ExecutiveAction Series

Corporate Oversight and Stakeholder Lines of Defense

Stakeholders Demand a Critical Review of Corporate Oversight

by Sean Lyons

The financial crisis of 2008 exposed weaknesses in corporate oversight at all levels—organizational, national, and international—and tarnished corporate reputations. The negative impact has been felt by shareholders, management, staff, clients, business partners, suppliers, regulators, local communities, and society at large. Stakeholders are now demanding higher standards of corporate citizenship and improved oversight to provide them with greater protection and assurances going forward. A corporate oversight framework needs to provide a clear structure of accountability and a solid foundation from which to safeguard stakeholder interests and optimize stakeholder value. This report outlines how to implement such a framework, which is at the heart of effective corporate oversight.

Stakeholders have been focused intensely on the importance of effective corporate oversight and are increasing scrutiny of oversight roles and responsibilities, including the accountability of these mechanisms for defending their interests. Such stakeholder scrutiny has prompted those with corporate oversight responsibility to critically review their own oversight roles and operations and has led to increased consideration of how these oversight roles might function more effectively.

A Holistic View of Corporate Defense

For many stakeholders, an organization's duty is to defend the interests of all stakeholders to ensure the long-term sustainability of the organization. In this context, corporate defense requires an integrated approach that goes beyond the boardroom focus on corporate governance and internal controls and involves far more than an isolated (or siloed) approach to risk management and compliance.

No. 365
OCTOBER 2011

THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

A holistic view of corporate defense means focusing on an organization's collective program (formal or otherwise) for self-defense.[1] It represents the measures taken by an organization to defend itself from a multitude of potential hazards (i.e. fraud, litigation, crime, natural disasters, unacceptable risk taking, reputation damage etc).

Corporate Defense Requires a Strategic Program

In the twenty-first century, the critical components of corporate defense are increasingly interconnected and interdependent. Therefore, safeguarding stakeholder interests requires all defense-related activities (see Appendix 1) to be strategically managed in a coordinated and integrated manner at the strategic, tactical, and operational levels. With a strategic program, it becomes possible to manage, coordinate, and align all components on an enterprise-wide basis, both vertically (top-down as well as bottom-up) and horizontally (across functions).

The following critical components of corporate defense must be managed effectively:

Governance addresses how the organization is directed and controlled, all the way from the boardroom to the factory floor. Management of governance involves specifying the distribution of rights and responsibilities among different stakeholders and spelling out the rules and procedures for decision making.

Risk identifies, measures, and manages the risks the organization is exposed to. Risk management is therefore concerned with addressing the relationship between potential risks and their related potential rewards while ensuring that risk exposures are in line with the organization's risk appetite.

Compliance ensures the organization's activities conform with all relevant mandatory and voluntary requirements. Successful management of this function involves clearly defining applicable laws, regulations, codes, best practices, and internal standards, and so on. This function must demonstrate how the organization ensures that it is in strict adherence with all relevant requirements.

Intelligence provides the organization with the right information, in the right format, to the right person, in the right place, at the right time, in order to arrive at the right decision. It relates to mechanisms, processes, and systems in operation as an organization identifies, gathers, interprets, and communicates the information and knowledge available within (and outside) the organization.

Security provides the ability for the organization to protect its assets (i.e. people, information, technology, and facilities) from threats or danger. This involves the ongoing management of both physical and logical security issues in order to secure the assets of the organization by mitigating threats and minimizing possible vulnerabilities.

Resilience enables the organization to withstand, rebound, or recover from the direct and indirect consequences of a shock, disturbance, or disruption. Organizational resilience relates to sustainability and involves adapting to the constantly changing business environment.

Controls ensure that appropriate actions are taken by the organization to address risk, and in the process, help ensure that the organization's objectives and goals will be achieved. This includes the practices employed to provide the board with at least reasonable comfort that the organization's objectives will be achieved in an effective and efficient manner.

