CORPORATE DEFENSE INSIGHTS

Dispatches from the Front Line

Expert commentators share their insights with Sean Lyons

CORPORATE DEFENSE INSIGHTS

Dispatches from the Front Line

A Q&A series produced by Sean Lyons
June – December 2008

CONTENTS

PREFACE

By Sean Lyons

About Corporate Defense

The term "Corporate Defense" has been in use over a long period of time, has a wide range of common usage, and has been used in many different contexts. As a result while it is perhaps intuitively understood, its specific meaning can differ from person to person and indeed from organization to organization. Its precise definition can also vary depending on the circumstances in which it is applied. As a result its role and purpose appears not to be fully understood or indeed its worth not fully appreciated. All too often it is considered in a very narrow focus, as discussions about the topic of corporate defense with senior executives will very often be restricted to corporate legal or security issues. Examples of other activities which also use this term include areas such as resilience, governance, risk, compliance, audit and investigations. The term is even used when defending against hostile takeovers. Each of these usages does however share the common high level objective, that of defending the organization, and therefore could be said to represent different lines of defense, or multiple layers of defense. Corporate defense therefore in its broadest sense could be said to represent an organization's collective program for self defense.

From this perspective defending an organization requires much more than simply concentrating on security or litigation threats. To help ensure corporate survival contemporary corporate defense requires a far more comprehensive brief as the challenge of enterprise-wide defense is to continually defend an organization from a multitude of potential threats and hazards. Consequently the task of defending the organization is not a once off activity or a point in time assignment. The challenge of defending against potential threats and hazards is without end, it is a constantly evolving process which requires ongoing vigilance and an iterative approach, in order to ensure constant revision and continuous improvement. Defending an organization includes defending the company name and all its stakeholders. This includes defending the shareholders, the business partners, and of course its clients. Defending the company name also means defending its people, both management and staff. Corporate defense also includes focusing on stakeholder's welfare and well-being, by focusing on them as human beings and not just focusing on numbers, quarter end profits or other bottom line financials. Therefore the defense of the organization is an extremely responsible station, as there are a large number of stakeholders who rely on this program to operate in an effective manner in order to defend their diverse interests.

Currently most organizations already implement a variety of what could be best described as corporate defense related activities, in order to address the potential dangers, threats and hazards they are faced with. Each of these defense activities represents an important link in the overall defense chain and all play an important role in order to help organizations defend themselves against both internal and external threats, and to work

together so that they are functioning in unison and thereby collectively protecting the organization from potential hazards.

Achieving successful corporate defense therefore requires a strategic outlook in order to ensure that these activities are in fact operating in unison, and this requires a level of collaboration, integration and alignment among a number of existing disciplines, all of which need to be managed and coordinated in a coherent and strategic manner. It should be noted that from a strategic perspective each of these defense related activities are increasingly inter-linked and inter-connected, leading more and more commentators to now acknowledge the symbiotic nature of these critical inter-dependencies. Each of the inter-actions between these activities can potentially have either a positive or negative impact on any one of the other activities. With this in mind organizations need to increasingly consider the possible cascade of consequences which can arise from these interactions, not only direct 1st order consequences but indirect 2nd and 3rd order consequences which can occur further down the line. Common sense alone should therefore dictate that the requirement for a progressive and proactive corporate defense program is not just a nicety it is a necessity, a necessity that should be demanded by all the stakeholders in the organization. Logically this can be best achieved by a coordinated approach to integrating and aligning the management of an organization's defense related activities across the entire enterprise.

About the Series

The series "Corporate Defense Insights: Dispatches from the Front Line" focuses on corporate defense as an umbrella term whereby the term corporate defense is used to represent the structures, mechanisms, processes and systems which form the component parts of an organization's program of self defense. This insight series places the spotlight on the critical components which make-up an organization's program for self-defense (e.g. Governance, Risk Management, Compliance, Intelligence, Security, Resilience, Controls and Assurance etc). The objective of including each of these activities in this series is to generate an awareness of the developments occurring in these areas and perhaps bring these activities to the attention of a wider audience. Each of the topics featured in this series have an important role to play in defending an organization from multiple threats and hazards. By examining these activities by way of a Q&A format it is hoped that the resulting dialogue will help readers to better gain an overview understanding, and perhaps a high level appreciation, of each of these activities and their critical roles in corporate defense.

The focus of this series is on gaining expert commentary and analysis in terms of recent trends, predictive views and opinions relating to future progress and developments in these areas. It features individual Q&A sessions with selected individuals from around the globe who were chosen as recognized and/or emerging commentators in their respective fields. Each of these commentators have specialist credentials in their particular area of excellence and by participating in this series have kindly agreed to share their experience and expertise on their featured activity with us. Commentators were invited to participate in only one session which primarily focuses on the specific defense related area which that commentator has a unique insight. Each Q&A session

focuses on a specific defense related activity and the associated commentator provides the audience with their views and opinions in this area. Please also bear in mind that in this series the focus is on each of these activities from a corporate defense perspective which means not just focusing on the mitigation of dangers, risks, threats and hazards but also focusing on overall performance which includes the provision of any additional added value provided by the activity in question, as all positive and proactive contributions to an organization's performance should also be considered to be an important part in helping to defend the varied interests of its stakeholders.

Acknowledgements
I would like to especially acknowledge the contributions made by each and every one of the commentators who have taken the time out of their busy schedules to participate in this series and to share their valuable insights with us. I would also like to thank Igor Lamsor the editor at the RiskCenter for his enthusiastic backing of this project from its inception and the other staff at the RiskCenter who helped to publish these interviews throughout the series. I would also like to thank all of those other individuals who although they may not have been available to participate in the series itself were kind enough to offer their support for and advise on this initiative.

GOVERNANCE

Richard M. Steinberg

CEO of Steinberg Governance Advisors, Inc.

About Richard M. Steinberg

Richard Steinberg is a nationally recognized expert in corporate governance, advising boards of directors and senior managements on a wide range of governance issues. He has long been a leader in shaping governance standards and practices, serving as chair or member of many committees, task forces and prestigious boards and councils. Steinberg previously was a senior partner at PricewaterhouseCoopers, where he served as the firm's corporate governance practice leader. He also was a founder of the firm's risk management and control consulting practice, and served as its global leader. A sought-after speaker, Steinberg has authored numerous highly acclaimed reports, including *Corporate Governance and the Board—What Works Best* and its companion, *Audit Committee Effectiveness—What Works Best*. As lead project partner, Steinberg formulated and wrote the Committee of Sponsoring Organizations of the Treadway Commission (COSO) *Internal Control -- Integrated Framework*, which is the global standard of internal control, and recognized by the SEC and Public Company Accounting Oversight Board for corporate use in meeting Sarbanes-Oxley's reporting requirements. He played a similar role in the COSO's *Enterprise Risk Management—Integrated Framework*. Rick Steinberg is also widely published on governance issues, authoring books, monographs and articles in leading journals, and is frequently quoted in the financial press, including *BusinessWeek*, *Fortune* magazine, *The Wall Street Journal*, *Investors Business Daily*, *Reuters News*, and the *Financial Times*. Steinberg is a monthly columnist for *Compliance Week*, and is an active speaker at major business and professional conferences. He has been featured on CNBC's *Morning Call* and Bloomberg TV's *On the Markets* and *The Bloomberg Report*, and has guest lectured at such leading business schools as Auburn, Columbia, Delaware, Duke, MIT and UCLA. He has served as a member of the Conference Board's Global Corporate Governance Research Center Advisory Board, he is a member of the Open Compliance and Ethics Group Executive Advisory Panel, and is chair or a member of several corporate advisory boards. He is also co-founder of the Directors' College, presented by PricewaterhouseCoopers and the University of Delaware Center for Corporate Governance.

