Risk Insights

Risk, Response and Reduction: Process

Attention to Process-Level Vulnerabilities Reflects Strategic Emphasis

ADDRESSING RISKS at the process level represents a continuation of the emphasis organizations place on recognizing and reducing vulnerabilities, an emphasis first directed toward threats accompanying business strategies.

Every organization has business strategies, strategies that provide a sense of purpose and direction. Those strategies may focus on attaining market leadership, developing an international presence or pursuing other aims deemed crucial to long-term organizational success. Effectively executing those strategies requires identifying and mitigating the risks that accompany those aims.

That strategic emphasis on recognizing and reducing risks extends to addressing external and internal entity-level vulnerabilities, such as revised compliance requirements, new product launch uncertainties or general economic downturns that emerge while the organization is pursuing its business strategies.

Identifying and mitigating risks that arise at the process level complements and supports efforts to address potential threats at the strategic and entity levels. That attention to process-level risks encompasses all organizational activities, including compliance, financial and operational functions.

With such an emphasis on addressing risks, the organization is better equipped to respond to potential adverse events and to capitalize on the opportunities for improvement that are also uncovered when potential risks are identified.

Entity-Level Risks Direct Focus to Supporting Processes

AN ORGANIZATION'S SENIOR MANAGEMENT, board of directors, audit committee and internal audit department are responsible for identifying crucial entity-level risks. Assessing those vulnerabilities leads to evaluations of supporting processes.

The attention various processes then receive may be based on risk ratings assigned. Such ratings consider a variety of factors, including inherent risk, existing controls, consistency of processes and the effectiveness of processes. Strategic and entity-level controls are designed to reduce inherent risk. Based on the strength and precision of these controls and their direct impact on a given business process, the remaining residual risk must be covered by process-level controls.

weaver
Assurance • Tax • Advisory

Risk, Response and Reduction: Process

Inherent risk is the unavoidable level of vulnerability present in a particular process. Cash received by a clerk for the sale of goods has obvious inherent risk of theft. Therefore, controls designed to control this risk are put in place, including the register process to ring up the sale, the locked cash drawer and the clerk's shift cash reconciliation. Inherent risks are present in every business process; some are more obvious than others. Spreadsheet programs, for example, give individuals considerable latitude to develop and update spreadsheets based on their own formulas, macros, links and other user-defined settings. That means spreadsheet data accuracy and integrity often hinges on individual proficiency, computing preferences and other personal characteristics. Due to that degree of inherent risk, spreadsheet-driven processes that support critical entity-level functions merit ongoing scrutiny.

> "The **effectiveness** of a process also determines how much attention it requires when **evaluating risk.**"

The effectiveness of an existing control also influences how much attention a process merits when evaluating risk. To deter fraud and guard against unauthorized disbursements, an organization may require two signatures on every check it issues. The effectiveness of that control, however, is compromised if someone routinely signs blank checks before departing on vacations or business trips to make the disbursement process easier for another authorized signer.

Consistency in processes is a factor in determining risk as well. Among a distributor's various facilities, cycle count inventory processes may vary. Such inconsistent practices raise questions regarding the accuracy of inventory data consolidated from those locations. Inventory processes at each facility must then be evaluated separately to assess their risk levels.

The effectiveness of a process also determines how much attention it requires when evaluating risk. An automobile insurance company may see an increase in accident claims payments, an increase above prior year or industry average. Such a rise should prompt the company to examine the processes it uses for claim acknowledgement, reviewing the validity of submitted claims and fault payments as well as other underwriting policies for existing customers.

Understanding the underlying causes of vulnerabilities allows organizations to then focus on mitigating the threats presented by those risks.

Reducing Process-Level Risks

A VARIETY OF STEPS can be taken to mitigate process-level risks deemed unacceptable or above the tolerable threshold, including improving processes, standardizing processes throughout the organization, segregating conflicting duties, eliminating IT incompatibilities, automating manual controls and implementing best practices.

Process improvement efforts focus on identifying risk potential, while also enhancing efficiency. In an organization that manually processes invoices, numerous individuals touch those documents and record related data before checks are cut. Each step presents opportunities for mistakes or delays to occur. With an electronic invoicing system, presentments for payment are automatically routed to appropriate individuals and related IT applications. That eliminates numerous process steps, saves time and reduces the risk of data entry errors or of an invoice being mislaid. Attaining such efficiency and enhanced accuracy also dramatically lowers the transactional costs associated with making such payments.