Assurance helps provide stakeholders with a degree of confidence or level of comfort that everything is operating in accordance with expectations. It involves independent conclusions about the impartial assessment or objective examination of a particular subject matter against specific pre-defined criteria.

> "The business community faces a crisis in confidence. Many are asking: how can corporations govern themselves more effectively?"
>
> Committee for Economic Development (CED)[a]

> "Boards are being asked……could they have done a better job in overseeing the management of their organization's risk exposure and could improved board oversight have prevented or minimized the impact of the financial crisis on their organization?"
>
> Committee of Sponsoring Organizations of the Treadway Commission (COSO)[b]

a Committee for Economic Development (CED), Restoring Trust in Corporate Governance: The Six Essential Tasks of Boards of Directors and Business Leaders, Policy Brief, January 2010, available at [http://www.businessweek.com/pdfs/ced.pdf]

b Committee of Sponsoring Organizations of the Treadway Commission (COSO), Effective Enterprise Risk Oversight: The Role of the Board of Directors, September 2009, available at [http://www.coso.org/documents/COSOBoardsERM4pager-FINALRELEASEVERSION82409_001.pdf]

1 Sean Lyons, Corporate Defense Insights: Dispatches from the Frontline, February 2009, available at [http://papers.ssrn/sol3/papers.cfm?abstract_id=1337635]

Stakeholder Lines of Defense

To gain a measure of comfort that all critical activities are being appropriately addressed, stakeholders commonly rely on various lines of defense to operate as oversight layers within the organization. Internal lines of defense provide stakeholders with a degree of confidence that the organization is operating effectively and appropriately.

External lines of defense help safeguard their interests in the event that the organization fails in its obligations to them.

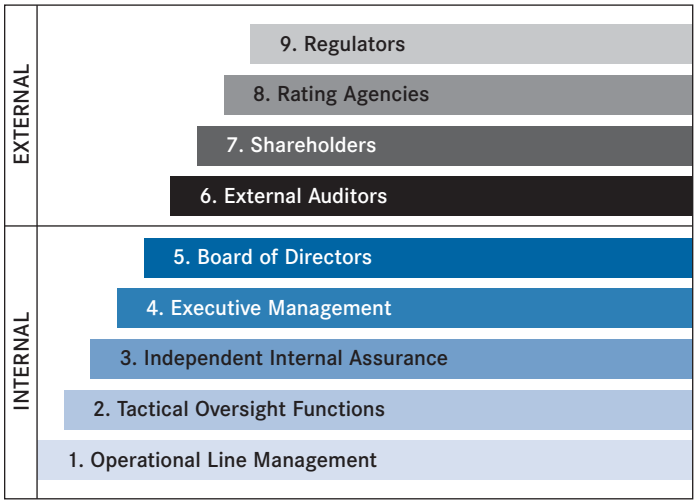
A number of internal and external lines of defense overlap in a hierarchy to help ensure that appropriate corporate oversight is in place at all levels within the organization and beyond. Each of these lines of defense has different oversight roles, responsibilities, and accountabilities, all of which are expected to make a valuable contribution to the overall oversight framework. Such an approach enables vertical and horizontal oversight of the organization's activities, providing the organization with both *defense-in-depth* and *defense-in-breath*[2] in the process.

Internal Lines of Defense and Their Oversight Roles

In the internal "lines of defense," each line has a responsibility for overseeing the layers beneath it. Conversely, accountability for oversight flows upward, as each line is accountable to the layer above it. Corporate defense is ultimately a team sport in which everyone in the organization is responsible for safeguarding their own turf, and, therefore, everyone is accountable to some extent in defending the diverse interests of stakeholders.

Figure 1

Stakeholder Lines of Defense



The Three Lines of Defense Model

The "Three Lines of Defense" model is a well established concept that has traditionally been deployed across different industries and sectors. The adapted model below represents a common internal approach to providing oversight and defending stakeholder interests. It recognizes operational line management, tactical oversight functions, and independent internal assurance as individual lines of defense. This is often regulators' preferred model when they review an organization's oversight structure. While this model recognizes the oversight roles of executive management and the board of directors, it does not specifically recognize these roles as additional lines of defense. From a broader stakeholder perspective, however, both roles represent additional lines of defense that safeguard their interests.

