To restrain the growth in human resources management costs amid regulatory pressure to improve employee benefit plan oversight, employers need a fresh approach for matching profitability goals and compliance behaviors.

SEISMIC FORCES UNSETTLE EMPLOYERS

In order to halt the breakdown of aging risk containment methods, enterprises in all sectors must wed a robust risk strategy to structural changes that are being driven by regulatory enforcement and litigation. This is not easy, especially in organizations where a business-as-usual approach is firmly entrenched in the human resources compliance culture.

An intervention is the process by which an internal controls specialist can show an employer that is worried about its regulatory readiness the negative impact of the risks for not getting it right and how to alleviate the risks.

Traditional risk management programs for employee benefit plans (especially retirement plans) rely heavily on operating levers with vendors for compliance assurance. That strategy simply wasn’t designed for the challenges facing enterprises today. Properly supporting a best-in-class risk culture requires something new; a change in strategy and structure. An enterprise will find it difficult to operate safely in today’s rough and tumble regulatory era without revamping its employee benefit plan oversight system.

The purpose of an intervention is to help employers, particularly their human resources managers that are struggling under the weight of multiple regulatory duties, enter an improvement program. Such an intervention is conducted by a qualified risk management professional.

There was a time when employers commonly took some refuge in the belief that regulatory agencies were too busy to audit every employee benefit plan program. For those who did, and for those who still feel that way, they tend to relegate their compliance efforts to a

Uncovering Risk Exposure

Naturally, it’s not possible to avoid all of the risks and potential adverse outcomes related to the duties that enterprises are exposed to when they sponsor employee benefit plans qualified under ERISA. A control framework focused on fiduciary standards of care, however, isolates ERISA related risks from other regulatory programs. A properly constructed framework not only places a bulls-eye on the cryptic compliance issues inherent in federal and state laws, but it helps sustain and improve benefit plan results.

Determining the extent to which an organization’s existing regulatory compliance approach aligns with the enterprise’s risk culture requires an examination of several key issues and they include the following:
If uncertainties exist in your organization for any of the risk exposures shown in the illustration above, it’s an indication that an intervention is needed.

**Elements of a Controls Framework**

Just as certain human resources activities that fall under the jurisdiction of the Health Insurance Portability and Accountability Act ("HIPAA") and workplace safety rules that are enforced by the Occupational Safety and Health Administration ("OSHA") demand specialized governance attention, employee benefit plans regulated under ERISA face unique risk management objectives, too. Due in large part to aggressive enforcement, organizations tend to maintain well-designed compliance frameworks for HIPAA and OSHA. On the other hand, the presence of internal controls frameworks for ERISA purposes is largely missing among employers.

A controls framework helps unit executives, managers, and human resources personnel function safely in the fiduciary arena without being overly prescriptive. It delineates when an activity imposes a legal duty on an individual and when internal control is being applied.

While the structure of an enterprise’s governance, risk management, and compliance ("GRC") framework is important, risk culture is that set of attitudes, comprehension of risks, and values that bridges structure to actionable results.

Many employers are suffering economic and reputational damage in the current hyper-litigation environment. While adequate compliance frameworks are in place for some of their activities, it is apparent that employee benefit operations do not enjoy the same status. Common symptoms found in risk cultures that are exposed to damage include:

- governance flaws;
- an undefined approach to risk;
- confusing accountabilities for compliance;
- excessive reliance on vendors’ risk mitigation claims;
- a lack of internal controls that capture compliance incidents in order to facilitate correction in the GRC system; and
- training of operations personnel in the risk culture’s objectives.

Internal controls are essential in order to confirm compli-
An adequate controls framework represents all of the policies and procedures management uses to achieve the goals inherent in the risk culture. To be most efficient, the greatest employee benefit risks, such as fees paid to parties in interest (that includes a plan’s vendors), should receive the greatest amount of effort and level of control.

Internal controls fall into one of two categories; controls that are designed to prevent errors and controls that are designed to detect errors. An effective employee benefit plan risk management system must have both. The one type (preventative) is proactive while the other type (detective) validates compliance quality.

Specialized internal controls for ERISA qualified plans were developed by the Investment Fiduciary Leadership Council. Participants in the work consisted of a constituency made up of legal experts, C-level human resources executives, with guidance on the fiduciary responsibility of ERISA plan sponsors published by the U.S. Department of Labor. Plan sponsors may obtain from Roland|Criss a free copy of the internal controls handbook titled Retirement Plan Administrator: Scope and Con-duct that was published by the task force.

Risk Assessment: The Key to Assurance

A risk assessment is a process to identify potential hazards and analyze what could happen if a hazard occurs. Simply put, a risk can’t be neutralized if its presence isn’t known. The relevancy of a risk assessment is heavily dependent on the makeup of the internal controls catalog. An understanding of how internal controls are functioning frees employee benefit plan managers to align their workflows in a way that fosters efficiency and shrinks confusion. Risk assessment and the control environment involve the entire system and evaluate the overall goals of the organization and how goals are accomplished.

