# Risk Insights

## Risk Assessments Pay Forward

## Risk response and reduction encompasses strategic goals, entity vulnerabilities and process level exposures

**RESPONDING TO RISKS** and lowering vulnerabilities enables an organization to sustain itself and thrive amidst the continual internal and external changes it faces. That function accompanies the organization's business strategy and provides a strategic advantage itself.

Strategic exposures—exposures that accompany an organization's strategic objectives or initiatives—are the most crucial risks to consider and cover. Those risks have long-term effects and pervasive impacts across an organization. Left unaddressed, those risks could prevent an organization from attaining its objectives and initiatives.

Significant entity-wide concerns support those objectives and initiatives. Various process-level activities likewise support those significant entity-wide concerns. There is risk across all business operations, risk that must be managed to ensure success. By taking a top-down approach in addressing risks, the organization assures that crucial strategic exposures receive the greatest degree of ongoing attention. Addressing those strategic exposures provides direction for identifying crucial entity-level and process-level vulnerabilities.

While following that top-down direction, addressing risks at all levels is a continual cycle. That cycle begins with identifying risks. Those risks are then assessed to determine their potential impact and likelihood of occurrence.

Every organization has a risk appetite or level of tolerance that defines the amount of exposure the organization is willing to accept. That tolerance or appetite will vary from one organization to another.

Assessed risks are compared to that risk appetite or tolerance. An organization then chooses the most appropriate response. If an assessed risk's potential impact or likelihood of occurrence is deemed low, the organization may respond by accepting that risk. If the degree of risk is deemed unacceptable, the organization can choose various means to reduce that risk.

That entire cycle—identifying risks, assessing risks, responding to risks and mitigating risks when necessary—is then repeated. With continual efforts that encompass strategic aims, significant entity concerns and crucial everyday activities, the organization protects itself from the adverse impact of uncertainty.

weaver
Assurance • Tax • Advisory

## Strategic-Level Attention Provides Foundation for Confronting Risks

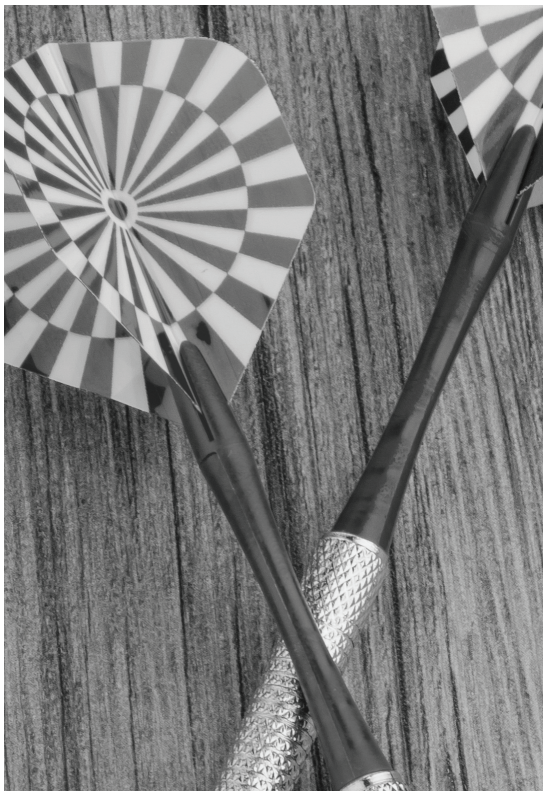
**A COMPANY DECIDES** to outsource significant portions of its production to overseas contract manufacturers. Such outsourcing promotes greater efficiency and the potential to focus resources and domestic operations on value-added activities.

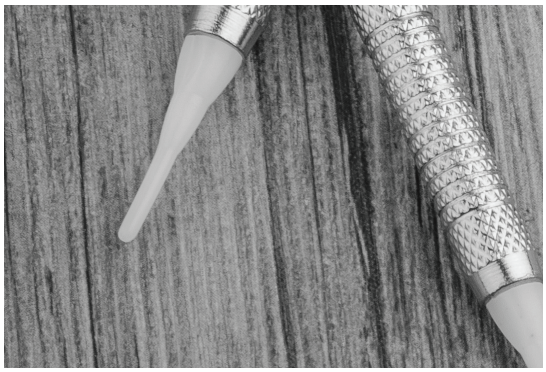
While offering those prospective benefits, that outsourcing strategy also exposes the company to an array of vulnerabilities that it must address to stay within its risk appetite.

