A common view of the lines-of-defense model is from the vantage point of executive management and the board of directors – that is, that there are three lines of defense. Business unit management and process/risk owners comprise the first line, independent risk and compliance functions are the second line, and internal audit is the third line. This point of view has considerable merit. However, from the vantage point of shareholders and other external constituencies (an external stakeholder's view), we see two additional lines of defense. A five-lines-of-defense model is depicted below:

**What Is the Lines-of-Defense Model?**

Essential to effective risk management, the lines-of-defense model is implicit in COSO’s recently issued internal control framework through the control environment, control activities, monitoring, and other components of an internal control system. It provides assurance to the board of directors, as the elected representatives of the shareholders to oversee the organization’s operations on their behalf, that risks are reduced to a manageable level as dictated by the organization’s appetite for risk. Much more than “segregating incompatible duties” and “ensuring checks and balances,” the lines-of-defense model emphasizes a fundamental concept of risk management: *From the boardroom to the customer-facing processes, managing risk is everyone’s responsibility.*

---

1 | protiviti.com
Together, the above five lines of defense support the execution of the organization’s risk management capabilities. The thinking underlying these five lines of defense is outlined below:

1. Senior management, under the board's oversight, must set and reinforce the “everyone is responsible” tone by positioning each of the lines of defense to function effectively. The other lines of defense reinforce this tone of the organization.

2. Those responsible for the units and processes that create risks must accept the ultimate responsibility to own and manage the risks their units and processes create, as well as establish the proper tone for managing these risks consistent with the “tone at the top.”

3. Effective risk management and compliance require an independent, authoritative voice to ensure an enterprisewide framework exists for managing risk, risk owners are doing their jobs in accordance with that framework, risks are measured appropriately, risk limits are respected and adhered to, and risk reporting and escalation protocols are working as intended.

4. Internal audit provides assurance that other lines of defense are functioning effectively and should use the lines-of-defense framework as a way of sharpening its value proposition by focusing its assurance activities more broadly on risk management.

5. Under the oversight of the board of directors, executive management must manage the inevitable tension between market-making activities and control activities by ensuring these activities are appropriately balanced such that neither one is too disproportionately strong relative to the other. Executive management must align the governance process, risk management and internal control toward striking the appropriate balance to optimize the natural tension between value creation and value protection. More importantly, they must act on risk information on a timely basis when it is escalated to them and involve the board in a timely manner when necessary.

Each of the above lines of defense are discussed further in the sections that follow.

**The First Line of Defense: The Tone of the Organization**

“Tone of the organization” is a phrase we coined to describe the collective impact of the tone at the top, tone in the middle, and tone at the bottom on risk management, compliance and responsible business behavior. While tone at the top is important and a vital foundation, there is an important business reality leaders must understand as they communicate downward the organization’s vision, mission, core values and commitment to appropriate ethical behavior: What really drives behavior in an organization is what its employees see and hear every day from the managers to whom they report. If the behavior of unit and middle managers contradicts the messaging and values conveyed from the top, it won’t take long for lower-level employees to notice.

---

**Some Warning Signs**

1. There is significant turnover of key executives and/or evidence of unrealistic strategies, inappropriate performance pressures, unbalanced compensation structures, or there is an overly dominant chief executive who punishes executives who deliver bad news, among other things.

2. Middle line and functional managers aren’t effectively aligned in terms of the organization’s vision, mission, core values, strategy, and risk responses.

3. Risk is an afterthought to strategy-setting and business planning (e.g., risk is not considered explicitly by management when updating the business strategy or plan); risk management is an appendage to performance management.

4. A clear escalation policy regarding significant risk and compliance matters does not exist.

5. There is tolerance for conflicts of interest in the execution of significant business activities.

The top-down emphasis on ethical and responsible business behavior in any organization is only as strong as its weakest link. That is why the organization’s tone at the top must be translated into an effective tone in the middle before it can reach the rest of the organization. Effective tone at the top is a prerequisite to a commitment to continuous improvement that is essential to reducing risks to an acceptable level and driving responsible business behavior in a changing business environment. Most importantly, actual actions and behaviors of executives either reinforce or undermine the implicit tone articulated by executive and line management through policies and other communications. For example, if management looks the other way when policies are violated or handles an ethical dilemma poorly, the example set is there for all to see with the attendant effects on the tone of the organization. Day-to-day words and deeds go hand in hand. The tone of the organization influences its risk culture – the manner in which the organization’s personnel perceive and manage risk. Without a clear tone of the organization and an effective reinforcement of the other lines of defense, people will tend to manage risk differently. It must be clear to everyone that executive management and the board value risk management and compliance as important disciplines in conjunction with managing the business and pursuing value creation opportunities. Unit managers and middle management must share that view as well. That means management at all levels must demonstrate, through policy and other top-down communications, incentive

---

compensation structures, and day-to-day decision-making, actions and values exhibited, that managing risk is an organization imperative – and everyone’s job.