As founder and CEO of Steinberg Governance Advisors, Inc., based in Westport, Connecticut, Rick advises boards of directors of major multinational, large and middle market companies on board responsibilities and governance best practices, and senior managements on governance, risk management, control and compliance.

GOVERNANCE AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line internationally recognized corporate governance expert Richard M. Steinberg, CEO of Steinberg Governance Advisors, Inc., shares his insights with Sean Lyons on the critical relevance of sound corporate governance and its role in corporate defense.

Sean Lyons: Governance is considered by some to be a somewhat abstract term. In its broadest sense it could be said to represent how an organization is directed and controlled, all the way from the boardroom to the shop-floor. Is their a particular description of governance which you feel best describes the term itself?

Rick Steinberg: Yes, though let's begin with the term "corporate governance". In my mind corporate governance is best described as the allocation of power between the board, management, and shareholders. This definition, which I believe can be traced to the Dey Commission report of the 1990s, appropriately places emphasis on the board of directors as the central point in governing a company, and its relationship with management and the company's owners. Of course, the term "governance" often is used much more widely, getting into what management does to run a company. We now see such terms as IT governance and project governance – including, as your question correctly suggests, even going to the level of the shop-floor. My view is that the term "governance" used in context of a business organization is best preserved for the workings of the board of directors, while any number of other "management" related terms are appropriately used for what a company's managers do in carrying out their responsibilities.

Sean Lyons: Could you please describe what you deem to be the core objectives of good corporate governance from an organization's perspective?

Rick Steinberg: Put simply, good corporate governance comes down to the board providing effective advice, counsel and where necessary direction to the CEO and senior management team – along with carrying out its required monitoring activities. From a legal perspective, this involves directors carrying out their duties of loyalty and care, and acting in good faith. But this really is a 40,000 foot level perspective. Learning about the nuts and bolts of directors' roles and responsibilities comes from board experience and any number of books, reports, journals, and directors "colleges" and conferences. A good starting point would be *Corporate Governance and the Board—What Works Best,"* which I had the privilege of authoring when I ran the corporate governance advisory practice at PricewaterhouseCoopers. While published some years ago, it continues to be relevant today and looked to as a key source of effective board protocols and practices.

Sean Lyons: Corporate scandals over the last decade have meant increased scrutiny in terms of corporate integrity, ethics, and accountability. This has also resulted in an expectation of higher standards in relation to corporate governance. What in your view have been the most significant developments in corporate governance practices in recent years as a consequence of these scandals?

Rick Steinberg: Perhaps most significant in the current environment is the questioning on a wide basis of whether directors truly have been doing their job. When we look at the recent failures of financial institutions with platinum brands that now are defunct or otherwise brought to their knees, shareholders and others are asking whether boards understood the risks those organizations were taking. One key board responsibility is to oversee what management is doing to identify, analyze, and manage risk, and understanding to what extent agreed limitations on the company's risk appetite are being met. With the recent scandals fresh in mind, directors of both financial and non-financial companies alike are looking more closely at how risks their companies face are being dealt with. Regarding integrity and ethics, scandals often provide impetus for boards to take the necessary steps to become comfortable that management has set the right "tone at the top," through not only words but also actions that permeate the culture of the organization. Boards are reconsidering whether they are sufficiently involved and knowledgeable not only whether an appropriate code of conduct and related support systems are in place, but also how the company deals with customers, suppliers, business partners and others in carrying out its business activities. And of course, with the current credit crunch and badly damaged economy, directors are appropriately focusing like a laser on actions to be taken to maintain revenue and profitability goals.

Sean Lyons: What do you believe are the main characteristics and critical areas which organizations should primarily focus on in terms of implementing sound governance practices?

Rick Steinberg: We've on touched on two – risk management and a corporate culture embracing integrity and ethical values. Other areas on which boards need to focus include making sure the company has the right strategy in place to meet today's challenges, as well as a sound implementation plan and the people and processes in place for effective execution. Also, ensuring that performance measures align with both the strategy and compensation metrics for the CEO and top management team. Compensation today is a lightening rod for institutional investors, and should be in line with long term performance. An area too often overlooked is having a sound plan for CEO succession – both in an emergency and longer term – and being prepared in advance for a crisis situation that may suddenly arise. Communications with shareholders, including transparency in financial reports and maintaining an open channel for major shareholders, also require attention.

Sean Lyons: Governance structures need to address an organization's multidimensional complexity, not only in terms of vertical and horizontal structures but also the alignment of multi-level objectives (strategic, tactical and operational). To be effective governance structures therefore need to be flexible and adaptable enough to address the continuously evolving environment. In your opinion, how is this challenge best addressed?

Rick Steinberg: Experience shows that organizations that have established truly effective enterprise risk management processes are positioned to see what's coming down the pike, and move proactively to both head off major problems and take advantage of opportunities – before competitors get there first. Unfortunately, while many companies

speak about ERM processes, often their risk management really is ad hoc and limited. So, in addition to embedding risk identification throughout the company, it's necessary for managers to ensure emerging risks are appropriately evaluated and timely actions taken to manage the risks to stay ahead of events. That means reorganizing units, processes, and personnel where necessary, and putting corporate resources where they'll provide the best results.

Sean Lyons: There are a number of governance best practice frameworks available to choose from (e.g. OECD, UK combined code, COBIT, ITIL etc). Are there any particular frameworks or best practices which you consider to be most suitable for organizations when considering the implementation of a program for governance?

Rick Steinberg: As you say, there are many frameworks out there, each serving a somewhat different purpose. Some are broad based whereas others focus on more narrow areas. My advice is to recognize the positives of what's available, and selectively draw from what's most useful to one's organization in developing a structure and supporting processes. It's important to begin with the corporate mission and strategy, as everything must flow from and support them. At the board level, I suggest focusing on guidelines that, while covering the basic fiduciary responsibilities, emphasize where and how the board can add real value to the organization to grow share value. At the management level, I've seen effective use of *Enterprise Risk Management—Integrated Framework*, issued by the Committee of Sponsoring Organizations of the Treadway Commission. I'm somewhat biased here, having led the report's development, but its use as a framework has proved highly effective for many organizations.

Sean Lyons: The responsibility for implementing, managing and monitoring governance practices can typically rest with the Board, the Audit Committee or even the Company Secretary etc. Where do you think responsibility for ensuring that the organization has a comprehensive and integrated governance framework in place should ideally be positioned within an organization's corporate structure? Why?

Rick Steinberg: At the board level, responsibility rests with the full board. With that said, many responsibilities can be and are best dealt with at the committee level, with many boards having established nominating/governance, compensation and audit committees. Some also have finance and risk committees, taking some of the load off of otherwise weighed down audit committees, and this usually proves effective. Certainly the corporate secretary can be an important support system, making the work of the board that much more effective and efficient. In most American companies the chief executive is a director, usually the board chair, and he or she plays a central role in governance. Any perceived conflicting responsibilities, sometimes real, can be dealt with effectively by a strong lead director. And the CEO of course has responsibility for establishing management structures to carry out the agreed strategy in light of his/her management philosophy and style.

Sean Lyons: The business value and benefits of sound governance practices can be difficult to measure and assess in strictly quantitative terms. What advice would you give

to those with responsibility for putting forward the business case for sound governance practices in order to secure organizational buy-in and long term sustainable commitment?

Rick Steinberg: Many researchers have tried to provide clear linkage between "good" governance and increased share value, but thus far I've not seen any that successfully do so. There are firms providing governance "ratings," but most if not all the underlying data come from public information. Unless and until an evaluator is able to get inside the boardroom and C-suite, it's simply not possible to provide an adequate assessment. On the other hand, there is sufficient anecdotal information and first hand experience working with boards and senior managements evidencing that sound governance practices indeed do drive positive performance. One word of warning: beware of jumping on the bandwagon of what sometimes are called "best practices." So called best practices often portray what many boards do, rather than what a handful of the best boards are doing and others would do well to learn from.

