10 ways

to improve risk management
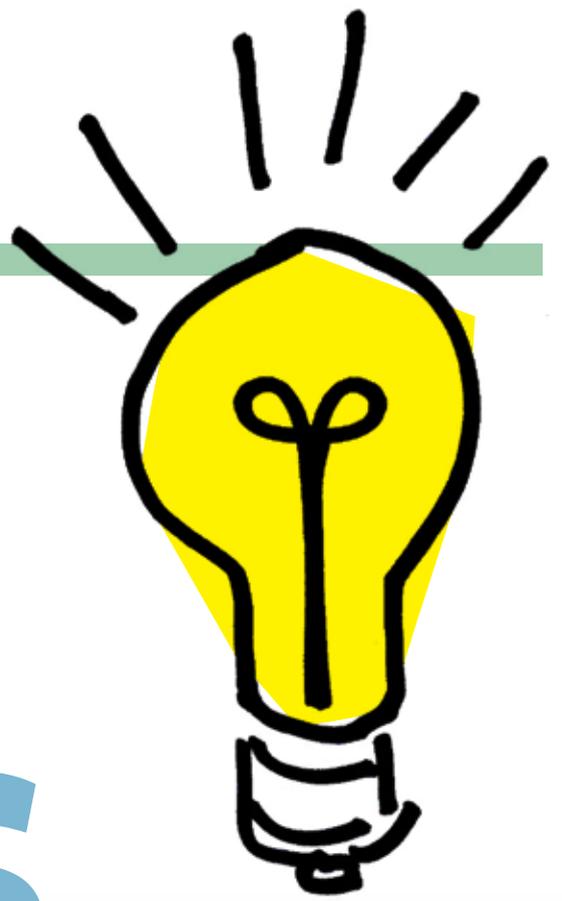
Marinus de Pooter

With an awareness of common shortcomings, internal auditors can help their organization better meet stakeholder expectations and ensure business objectives are achieved.

Why do risk management implementations and functions often fail to deliver what is expected? And what causes senior management to feel that its investments in risk management systems are not delivering the expected returns? Many factors, potentially, are to blame, stemming from various parts of the organization and its systems. But most often, the culprits come down to a handful of common dysfunctions.

Ten key practices, in particular, are regularly neglected in organizations across industries and geographies, and in both large and small business settings. Successfully addressing these areas can help enhance the organization's ability to deal with the uncertain future, improve decision-making, and increase the reliability of periodic forecasts. Accordingly, these measures will augment the "predictive power" of the organization, resulting in greater stakeholder confidence. Understanding the pitfalls, and recommending solutions to them, can provide internal auditors with a solid basis for helping to improve risk management in their organization.

1 ASK THE KEY QUESTIONS

Observation Risk management discussions typically do not evolve around the question, "How can we better manage stakeholder expectations?" In fact, the external customer perspective is often absent entirely. Questions like, "To what extent will our customers benefit from our control measures?" are not asked, even though customers are key stakeholders and the organization is expected to create and preserve value for them.

Recommendation Remaining "in control" is a relative concept in a largely unpredictable world. There are no risk-free organizations or error-free managers. When presenting strategies and plans, senior management should recognize that the future is inherently uncertain and that its endless possibilities are too complex for anyone to predict with great accuracy. Instead of maintaining the illusion that the future can be fully understood or controlled, senior management should show courage and honesty when updating key stakeholders based on the latest forecasts.

2 CREATE THE RIGHT CULTURE

Observation The organization is led by a dominant individual who has little interest in, or tolerance for, deviating opinions. When negative events occur, the leader's primary response is to seek blame rather than trying to learn from mistakes. Consequently, managers and staff prefer to keep issues quiet as long as possible, creating a culture where learning is not valued and self-preservation is the prevailing mode of behavior. Moreover, the board does not clearly communicate its expectations with regard to acceptable risk exposures.

Recommendation The organization's culture will benefit from clarity on what is expected from managers and staff employees. Clear communication regarding what constitutes acceptable behavior and what doesn't, as well as the bandwidths of acceptable deviations from stated objectives (i.e., the risk tolerances) must be provided. The board should initiate open discussions about the level of internal control required to manage key stakeholders' expectations, and senior management should encourage learning from company errors rather than simply tearing down those responsible. Above all, senior management and the board should lead by example—a prerequisite for effective risk management.

3 CLARIFY RESPONSIBILITIES AND RULES

Observation Senior management has not clearly delineated responsibility for achieving business objectives, including those associated with meeting compliance requirements. Uncertainty exists regarding who's in charge of developing which organizationwide policies and procedures. Senior management places more reliance on detailed policies and procedures than on experienced people with sound judgment, and line managers equate being "in control" with following extensive guidelines and protocols prescribed by central support functions—even if these procedures do not produce the desired results. Moreover, business managers are only held accountable for their results to a certain extent. Their supervisors rarely ask the simple, core question, "How sure are you that you are going to achieve the agreed-upon objectives and that there won't be unpleasant surprises in the upcoming period?"