These lines of defense are in place in most organizations, but they often have developed organically rather than as part of a deliberately planned program.

Figure 2

Three Lines of Defense Model

THE BOARD
Strategic Framework

SENIOR MANAGEMENT
Strategy Execution & Performance

1st Line of Defense Culture & Environment	2nd Line of Defense Policy & Principles	3rd Line of Defense Independent Review
Operational Line Management	**Tactical Oversight Functions**	**Independent Assurance**
Monitor day-to-day practices	Monitor front line	Independent monitoring
Organizational structure – Business units – Divisions – Departments – Branches – Subsidiaries Activities – Front office – Middle office – Back office	Defense functions – Governance – Risk – Compliance – Intelligence – Security – Resilience – Controls – Assurance	Assurance functions – Audit committee – Internal audit Board committees – Risk committee – Governance committee – Board sub-committees

Sources: Adapted by author from various "Three Lines of Defense" frameworks including material from FERMA/ECIIA, KPMG, Booz & Co., PWC, and ACCA. FERMA/ECIAA, *Monitoring the effectiveness of internal control, internal audit and risk management systems: Guidance for boards and audit committees*, Guidance on the 8th EU Company Law Directive article 41, September 2010, [http://www.ferma.eu/portals/2/documents/press_releases/20100921-ecia-ferma-guidance-on-the-8th-eu-company-law-directive.pdf]

2 National Institute of Standards and Technology (NIST), Integrated Enterprise-wide Risk Management, Special Publication 800-39 – Final Public Draft, December 2010, available at [http://csrc.nist.gov/publications/drafts/800-39/draft-SP-39-FPD.pdf]

Operational Line Management

As the first line of defense, operational line management (OLM) oversees business operations in which transactions are entered, executed, valued, and recorded,[3] including the practices an organization uses for day-to-day business, both internally (front, middle, and back office) and externally (clients, supply chain, etc). OLM therefore has responsibility for the daily operations of staff, services, practices, mechanisms, processes, and systems. As the front line of defense, it has ultimate ownership, responsibility, and accountability for executing corporate defense activities on an ongoing basis within its sphere, in accordance with established protocols and consistent with the values of organization. OLM is responsible for ensuring there is an appropriate operational environment in place and that an operational culture is prevalent across the entire organization. This line of defense is accountable to the lines above it for ensuring that its practices are in accordance with the organization's policies.

OLM assigns responsibilities to individual line managers in specific processes, functions, or departments. Accordingly, each line manager plays a hands-on role in executing particular day-to-day practices. For instance, they identify, assess, and determine appropriate practices through the development of procedures. OLM is responsible for the delegation, supervision, and routine verification of the execution of procedures and should be in a position to provide other lines of defense with up-to-date information about key indicators (i.e., Key Performance Indicators (KPIs), Key Risk Indicators (KRIs) etc) associated with defense activities.

OLM's effectiveness depends on a number of issues, such as support from executive management and the board for corporate defense objectives. This will generally determine the organization's corporate defense maturity, its allocation of resources, and the extent to which these defense activities are embedded into day-to-day operations. The relationship between OLM and the tactical oversight functions (and the support received from these functions) will also have an impact on effectiveness, as will the commitment to education and training in this space.

Tactical Oversight

Tactical oversight functions, the second line of defense, use centralized functions (or competence centers) to address the tactical planning of individual corporate defense activities. Various defense-related functions (i.e., risk management, compliance, security, etc.) are established to provide oversight of frontline activities. These tactical oversight functions monitor, facilitate, and coordinate the consistent and effective operation of defense activities established by OLM. The tactical oversight role does not in any way diminish the duties and responsibilities of OLM for managing these activities in the front line.