Sean Lyons: You mentioned how an organization's culture can have a significant impact on the enterprise. What in your view is the most appropriate approach to ensuring that governance becomes pervasive throughout the enterprise and becomes embedded into the corporate culture?

Rick Steinberg: We know that an organization's culture is shaped by management's philosophy and operating style, the company's organizational structure, and its policies, processes and people. The culture is established over the history of a company, and has a profound effect on how it responds to internal and external events. When a new chief executive or senior management team arrives and seeks to change the culture, they usually find that it takes much effort and time – akin to turning around a battle ship. There are, however, exceptions to that general rule. I've worked with a number of chief executives who have been successful in changing their organization's culture rather quickly, in each case not so much with advance planning but rather reacting to troubling circumstances requiring a challenging executive decision. The actions taken by these chief executives – especially where integrity and ethical values were on the table – have had a significant positive effects on culture. These decisions made behind closed doors to "do the right thing," while in each case sacrificing short term gains, in short order became known throughout the management ranks and created significant long term benefits.

Sean Lyons: Corporate governance needs to address the multi-level requirements (and perhaps the often conflicting interests) of the various stakeholders of the organization (i.e. shareholders, clients, business partners, management and staff etc). What in your opinion is the best approach to addressing and balancing stakeholder expectations?

Rick Steinberg: A board's responsibility is to serve the interests of the company and its shareholders, centered on enhancing long term share value. My experience is that successful managers find common ground developing "win-win" environments, where working effectively with suppliers, customers, staff and others provides the best results. In one example, I worked with a senior executive who decided on a course of action to make the unit's people the highest paid in the industry. In contrast to competitors

working to keep compensation down, the objective here was to recruit and retain the best talent to best develop products and serve customers, with the result an outstanding and long-lasting success. Regarding relationships with shareholders, I believe it's most useful and mutually beneficial to recognize that the board, not shareholders, has the responsibility to oversee management. Institutional and other investors are looking to expand their influence, especially on CEO compensation through "say on pay" initiatives or withholding votes from compensation committee members. Shareholders indeed are gaining influence in this area, looking at compensation not only for its monetary effect but also as a "window" on the workings of the board. Shareholders have the right to take these actions, and forward looking boards are establishing channels for communicating with shareholders. There are positive overtones here, and we can see this trend continuing. My only warning is that anyone – shareholders included – trying to make business decisions from outside the company usually will find they can't and don't have the needed information. My advice is, yes, improve communication, but for the most part let management manage, let the board carry out its oversight responsibilities, and let shareholders reap the benefits.

Sean Lyons: Other defense related activities such as risk, compliance, intelligence, security, resilience, controls and assurance, all increasingly require good governance in order to operate effectively. In your opinion, to what extent does governance need to become integrated with these processes and why?

Rick Steinberg: As noted, these are management's responsibilities, and must be subject to oversight at the board level. Management must establish appropriate business processes to deal with risk, ensure compliance, secure its information and resources, and the like, and provide sufficient information to the board so it can become comfortable with these activities. By the same token, the CEO needs to be sure his/her direct reports are taking the necessary actions to manage effectively in their areas of responsibility. Importantly, I advise my clients to be careful of placing too much responsibility on a chief compliance officer, chief risk officer, general counsel, or chief audit executive. Those staff functions can and should provide important support and monitoring, but experience clearly shows that unless line leadership accepts responsibility for risk, compliance and related activities, there are likely to be problems.

Sean Lyons: In your view where does the role of governance currently fit into the broader concept of an organization's program for self-defense and how do you see its role developing going forward?

Rick Steinberg: Effective governance at the board level, and what's done throughout the management structure, is critical to defend against a broad range of challenges and threats. Processes and related activities at all levels must be established and executed effectively to avoid harm. But just as important is ensuring the organization is well positioned to react positively to potential events with upside impact, in order to take advantage to changes in the environment and marketplace. It's not a case of "either-or," but rather both. That's how successful companies avoid the downside and achieve their goals to grow the business and add share value.

Sean Lyons: I know you bring vast experience working with boards of directors and senior managements on a broad range of governance matters. Would you share with our readers how they can get in touch with you?

Rick Steinberg: Of course. In my "spare time" I write a monthly column for the governance and compliance journal *Compliance Week*, and readers can contact me at rms@complianceweek.com.

Originally published at the RiskCenter (www.riskcenter.com) *on the 22nd December 2008*

RISK MANAGEMENT

Dr. David M. Rowe

Director of the Professional Risk Managers' International Association (PRMIA)

About Dr. David M. Rowe

David Rowe currently serves as a director of the Professional Risk Managers' International Association (PRMIA) until his term expires in 2010. As Group EVP of risk management for SunGard, he is responsible for the strategic direction of SunGard's solutions for risk management, having joined SunGard in July of 1999. In this role he advises operating units on risk management functionality and development priorities in their software applications. He holds a Ph.D. in econometrics and finance from the University of Pennsylvania, an MBA in finance with a concentration in money and banking from the Wharton Graduate School of Business Administration and a BA in economics with distinction from Carleton College. Dr. Rowe appears frequently at industry risk management conferences and writes a monthly column for Risk Magazine. Prior to joining SunGard, Dr. Rowe spent more than 25 years in the economic forecasting and banking industry, most recently as senior vice president of the Risk Management Information group at Bank of America in San Francisco.

The Professional Risk Managers' International Association (PRMIA)

The Professional Risk Managers' International Association (PRMIA) was founded in 2002 as a non-profit, member-led association of risk professionals dedicated to the advancement of the profession worldwide through the free exchange of ideas about risk management.

For more information visit: **www.prmia.org**

RISK MANAGEMENT AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Dr. David M. Rowe, Director of the Professional Risk Managers' International Association (PRMIA) shares his insights on risk management and its role in corporate defense with Sean Lyons.

Sean Lyons: The term risk management is generally associated with identifying, measuring and managing risk. Is there a particular definition of risk management which you feel best describes its mission or purpose?

David Rowe: I view risk management as the process of assuring that risk vs. return decisions are made on a well informed basis with as much insight as possible into possible adverse events. It is important for risk managers to recognize that the goal is not to eliminate risk but rather to assist their organizations in judging whether prospective returns warrant assuming the risks involved.

Sean Lyons: Over the years you have no doubt seen many different trends occurring in the area of risk management in general, what in your opinion have been the most significant developments in risk management over the last 5-10 years and why?

David Rowe: Advances in computing power have both enabled risk management and presented an ever growing challenge. The challenge arises from the growth in product complexity and volumes that these technological advances have made possible. This is combined with the inescapable reality that risk analysis inherently demands far greater computing power than front-office pricing and processing. By its nature, risk management always must react to innovations on the business side of an organization, creating an inevitable lag in the ability to deploy comprehensive assessments of the risks. The key challenge is to manage the gap between ideal risk management information functionality and the reality of risk systems actually in place and operational to assure it does not grow dangerously large.

Sean Lyons: Generally speaking how important is risk management to an organization and how can an organization hope to contribute to enhanced profitability by implementing a comprehensive risk management program?

David Rowe: Risk management is vital to long-term success of almost any organization. The value of a firm is driven largely by two fundamental factors, the market's expected growth in a firm's earnings and the discount rate it applies to those future earnings. Risk management's role is to enhance long-term value by reducing the risk-based discount rate applied by the market to its expectation of a firm's future earnings. The task of the business side of an organization is primarily to raise the expected growth in earnings (subject to a constraint on risk.)