Recommendation The organization will benefit from establishing a structured process for managing its charters, protocols, instructions, and other key policy and procedure documents. Senior managers should avoid giving too many separate internal regulators and specialized staff functions the ability to issue these "rules of the house" independently, without extensive coordination and consistency in their approaches. They should also make clear what is decided at the corporate level (e.g., centralized procurement) versus what is left to the discretion of local management. Moreover, senior management should arrange "reality checks" from business managers when designing and implementing new rules for the organization, in an effort

to prevent "rules obesity" from proliferating. Effective policy management eliminates gaps, overlaps, and inconsistencies in the organization's rules of the house, which effectively serves as its business control framework. In turn, it enables internal auditors to use this framework as a clear reference against which to perform their audits.

4 USE SUITABLE REWARD SYSTEMS

Observation Business managers are under undue pressure to achieve goals that are unrealistic. In addition, senior management promotes excessive risk-taking by rewarding it with attention, bonuses, promotions, and other forms of compensation.

Recommendation Adequate remuneration policies are necessary to steer people's behaviors in the desired direction. Senior managers should lead by example and only accept compensation packages for themselves that are consistent with serving the long-term interests of the organization. Doing so will encourage managers and other employees to embrace the stated objectives and to commit to pursuing them.

5 FOCUS ON THE BUSINESS OBJECTIVES

Observation The organization's risk management activities are not linked to the board's strategic agenda, which typically includes the board's aspirations regarding growth, efficiency, innovation, standardization, and sustainability. Moreover, confusion exists regarding how the organization will deliver value for each individual stakeholder segment, and the business objectives are not SMART (specific, measurable, attainable, relevant, and timely) enough to allow gauging actual progress against goals. Senior managers have little motivation to address this situation, because ill-defined objectives make it harder to hold them accountable for performance results.

Recommendation The primary purpose of all risk management, internal control, internal audit, and other support functions'

activities is to contribute to the realization of the organizational objectives. Senior management should emphasize that these objectives, in turn, are aimed at creating and preserving value for key stakeholders. These stakeholders, after all, are essential to the entity's continued existence.

6 RECOGNIZE THE LIMITATIONS OF RISK ASSESSMENTS

Observation The risk management program is focused on identifying, categorizing, and weighing all sorts and types of risks, but not on actively managing uncertainties associated with the achievement of the business goals. Due to the extensive use of risk profiles, top-10 risk lists, and other tools, the risk categories become the "end" instead of the "means." Additionally, senior management believes, or pretends, that enterprisewide quantification of risk exposure is feasible, failing to consider that building all-encompassing risk models is impossible. In reality, correlations among multiple risk factors are hard to define, essential data often is missing, loss databases are of limited use to help predict the future, and past effectiveness of control measures is no guarantee for the future.

Recommendation Risk assessments result in mere opinions about the future. These analyses are colored significantly by factors such as the personal preferences, knowledge, recent experiences, and character traits of those involved. Moreover, risk assessments should not be one-sided. To determine the extent to which the organization is ready to deal with the future, the analyses need to include matters that could help the realization of business objectives (the opportunities) in addition to those that potentially hamper the objectives (the risks). Furthermore, senior management should treat risk management (dealing with events that could happen) and incident management (dealing with events that have happened) in concert. They should ask questions such as: "How well trained is our organization to handle serious incidents when they occur?" and "How well established is our continuous improvement cycle?" They should also

convince the business managers that a proactive, integrated approach for both risks and incidents is needed to keep the business control framework fit for purpose.

7 PUT BUSINESS MANAGERS IN THE DRIVER'S SEAT

Observation The risk management systems primarily comprise support functions such as risk management, internal control, quality management, health and safety, information security, revenue assurance, and internal audit. Line managers, who have to balance risks and rewards when making business decisions, are conspicuously absent from the process. At most, project managers are expected to include a separate risk section in their project plans. However, more often than not, this section includes only obvious, generic risks. The support functions tend to focus on introducing and fine-tuning compliance measures, and they seem to have limited consideration for the daily struggles of business managers serving their demanding customers. These functions tend to categorize the world into "lines of defense." Hence, they speak a different language than their client-facing colleagues, who are busy "attacking the market" and "conquering market share."

Recommendation Risk analyses should provide the more balanced view of the future that business managers prefer — in other words, they should include opportunities. Senior managers should prevent the support functions from viewing risk mitigation as the most important strategy. They should explain that there are alternatives to fencing off the business processes with lots of preventive control measures and better ways to address risks than just adding more controls.