Tactical supervision should help set implementation goals, as well as provide and review the framework for implementation, but it should also monitor and advise OLM.[4] The operational culture set by OLM is supported and enabled by this second line of defense through the clear allocation of roles, delegation of responsibilities, and the establishment and implementation of appropriate organizational infrastructure and technological architecture.

Effectiveness will very much depend on the level of collaboration between the different tactical oversight functions. The most effective approach "is a collaborative process that pulls together and leverages from all the various control functions within the organization."[5] Success depends on the functional and cross-functional maturity that exists within the organization. Depending on the governance structure, tactical oversight functions may be accountable directly to executive management, individual sub-committees of the board, or the board of directors. Independence from executive management will increase the authority and status of the tactical oversight function within the organization.

Independent Internal Assurance

The third line of defense, independent internal assurance, includes those functions that can provide the board (and to a lesser extent executive management) with an independent assessment of the corporate defense program's effectiveness. Oversight responsibilities include OLM activities and tactical oversight functions and, to varying degrees, the activities of the executive management function. This line of defense includes the board audit committee, the internal audit function, and other board committees and sub-committees (e.g. risk and governance committees) that can help provide an *independent* perspective on the overall corporate defense program.

3 KPMG in Thailand, Enterprise Risk Management: The 3 Lines of Defense, Audit Committee Forum Volume 1, October 2009, available at [http://www.kpmg.ru/russian/aci/_docs/mag_12_en.pdf]

4 Booz & Co., Bringing Back Best Practice in Risk Management: Banks' Three Lines of Defense, October 2008, available at [http://www.booz.com/media/uploads/Bringing-Back-Best-Practice-in-Risk-Management.pdf]

5 PricewaterhouseCoopers, Three lines of defence: How to take the burden out of compliance, Insurance Digest, available at [http://www.pwc.com/en_GX/gx/insurance/pdf/three_lines_of_defence.pdf]

The audit committee provides the board with an independent assessment of the effectiveness of the organization's internal control framework. This involves reviewing the adequacy of the internal control systems and monitoring their effectiveness, and reviewing internal audit and, where applicable, other defense systems (e.g., risk management).

The independence of the audit committee ideally requires "a committee of non-executive directors chaired by a senior independent director."[6] Internal audit plays an important role in assisting the audit committee and generally, there is at least a reasonable expectation that internal audit will identify weaknesses in the first and second lines of defense and recommend appropriate remedial action. As well as assessing their work, internal audit can also add value by serving as an in-house consultant, suggesting improvements in the structure and operation of the organization's defense program.

Effectiveness will be determined by the audit committee structure, the competence of their individual members, their terms of reference, and the quality of management information received, and other factors. For internal audit to act as an effective steward, it should not only have a good understanding of corporate defense disciplines, but also a deep understanding of the business itself. Ultimately, this third line must have the appropriate status and authority to empower it to enforce its recommendations.

Executive Management

The executive team appointed to run the business and provide assurance to the board of directors that the organization's objectives are being achieved represents the fourth line of stakeholder defense. Executive management is accountable to the board and has responsibility for discussing, debating, and agreeing upon corporate strategies for approval by the board.

The CEO is responsible for setting the "tone at the top" and assumes executive ownership for defending the organization, while at the same time supporting the executive management team and its responsibilities. Central to executive management's role is to provide leadership and direction to both OLM and the tactical oversight functions, while also prioritizing and optimizing the limited resources of the organization. Executive management also has responsibility for aligning an organization's corporate defense strategy with its broader business strategy and for converting this strategy into operational objectives.

Board Committees and Sub-Committees

The third line of defense, independent internal assurance, is supported by additional board committees and sub-committees that specifically provide oversight of individual defense activities, such as governance, risk management, and compliance. These committees provide additional assurance to the board and the audit committee through their specific areas of expertise.