Executive management initiates this tone by driving the “everyone is responsible” perspective throughout the organization and positioning each of the respective lines of defense to function effectively. The board must be vigilant to ensure there is nothing constraining risk management and compliance functions (third line of defense) and internal audit (fourth line of defense) from reporting to it when critical risk issues arise. Periodic executive sessions with the appropriate functional leaders and chief audit executive can help in this regard. As for a formalized escalation process, even in circumstances where the chief executive officer (CEO) (or preferably, an executive risk committee) resolves disputes between the second and third lines of defense, the board should be informed if such disputes are about significant matters or close calls.


Given the tone of the organization, implementing a risk management framework requires the identification of risk owners because without them, no one is accountable for managing risk. Resolution of the ownership question for critical risks is a key task in implementing risk management. If there are gaps (no owner of a risk) or overlaps (too many owners of a risk), they must be addressed and, if the risks are critical, this must happen as quickly as possible. Who decides the capabilities needed to manage a given risk? Who designs these capabilities? Who executes? Who monitors performance?

These considerations are implicit in the risk ownership question and are important because risk owners constitute the second line of defense.

Risk owners, at minimum, must do three things:

- First, they must decide on the risk responses to implement. While they may obtain approval from executive management, the risk response strategy is theirs, and they accept it as their own.
- Second, they must design the capabilities for managing the risk in accordance with the selected risk response and consistent with the defined risk appetite. Preferably addressing the source or root causes of the risk, the specific design should consider the appropriate policies, specific processes and control activities, necessary personnel and skills, management reporting mechanisms, supporting methodologies, and systems and data needed to ensure the selected risk response is implemented effectively.
- Finally, risk owners monitor established risk management capabilities over time to ensure they perform as intended. If deficiencies are noted, they fix them on a timely basis.

With respect to building and executing risk management capabilities, risk owners may elect to outsource these responsibilities; in doing so, their ownership of the risk is not compromised as long as they continue to decide, design and monitor. The premise here is if a person can’t make significant decisions, isn’t accountable for the adequacy of the design, and doesn’t monitor the operational effectiveness of the risk response, how can he or she be an effective owner of the risk?

Risk owners include business unit managers and process owners. As they assume primary accountability for identifying, prioritizing, sourcing, managing and monitoring risks, they constitute the second line of defense. As the principal owners of risk, they set objectives, establish risk responses, train personnel and reinforce risk response strategies. In short, they implement and maintain effective internal control procedures on a day-to-day basis and are best positioned to integrate risk management capabilities with the activities that create the risks.

The Third Line of Defense: Independent Risk Management and Compliance Functions

The third line of defense consists of risk management, compliance and other independent functions that establish risk management policies, set standards for managing risk, enforce limit structures and provide appropriate oversight over specific risk areas. These functions determine the appropriate framework for managing risks and ensure it is implemented by business unit managers and process owners effectively and consistently across the enterprise.

---

4 In addition to risk owners, independent risk management and compliance functions (which comprise the third line of defense) also monitor risk management capabilities.
Depending on the industry, these functions may include compliance, environmental, financial control, health and safety, inspection, legal approval, quality assurance, risk management, security and privacy, supply chain, and contracting. As centers of excellence, these functions collaborate with unit managers and process owners to develop and monitor controls and other processes that mitigate identified risks. They also may conduct independent risk evaluations, develop risk management programs, and alert management to emerging risk issues.5

### Some Warning Signs

1. Risk management and compliance are not viewed as peers to business line leaders.

2. Risk management and compliance have no reporting line to the board or face constraints in reporting to the board.

3. The board, senior management and operating personnel believe that managing risk is a single person's or function's job and is not an organizational imperative or everyone's job.

4. Management does not value risk management and compliance functions at the same level of importance as opportunity pursuit, or views them as obstacles to getting things done.

5. There is lack of clarity/definition in risk management and compliance functions and how they interface with senior line management, leaving these individuals constantly justifying their place in the conversation or fighting distracting “turf issues.”