Line managers should not feel as though risk management duties are an afterthought or a mere distraction from their "real job." The board should orchestrate "pre-mortem" reviews of important strategies, plans, and projects to establish whether the existing business control system is robust enough to achieve the organization's stated objectives reliably. The board should also ask senior management to explain the extent to which the achievement of its objectives

(regarding quality, time, and money) is uncertain — a central issue for stakeholders. At the same time, senior management needs to encourage business managers to take advantage of risk managers' and internal auditors' risk and control expertise. These "generalists" should have a seat at the table when acquisitions are planned, new products are developed, or new markets are entered. Pursuit of new business opportunities should go hand in hand with serious discussions of the risks associated with the oftentimes crescendo projections of the promised results.

8 DEMAND INTEGRATED MANAGEMENT INFORMATION

Observation Senior management receives separate periodic reports from multiple support functions regarding performance levels, risk exposures, incidents, and trends. However, no integrated reports are produced that provide a shared view of the organization's current and expected future levels of control effectiveness — parsed by entity, division, country, service line, location, etc. Consequently, senior management is left to obtain a clear understanding of the actual situation from many separate reports that may contradict one another.

Recommendation Senior management should demand single integrated reports, thereby expecting the numerous functions providing this information to work together. Its aim should be to build a shared view of the extent to which the business objectives have been achieved in the previous period and the extent to which they are expected to be achieved in the next period. Senior management should insist that those providing the information use contemporary tools and techniques to analyze the available business data. They should monitor the effectiveness of the control framework not primarily based on checking samples, but on analyzing large transaction volumes. They should use continuous monitoring of transaction flows to spot irregularities and negative trends timely and develop robust business intelligence capabilities aimed at reducing uncertainty when making management decisions.

9 MAKE SURE RULES ARE ENFORCEABLE

Observation The organization is abundant in elaborately designed rules, developed by specialists who are capable of issuing the most technically advanced policies and procedures (e.g., on information security). However, these rules are too complex for line managers to translate and incorporate into their daily operations, rendering enforcement difficult. In addition, there are significant gaps in the audit coverage pertaining to essential controls, important audit findings are not taken seriously, and managers get away with not following up improvement plans adequately.

Recommendation Organizational leaders should insist on having clear rules of the house that can be realistically executed in practice. The level of detail these rules contain depends on factors such as management philosophy, business process maturity, industry practices, expectations from regulators, and certification requirements. Senior managers should arrange support for the busy line managers when translating corporate policies into specific control measures in their business processes. If they want the rules to be taken seriously, they must also demonstrate that violations must be met with consequences.

10 ALIGN INTERNAL AUDIT WITH THE BUSINESS

Observation The risk assessments prepared for the annual audit plan are not aligned with the organizationwide risk analyses performed on behalf of business management. Internal audit doubts the ability of other support functions to collectively design and implement appropriate internal controls. Due to fear of losing their objectivity, the internal auditors refrain from opining on the design of the control framework. When performing their audits, they prefer to use their own norms and perceived best practices—instead of the agreed-upon business control framework—much to the surprise and irritation of their clients and colleagues from other support functions.

Recommendation The chief audit executive should be clear about the contributions he or she expects internal audit to make toward realization of the organization's objectives. Senior management should involve the internal audit function as a trusted adviser to help establish the organization's rules of the house. The more mature the rules become, the more efficiently internal audit can deliver independent assurance. Internal auditors should demonstrate that they understand which risks, if managed well, give their organization the greatest competitive advantages. They should gladly accept the challenge of actively managing information on how their organization earns the trust, respect, and financial support of key stakeholders.

MANAGING EXPECTATIONS THROUGH PREDICTIVE POWER

Business managers view risk management as helpful to the extent that it enables them to better manage the expectations of their key stakeholders. Accordingly, a thorough stakeholder analysis should always be the first step in any risk management process. The stated business objectives should reflect the choices made by senior management regarding the specific value they want to create for each stakeholder constituency. Risk assessments should be aimed primarily at estimating the likelihood and extent to which the stated objectives will be achieved.

Risk management activities should serve the continuous improvement of an organization's predictive power, which hinges largely on the quality of the periodic forecasts prepared by the responsible business managers. Producing reliable forecasts requires that these managers be aware of the available opportunities, the levels of risk exposure, and the quality of internal control. The more realistic these forecasts are, the higher the level of control the managers achieve.

Following this approach shifts business managers' attention from gauging actual results (versus plan, budget, etc.) to managing stakeholder expectations more proactively. Ultimately, improving the predictive power of an organization leads to a reduction in the overall uncertainty to which the entity is exposed. This, in turn, leads to enhanced confidence and trust in its senior management. And that is the best return leadership can receive from the time, effort, and money invested in risk management. Ia

MARINUS DE POOTER, RA, CIA, CMA, CFM, *is owner of MdP | Management, Consulting & Training in Deurne, The Netherlands.*