Sean Lyons: The role of the Chief Risk Officer (CRO) is a somewhat evolving role within the corporate world. In your view how has this role evolved to date and what can we expect to see in the future?

David Rowe: I expect the roles of the CRO to grow to encompass broader responsibility for strategic and business risk in addition to narrower risk measurement, monitoring and management functions. A primary problem during the sub-prime crisis was a failure of organizations to think about risk in a macro strategic fashion. Too much reliance was placed on technical quantitative modeling without questioning the underlying data and assumptions involved.

Sean Lyons: Effective risk management requires investment, however tangible return on risk management investment is not always that obvious to those involved in the business side of the organization. Firstly, what advice would you give to CRO's when preparing to put forward the business case for risk management within their organization? Secondly, what in your view is the most critical aspect of presenting the business case for risk management to the stakeholders?

David Rowe: I think both issues relate to my earlier comment. By building a sound risk assessment process, based on both technical quantitative analysis blended with judgmental inputs from a wide range of sources, a firm can gain a reputation for avoiding the most damaging mishaps. This in turn lowers the market rate of discount and raises the share price for any given level of earnings. Emphasizing this to the shareholders is part of reaping the benefits of sound risk management.

Sean Lyons: What do you consider to be the biggest obstacles or challenges currently facing those responsible for risk management in terms of getting business buy-in on the importance of risk management to an organization?

David Rowe: A major challenge is neutralizing the tendency to overvalue a dollar of profit coming in the front door relative to a dollar of profit prevented from leaving the back door. In effect, profit that is easy to see in the accounting statements tends to be given greater weight than less explicitly visible achievements in loss prevention. Balancing these two contributions fairly is a constant battle and always will be.

Sean Lyons: Most organizations are faced with the continuous interaction of multiple risks and an uncertain cascade of consequences resulting from this interaction. To what extent do you believe that is it really possible to accurately predict probable outcomes under such complicated circumstances?

David Rowe: Accurate prediction is a pipe dream. Management of all kinds is a constant challenge of making decisions under uncertainly. The trick is to have as much or more information and insight in making these decisions than the competition. It also requires thinking holistically so that some thought has been given to how certain events might play out in practice. This enhances the ability to respond quicker to an emerging crisis, since some of its implications will have been reasoned out in advance. This is what Nassim Nicholas Taleb calls converting Black Swans into Gray Swans.

Sean Lyons: Traditionally the management of risks was classified into credit, market or operational risk however we are now seeing the emergence of risk specialists in the areas

of financial risk, governance risk, compliance risk and security risk etc. At the same time we are also seeing the development of high level approaches to risk management which include the use of such terms as corporate risk management, strategic risk management, enterprise risk management and integrated risk management. What are your views on these latest developments?

David Rowe: Both perspectives are necessary. Specific areas of risk require a wide range of detailed idiosyncratic indicators that are appropriate to issues of a particular type. The challenge at the enterprise level is to capture how these risks may interact if things go wrong. For example, a security breach that results in the loss of personal details or revelation of deceptive sales practices in a single business area can have reputational implications that go well beyond the immediate impact of a single incident. Often it is these secondary ramifications that justify the cost and effort to minimize risk in a given detailed area. Integrated risk management should not mean trying to distill risk down into some single summary metric. Rather it is the continuous process of evaluating how specific risks in different areas may accumulate or reinforce each other in especially damaging ways.

Sean Lyons: There is certainly no shortage worldwide of associations representing risk management as a specialist area. Do you view the existence of so many organizations in a positive or negative light, and is there now a requirement to get these organizations to come together in some sort of forum to collectively represent risk management internationally?

David Rowe: The existence of multiple risk management organizations is a double edged sword. On the one hand failure to speak with one voice can dilute the impact of risk professionals in debates over appropriate public policy. On the other hand, competition can be valuable in encouraging multiple organizations to improve their products and services to the procession. In the end, however, it is not a simple matter of choosing one model or the other. Risk professionals, like all human beings, are prone to independent thinking and tend to resist acquiescing to institutional views and policies with which they disagree. Risk is such a pervasive and heterogeneous aspect of the human condition that the existence of multiple organizations to represent risk managers is inevitable.

Sean Lyons: The financial risk management metrics used by many organizations tend to focus primarily on quantitative aspects which are more easily measured? How can the more qualitative aspects of corporate social responsibilities which address human issues such the health, safety, welfare and wellbeing of stakeholders be best addressed from a risk management perspective?

David Rowe: To a degree I see risk management experiencing an evolution that I observed over thirty years ago in economic forecasting. At one stage there was great optimism among some economists that behavioral relationships could be defined and modeled successfully with mainly quantitative tools. Over time it became clear that the world was too complicated for this vision to be realized. In the end a consensus emerged that blended econometric modeling with seasoned judgment. The practice of risk

management was rapidly evolving toward this same messy, but necessary, blend of quantitative analysis and judgment when the subprime mortgage crisis struck. I think the painful consequences of this experience will serve to accelerate that transition. In the end, risk management needs to involve a process that regularly incorporates feedback from macroeconomists, country risk specialists, lawyers, accountants, operations managers and others into a continuing dialog around large emerging risk issues. Orchestrating this dialog will be a central responsibility of the Chief Risk Officer.

Sean Lyons: Risk management involves considering risk implications in other defense related activities such as governance, compliance, intelligence, security, resilience, controls and assurance. In your view, to what extent is risk management becoming embedded into the management of these processes?

David Rowe: I feel sure that progress in embedding risk management in these diverse areas differs widely across organizations. Making such risk awareness part of a corporation's culture is Sisyphean task of immense proportions. Even interim success will only be possible if the Board, the CEO and the senior management team are actively and wholeheartedly insistent on its importance. Risk management's worst enemy is a senior management that says, in effect, "Give me 15% more than last year no matter what. Don't give me excuses, give me the numbers!"

Sean Lyons: In your opinion where does the role of risk management currently fit into the broader concept of an organization's corporate defense program and how do you see its role developing going forward?

David Rowe: In my view risk management is effectively synonymous with the corporate defense function leavened with the recognition that some risks are necessary for a business to survive and prosper. It is the breadth of the potential dangers that makes the emerging role of the CRO especially challenging. As in politics so it is in risk management, there are no final victories. One requirement for long-term corporate success is constant vigilance and the will to act when threats emerge.

Originally published at the RiskCenter (www.riskcenter.com) *on the 8th July 2008*

OPERATIONAL RISK

Philip H. Martin

Chairman of the Institute of Operational Risk (IOR)

About Philip Martin

Philip Martin is the Chairman of the Institute of Operational Risk. He has been a member of the Institute of Operational Risk since being accepted as a Fellow in December 2005. He has been chairman of the council of the Institute of Operational Risk since February 2007 and was previously chairman of its executive committee. In 2005, he founded Enterprise Risk Advisors, which provides risk management advice to the financial services industry. Philip started his career in 1977 specialising in fraud and professional liability insurances for the global financial services industry. He was an executive director at HSBC Insurance Brokers from 1985 - 2004 and managing director of HSBC Operational Risk Consultancy Division from 1995 – 2004 where he delivered operational risk software solutions to global financial services clients. He has specialised in the design and provision of Operational Risk Management solutions to global financial services clients. He is currently a director of operational risk at Kinetic Partners LLP with responsibility for expanding operational risk solutions for Kinetic's asset management clients. Philip has worked in over 40 countries and is a regular speaker at industry conferences and has an obvious passion for the subject of Operational Risk and for the Institute he represents. He is regarded as one of the leading experts in this field and has lectured extensively around the world in addition to contributing articles to trade magazines and publications. In January 2009, Philip was elected as one of the global "Top 50 Faces in Operational Risk" by OpRisk & Compliance Magazine.