Potential political instability abroad is an issue the company faces. Through various online news services, the company can monitor that concern. Uncertainties regarding the internal operations of foreign contract manufacturers present considerable risk. In response, the company can require appropriate ISO certification from its contract manufacturers. Such certification presents a measure of international assurance regarding the consistency and quality of a manufacturer's operations.

While responding to those and other concerns, the company can also take steps to mitigate vulnerabilities that still present unacceptable levels of risk. In addition to requiring ISO certification, the company can have an employee on-site at each overseas location to immediately address any difficulties that may arise. The company can also reduce the volume of work it initially planned to outsource as a way to mitigate the risks that accompany any substantial operational change. Through such efforts, the company assures that the remaining level of uncertainty—the residual risk—does not exceed its risk threshold.

> "Every organization has such a **risk threshold** or appetite that defines how much exposure it is willing to accept as being part of its **strategic objectives and initiatives.**"



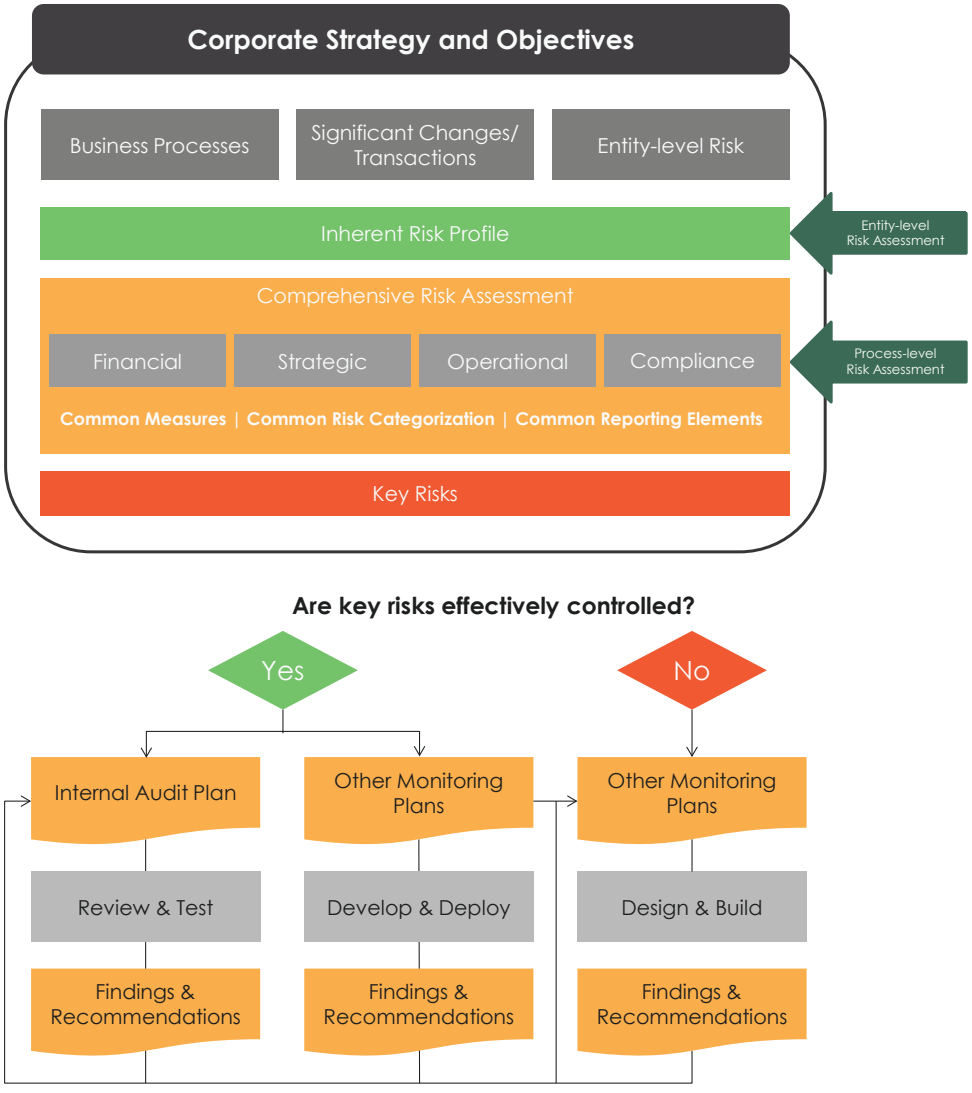


Every organization has such a risk threshold or appetite that defines how much exposure it is willing to accept as being part of its strategic objectives and initiatives. Some organizations, such as those that invest heavily in research and development, or those operating within industries subject to considerable market volatility, need to have a higher risk appetite or threshold than many other businesses. A company with long-established product lines in a mature industry would likely have a less substantial risk appetite, a lower threshold for accepting risks.