Improving processes reduces risk and improves productivity and efficiency. So does standardizing processes throughout an organization. Various subsidiaries of one corporation, for example, may have their own accounts receivable processes, with each subsidiary setting its own interest rates and collection policies. Standardizing those accounts receivable processes makes it easier to monitor that activity and evaluate company-wide performance. Such standardization also makes it much easier to train and transfer individuals for work within the various subsidiaries.

When an individual holds conflicting or incompatible duties, mistakes or improper activity can go undetected or unreported. One person, for example, should not be responsible for both ordering supplies and verifying that supply shipments arrive as ordered. Another individual should not be responsible for both assigning and approving overtime for payroll purposes. Segregating such duties creates a system of checks and balances that mitigates risks.

Companies continually upgrade various IT elements, creating potential incompatibilities among existing systems. Mergers or acquisitions often result in various divisions or business units relying upon differing technology, too. Too often, completing processes amidst such IT disparities requires using custom interfaces or manual intervention to transfer data from one system to another. That results in inefficiency and increased risk of errors. Whenever possible, IT incompatibilities should be eliminated.

Automating manual controls provides another means of lowering risk and increasing efficiency and effectiveness. To meet compliance requirements, a health care provider must restrict IT access to patients' private information. Application controls based on username and password provide initial access restriction, while automatic log-off controls ensure that such information will not remain visible for long if individuals forget to close files before leaving their workstations.

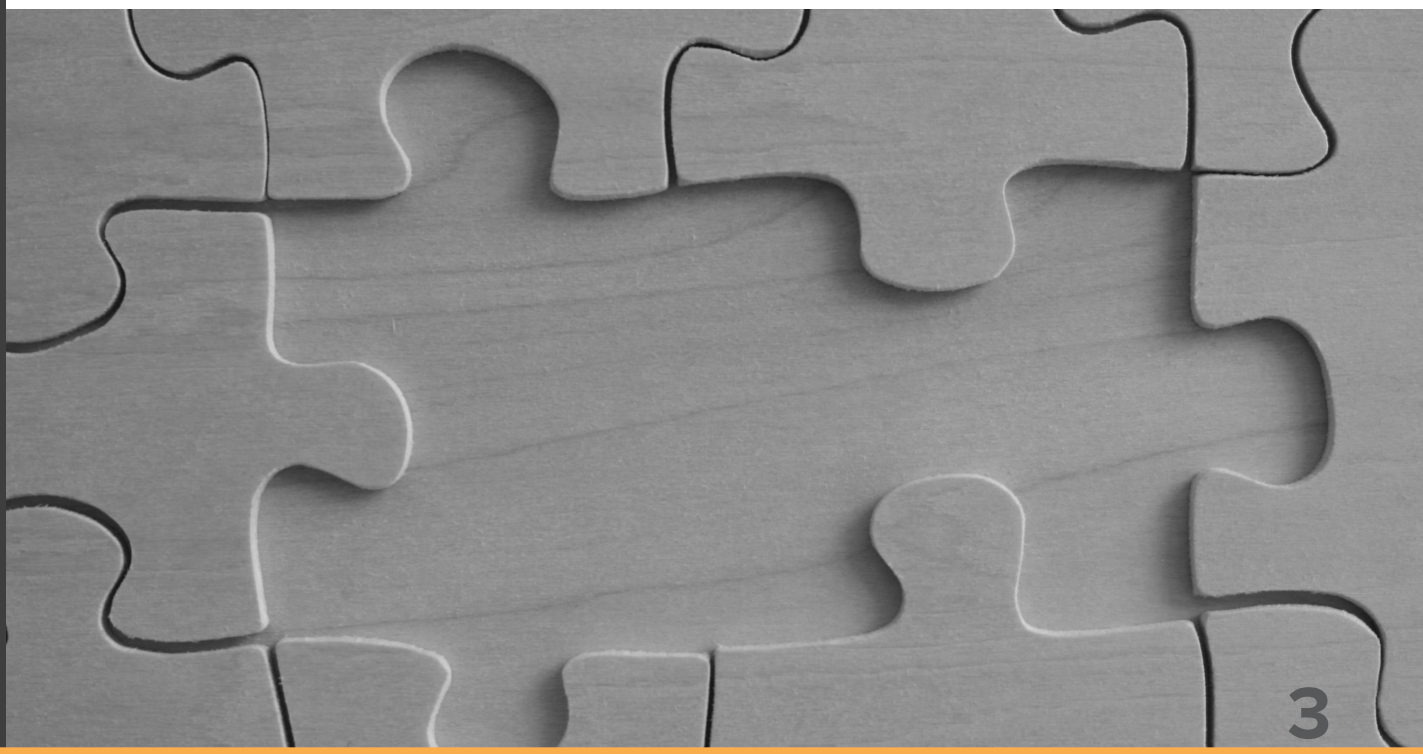
Utility companies often require that a repair person place orange safety cones around a company van at any work location, including sites in low-traffic residential areas. Before leaving the worksite, the driver has to walk around the van to pick up the cones. He will then see any child sitting close to the vehicle, a child that might not have been visible from the van's mirrors. Such a process represents a best practice for preventing worksite accidents involving company vehicles.