Executive management effectiveness depends on attracting the right caliber of people to the management team and on the delegation, accountability, and transparency of their individual roles and responsibilities. These responsibilities may be disparate, with each C-suite member having responsibility in their own areas of influence. Or, individual C-suite members may have sole responsibility for specific corporate defense components as chief risk officer, chief compliance officer, chief intelligence officer, and so on. In other organizations, responsibility for all corporate defense activities may be the sole responsibility of one individual at the C-suite level.[7]

The Board of Directors

The stakeholders fifth (and final internal) line of defense is the elected board members who are responsible for overseeing the activities of the organization and are accountable to the shareholders for the organization's strategy and performance. The board exercises a supervisory role; responsibility for managing the organization is delegated to the executive management team. Board responsibility includes overseeing the activities of its standing committees (and subcommittees) and executive management. Other duties include helping executive management to formulate strategy, ensuring the availability of adequate financial resources, and approving appointments, policies, and budgets.

As the last custodians of the internal corporate oversight process, board members should constructively challenge executive management and provide independent views and contributions on all board matters. Executive directors, being board representatives from the executive management team, are not independent and therefore do not add an additional level of oversight at the board level.

6 Paul Burden, Three Lines of Defence Model, *ACCA IA Bulletin*, February 2008, available at [http://newsweaver.co.uk/accaiabulletin/e_article001026154.cfm?x=b11,0,w]

7 Sean Lyons, *Requirement for a Director of Corporate Defence in UK Banking Institutions*, available at [http://www.frc.org.uk/documents/pagemanager/frc/Responses_to_March_2009_combined_code_consultation/RISC%20International.pdf]

Division of Powers

The division of responsibilities for running the board and executive responsibility for running the company's business is often a complex issue that is addressed differently in different jurisdictions. In the United States and United Kingdom, this separation tends to be addressed through the segregation of duties between the unitary board and executive management. In certain European jurisdictions, however, there is a preference for additional segregation of governance and management duties through multiple boards, with supervisory boards having governance responsibility and management boards having management responsibility.

The board has responsibility for providing direction, strategic oversight, support for defense activities, and an oversight framework to address these obligations. The board should ultimately remain accountable to stakeholders for the quality of the organization's defense structure and capabilities. The board also has responsibility for reviewing and approving the corporate defense program on an ongoing basis, taking into consideration the organization's changing circumstances and the constantly mutating challenges it faces.

Effectiveness depends on the board's size, composition, and qualifications. The board should have the appropriate balance of skills, experience, independence, and knowledge. From a stakeholder perspective, separating the roles of chairman and CEO provides additional oversight independence and reduces many of the risks associated with a concentration of power with the CEO.

External Lines of Defense and Their Corporate Oversight Roles

Parties external to the organization also perform oversight functions and often provide information useful for carrying out the duties of the organization. While stakeholders may place a certain degree of reliance on these parties as additional lines of defense, they are not traditionally considered to be a part of the organization's own defense program. However, the oversight responsibility and accountability associated with these external parties does not necessarily follow the same linear pattern as outlined in the internal lines of defense.

External Auditors

External audit professionals who are independent of the organization can provide an unbiased and independent evaluation of the financial statements of that organization. The primary role of the external auditors, the sixth line of defense, is to express an opinion on whether an organization's financial statements are free of material misstatements. The auditor can therefore provide the organization's stakeholders (including shareholders, the board, and senior management) with a true and fair view of the organization's preparation of accounts.

During the audit process, an external auditor may review the organization's internal control procedures when assessing and evaluating the organization's overall internal controls. However, given the specific scope and objectives of their mission, the information gathered by external auditors is limited to financial reporting only. This process generally does not include assurance on the way the board or executive leaders are managing corporate defense activities—the second and third lines of defense separately provide assurance for these. Assessments and evaluations by the second and third lines of defense can provide significant information for the external auditors assessment of risks and controls affecting the financial statements.

The effectiveness of this sixth line of defense depends on the relationship between the external auditors and the organization that appoints them and pays them for their services. It will also be dependent on the agreement of the scope of work to be undertaken, the methodology adopted, and the audit coverage. The external audit team's experience, expertise, and knowledge of the organization are also factors.