Defining that risk appetite enables an organization's leadership to determine the significance of identified and assessed exposures. An organization can then choose the most appropriate response. If an assessed risk is within the organization's risk appetite, the organization can respond by accepting that degree of exposure. If an assessed risk exceeds that risk appetite, the organization can respond by mitigating those risks.

*Being aware of the organization's risk appetite provides a benchmark for addressing strategic risks, which present the most significant degrees of exposure.* Addressing those exposures as the first priority assures that the organization takes a top-down approach toward evaluating and responding to the risks it faces. Through such assessment and responses, the organization can reduce risks when necessary to ensure that they remain at an acceptable level. Addressing the strategic risks first also helps identify the most crucial entity and process-level risks facing the organization.

Exhibit **1**



## Strategic Emphasis Directs All Risk Evaluations

**RECOGNIZING THE IMPORTANCE** of addressing and mitigating risks at the strategic level provides a foundation for continually addressing vulnerabilities as they emerge. Exhibit 1 illustrates risk assessment methodology.

Those risks may come from new or revised compliance requirements, an increasingly integrated global economy, technological advances, marketplace changes, and other internal or external vulnerabilities that arise as a company executes its business strategies.

Continually integrating risk recognition with business strategies allows an organization to focus more on anticipating change, rather than just reacting to events as they unfold. Such responsiveness enables an organization to reduce the likelihood or potential impact of adverse events.

Continually evaluating potential vulnerabilities also uncovers opportunities that would have otherwise gone unnoticed. The need to identify and mitigate risks associated with Sarbanes-Oxley compliance, for example, spurred many publicly-traded corporations to examine and resolve long-standing disparities in transactional processes and IT systems, thereby enhancing organizational efficiency.

Responding to risks at the strategic level protects the organization, and related efforts to reduce vulnerabilities assure that identified risks do not exceed the organization's risk appetite. That strategic emphasis provides a foundation and direction for addressing and mitigating risks at the entity and process levels.

## Leadership Commitment Builds Strategic Value

**CONTINUALLY ADDRESSING RISKS** to reduce vulnerabilities requires involvement from the audit committee, board of directors and senior managers, including the chief executive officer, chief risk officer and chief financial officer.

Senior managers must continually emphasize the importance of ethical behavior, the need to protect the company's assets, and the value of recognizing, addressing and reducing risks as they emerge. Effective governance also entails defining and documenting steps the organization will take in response to adverse events.

A disaster recovery plan, for example, details how an organization will respond in the event of a tornado, flood, hurricane or other catastrophe. Rather than relying upon ad hoc decisions made under duress, proactive planning drives a company's response to such events. That preparation enables the organization to not only address the immediate impact of a disaster more efficiently and effectively, but to also minimize the cost of ensuing business disruption.

Such leadership commitment provides institutional support for applying similar diligence throughout the organization, thereby promoting attention to risks at all levels.

> "Incorporating **best practices** represents an **effective means** of continually addressing and mitigating risks."

## Addressing Risks Requires Continual Attention

**TO PROVIDE LONG-TERM STRATEGIC VALUE,** an organization's focus on responding to vulnerabilities and mitigating risks must remain constant amidst whatever changes or events the organization faces.

Dashboard reporting systems provide efficient tools for monitoring key performance indicators (KPI) in real time. Those KPIs can signal a potential downward trend in sales or other potential risk, allowing managers to take steps to reduce those vulnerabilities. For financial reporting and other crucial functions, automating manual processes whenever possible promotes further efficiency and constant vigilance through preventative controls.

Incorporating best practices represents an effective means of continually addressing and mitigating risks. Organizations outsource a host of data processing functions to service providers. Requiring that a service provider supply a Service Organization Controls (SOC) Type 2 report constitutes a best practice for such outsourcing. That report assures that the vendor's efforts in identifying and mitigating its risks were deemed effective by an independent auditor.

A company must sustain its efforts to identify and mitigate vulnerabilities. Investigating tips from employees enables companies to uncover incidents of fraud or other improper behavior. Deploying a hotline that enables individuals to anonymously report suspicions of such conduct provides a sustainable means for continually addressing that risk.

To accommodate organizational changes that occur over time, efforts to limit vulnerability must be scalable. Imbedding responsibilities for addressing and reducing risks within routine processes and work responsibilities ensures that such diligence remains constant amidst evolving operational functions and organizational expansion.

Incorporating such characteristics into risk identification and mitigation efforts enables the organization to continually respond to potential vulnerabilities as they emerge.