The Institute of Operational Risk (IOR)

The Institute of Operational Risk (IOR) was created as a professional body whose aim is to establish and maintain standards of professional competency in the discipline of Operational Risk Management.

For more information visit: **www.ior-institute.org**

OPERATIONAL RISK AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Philip Martin, the Chairman of the Institute of Operational Risk (IOR) shares his insights on the management of operational risk and its role in corporate defense with Sean Lyons.

Sean Lyons: While no agreed universal definition exists for operational risk, traditionally it was often considered to be all risks apart from either market or credit risk. In your opinion what are the main characteristics of operational risk and what is its relationship with credit and market risk?

Philip Martin: Operational Risk is unique in that it touches all parts of a Company's business - unlike either Market or Credit Risk. If one considers major Market or Credit Risk events, it is highly likely that a significant component of any such event is actually Operational. Take four simple examples:

a. LTCM – Models failed to anticipate particular movements in the market – this is an operational failure to consider all possible outcomes.
b. Bradford & Bingley – Mortgage fraud to the tune of £15mm. Undoubtedly a control failure in checking the efficacy of valuations and collateral documentation.
c. HSBC – Sub-prime lending in the USA. The purchase of third party sub-prime mortgage portfolios which were not then subjected to HSBC's credit rating software.
d. Northern Rock – Liquidity disappeared – failure to consider an alternative business strategy.

These are just a few examples, but it is also worth noting that it is major Operational Risk Events that destroy companies rather than Credit or Market Risk events. Little work has been done around the correlation of Operational, Credit and Market Risks and it is certainly worth further consideration. Aspects of the current credit crunch can be put down to a failure to understand the effects on a product or a portfolio when the three risk categories collide. Where was the operational risk review when a mortgage portfolio (credit risk) was bundled together with other portfolios of dubious quality and securitized (market risk)? UBS admitted that their internal controls failed to identify the underlying value of the securitized assets they were purchasing – and they were not alone. Ultimately Operational Risk events are largely caused by two things. Either it is an Act of God (earthquake, windstorm, flood), or it is a Person – doing something they should not be doing, or not doing something they should be doing. Accordingly the characteristics of Operational Risk are very different from either Market or Credit risk.

Sean Lyons: Operational risk is perhaps an unavoidable consequence of doing business and the sources of operational risk can be wide ranging and can be spread across the entire organization. Given the nature of operational risk, to what extent do you agree with the view that everyone in the organization is to some extent a risk manager?

Philip Martin: It is a well-worn cliché that everyone in an organization is a risk manager – but it is absolutely true. Each employee, from the Chairman of the Board to the

Security Guard on your front door, has a role to play. Of course each employee will have a different role depending on their responsibilities, but it's almost like a neighbourhood watch scheme in your local community. If everyone participates in the effort to prevent crime, pretty soon the incidents of crime will reduce. So it is for operational risk. By building awareness across the Company and training staff so that they understand what they are looking for and what is their required behaviour, a company goes a long way towards the development of a robust operational risk management framework.

Sean Lyons: When you look back on where operational risk management (ORM) has come from over the years, what developments most stick out in your mind?

Philip Martin:

a. The recognition that Operational Risk is a discipline in its own right. This is significant, but there is still a long way to go before Operational Risk management is on the same footing as Credit or Market Risk management disciplines. To those involved in the management of Operational Risk this is frustrating as history indicates that neither Credit nor Market risk will bring down a company, whereas the past is littered with dramatic failures of companies, both large and small, as a consequence of Operational Risk.
b. The recognition that the measurement of Operational Risk has limitations and it is not the nirvana we are seeking. Operational Risk is unique in its characteristics – it makes a mockery of those who argue that "if you can't measure it, you can't manage it!"
c. The recognition that Operational Risk Management is a leadership role within a business and has a significant role to play in the strategic planning and business development of a company.

Sean Lyons: We have seen a number of examples in the not too distant past of corporate scandals where operational risks were not addressed which proved to be unexpectedly costly and in some cases catastrophic to the organizations concerned. This has resulted in increased regulatory intervention. In light of this intervention how have regulatory developments such as Sarbanes Oxley and Basel II impacted on ORM as a discipline?

Philip Martin: BASEL II – I just wish the Regulatory community had called the AMA the "Advanced MANAGEMENT Approach" rather than the "Advanced Measurement Approach". It took far too long for the international regulators to admit that they would rather see institutions spending money on preventing operational risk events, rather than spending money on counting the cost of such events. Nevertheless, Basel II gave a name to the discipline of Operational Risk management. It allowed a more formal process to emerge for the management of Operational Risk and it almost forced institutions to invest in the development of risk management frameworks. It is doubtful that such investment would have been forthcoming without Basel II. What happens next will be interesting to watch. Basel II is overly prescriptive and has done little to help through the current financial difficulties. There is much to be said for Basel II to become counter-cyclical, i.e. to force Banks to hold more capital when times are good and to allow them to hold less in times of stress. Sarbanes Oxley (SOX) – A classic example of a political knee jerk

reaction to a problem. The SOX legislation was rushed into law without enough time to consider the consequences. The result was the emergence within companies of a cottage industry around the management of financial controls and beyond. This was a huge and unnecessary cost for most companies and went as far as causing companies to de-list in the USA as a way to avoid the burden.

Sean Lyons: In recent years a great deal of time and effort has been spent on attempts to measure, quantify and model operational risks, particularly in financial institutions. What in your view have been the major benefits to organizations of such a metrics driven approach?

Philip Martin: There has been an inordinate amount of money spent on attempting to measure Operational Risk, with limited benefit in my view. For a while, it seemed like the Quantitative world was dominating and even controlling the Operational Risk management debate – and therein lay the road to madness! Attempting to place a number on a risk that depends on an individual's behaviour and then use that to drive a capital requirement made little sense. Further, some of the measurement approaches were so complicated that they could only be understood by the individual who designed the mathematical equation. Companies have spent millions of dollars in developing such "black-box" approaches which have been of little use to those who run the business. Thankfully, the use of scenario analysis and stress tests has emerged as a credible manner in which to gain an understanding of the capital requirements of a company. This allows a company to ask itself a series of "what if" questions in planning its strategy and in examining significant risks that have been identified by the company. Such an approach allows the company to factor in the quality of its operations and control environments and mitigate the cost of Operational Risk. From there, Executives can use the information to better run their company.

Sean Lyons: Risk quantification and modeling place a great deal of importance on the historical data available within an organization. Some would argue that operational risk is far less predictable than other risk types, and that in terms of operational risk the occurrence of past events gives far less guidance on the occurrence of future ones. In your opinion what reliance can be placed on operational risk models which are based solely on historic data?

Philip Martin: Well, it depends what you are looking for and what you are going to do with the information. If you want a number to demonstrate the potential cost of Operational Risk at a given point in time, then the use of loss event data can give you a snap-shot at a given point in time. This assumes of course that you have enough internal data available to build a credible model and that there is limited reliance on external data. If you are looking for such models to provide an indication of what is likely to happen tomorrow, or the day after, or any period in the future, then little reliance should be placed on them. Backward looking models can be useful from an educational perspective in looking at what costs have been incurred and may be useful in helping to determine capital allocation across a company.

Sean Lyons: Many operational risk courses and books tend to focus on the more theoretical aspects of risk absorption and mitigation, at the expense of how to manage the ongoing on the ground day to day responsibilities which help prevent risks from materializing. To what extent do you feel that there has been a disconnect developing between the theoretical aspects of ORM and its more practical responsibilities?

