Risk Insights

Process Level
Risk Assessment

Dealing with risks at every level

A TOP-DOWN APPROACH TOWARD RISK ASSESSMENT focuses attention on the most significant vulnerabilities and threats facing an organization. That assessment illuminates vulnerable supporting activities. Examining those activities or processes enables management and the internal audit staff to determine whether or not existing controls sufficiently mitigate identified risks.

A manufacturer, for example, may risk not being able to produce enough parts to fill major customer orders on time. The likelihood of that event occurring and its impact on the organization may make it an unacceptable risk. That leads to assessments of supporting activities or processes, such as material requirements planning, purchasing, production scheduling, inventory control, manufacturing loss/waste management, manufacturing equipment maintenance and quality control inspection. Those assessments may be based on interviews, knowledge of those processes or activities and personal observations.

Management may take a variety of steps to mitigate unacceptable risks identified during assessments. Effective measures can include hiring additional personnel, segregating conflicting duties, automating manual processes or requiring more frequent communication among supervisors or departments.

Recognizing Potential Process Level Risk Factors

THE TYPE AND COMPOSITION OF PROCESSES VARY not only among entities, but also among an organization's facilities and locations, business units and departments. There are factors, though, that may indicate that a process presents an unacceptable level of risk and merits further evaluation. Those factors include a history of errors, volume, machinery downtime, complexity, frequency of change, required skills, number of interfaces and degree of automated controls incorporated into a process. Rapid growth in the volume of transactions or the financial impact of a process may also indicate a greater likelihood of risk.

More than one factor may characterize a process, too. A history of errors may accompany call center processes for accepting and entering customer orders. The volume of transactions handled by that call center may have also increased, without a corresponding increase in staffing or automation. A wider range of products may have been introduced, making call center staff responsibilities more complex.

For example, a company's product number format may be a two-letter combination, followed by a four-digit number. When entering a product number, however, call center staff members may be transposing the second letter and the first numerical digit. Absent a data validation control, the application will not automatically reject entries lacking that correct sequence of letters and numbers.

Process Level Risk Assessment

Some processes have a higher level of inherent risk than others, particularly in processes related to a company's financial reporting and custody of assets. For example, processes that govern accounting for cash and negotiable securities would be considered to have higher inherent risk than processes for prepaid expenses or non-liquid investments. Likewise, different processes pose varying degrees of fraud risk. Weak controls in processes for easily convertible assets would be assessed more severely than in processes for assets or activities not susceptible to fraud.

Being aware of such factors and recognizing their significance helps management and staff determine which processes may pose unacceptable risks.

Internal Control and Compliance Efforts

INTERNAL CONTROLS AND COMPLIANCE EFFORTS are established in an organization to mitigate the risks that are unacceptable and outside of the entity's risk profile. Environmental or workplace safety compliance processes may present vulnerabilities and exposure to liabilities. Ineffective processes for granting or restricting access to warehouses, stock rooms or crucial IT functions may also leave entity assets vulnerable to fraud. Mitigating such risks provides management a solid foundation to make decisions that affect company growth and profitability.

Risk mitigation controls will include both manual and automated tasks performed throughout the process cycle. More often than not, these steps rely on system information and reports to assist management in effectively executing controls and evaluating business performance. The reports that are used to monitor key operational and performance metrics are often used to help determine strategic initiatives and can reveal complex, operational risks. These reports do not only include the crucial financial reports, but expand beyond financial reporting to include internal management and compliance reporting to provide relevant information for company management.

In today's evolving environment, many internal controls, processes and reports are heavily dependent upon technology and the safeguards provided by application and general IT controls. Processes lacking those automated controls present activities that create greater risk. Those activities include generating ad hoc reports, manual monitoring activities or manual calculations as part of reporting.

Incompatibilities between legacy technology and newer platforms increase risk because extracting or consolidating data from one system to another may require manual intervention. Processes driven by spreadsheet data likewise merit examination because of the impact that user-defined spreadsheet application functions can have on data integrity.

Factors with Impact

EXAMINING CRUCIAL PROCESS LEVEL RISKS and related controls throughout an entity is an important part of monitoring processes that have a significant impact on business operations. A top-down evaluation approach focuses on the most important and highest risk areas of an organization's key processes. Through that risk assessment, it is imperative that companies evaluate the risks that impact their business the most. Evaluating the inherent probability, impact, velocity and persistence of risks as they have an effect on each significant process provides management a clear picture of which risks have the most influence over their day-to-day operations and their company as a whole.

Risk assessments should expand risk evaluation beyond financial and fraud risk categories to include additional internal risks that are more than just the risks of failing to have the necessary cash flows, liquidity, financial results or budgets, and the concealment of illegal acts. Additional internal risks that should be considered in a risk assessment include governance, IT, operational, complexity and other risks. Including these risk categories will allow company management to have insight into the influence that the company's board and strategic leadership, IT infrastructure and systems, and the sophistication of operations have on the organization.