## Top-Down Approach Directs Attention to Most Crucial Risks

**A COMPANY CANNOT ELIMINATE** all vulnerabilities; varying degrees of residual risk will always remain. By taking a top-down approach that focuses attention on the most crucial risks first, an organization assures that the residual risk remains within its risk appetite.

Oil companies face industry cycles of expansion and contraction, along with constant fluctuations in price. To respond to the risks that accompany such cyclical movements, those companies rely upon detailed actuarial analysis to project future price movements and to assess where current prices stand in relationship to upward or downward trends. They also mitigate price volatility through hedge contracts that establish fixed payment rates and through partnerships or joint operating agreements with other companies.

Organizations operating in other business sectors face their own industry-specific exposures. They face crucial risks related to their business strategies and goals, too. A regional company wishing to grow into a national entity, for example, faces risk from taking on too much debt to finance expansion or from not having strong enough internal functions in place to manage growth.

Crucial risks vary over time as well. Negative industry publicity may pose a serious concern one year, while proposals for potentially adverse legislation could require attention the following year. Identifying risks that present exposure at the entity level leads to evaluation of the internal processes related to those risks.

*With whatever scenarios an organization may be facing at any given time, taking a top-down approach in evaluating risks assures that the most crucial exposures are addressed, that unacceptable vulnerabilities are reduced and that the remaining residual risk stays within the organization's risk appetite.*

## Strategic Emphasis Delivers Lasting Value and Direction

**PLACING STRATEGIC EMPHASIS** on addressing and mitigating risks assures that identified risks do not exceed an organization's risk threshold and that the company's risk appetite remains aligned with its business strategies. That emphasis protects an organization amidst the constant changes it faces in its internal and external environments.

Recognizing and reducing strategic risks provides further direction for identifying, evaluating and mitigating exposures, thereby enabling the organization to effectively confront significant exposures throughout the organization.

## Strategic Emphasis Extends to Addressing and Reducing Entity-Level Risks

**ORGANIZATIONS VARY** in their business strategies. Being aware of those strategies and the accompanying risks provides direction for identifying and focusing on the related entity-level exposures.

A manufacturer seeks to enhance efficiency through outsourcing production to overseas contract manufacturers. A distributor focuses on becoming a one-stop supplier source for prospective customers. A utility provider strives to be the low-cost option in its regional service area.

Every business strategy carries risks. Recognizing the value of responding to risks and reducing vulnerabilities at the strategic level provides a foundation for addressing entity-level exposures as they emerge. The response at the entity level assures that the vulnerabilities an organization faces while executing its business strategies are responded to appropriately and within the entity's risk appetite.

Entity-level risks can arise from a business strategy or from sources outside the organization's controls. Entity-level risks are often created from external events, such as new competition or an increase in price for materials and supplies. Changing customer demographics may pose a risk to a company's existing market position and product offerings. New or revised compliance requirements present risks as well, as do changing international, political or economic conditions for companies doing business abroad.

Internal events may also present new entity-level risks. A host of risks can arise in launching a new product, including production difficulties or shipping delays and uncertainties regarding marketplace acceptance. Implementations of new IT systems present risks, including system incompatibilities or data security weaknesses not recognized during change management planning processes.

When a company opens a new facility or expands an existing site, construction deficiencies not identified in previous inspections may require attention. New and approved interior design configurations might not readily accommodate actual work needs. Facilities at new locations are often staffed with newly-hired employees who may lack the training and general experience necessary to resolve various dilemmas they confront.

Human resources risks arise, too, whenever there is turnover in key operational or management positions. Through years of service with a company, individuals acquire insight and institutional knowledge that cannot be easily replaced by even the most qualified successors. Errors in judgment or execution can follow such transitions.

Companies need to identify those and other entity-level exposures through annual risk assessments. Based on those risk assessment findings, an organization can then address and mitigate those risks to ensure that any identified entity-level vulnerabilities do not exceed the risk threshold accepted by management and the board when setting its business strategies.

## Addressing and Mitigating Entity-Level Risks

**EFFECTIVELY RESPONDING** to entity-level risks and reducing those vulnerabilities requires involvement from the audit committee, board of directors and senior management, including the CEO, CFO and chief audit executive or chief risk officer, as applicable. Collectively, those individuals lead the organization in evaluating identified risks, analyzing the potential impact or likelihood of those risks occurring, and determining how any identified vulnerability is adequately covered within the organization's risk appetite and risk threshold.