External Expertise

From time to time individual lines of defense may employ the services of external experts to provide assurance or direction on non-audit activities (e.g. risk management, compliance, or security) or to address a specific corporate defense issue. Such external services are generally considered as a supplement or support to the efforts of that line of defense rather than as an additional line of defense.

Shareholders

Shareholders are a seventh line of defense when they participate to guard their investments in the organization as legal owners. While the shareholders cannot control the board directly, by acting together in the organization's general meetings (i.e. AGM, EGM etc) they can exert a level of control indirectly by appropriately exercising their rights.

Through "the constructive use of the AGM"[8] they are in a position to raise issues about the organization's strategy, the direction of the organization, and the performance of the board. The general meeting can only interfere with the board's exercise of power by altering the articles of association by special resolution. The right to vote on the appointment or removal of directors nominated by the board, the right to propose directors themselves, the right to propose shareholder resolutions, and to vote on proposals—are all fundamental to the shareholders role in corporate oversight.

This seventh line of defense depends on the active participation of the shareholders. Although not a primary oversight role, shareholder activism represents an opportunity for public scrutiny of the board. In recent times shareholder activists have made significant progress in gaining more information and in shifting power away from the corporate boards and management towards shareholders (particularly institutional investors) so that they can wield greater influence. By participating actively, shareholders can exert pressure on the board to be more transparent, thereby encouraging openness, integrity, and above all the accountability of the board, and in so doing, further enhance effective oversight.

Rating Agencies

Independent professional agencies and research analysts who specialize in analyzing, benchmarking, and rating organizations with their expertise in credit, corporate governance, risk management, and so on, represent another line of corporate defense. While these agencies are hired by the organization, the question of whether their accountability should be to market forces or to more stringent regulation has been the subject of much debate. In essence, the rating agency's role is to formulate and publish their neutral opinion through ratings, which serves as a yardstick to stakeholders. Ratings can reduce the level of work required by stakeholders (particularly investors) in evaluating an organization themselves.

The reputation and trustworthiness of the rating agency matters. To be rated by one of the more reputable rating agencies sends a signal that the organization takes the issue of its rating seriously. An organization can therefore expect to acquire a more favorable reputation among its stakeholders if they are willing to operate under a rating agency's ongoing scrutiny. Employing and collaborating with a highly regarded rating agency is one way to distinguish the organization from its competitors.

Similar to the sixth line of defense, the effectiveness of rating agencies will turn on whether the agency is "free from material conflicts of interest that might compromise the integrity of their analysis or advice."[9] It will also depend on both the quality of the review process itself and on the stakeholders' perception of the reputation of the rating agency. The rating agency's reputation is determined by its history and on the level of endorsements and certifications it publicly receives. While these ratings do provide a degree of assurance, stakeholders must also be aware that to a certain extent, the rating agency acts as an information intermediary between the organization and its stakeholders, and therefore it very much relies on the information provided by the organization in question.

There is now some anecdotal evidence that credit rating agencies (e.g. S&P) are placing more emphasis on corporate defense initiatives (e.g. ERM programs) than was previously the case. The rating agency's assessment may be affected by the quality of defense initiatives. Consequently ratings should increase the level of transparency surrounding the quality of corporate defense.

Regulators

Typically regulators are responsible for codifying and enforcing rules and regulations, and imposing supervision or oversight of a particular industry or service for the benefit of the public at large and in this capacity, they also provide protection for stakeholders. The government generally determines the level of regulation or deregulation deemed appropriate in a particular market, industry, sector, or profession, and is accountable to its electorate.