Philip Martin: I haven't sensed a disconnect in the manner described, if anything I think it may be the reverse. Recent conferences and workshops have focused very much on the practical aspects of Operational Risk management techniques rather than the theory. There will always be room for quantitative techniques, the work that is being undertaken is important, but this will be for the minority – for a specialist department of an Operational Risk management function. The majority of Operational Risk professionals are much more concerned about the development of practical approaches for Operational Risk management techniques.

Sean Lyons: In many organizations decisions to develop new products and services are driven by the business requirement without sufficient consideration for the operational risk implications. In your view what can be done to ensure that those responsible for operational risk have sufficient and appropriate status and authority within their organizations to ensure that the organization is not exposed to excessive operational risks?

Philip Martin: This is all about the "tone at the top". Senior Management, starting with the Chief Executive, must support the involvement of the Operational Risk management function in the planning of new business initiatives. Without it, it is unlikely that frontline business units will invite risk management to the table – in much the same way that they would not invite compliance or legal if they thought they could get away with it. A robust Operational Risk management function will strive to prove its value to the business units and will strive to win the position of "trusted advisor" within the company. Assuming that the right personnel are in place with the right experience and expertise, and are provided with the total backing of senior management, the business units will quickly see the value of including Operational Risk personnel early in a process. But without this management support, it can be a real uphill battle for the risk management function. There is still an image issue in that the Front Office will frequently view Risk as a business "disabler" rather than an "enabler".

Sean Lyons: Certain organizations have adopted the COSO ERM framework as their chosen ORM framework. What are your views on this approach and are there other frameworks which you consider to be more suitable for ORM?

Philip Martin: COSO will work for some, others may choose the Australian/New Zealand standard and others may choose a hybrid. The concept of "Enterprise Risk Management" is an interesting one – it's easy to say, but not easy to do. Within the financial services industry, ERM is still a relatively new concept and there are few companies who are prepared to put their hands up and say that their ERM initiative has been a success. Certainly it makes sense for all risks to be proactively managed across a

business rather than in silos – but is this not the responsibility of a Chief Risk Officer? Is it not his role to report to the Board of Directors or Executive Management Committee on risk across the "enterprise"? Proactive risk management is about excellent communication across business lines so that all business units understand how their actions can impact on others and having the discipline to tackle potential obstacles. Some suggest that ERM is about the bringing together of Operational Risk, Credit Risk, Market Risk management with Compliance and Internal Audit. While this sounds good in theory, it really takes enlightened and determined management to successfully implement. There are very real practical issues to overcome and manage. For example, in practice, rarely are the Heads of Risk, Heads of Compliance and Heads of Internal Audit shrinking violets. An ERM initiative can create considerable conflict as to who will be responsible for what and it takes strong leadership to make this work. Further, care must be taken to ensure that the independence of Internal Audit is not conflicted. And finally, it must be recognized that as Operational Risk management is a leadership function, Compliance and Internal Audit are assurance functions – very different roles within a business! So, while ERM does appear to have much going for it, we must recognize that it is not easy and should be approached with care.

Sean Lyons: What advice would you give to those with responsibility for ORM when putting forward the business case for operational risk in their organization?

Philip Martin: Focus on the business benefits! A good Operational Risk management function will:

- help a business achieve its strategic objectives;
- help smooth earnings;
- educate the business about the risks it may potentially face;
- develop solutions to business obstacles and risks;
- reduce the level of operational risk events;
- be a "trusted advisor";

to name a few benefits.

Sean Lyons: In your opinion where should the responsibility for ORM ideally rest in the corporate framework in order to be most effective?

Philip Martin: The responsibility MUST rest with the Board of Directors. The Board should be under no doubt that they are responsible and that the Regulatory community will take action against them in the event of a significant ORM failure. The Board should formally adopt the Operational Risk management framework, develop a clear statement of Risk Appetite and set the objectives to be met by the Operational Risk management function. They then pass the responsibility for delivery of the objectives to Senior Management.

Sean Lyons: In your view where does ORM currently fit into the broader concept of an organizations program of self-defense and how do you see it developing going forward?

Philip Martin: I rather suspect that anybody answering this question 18 months ago might answer it differently than they will today. It is quite clear that the events of the last 12 to 18 months within the global financial services community have significantly moved the risk management goal posts. The disturbing thing is that it looks like this is a cyclical issue. One just has to look at the internal reports issued by UBS and Société Générale to observe the breakdown and failure of the risk management infrastructure. When the good times roll, profits can cover up a multitude of problems and what we are seeing today is very reminiscent of the mid-1980's, late-1990's and early 2000's. During each of these periods we saw a series of corporate scandals emerge, largely driven by greed and, in some cases, fraud. In all cases, there was a massive failure of the management of operational risk. There is no doubt that the behaviour of some large companies – or, more to the point, the behaviour of those running such companies - has fell far short of an acceptable standard. Operational Risk Management ought to be front and centre in a company's program of self-defense. If you go back to the empty-space definition of "if it's not market or credit risk, it must be operational risk", then this would suggest that ORM must take the lead. I would like to think that the discipline of Operational Risk Management will continue to grow in importance, but this will depend on the skills of the ORM professionals. This is not an easy discipline, its benefits are hard to measure and it is entirely dependent on the culture of the company in which it resides. Implemented properly, the benefits for companies are clear – but there is still a long way to go to get this message adequately understood.

Originally published at the RiskCenter (www.riskcenter.com) *on the 18th June 2008*

ENTERPRISE RISK MANAGEMENT (ERM)

Steven J. Dreyer

Managing Director at Standard & Poor's

About Steven J. Dreyer

Steve Dreyer leads the S&P research project on the applicability of Enterprise Risk Management (ERM) analysis to the credit analysis process for corporate ratings globally. He is also the U.S. practice leader for Utilities & Infrastructure Ratings, overseeing a group of analysts providing credit ratings and research on investor-owned electric, gas, and water utilities, independent power producers, gas pipelines, project finance, and public-private infrastructure partnerships. He was recently made responsible for leading a research project exploring opportunities to increase transparency in carbon trading markets. From 2000 to 2006, Steve was North American practice leader for Insurance Ratings. He joined Standard & Poor's in 1990 with its acquisition of ratings firm Insurance Solvency International, Ltd, whose U.S. subsidiary he managed. Previously he was responsible for insurance industry forecasting at Chase Econometrics. Steve earned a B.A. in Statistics from the University of Delaware and did graduate work at Drexel University. He completed executive development programs at the University of Virginia (1996), Columbia University (2005) and INSEAD (2007). Steve was named to Insurance Newscast's "List of 100 Most Powerful People in Insurance in North America" from 2002 to 2006. In 2003, he contributed to the Greater New York Safety Council's "Roundtables on Sector Preparedness", reporting to the 9-11 Commission. He is a director of the Insurance Marketplace Standards Association, which sets ethical standards in the sale of life insurance and annuities.

Standard & Poor's

Standard & Poor's is a leading provider of financial market intelligence. The world's foremost source of credit ratings, indices, investment research, risk evaluation and data, Standard & Poor's provides financial decision-makers with the intelligence they need to feel confident about their decisions.

For more information visit: **www.standardandpoors.com**

ERM AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Steven J. Dreyer, Managing Director at Standard & Poor's shares his insights on Enterprise Risk Management (ERM) and its role in corporate defense with Sean Lyons.

Sean Lyons: For those unfamiliar with the term "Enterprise Risk Management (ERM)" could you briefly describe what ERM involves and how it differs from traditional risk management?

Steve Dreyer: We see ERM as an organizational commitment to manage risks holistically across the enterprise. While many firms can be successful at silo-based risk management, and be recognized for it favorably in our ratings process, the idea of looking at managing risks more broadly is a new concept in our ratings process.

Sean Lyons: ERM is seen by some as being the process of embedding sound risk principles throughout the enterprise. What in your view are considered to be the main risk principles or components of ERM which organizations should focus on?