Today, entity-level risks related to internal control over financial reporting are commonly identified along with the control activities designed to mitigate this risk. Operational entity-level risk identification and response documentation is less formal. An organization should seek to balance the entity-level risk assessment and design control activities to respond to the risks proactively within the risk appetite of the organization. Consistent and visible high-level commitment from senior management and the board provides institutional support for addressing risks throughout the organization and nurtures a corporate culture that values recognizing and mitigating vulnerabilities whenever they emerge.

An organization will always face uncertainty, and it cannot mitigate or eliminate every potential risk it faces. It should, however, address significant entity concerns regarding the organization's board, quality, IT systems, reputation or other critical factors. While embracing such factors, the approach to addressing entity risks focuses on exposures unique to the organization and its business strategies.

All airlines, for example, face possible declines in air travel when a broad economic recession unfolds. Airlines share that crucial recession risk with businesses operating in a diverse range of industries. Fuel costs are a major operating expense for any airline, and rising fuel prices pose a significant risk for all companies in the air travel industry.

While facing such common exposure, however, each airline also faces its own critical, unique entity-level risks. One airline's labor costs and pension liabilities may present substantial entity-level risk, making it especially vulnerable to any rising costs or declines in revenue. Another airline that handles considerable volumes of international travel may face exposure from political instability in overseas regions it serves. A discount carrier whose business model is based on offering frequent short flights faces risk due to proposed legislation that would restrict the number of departures and arrivals it can schedule during peak travel hours at its most popular airports.

Each organization must identify and address the most crucial entity-level risks that it faces as they relate to its business strategies and risk appetite. Such an approach assures that the most critical risks receive attention. The organization can then decide how to respond to those risks in order to reduce vulnerabilities within its risk profile.

## Implementing a Risk Assessment Program

**ADDRESSING ENTITY-LEVEL** vulnerabilities requires involvement from senior management. It also entails deploying risk assessment methodology to identify entity-level vulnerabilities and determine their likelihood or potential impact.

*Entity-level risk assessment may be initiated by developing and distributing self-assessment questionnaires (SAQs) to management members responsible for creating policies and processes to appropriately mitigate risks.*

Those SAQs help determine the probability of risks present by defining what risks are important to the company. In the SAQs, respondents are asked to assign one of the following ratings to each statement:

- 0 = Not applicable or I don't know
- 1 = Very remote (not at all like my company)
- 2 = Unlikely (somewhat unlike my company)
- 3 = Likely (some comparison but not completely)
- 4 = Probable (somewhat like my company)
- 5 = Highly probable (good description of my company)

The SAQs need to be tailored to the organization's industry and business characteristics. Risk types are separated into major categories, such as:

- Business environment risks
- Reputation risks
- Operation risks
- Regulatory risks
- Defalcation risks
- Fraudulent financial reporting risks
- Technological risks

Each category contains risk statements that are customized and pertinent to the organization.

Members of management who are responsible for mitigating risks receive questionnaires and rate each risk statement on the 0-5 scale, with 0 equaling "not applicable" and 5 signifying "highly probable." Management can include written commentary for each question.

**Quantitative analysis.** Responses are tabulated for each respondent and summarized overall and by division. A detailed analysis of risk responses is conducted and a composite is calculated. Aberrations—or outliers—are identified for further analysis.

**Qualitative analysis.** Comments offered by management yield insight beyond what is available from the numerical grades offered for various risk concerns. Those comments offer a greater understanding of management's perspective. Outliers that were previously identified require additional attention, too. Such outliers or aberrations are investigated via interviews with respondents to determine:

- *Are the responses accurate?* Respondents may not have understood the question. In such instances, the SAQ may need to be updated to reflect the accurate answer.
- *Do the changes identify legitimate issues that need to be addressed?* In some instances, the answers uncover significant issues that require attention.

**Qualified validation.** In the process of clearing response outliers in the assessment, managers should be asked to list their top three risks, or "What keeps them up at night?"

Management succession may be a crucial concern. Are there individuals qualified to take over key positions following retirements of current managers? If an unexpected event were to occur that required an immediate succession, who would be qualified to step up? Would the transition be as orderly as could be expected?

Competition is always a top concern. How well can an organization's services or products stand up to competitors' offerings? Is the organization capable of responding to what other companies are doing?

Innovation is another critical factor. The importance of product innovation may vary from one industry to another, but innovation also encompasses finding ways to enhance efficiency and product quality. Is the organization doing enough to capitalize on advances and opportunities?

The top three to five risks—whatever they may be for the organization—are evaluated and summarized. The purpose for determining those risks is to validate that the correct risks were identified in the entity-wide risk assessment.

**Outlier interviews.** Individuals who gave outlier responses should be interviewed to gain a better understanding of their answers. Once an understanding of their responses is gained, the auditor and the respondent can reach a consensus on the response. Changes to the respondent's answers are made, as appropriate, and marked as changed. The responses are then re-summarized, and a new final composite analysis is created.

