lack familiarity with the primary criteria used to construct a tailored risk framework. Those criteria must align with the culture set by the board of directors, and their impact weaves throughout the practices that comprise an EBP's risk strategy.

An enterprise's risk culture includes the values, beliefs, and behaviors about the governance, assurance, and management of risk, including setting risk appetite and tolerances, views about the impact of risk on conduct and decisions, and modeling of appropriate risk-taking behavior. When boards of directors decide to sponsor EBPs, they understand inherent risks and residual risks lurk in implementing such plans. Inherent risk is the level of risk without actions and controls, and residual risk is the level after measures and controls are in place.

In order to develop and maintain an EBP risk management framework, it is essential to know the parameters the enterprise's board or governing authority established in each of the three vital decision-making criteria of risk tolerance, risk appetite, and risk capacity:

- **Risk tolerance** is the level of risk from external and internal threats the enterprise is **unwilling** to exceed to achieve objectives. (A threat is an event that has, on balance, an undesirable effect on achieving objectives.) Risk tolerance is a grade higher than risk appetite. Errors in payroll operations resulting in misapplied defined contribution plan deferrals from participants' paydays exemplify a risk tolerance issue.

- **Risk appetite** is the level of exposure to threats the enterprise is **willing** to accept to achieve its objectives. This criterion reveals the upper exposure limit the enterprise is ready to accept. When reaching that limit, the framework would mandate an immediate assessment to find a way to reduce the risk to a level at or below the risk tolerance level. An example is deficiencies found during an independent audit of a service provider's data security policies or procedures.

- **Risk capacity** is the maximum level of peril the enterprise can **handle**, and this criterion defines the total financial resources available to finance a catastrophic event. Many EBP sponsors acquire insurance to cover fiduciary-related dangers that supplement their capability of funding adverse results in scenarios like class action lawsuits for breaches of fiduciary duty and data security intrusions.

CONSTRUCTING A RISK MANAGEMENT FRAMEWORK

As threats to the safe operation of EBPs continue to grow and regulatory controls expand, many C-suite executives now recognize the value of having a formal risk management framework but do not know where to start. This article has insufficient space to define the steps in detail; fortunately, they separate into clear strategic and tactical categories.

The EBP risk management standards should address at least the following three strategic topics:

1. **Assessment of practices:** A risk management framework assessment is a systematic procedure involving gathering and analyzing data about an EBP's operations to assess how closely those procedures adhere to the framework's standards. The assessment schedule should embrace EBP committee performance, service providers, and internal support functions such as payroll and information technology. Not to be confused with a certified public accountant's (CPA)

annual plan audit, an independent risk management firm employing properly credentialed experts (for example, GRCP-certified) should perform an assessment yearly.

2. **Governance documents:** Employers should use clear, orderly, and concise language in all policy statements and plan governance documents. Descriptions of EBP plan features for participants must be concise, including a summary of the terms and conditions of the plan in clear language, and distributed promptly on a well-thought-out schedule. The plan administrator should always engage legal counsel to examine the plan documentation.

3. **Fiduciary and cybersecurity liability insurance:** Insurance is a critical component of a well-constructed structure because it transfers some risk from the EBP sponsor to a financial underwriter. Such a transfer can create a risk management strategy that is more quantifiable and economical, especially when it comes to unforeseen costs like litigation defense. Errors & omissions (E&O) and directors & officers (D&O) policies may not embrace fiduciary and cybersecurity exposure, nor does an ERISA bond.

The tactics to develop an EBP risk management framework require explicit knowledge of the parameters defined in the enterprise's risk culture. Acquiring answers to the following issues is the starting point for EBP leaders:

- What is the governing authority's blueprint for risk culture (that is, tolerance, appetite, and capacity)?
- How do EBP governance policies and operations procedures allocate into inherent and residual risk categories?
- What are the existing threats to the EBP complex and the resources that support them?
- Analyze the explicit and implicit risk messages that managers and leaders convey.

Senior human resources and finance leaders typically lead the development of the actions and controls in EBP risk management frameworks. The following checkpoints form a blueprint for their design:

- What procedures and safeguards must we implement and evaluate for ongoing risk management?
- Establish channels for information-gathering and notification concerning hazards and opportunities.
- Implement several control types to prevent, detect, and address unfavorable risk events.
- Managers and staff should receive training on risk decision-making criteria (that is, tolerance, appetite, and capacity).
- Create curricula for risk-based education for various workforce audiences.
- Review established actions and controls periodically (at least once a year) and sometimes continuously to ensure their design remains suitable and functions as intended.

WHO PARTICIPATES IN DEVELOPING AND EBP RISK MANAGEMENT FRAMEWORK?

The widely held view that risk management embeds deeply in governance and compliance unavoidably involves cross-functional participation. Accordingly,

board members, senior executives in finance, human resources, and information technology all have a role in EBP risk framework development.

A governing authority such as a board of directors must prioritize monitoring over the direction and control exercised by people in charge of EBP programs. Giving committees guidance and criteria for making decisions is essential to leadership. That entails establishing the enterprise's mission, vision, values, appetite for risk, tolerance for risk, capacity for accepting risk, ethical standards, and a high-level declaration of goals and objectives.

Modern chief financial officers (CFOs) are responsible for much more than just maintaining assets and keeping track of finances. The CFO handles the purse strings and drives risk management by selectively forming and supporting business improvement projects. The CFO is now an essential strategic team member and contributes to setting the organization's direction. The success of EBP risk management depends on the CFO's backing.

Executives in human resources oversee the organization's "human capital" and carry out duties crucial to EBP risk management. The tactical responsibility for advancing and fostering the enterprise's purpose, vision, and values, as established by the governing authority, frequently rests with the human resources team. As frontline managers of EBP operations, they are often the first to encounter the events with the most significant potential harm for plan participants and the enterprise.

The chief information officer (CIO) must set up the necessary systems to ensure that the enterprise gathers and keeps data for EBPs in a way that enables the distribution of the appropriate data to the proper individuals at the right time and in the suitable format. Protecting personally identifiable information is imperative and depends on sufficient technological resources. The CIO must participate in developing the EBP risk management framework and then collaborate with the EBP committee to identify the current technologies, assess them, and decide which needs upgrading when regulatory requirements call for it.

THE CASE FOR EBP RISK MANAGEMENT

Many organizations (both at the corporate level and on EBP committees) fail to establish goals and strategies based on a thorough understanding of performance, risk, and associated compliance issues tailored to the uniqueness of their environment. Many also fail to implement their plans, keep track of results, and make required adjustments.

Many find it challenging to comply with regulatory and other requirements, or even stay on top of the requirements that apply to them internally. Even those that do a somewhat adequate job often fail to demand or confirm the same for third parties they employ. In short, the status quo for many organizations is neither sustainable nor acceptable.

Forward-thinking enterprise leaders have adopted a vision of EBP risk management, enabling them to reliably achieve goals while addressing uncertainty and behaving with integrity to meet this expanding web of problems. That enables performance while considering threats and opportunities, upholding voluntary commitments in declarations of mission, vision, and values, contracts, employee agreements, and legally required conduct.

CONCLUSION

A growing number of employers are experiencing the consequences of the dangers associated with sponsoring EBPs. Profound economic and reputational damage to those organizations and the careers

of their fiduciary committee members signal the need for a dramatic change in attention to risk management. Managing EBPs on an outdated or intuition-based approach is not a strategy but foolishness. Implementing an integrated governance, risk management, and compliance framework can reduce inherent risks in operations, investment decision-making, third-party service providers, and internal support services significantly and should be a priority consideration by C-suite leaders.