Steve Dreyer: Our ERM analysis will focus initially on risk culture and strategic risk management. We believe that these elements are universally applicable and comparable across organizations of various sizes, sectors, and locations. We will be less concerned with drilling down to all levels of the organization to identify risk principles in action, but will focus more on understanding how senior management and the board sets and implements risk policy.

Sean Lyons: In terms of the ERM framework which an organization should adopt, do you have a preference for one framework over another (e.g. COSO ERM framework over the AS/NZS 4360 or vice versa)?

Steve Dreyer: We are agnostic about particular frameworks, other than to recognize that an organization that effectively employs a generally recognized framework such as COSO or AS/NZS 4360 would be supplying evidence that it has made a commitment to manage risks consistently across the enterprise. Companies may be able to demonstrate such evidence in other ways.

Sean Lyons: Standard & Poor's appears to be focusing increased attention on ERM analysis in its evaluation of not only financial but also on non financial institutions. To what extent does this analysis influence the final credit rating received by an institution?

Steve Dreyer: It's too early to answer this question. By late 2008 or early 2009, we expect to form an opinion of the value of information acquired through the ERM discussions we have with rated companies.[1] After benchmarking performance across a

[1] Due to the diversion of their principle attention to matters dealing with the current credit markets, S&P have since pushed back their expectations for integrating ERM scores into credit ratings to the latter part of 2009.

large number of companies, we will determine the importance or "weight" of ERM in the credit ratings process. At that time we will publish our findings and provide the market more explicit evaluation criteria.

Sean Lyons: In terms of the scoring of this ERM analysis are their fundamental differences between the scoring systems used for financial and non financial institutions?

Steve Dreyer: We have not yet determined scoring criteria for non-financial companies. While we expect that there will be differences across sectors in the risk control processes utilized, we will focus on the common elements of risk culture and strategic risk management.

Sean Lyons: How can implementation of a comprehensive ERM program help an organization to enhance its profitability?

Steve Dreyer: First, firms can avoid outsized, unexpected losses with effective ERM. Those that achieve the full benefits of ERM may be able to optimize risk/return tradeoffs in making strategic decisions, which can lead to enhanced returns over a long period of time.

Sean Lyons: Many organizations prefer to manage operational risks in separate silos while others espouse a more holistic approach to risk management. What advice would you give to an organization considering the merits and demerits of such approaches?

Steve Dreyer: Effective silo-based risk management is considered a minimal requirement for strong credit ratings, but would not by itself indicate that a firm was optimizing ERM as a tool for enhanced risk-adjusted returns, resilience in responding to adversity, and overall stability. At the same time, we do not expect to see many firms that demonstrate an advanced holistic approach.

Sean Lyons: ERM is generally seen as an evolving process within an organization. Is there a particular maturity model which best reflects this evolution and what phases of development can organizations expect to go through?

Steve Dreyer: We expect that maturity of risk management culture and strategy will be greatest in industries exposed to the most volatile external risks, e.g., energy, financial institutions, and agribusiness. Other than that general expectation, we do not prescribe nor expect a rigid path to successful enterprise risk management. Different companies may use different models to greater or lesser success.

Sean Lyons: The recent emergence of "Governance, Risk and Compliance (GRC)" in the US is seen by some as a natural progression beyond ERM while others would argue that GRC is simply ERM by another name. What are your views in terms of the relationship between ERM and GRC?

Steve Dreyer: We try not to get hung up on labels. The bottom line for us is in attempting to get a better handle on the effectiveness of an organizations' management team. In general, we do not include a heavy emphasis on compliance in the ERM analysis framework we are employing because we are focusing on broad culture and strategy themes. A company can not comply its way to effective culture and strategy.

Sean Lyons: In your opinion where should the position of CRO and/or the responsibility for initiating an ERM program reside within the corporate framework?

Steve Dreyer: The CRO is of interest to us if that person is accountable for important risks the firm faces, has significant visibility with senior management, and has a direct line of communication with the board of directors. Equally, a company may be able to achieve the appropriate visibility, communication, and implementation of effective risk management across the organization without a Chief Risk Officer.

Sean Lyons: To what extent should those with responsibility for ERM also have responsibility for the management of the on the ground day to day operational activities which address enterprise-wide risks?

Steve Dreyer: We will be looking for consistency of communication, which may be achieved by particular individuals having dual responsibilities as posed in the question, but could also be achieved in other ways.

Sean Lyons: In your view where does ERM currently fit into the broader concept of an organizations program of self-defense and how do you see it developing going forward?

Steve Dreyer: We view self-defense or resilience as a key ingredient in ERM, focused as it is on downside risks. We are considering ERM to be a broader concept, encompassing also the exploitation of risks on the upside. Companies with effective ERM avoid surprises but also optimize risk-adjusted returns.

Originally published at the RiskCenter (www.riskcenter.com) *on the 5th August 2008*

COMPLIANCE

Roy Snell

CEO of the Society of Corporate Compliance and Ethics (SCCE)

About Roy Snell

Roy Snell is the CEO of the Society of Corporate Compliance and Ethics (SCCE) and was a co-founder and the organization's first President. He has developed numerous partnerships with government, industry, and other professional associations, and he has facilitated collaboration between the compliance/ethics profession and the enforcement community. Roy has a Masters degree in Health and Human Services Administration. Through his work as CEO of the society, he has overseen the development of compliance and ethics books, manuals, videos, conferences and audio conferences. He has been a regular speaker in the compliance profession for more than 10 years and has spoken internationally for the United Nations on compliance and ethics. He is a Certified Compliance and Ethics Professional. Roy writes more than 25 compliance articles annually and has written for several international publications, including the European CEO and The European Business Review. Roy is the coeditor of the Health Care Compliance Professional's Manual and serves as editor, co-editor and advisory board member of several other books, magazines and newsletters. He has served as a source for many media reports, including national publications such as the Wall Street Journal, Forbes Magazine and Business Week. He has been quoted in international publications such as Financial Times and Ethical Corporation. Roy is a former Mayo Clinic administrator, consultant and Compliance Officer. He has participated in the development of compliance program guidance, professional certification programs and the Compliance Professionals Code of Ethics. He has dedicated more than 10 years to the compliance profession and to the development of compliance programs on an international basis.

The Society of Corporate Compliance and Ethics (SCCE)

The Society of Corporate Compliance & Ethics (SCCE) is dedicated to improving the quality of corporate governance, compliance and ethics. SCCE exists to champion ethical practice and compliance standards in all organizations and to provide the necessary resources for compliance professionals and others who share these principles.

For more information visit: **www.corporatecompliance.org**

COMPLIANCE AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Roy Snell, CEO of the Society of Corporate Compliance and Ethics (SCCE) shares his insights on compliance and its role in corporate defense with Sean Lyons.

Sean Lyons: Corporate compliance is concerned with how an organization adheres to laws, regulations, industry codes and best practices, and internal standards. Is there a particular definition of compliance which you feel best describes the term and its core objectives?

Roy Snell: Although it might be considered US-centric, the United States Sentencing Commission outlined several essential elements of a compliance program in 1991. Since then, many countries have adopted a similar set of compliance program elements. Stock exchanges worldwide are actively implementing similar requirements. Implementing the essential elements of a compliance program is a critical first step in any corporate defense activity. The key elements of a compliance program include auditing, monitoring, education, anonymous reporting mechanism, reporting to the Board, discipline, investigations, and policies and procedures.

Sean Lyons: The compliance imperative in many organizations is motivated by the threat of sanctions against the institution and prosecutions against individuals. To what extent do you feel that compliance education and training is the way forward in developing a culture of compliance within an organization?