Internal risks are not the only risks that should be in risk assessment. In the expanding global scope of today's economy, businesses are more keenly aware of all the stakeholders who affect and are affected by their organization. Vendor and customer relationships, entity structure, constantly evolving regulatory requirements, public opinion and real-time media coverage play key roles in many of the business decisions made today. Incorporating economic, regulatory and compliance, and reputational risks into a risk assessment provides a well-rounded evaluation of all the risks associated with the stakeholders in today's corporate environment.

Risk Evaluation Objectives

THE OVERALL GOAL OF A RISK ASSESSMENT is to identify and assess risks that could prevent an organization from achieving its intended targets. As part of the overall objective, other objectives should be considered to help mitigate the risks that threaten organizational goals. Identifying or establishing internal controls, appropriate segregation of duties, data protection and security are fundamental components of effectively mitigating process level risks that are inherent in every company. These components are traditionally financial in nature, but there are also operational objectives that are critical to the success of every company.

Developing automated processes and establishing processes that are efficient and scalable for company growth are also important factors in mitigating risks that affect organizational goals and objectives. Evaluating operational performance objectives in combination with financial objectives, as they relate to managing risks, provides senior leadership opportunities to develop internal controls and monitoring functions to mitigate the risks inherent to their organization.

Based on the fundamentals in each risk category and the objectives of the risk assessment, the natural risk at the process level can begin to be evaluated. It all starts with the question, "What can go wrong?"

Questions to Address When Examining Process Level Risks

WHILE EACH ORGANIZATION faces specific vulnerabilities, asking the following questions addresses the "What can go wrong?" concern associated with each process:

Financial and Fraud Risk

- What risks are inherent?
- How can those be minimized?
- What controls might be missing?
- Do controls require appropriate follow-up?
- Are duties properly segregated?
- What consideration has been given to fraud prevention/ detection or asset protection with current controls?

Governance Risk

- Does executive management and the board provide adequate oversight?
- Is there a clear strategic direction?
- Do employees recognize appropriate "tone at the top"?

IT Risk

- Is the organization heavily dependent on IT to execute strategic operations?
- Are IT systems stable and up-to-date?
- Are IT systems internally developed?

Operational and Complexity Risk

- What controls exist around the process, and are they functioning as intended?
- What breakdowns of those controls have occurred in the past?
- How have breakdowns been resolved?
- What impact did the breakdown have on the organization?
- Are transactions high volume, complicated or both?

Economic Risk

- Are there concentrations in business relationships?
- How susceptible is the industry to market fluctuations?

Regulatory and Compliance

- How stable is the regulatory environment?
- Is the industry highly regulated?
- How much influence does the company have over the regulatory environment?

Automation, Efficiency, Scalability

- Are processes heavily automated?
- Are process steps consistent? If not, what are the differences?
- What are the best practices surrounding each process?
- What are the efficiencies and control enhancements that could be derived?
- Are processes scalable for anticipated future growth?

Process Level Risk Assessment

While each question addresses a specific concern, the answers provide an integrated assessment of the risks associated with each process. For example, proper segregation of duties is an essential control for preventing and detecting fraud. To safeguard company assets, an individual responsible for procuring supplies should not oversee physical inventories to verify the existence of those items. Segregating other conflicting duties likewise deters fraud.

Examining the best practices surrounding a process provides answers for preventing control breakdowns. In one manufacturing facility, a manager may surround existing controls by posting additional workplace safety information on bulletin boards and by holding regular meetings with employees to discuss ways to further reduce the likelihood of workplace accidents occurring. As a result, that facility enjoys an exemplary record in adhering to safety controls and reduced downtime due to incidents. Incorporating those best practices at each manufacturing facility could prevent control breakdowns.

Evaluating the consistency of process steps provides further insight regarding efficiencies and control enhancements that can be derived. Processes for granting and tracking overtime expenses, for instance, may vary from one entity facility to another, leading to wide variances in labor costs at those different sites. Examining that lack of consistency leads to controls for adhering to uniform processes throughout the organization.

Responsibility for Process Level Risk Assessment

MANAGEMENT AND THE INTERNAL AUDIT STAFF are responsible for assessing process level risks and implementing effective controls. That responsibility includes creating a "tone at the top" that emphasizes the value of ethical behavior, preventing and detecting fraud, and continually monitoring risk assessment efforts. Management and the internal audit staff are also responsible for disclosing areas of risk and steps taken to mitigate those risks to the audit committee and the external auditor.

By embracing such practices, management and the internal audit staff function as watchdogs over the controls implemented throughout the entity. The external auditor and the audit committee can then focus on examining process level risks most crucial to entity level risks.

Residual Benefits of Process Level Risk Assessment

PROCESS LEVEL RISK ASSESSMENT ENABLES management and internal auditors to identify instances where fraud, misstatements and other significant adverse activities can occur and to devise controls to mitigate those risks. That assessment promotes process improvement throughout the entity, leading to enhanced productivity and quality. Control functions and continual monitoring foster a culture of accountability. Improved process documentation provides clearer audit trails, making it easier for auditors to attest to the accuracy of the entity's financial reports. Overall, the entity becomes more efficient, more capable of responding to uncertainties and more transparent to all stakeholders.

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

weaver
Assurance • Tax • Advisory