To be truly objective and effectively positioned within the organization, risk management and compliance functions should be insulated from and independent of business unit operations and lines of business and front-line, customer-facing processes of the business. Do the CEO and board want someone to coordinate, educate, facilitate, evaluate and integrate risk management activities? While that may be a valuable role for someone to play, such activities do not constitute a viable line of defense if there is no veto and escalation authority. At the other extreme, do the CEO and board want:

- An objective assessment of the risks resulting from a line of business, process, transaction, deal or business plan, broken down into the fundamental components of risk so that the risks can be measured and systematically evaluated and managed?
- Advice on the actions to take if the risks inherent in a strategy, plan, process, transaction or deal are inconsistent with the desired risk appetite?
- A qualified, independent party to exercise veto and/or escalation authority when situations involving

noncompliance with legal and regulatory requirements and internal policies arise?

- Meaningful and actionable risk reporting to the overall board, specific board committees and senior management that is independently developed from the risk owners?

- Ongoing assessments of the appropriate mix of centralized and decentralized approaches to establishing risk policy and standards, defining risk appetite, and setting risk thresholds and limits?

- Periodic reviews of compensation plans to consider the impact of risk factors and the design of the compensation structure on behavior?

Clearly, the expectations of the CEO and the board set the tone in determining whether there is a robust third line of defense.

Consistent with the premise that risks must be owned by the lines of business and process owners that generate them, the risk management and compliance functions do not typically own responsibility for managing specific risks. They generally operate in a strategic oversight role with authority vested by the executive committee (or a designated risk management committee), the CEO and/or the board (or a committee of the board). This strategic oversight focus is important because severe consequences can arise when there are strategic shifts and the resulting risks are not comprehensively analyzed and understood.

Positioning of risk management and compliance functions entails several important principles:

1. The more significant the risk area to the execution of the business model, the greater the need for the functional leader (such as a chief risk officer [CRO]) to be viewed as a peer to business line leaders in virtually all respects (e.g., compensation, authority, and direct reporting to the CEO) and likewise down through the business hierarchy and across the organization. The only way that will happen is if the CRO has the scope of responsibilities, authority, compensation and direct reporting lines that demand respect. The total package of actively participating in the strategy-setting process, leading the formulation of the organization’s risk appetite statement, developing risk reporting mechanisms, chairing or participating in management risk committees, and when appropriate, escalating risk issues to the CEO and the board, must convey to the lines of business and across the institution that the CRO is a player. That means the CRO should be a key executive who reports directly to the CEO or the board. Depending on the industry, the same point may apply to sensitive aspects of a company’s operations, including environmental, health and safety, product quality, contracting, security and privacy, and other areas. Either these executives have real authority and clout, or they are relegated to the role of a mere “champion.” The “C” in CRO needs to mean something.

---

2. The functional leader should have a reporting line to the board or a committee of the board and face no constraints of any kind in terms of access to the board.

3. The functional leader’s position and how it interfaces with line-of-business management must be clearly defined.

4. The board or a committee appointed by the board should conduct periodic executive sessions with the functional leader – these sessions should be mandatory and regularly scheduled.

5. A formalized escalation process should exist (e.g., written procedures and agreements requiring escalation of any significant issues raised by the risk management and/or compliance function that are being argued by line-of-business executives).

For the above principles to work effectively in practice, the board and CEO must have mutual understanding of the value contributed by the functional leader’s role with the intent of preserving his or her independent role within the organization.

The Fourth Line of Defense: Internal Assurance Providers

Internal audit reviews controls and risk management procedures; identifies risks, issues and improvement opportunities; makes recommendations; and keeps the board and executive management informed of the status of open matters requiring resolution. Two things distinguish internal audit from the other lines of defense: (1) its high level of independence and objectivity enabled by the chief audit executive’s direct reporting line to the board, and (2) its authority to evaluate the design effectiveness and operating effectiveness of the organization’s overall governance, risk management and internal control processes, and make recommendations to strengthen these vital activities for the board and management to consider.

Due to its distinct responsibilities and independent positioning, internal audit provides assurance to executive management and the board on the adequacy and effectiveness of these activities. In some organizations, internal audit is charged with the responsibility to serve as the Sarbanes-Oxley project management office (PMO), and implement enterprise risk management or other similar tasks in other areas. While every organization is different and internal audit may be viewed as a source of resources, such assignments may limit the function’s capabilities as a separate line of defense.