Where a market or profession is self-regulated, a non-government agency is typically established by representatives within that industry or profession that is accountable only to market forces. Government regulators oversee whether organizations comply with administrative law or other rules

8 Financial Reporting Council (FRC), The UK Corporate Governance Code, June 2010, available at [http://www.frc.org.uk/corporate/ukcgcode.cfm]

9 Organization for Economic Co-operation and Development (OECD), The Corporate Governance Lessons Learned from the Financial Crisis, February 2009, available at [http://www.oecd.org/dataoecd/32/1/42229620.pdf]

The Market and the Media

A number of additional players such as the market and the media (including social media) also contribute to corporate oversight and help ensure that stakeholder interests are being adequately defended. Commentators and analysts are increasingly providing stakeholders with additional channels of information.

that outlines specific requirements, restrictions, or guidelines, applicable within the mandated territory. The regulator's role might also involve licensing, supervision of entrants, enforcement of requirements, and discipline for misconduct. In certain cases regulators will perform specific investigations and ongoing reviews. The sanctions available to regulators can vary considerably and include the authorization to revoke a business license, the imposition of fines, or even the initiation of criminal proceedings against organizations and their officers.

This last line of defense is effective when the regulator is perceived to be competent, and has good standing within its industry or with the general public. The prevailing culture within the state or market, the appetite among the electorate (for either a passive or aggressive stance toward regulation), and whether the electorate can hold the government accountable for oversight are contributing factors as well.

Corporate Oversight Going Forward

Corporate stakeholder responsibility should take into account various stakeholder groups, including shareholders, employees, customers, suppliers, special interest groups, communities, regulators, politicians, and, ultimately, society. Consequently, a comprehensive corporate oversight framework should be multi-faceted to safeguard the diverse interests and varied expectations of all stakeholders. Increasingly, stakeholders are demanding oversight that safeguards a multitude of their interests, be they financial, economic, social, or environmental. Such an inclusive approach should include an appreciation of the symbiotic relationship that exists between business, society, and nature. Organizations should understand the complexity of this interconnectedness to fulfill their social responsibilities.

A holistic focus that includes the various lines of defense approach helps provide different stakeholders with the comfort that their interests are safeguarded, if implemented appropriately. A lines-of-defense framework provides stakeholders with a comprehensive system of "checks and balances." The existence of such an integrated framework means that stakeholders can reasonably rely on it to ensure that the organization is fulfilling its fiduciary duties, legal obligations, and moral responsibilities, while creating durable value and sustainable economic performance in the process.

For this approach to operate effectively, however, each line of defense must play its part both individually and collectively—fulfilling its oversight duties within a holistic framework. Accordingly, each line of defense collaborates with and challenges the other (complimentary yet antagonistic) lines of defense, as it acts in its own enlightened self-interest. Enhanced cooperation and communication between these lines of defense should be facilitated by better interaction between stakeholders through regular dialogue which is based on mutual understanding of the organization's objectives. This, however, must be achieved without allowing respective responsibilities or accountabilities to become blurred in the process.

To strengthen corporate defense capabilities, organizations should consider fortifying the second line of defense, which provides the critical link between operational line management and executive management. For many organizations, this is still perhaps the weakest link in the chain. Unfortunately, in many organizations, the defense activities at this layer are operating in a silo; they are not in alignment with other lines, but rather, operate in isolation, with little or no interaction, sharing of information, or collaboration. The activities of an effective second line of defense must be managed in a coordinated and integrated manner.[10]

Each of the other lines of defense requires differing degrees of fortification, but this perhaps has as much to do with best practices rather than any radical makeover. The goal is to reach a more effective balance between the spirit of guidelines based on principle and the interpretation of guidelines that are legal or more prescriptive.