**Entity-wide risk assessment—top risks.** Each risk statement that was scored by respondents contains a specific root issue. The individual risk statement scores are sorted from highest to lowest risk. The table is split into groups, based on the total responses and various organizational divisions or locations.

Reviewing risk scores of the individual risk statements enables examiners to expand upon the composite analysis and see the risk factors in a given category that create risk for the company.

Comparing risk ratings by locations shows the differences in the environment and perception among different management groups, depending on their area of responsibility.

## Assessing Risk Impact and Mapping Risks

**INTERNAL AUDITORS,** in consultation with management, determine the significance of identified risks. This determination is based on the profile of the company, taking into consideration such factors as customer concentration, economic climate, regulatory environment and other crucial concerns. Those risks are then plotted in a heat map format based on:

- **Probability**: The likelihood of an error or omission occurring related to this risk
- **Impact**: The severity (monetary, operational, social, etc.) of a potential error or omission occurring related to this risk

The heat map (see Exhibit 2) includes a vertical axis that indicates a particular risk's financial statement impact. The lowest impact risks are near the vertex with the horizontal axis. The horizontal axis indicates the likelihood of the risk occurring, with the least likely risks occurring near the vertex with the vertical axis.

The map is divided into four quadrants. Risks falling within the upper right-hand quadrant indicate vulnerabilities requiring organizational improvement. Areas of high inherent risk with a low level of control must be a key priority for controls improvement activity.

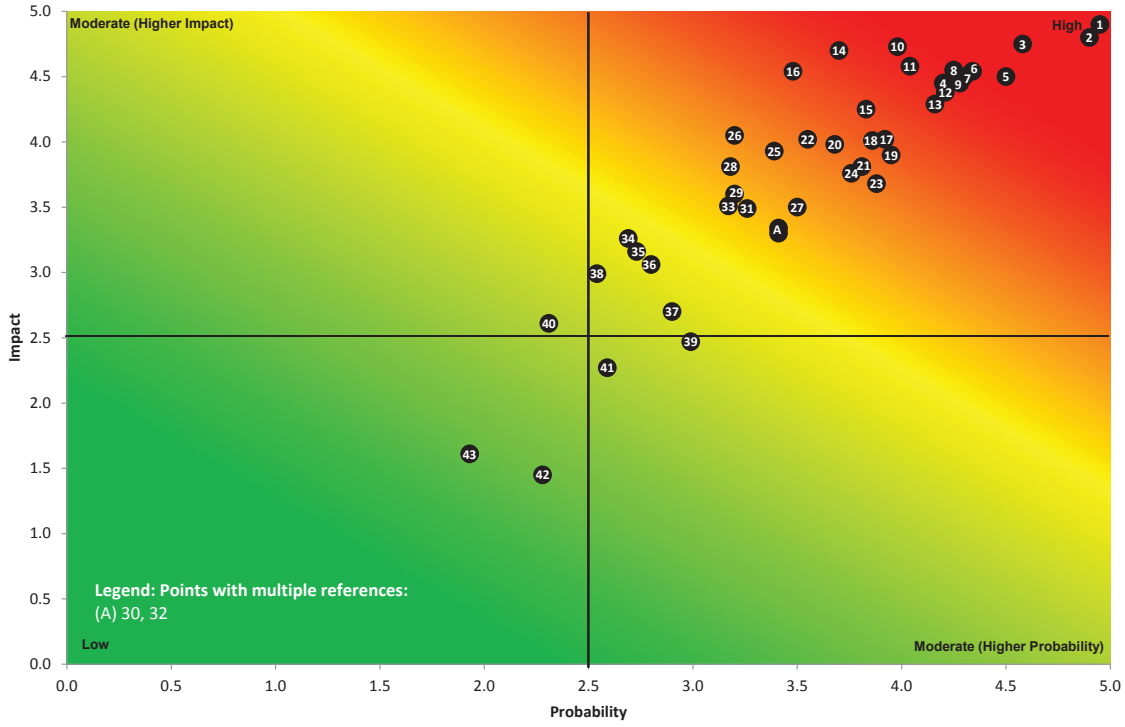
Risks plotted in the upper left-hand corner indicate vulnerabilities that should be monitored. The lower right-hand quadrant indicates risks requiring acceptance. Risks that also have a low level of control may be consciously accepted by the organization.

The lower left-hand quadrant illustrates risks whose controls can be optimized. Risks with a low inherent exposure with a high level of control may generate opportunities to optimize the process and control for efficiency.