Addressing Process-Level Risks Requires Scalable, Sustainable Efforts

ORGANIZATIONS OPERATE IN dynamic environments and must continually respond to various internal and external events, including organic growth, mergers, acquisitions, competitive pressures and marketplace shifts. Efforts to address and mitigate risks at the process level must be scalable and sustainable, so that attention remains focused on recognizing and reducing vulnerabilities amidst such change.

Assigning ownership to each process assures that someone is accountable for overseeing that activity and addressing related risks. That accountability includes identifying any gaps that may exist between processes. Such ownership promotes continual monitoring of process-related vulnerabilities.

Incorporating risk-related responsibilities into job descriptions further informs individuals that identifying and mitigating vulnerabilities requires continual attention. Individuals should be informed, too, that the diligence they display in monitoring risks will influence performance reviews and compensation decisions. Such an emphasis further promotes continuity and accountability throughout the organization for addressing threats at the process level.



Risk, Response and Reduction: Process

Embedding controls into processes provides further continual risk protection. Requiring frequent, regular reconciliations for various transactional processes limits the amount of time a mistake can go uncorrected or that fraud-related activity can go unnoticed. Automated functions and event-driven application settings for those and other activities provide additional means for embedding control measures into various processes.

> "**Embedding controls** into processes provides further continual **risk protection.**"

Through such tactics, an organization maintains a constant emphasis on addressing process-level risks, regardless of any other internal or external changes it faces.

Long-Term Benefits of Addressing Process-Level Risks

SUSTAINED ORGANIZATIONAL SUCCESS requires recognizing and mitigating the risks that accompany a company's business strategies. That emphasis is supported by efforts to address risks at the entity level, enabling the organization to respond to the changes and accompanying threats it faces while pursuing its business strategies. Attention paid to vulnerabilities within supporting processes complements those efforts.

A range of benefits accompany addressing process-level risks. Identifying and mitigating those vulnerabilities prompts organizations to automate, improve and standardize processes whenever possible, resulting in greater efficiency and productivity. Incorporating scalability and sustainability into risk response and reduction efforts assures that those activities receive continual attention, regardless of changes affecting internal processes.

Establishing ownership and accountability for addressing process-level risks throughout the organization nurtures a corporate culture that values the importance of identifying and mitigating threats. Over time, such a culture becomes not just a control in itself, but a competitive advantage.

CONTACT US

Alyssa G. Martin, CPA, MBA
Partner-in-Charge
Risk Advisory Services
alyssa.martin@weaver.com

Weaver's risk advisory services are strategic, executable and measurable–and our nimble process is designed to help companies remain optimally functional as they identify and manage risk. We work closely with our clients to customize services that fit their existing staff structure and operations. Integral to this sensitive work, we believe our communication skills are as valuable as our technical knowledge and professional insight. You will experience thoughtful, purposeful communication throughout the process. Specific services we provide include:

- Business continuity planning
- Business process improvement
- Contract monitoring and compliance
- Enterprise risk management
- Internal audit
- Internal control evaluation
- Integrated financial and IT audit
- Performance audit and measurement
- Regulatory compliance
- Risk assessment
- Sarbanes-Oxley compliance

Disclaimer: This content is general in nature and is not intended to serve as accounting, legal or other professional services advice. Weaver assumes no responsibility for the reader's reliance on this information. Before implementing any of the ideas contained in this publication, readers should consult with a professional advisor to determine whether the ideas apply to their unique circumstances.

© Copyright 2014, Weaver and Tidwell, L.L.P.

weaver
Assurance • Tax • Advisory