The Final Line of Defense: Board Risk Oversight and Executive Management

Having knowledge of an emerging opportunity or risk without converting that knowledge into hard choices and actionable plans is as ineffective as not having any knowledge at all. The litmus test for risk management and compliance is really all about the decisions management makes at the crucial moment under the direction of the board. After every line of defense has done its job and the significant issues and risks are escalated to the top of the organization, what happens next?

Some Warning Signs

1. Management does not involve the board in strategic issues and important policy matters in a timely manner.

2. Risk management ownership gaps and overlaps, unremediated significant control deficiencies, unaddressed compliance violations, or violations of risk tolerances and limits continue unabated.

3. The organization is too insular in its outlook, leading it to not “reality test” its assumptions about markets and the operating environment regularly (e.g., management continues to execute the same strategy and business model regardless of whether market conditions suggest the assumptions underlying the strategy may be invalid).

4. There is evidence of executive resistance to bad news, such as a dominant senior executive who resists contrary facts suggesting the current strategy requires adjustment to conform to market realities.

5. There is tolerance for conflicts of interest in the execution of significant business activities.

The board of directors and executive management play separate and distinct roles in providing the final line of defense. The ability to act on escalated risk information implies the absence of “blind spots” spawned by such dysfunctional behavior as an unengaged board, myopic short-term focus on “making the numbers,” lack of transparency, an unbalanced compensation structure,

---

Some Warning Signs

1. The internal audit plan is narrowly focused on compliance matters.

2. Internal audit has no reporting line to the board or a committee appointed by the board, or faces constraints in reporting to, or is unable to meet with, the board or board committee in executive session.

3. Internal audit is responsible for risk management.

4. Internal audit budget and resources are limited in terms of acquiring the competencies needed to broaden its focus to risk management.

5. Executive management does not support internal audit recommendations, so improvement opportunities are left unaddressed.

---

6 Ibid.
and other tone-at-the-top issues. Organizations should pay attention to the root causes of executive management ignoring or deferring a decision on the warning signs that tell them something is wrong or isn't working, particularly in situations in which objective parties, in hindsight, can see easily that there was a problem requiring immediate attention.

Often, “blind spots” arise when the organization or business unit is making a lot of money and no one at the top wants to “rock the boat.” Profits can mask risk and are usually unadjusted for risk. A leadership failure to act and the organizational blind spots arising from dysfunctional behavior will usually undermine even the strongest risk management capabilities – regardless of the various lines of defense in place. The board’s risk oversight plays an important role in ensuring executive management appropriately handles escalated risk issues and involves the appropriate board committees in a timely manner. Ultimately, executive management must answer to the board on its handling of escalated issues. In this manner, executive management and the board are the last line of defense when significant issues are escalated upward. At that point, all heads in the organization look to the top for direction.

**External Assurance Providers and Regulators Are Not a Line of Defense**

When regulatory examiners and authorities or external auditors discover significant issues in exercising their oversight or attestation responsibilities, a cost accrues to shareholders in the form of market capitalization declines resulting from fines, penalties, lost revenue or brand image erosion. Therefore, while the existence and functioning of these external groups adds credibility to the capital markets, they do not constitute a line of defense in the model we have asserted.

**Summary**

The five-lines-of-defense model outlined in this publication is an integrated approach through which an organization responds to risk. It sets the proper tone for the organization. It positions line-of-business leaders and process owners as the ultimate owners of risk and holds them accountable for results. It positions independent risk management and compliance functions with the necessary veto and/or escalation authority to serve as a viable line of defense versus serving as mere champions, facilitators or reporters. And it positions internal audit to broaden its value proposition to risk management.

In addition, this model provides direction to executive management and the board as to how the organization should approach risk management and compliance and reminds them that when significant issues are escalated to their attention, it is ultimately up to them to strike the appropriate balance between creating and protecting enterprise value. Their action or inaction at the crucial decision-making moment could significantly influence the organization. The five lines of defense also provide a powerful “line of sight” to the board’s risk oversight process in terms of what to look for and expect.

How do 40% of the FORTUNE 500® solve their critical business and technology problems?

**They ask Protiviti.**

Protiviti has helped companies throughout the FORTUNE 500®, as well as smaller, growing companies to address opportunities to improve one, some or all of the five lines of defense discussed in this issue of The Bulletin. With a network of more than 70 offices in over 20 countries, our professionals partner with you to solve problems in finance, technology, operations, governance, risk and internal audit. Learn more about how Protiviti can help your organization solve its critical business and technology problems today at protiviti.com.