Identifying such entity-level risks helps organizations identify the process-level vulnerabilities linked to those risks.

Exhibit **2**

**Financial and Operational Risk Map Combined**



## Responding to Identified Risks

**BASED ON COMPARISON** of an identified entity-level exposure to its risk appetite, an organization can choose the most appropriate response to that risk. The COSO (Committee of Sponsoring Organizations of the Treadway Commission) Enterprise Risk Management Framework defines avoidance, reduction, sharing and acceptance as general risk responses.

An organization may decide that the likelihood or potential impact of an identified risk is simply too high and that the most appropriate response is to avoid that vulnerability completely. A retailer seeking to expand beyond its regional market may decide that local competitors within a particular state are very well-entrenched. Because it could take an inordinate amount of time and resources to gain significant market share in that state, the retailer decides to avoid that risk by directing its current expansion efforts elsewhere.

Reducing risk is another option for responding to a recognized vulnerability. An increase in traffic accidents poses a significant entity-level risk for a package delivery company. To reduce that risk, the company implements more extensive defensive driving training programs for its drivers. It also purchases greater insurance to reduce its liability exposure in the event of accidents.

Sharing risk provides another option for mitigating an unacceptable vulnerability. An oil company discovers substantial new reserves. Exploiting those reserves, however, requires expertise beyond its exploration capabilities as well as massive, long-term capital commitments in a very cyclical industry. To share the risks that accompany exploiting those reserves, the company enters into a partnership with another oil company that specializes in oil field production.

An organization may also decide that an identified vulnerability is within its risk appetite and does not require further response. A domestic software developer, for example, may rely upon service providers in Asia to perform crucial tasks, including writing software code and providing technical support. Dependence upon such distant operations presents numerous risks. However, the company has an employee on-site at each service provider's location and utilizes real-time reporting systems to continually evaluate their performance. Because it feels its monitoring efforts are sufficient, the software company accepts the risks that accompany its outsourcing.

Responding to and reducing crucial risks at the entity level complements an organization's efforts to address risks accompanying its business strategies. Focusing on risks at the entity level leads to evaluation of the processes associated with those entity-level vulnerabilities. With such an approach, the organization addresses risks in a comprehensive, consistent manner.

Responding to entity-level risks and mitigating unacceptable vulnerabilities enables an organization to ensure that identified exposures do not exceed its risk appetite. That protects the organization and allows it to pursue its business strategies.

> "Responding to and **reducing crucial risks** at the entity level **complements** an organization's efforts to address risks accompanying its **business strategies.**"

Organizations operate in dynamic environments, and new risk exposures will always emerge. Addressing those emerging risks enables a company to minimize the degree of uncertainty it faces. Such responsiveness uncovers opportunities that may have otherwise gone unnoticed. Such responsiveness also helps identify processes—crucial everyday activities—that support significant entity-level concerns.

## 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 exposures accompanying business strategies.

Every organization has business 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 vulnerabilities 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 AUDIT** committee, board of directors, senior management 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 respective direct impact on a given business process, the remaining residual risk must be covered by process-level controls.

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 the register process to ring up the sale, the locked cash drawer and the clerk's shift cash reconciliation are each controls designed to cover this risk.

Inherent risks are present in each 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 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 exposure presented by those risks.

## Implementing a Risk Assessment Program for Process-Level Risks

**THE METHODOLOGY USED** for identifying and evaluating process-level risks is similar to that used for assessing entity-level exposures. Evaluating significant vulnerabilities facing the organization, though, extends to other processes—discrete functions—within the organization that are critical for business operations, such as:

- Online technology support
- Management training
- Customer service
- Quality control

Examining those areas helps create the audit universe, which includes all crucial activities.

**Determining the process-level risk rating.** Once the audit universe has been defined, the significant financial and operational processes are risk rated for the entity-level risks identified.

A risk assessment forum, involving management and the internal audit function, is used to rate each organizational risk at the process level. The forum participants define the probability and impact of each entity-level risk as it applies to the organization's processes.

Risk rates are based on the level of importance placed on the risk during the entity-level forum meeting. Calculations to quantify the risks related to each significant process are then performed. The calculations are based on the consensus rating from the risk assessment forum by taking the sum of all process-level risk weights when multiplied by the entity-level risk weights for both the probability and impact of each risk.

The probability and impact risk ratings calculated determine the heat map risk quadrant in which the significant risk is plotted. The risk-rated universe is then reviewed to identify the risk ratings that may be excessively high or low.

Once that review is complete, the items in the risk-rated internal audit universe are plotted on a heat map to illustrate the significance of each risk. Maps are created for various views, including the internal audit universe, financial processes, operational processes and processes within various divisions.