The range of ERISA regulatory and litigation risks facing an enterprise is multifaceted. A vigorous assessment should, therefore, be integrated in an often-repeated cycle that uses a formal framework and a predefined methodology. The framework delineates the spheres of risk facing the enterprise, while the methodology uses quantitative and qualitative tactics to measure those risks. A risk assessment should adhere to a five-step discipline, which includes:

Step 1
Develop a thorough awareness of the potential threat posed by the enterprise’s violation of its fiduciary responsibilities and how its fiduciary duty translates into actionable controls.

Step 2
Identify the enterprise’s vulnerabilities. This activity will involve the use of a proven framework against which the enterprise’s exposure can be confirmed. Rank any gaps that appear between the framework and the methods used historically to manage the benefit plan complex.

Step 3
Evaluate the rankings from Step 2 and decide on what precautions are needed that do not exist currently. Because ERISA is a highly regulated program automation of fiduciary controls should be considered in this step by enterprises that:

- possess a high level of operational complexity in their human resources function;
- employ a community of workers diversified across several job types; and
- want to reduce the
Step 4
Publish the results of the work thus far in a risk assessment report. Commission the activities needed to align management practices and technology tools with a rehabilitated internal controls framework. Implement the improvements.

Step 5
Review annually the risk assessment and update it if necessary. Pay close attention to upgrades in industry best practices as well as any changes in regulators’ enforcement focus.

Technology Simplifies Intervention

An intervention is the process by which an internal controls specialist can show an employer that is worried about its regulatory readiness the negative impact of the risks for not getting it right and how to alleviate the risks.

Strong internal controls are essential components of an intervention. In order to prove controls are active, chief financial officers and compliance managers are turning to technology to streamline and automate their fiduciary practices. Paper based manual processes and electronic spreadsheets have proved to be inadequate.

While spreadsheets are a widely-accepted go-to for compliance and risk management activities, they pose a number of limitations. Spreadsheets inhibit ease of collaboration among multi-stakeholders, require continuous manual updating, are prone to errors and omissions, and adapt poorly to regulatory changes. Simply, spreadsheets as a compliance tool are cumbersome, labor intensive, costly to maintain, and foster errors.

Notwithstanding the limitations of spreadsheets and other manual procedures, current regulatory trends and a growing number of class action lawsuits place a premium on having the best GRC fiduciary risk management system.

GRC systems are in widespread use throughout the U.S. economy tackling many tough regulatory programs such as the Sarbanes-Oxley Act and HIPAA. Until recently, however, they have not been available for the fiduciary community. Automation of an internal controls framework can dramatically improve efficiencies and remove the guess work about ERISA’s vague fiduciary principles.

The need for regulatory solutions is acute. The Employee Benefits Security Administration (“EBSA”) is the agency responsible for investigating and enforcing the fiduciary duties under ERISA. In 2017 alone, the EBSA recovered $1.1 billion, including $682.3 million in enforcement actions.

The EBSA is not the only source of risk exposure for enterprises that sponsor ERISA plans. The courts are another source of “regulation” in the form of lawsuits filed by activist employees against their employers. The costs of defending such lawsuits, not counting settlements and judgments, also argue for an advanced system of internal controls.

Admittedly, it’s a challenge for executives to manage a manual procedures approach to risk management. That’s why savvy enterprises are turning to a GRC technology tool that centralizes data, automates their workflows, and improves reporting and metrics.

Making the move to a GRC technology tool produces many tangible benefits that reduce costs, formalize compliance steps, reinforces the principle
of excellence, and eliminates many routine manual tasks:

- lower costs through greater efficiencies;
- standardized processes that match regulatory mandates;
- reinforces a culture of excellence; and
- computerized workflows transform manual risk management tasks.

CONCLUSION

Constant change in the employee benefit regulatory environment exposes most organizations to compliance risk. Especially vulnerable is the organization whose risk culture is in the grip of anti-fiduciary behaviors. The penalties for not altering such behaviors make an intervention an essential activity. Implementing an internal controls framework, engaging a risk assessment, and making use of readily available GRC technology are the key elements in a comprehensive risk intervention. The benefits of an intervention include:

- reduced likelihood of a major noncompliance event;
- protection from an ethics failure;
- elevated status in the eyes of regulatory agencies and CPA plan auditors;
- increased competitiveness in the marketplace; and
- better outcomes for employees.

Roland|Criss conducts risk assessments and offers a GRC system demonstration. A demonstration can be scheduled by calling 800-440-3457 or inquiring via email at admin@rolandcriss.com.