10 Sean Lyons, *Optimized Corporate Defense Programs: A 5 Step Roadmap*, EDP Audit Controls and Security (EDPACS) Newsletter, July 2009, available at [http://papers.ssrn/sol3/papers.cfm?abstract_id=1557743]

Appendix

Examples of Defense-Related Activities

Governance

Culture/Environment
Ethics & Integrity
Stakeholder Relations
Design/Structure
Strategy/Planning/Organization
Corporate Responsibility
Accountability
Framework
Methodology

Risk

Strategic Risk
Macro Economic Risk
Geographic Risk
Business Sector Risk
Reputation Risk
Operational Risk
Credit Risk
Market Risk
Enterprise Risk

Compliance

Regulatory Compliance
Legal Compliance
Workplace Compliance
Industry Codes
Best Practice Guidelines
Internal Standards

Intelligence

Business Intelligence (B.I.)
– Operational Intelligence
– Market Intelligence
– Competitive Intelligence

Knowledge Management
– Content Management
– Record Management
– Document Management
– Filing/Storage/Archiving Management

Communication
– Monitoring & Reporting
– Telecommunications

Security

Physical Security
– Premises Security
– People Security
– Materials Security
– Facility Security
– Operations Security

Information Security
– Endpoint Security
– Application Security
– Operating System Security
– Database Security
– Network Security
– Gateway Security

Resilience

Incident Response
Emergency Operations
Crisis Management
Disaster Recovery
Contingency Planning
Continuity Management
Interruption Protection
Health & Safety
Insurance

Controls

Internal Controls
Financial Controls
Operational/Processing Controls
Supervisory Controls
Compliance Controls
Security Controls
Preventative/Detective Controls
Primary/Compensating Controls

Assurance

Inspection Review
Internal / External Audit
Regulator Review
Rating Agency Review
Standards Certification
Self Assessment Review
Due Diligence Review
Fraud Examination
Forensic Investigation
Litigation Support

About the Author

Sean Lyons is the principal of Risk Intelligence Security Control (R.I.S.C.) International (Ireland) and a recognized corporate defense strategist. He is published internationally and has lectured and spoken at seminars and conferences in both Europe and North America. His contributions have been acknowledged in the *Walker Review of Corporate Governance in UK Banks and Other Financial Institutions*, the Financial Reporting Council (FRC)'s *Review of the Effectiveness of the Combined Code* and the International Corporate Governance Network (ICGN)'s *ICGN Corporate Risk Oversight Guidelines*. In 2010 Sean was shortlisted as a finalist in the GRC MVP 2009 Awards organized by US based GRC Group (SOX Institute) co-chaired by Senator Paul Sarbanes and Congressman Michael Oxley.

About The Conference Board

The Conference Board is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance *and* better serve society. The Conference Board is a non-advocacy, not-for-profit entity, holding 501 (c) (3) tax-exempt status in the United States.

Related Resources from The Conference Board

Reports

SEC Enforcement Actions against Outside Directors Offer Reminder for Boards
Report Number:DN-V3N12-11,June 2011

Corporate Governance and Business Preparedness
Report Number:DHS1-11-RR, March 2011

Preparedness in the Private Sector—2010
Report Number: R-1439-08-RR, October 2010

Security as a Critical Component of Corporate Defense
Report Number: A-0330-10-EA, July 2010

Risk and Security in Corporate Supply Chain Networks
Report Number: A-0329-10-EA, June 2010

Councils

Business Continuity & Crisis Management Council
Corporate Security Network
Council of Chief Privacy Officers
Council of Corporate Security Executives
Digital Strategy Council
Environment, Health and Safety Legal Council
European Council on Environment and Product Stewardship
European Council on Health and Safety
European Council on Strategic Risk Management
Strategic Risk Management Council

For more information on this report, please contact:
Carol Courter at +1 212 339 0232 or carol.courter@conferenceboard.org

THE CONFERENCE BOARD, INC. www.conferenceboard.org
AMERICAS +1 212 759 0900 / customer.service@conferenceboard.org
ASIA-PACIFIC +65 6325 3121 / service.ap@conferenceboard.org
EUROPE/AFRICA/MIDDLE EAST +32 2 675 54 05 / brussels@conferenceboard.org
SOUTH ASIA +91 22 23051402 / admin.southasia@conferenceboard.org

THE CONFERENCE BOARD OF CANADA +1 613 526 3280 / www.conferenceboard.ca