> "Within discrete functions, processes need to be evaluated to determine: **"What can go wrong?"**"

### Identifying Process-Level Risks

**WITHIN DISCRETE FUNCTIONS,** processes need to be evaluated to determine: "What can go wrong?" Risks at the process level are easily identified by examining each step in a particular process to determine:

- What risks are natural or inherent in each process?
- How can those risks be minimized?
- What controls exist around the process and are they functioning as intended?
- What breakdowns of these controls have occurred in the past?
- How have breakdowns been resolved?
- What controls might be missing?
- Are proper segregation of duties present?
- What consideration has been given to fraud prevention/detection or asset protection with current internal controls?
- Are the process steps executed consistently? If not, what are the differences?
- What are the best practices you see around each process?
- What are the efficiencies and control enhancements that you know could be derived?

The answers vary from one activity to another. The same person may be responsible for receiving and depositing cash receipts. Because those duties are not segregated among two or more individuals, the potential exists for that person to deposit cash into a personal account without anyone noticing, thus defrauding the organization.

For a manufacturer, quality assurance processes and standards may vary from one location to another, leading to inconsistent production, run examinations and measurements. Uncertainties regarding who has responsibility or ownership for responding to various types of customer concerns may hinder an organization's ability to provide prompt, effective customer service.

Examining each process in a specific manner provides a basis for assessing the degree of risk associated with each activity.

### Reducing Process-Level Risks

**EVALUATING THE RISK** ratings for each assessed process enables managers to determine how much exposure exists for each activity. In some instances, that level of exposure may be relatively low, indicating that existing controls and safeguards not only work fine, but may be optimized to yield greater efficiency. Degrees of exposure for other processes may indicate that periodic monitoring is sufficient.

A variety of steps can be taken to mitigate process-level risks deemed unacceptable and 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.

> "**Process improvement** efforts focus on identifying risk potential, while also enhancing **efficiency.**"

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. Other processes throughout the organization may likewise be improved by automating activities currently performed manually.

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 receivables processes, with each subsidiary setting its own interest rates and collection policies. Standardizing those accounts receivables 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 those 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 incorporates a system of checks and balances that mitigates risk. Segregation of duties is a foundational control for risk mitigation.

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 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 for 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 user name and password, provide initial access restriction. Those restrictions might include only presenting truncated versions of data fields. Such a restriction enables an employee to complete required tasks without viewing full disclosures of private information. Automatic logoff controls likewise ensure that such information will not remain visible for long if individuals forget to close files before leaving their workstations.

"**Automating** manual controls provides another means of **lowering risk** and **increasing efficiency** and **effectiveness.**"

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 work site, 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 work site accidents involving company vehicles.

## Addressing Risks at All Levels 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 must be scalable and sustainable, so that attention remains focused on recognizing and reducing vulnerabilities amidst such change.

At the strategy and entity levels, for example, the dashboard reporting capabilities allow leaders to continually monitor crucial internal and external exposures. Such capabilities can also accommodate company expansion and other organizational changes, thereby providing continuous, accurate data for ensuring that any exposures remain at an acceptable level.

That emphasis on scalable, sustainable risk mitigation efforts extends to everyday activities that support entity and strategic concerns. 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 require 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 exposure.

Imbedding 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 imbedding control measures into various processes.

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

## Risk Insights: **Risk Assessments Pay Forward**

### Continual Diligence Delivers Long-Term Benefits

**RESPONDING TO RISKS** and reducing vulnerabilities is an ongoing function, a function supported by annual risk assessment refreshments, a function that yields a variety of benefits.

Domestic economic conditions change, as do economic conditions in countries abroad where the organization may have facilities, major suppliers or substantial customer bases.

Political and regulatory environments change. Technological advances may widen exposures for various service or product markets. Demographic trends, downturns in industry cycles and a host of other factors influence an organization's ability to execute its business strategies.

Monitoring such strategic vulnerabilities helps an organization maintain a risk profile that remains within its risk appetite. That ongoing monitoring gives an organization's board members and senior managers the time and information they need to respond to emerging exposures and to implement steps to reduce the likelihood or potential impact of those vulnerabilities.

Identifying and mitigating emerging vulnerabilities extends to the entity and process levels. In addition to providing immediate identification, assessments and response for potential adversities, such attention to risks 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 potential exposures receive continual attention, regardless of internal or external changes.

Establishing ownership and accountability for addressing risks throughout the organization nurtures a corporate culture that values the importance of addressing exposures. 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



weaver
Assurance • Tax • Advisory