Roy Snell: I would like to take the question a step further. Compliance training is not only important within an organization, but it is important that business schools begin to teach the essential elements of a compliance program and the role of the compliance officer. Compliance training is very important. Compliance programs are important. We do way too much talking about doing the right thing. We need to start auditing, monitoring, and enforcing the behavior we are looking for. Employees are tired of all the talk; they want to see leadership back up their words with action. I would do it for the employees as much as I would do it to reduce the threat by the enforcement community.

Sean Lyons: In terms of a best practice framework which an organization should adopt, are there any particular frameworks which you consider most suitable when implementing a compliance program in the corporate world?

Roy Snell: Compliance is not complex. It's hard, because most people don't have enough courage to implement the basic elements of a compliance program. The elements of a compliance program listed above are what you need to be successful. Too many people are developing complex frameworks that are overwhelming and so complicated people lose the whole point of compliance programs. The intent is to find and fix regulatory compliance problems.

Sean Lyons: What have been the main trends and developments that you have seen over the last 5-10 years in the area of compliance which have had the greatest impact on corporate compliance culture?

Roy Snell: The growth has been interesting. The job of compliance officer has made the top ten lists of the hottest jobs in the country. Our compliance professional membership organization has grown to 6,700 members in the last 12 years. This is a very exciting time. I am concerned about many of those who are trying to cash in on the growth. Many claim to be experts and are not. Many of these "experts" are pushing unnecessarily complex frameworks that dilute the compliance efforts and distracting leadership from finding and fixing problems.

Sean Lyons: So far in the 21st century, we have seen a large degree of regulatory intervention in the corporate world. In your view, to what extent has this intervention, and in particular the introduction of the Sarbanes-Oxley act 2002, been successful in modifying corporate behavior in terms of corporate integrity and corporate ethics?

Roy Snell: The settlements drive the implementation of compliance programs and the hiring of compliance officers. SOX has been a very small part of it, although it has received a lot of press and attention. SOX was oversold by some to make money. SOX could go away tomorrow and nothing would change. Society is tired of corporate wrongdoing. The enforcement community is reacting to the society's request for change.

Sean Lyons: Since the introduction of the Sarbanes-Oxley act, the role of the Chief Compliance Officer (CCO) has been given a higher priority in the corporate world. Where do you believe the CCO and/or the responsibility for initiating a compliance program should be positioned within the corporate framework and why?

Roy Snell: The key is independence. They need to be able to act without pressure to look the other way. The only way independence can be ensured is to have the CCO report to the Board.

Sean Lyons: Given the volume of laws and regulations which an organization already is required to comply with, and the number of new laws and regulations already in the pipeline, in many organizations, compliance represents a reactionary function which is constantly struggling just to keep pace with the organization's current compliance requirements. In your opinion, what can a compliance function do to get beyond simply playing catch-up and develop into a more a strategic asset for an organization?

Roy Snell: Delegation is the key. Compliance professionals are not responsible for regulatory compliance. The entire organization is responsible for regulatory compliance. Each department is responsible for their own operation, finance, and human resource activity. They are also responsible for compliance with laws that affect their department. An effective CCO makes sure that each department implements and maintains the essential elements of a compliance program.

Sean Lyons: What advice would you give to those with responsibility for compliance when putting forward the business case for compliance in their organization?

Roy Snell: This very difficult. If leadership doesn't get it now, you are in for a long tough job. I would show leadership the settlements that have already occurred. I would try to get a top manager and a Board member to a compliance conference. The problem is most CEOs work strictly off of numbers. They need proof. We, the Society of Corporate Compliance and Ethics, are in the middle of a study that will look at three different organizations' ethical environment and correlate it with their variable costs, such as:

- Employee turnover
- Employee sick leave
- Worker's compensation claims paid, both number and cost
- Customer satisfaction, and
- Theft/loss (e.g. inventory loss, property damage/loss)

The study was done once before in the city of Austin, Texas and they found a correlation between the ethical culture and a reduction of costs. If our study has the same results, we may be able to give CEOs the numbers they need to support compliance efforts.

Sean Lyons: Increasingly compliance requirements are spreading across all aspects of business. What in your view are the main obstacles to getting compliance principles embedded into the business processes throughout the enterprise?

Roy Snell: It's very simple. If you make it a part of the review process or the bonus calculation, you will see results. If you just talk about it and don't measure it or reward it, it won't happen. If you only measure financial success, you will not only negatively affect compliance efforts, you may encourage non-compliant behavior.

Sean Lyons: Compliance is generally seen as an evolving process within an organization. Is there a particular maturity model which best reflects this evolution? What phases of development can organizations expect to go through?

Roy Snell: I have seen a lot of work on maturity models. I am not sure they are all that helpful. All the time creating and studying maturity models could have been spent on looking for and finding regulatory compliance problems. People seem to want to get ready and spend time getting ready, followed by more time spent getting ready. We need to stop talking and start doing something. I would rather investigate, educate, audit, monitor, respond to complaints, etc.

Sean Lyons: In your view, where does compliance currently fit into the broader concept of an organization's program of self defense, and how do you see it developing going forward?

Roy Snell: I just try to keep things simple. Successful people try to keep things simple. If you want to eliminate the need to defend yourself, don't do anything that would require you to defend yourself. Implement a compliance program, avoid all of the distractions,

find and fix problems, and you will reduce the need to defend yourself. Compliance (finding and fixing problems) is the single most effective use of your time and money.

Originally published at the RiskCenter (www.riskcenter.com) *on the 16th July 2008*

INTELLIGENCE

Stephen M. Walker II, Esq.

Technology Markets Analyst at the Aberdeen Group

About Stephen Walker

As a GRC specialist Stephen Walker focuses on key Governance, Risk Management, & Compliance (GRC) issues in the market as well as Managed Services and Outsourcing within Aberdeen's Technology Markets group. He has been focusing on GRC strategies in Financial Services organizations, and the benefits of assimilating separate solutions such as Business Intelligence (BI) tools into GRC programs. Recently he co-authored the benchmark study entitled "Is Your GRC Strategy Intelligent? Analytics for Accurate, Real-Time Visibility and Decision Making". He is primarily focused on the interconnections and impact Governance, Risk Management & Compliance (GRC) solutions have on organizations in today's increasingly risky and regulated global market. Most recently he has been exploring the significant high-level business benefits of comprehensive GRC initiatives and the transition from reactive, fragmented compliance processes and towards a proactive, comprehensive continuous compliance framework. Stephen is currently focusing on diving deeper into the rapidly growing GRC market and covering a variety of topics including: Enterprise Risk Management (ERM), IT GRC, internal auditing and identity and access management. Additionally, Stephen also devotes time to exploring several topical areas inside the Managed Services and Outsourcing practices. Stephen holds a B.A. in Economics and Business with a concentration in Financial Management from the Virginia Military Institute and received his Juris Doctor (JD) from the West Virginia University College of Law.

The Aberdeen Group

The Aberdeen Group is the leading provider of fact based research focused on the global-technology driven value chain. Aberdeen's mission is Technology Answers for the Global Value Chain: "Educating Buyers to Action," as time matters in today's business environment and technology investment mistakes are not tolerated. Aberdeen's fact-based research educates technology buyers with the facts they need to act on business and technology decisions.

For more information visit: **www.aberdeen.com**

INTELLIGENCE AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Stephen Walker, technology markets analyst at the Aberdeen Group, shares his insights on intelligence and its role in corporate defense with Sean Lyons.

Sean Lyons: Generally speaking corporate intelligence is concerned with how an organization gets the right information, to the right person, in the right place, at the right time. Is there a particular definition which you feel best describes the role of intelligence in the corporate world?

Stephen Walker: Intelligence in the corporate world is fundamentally about driving improved business performance. Most effective as a full circle process characterized by not only ensuring that the right individual within the organization has real-time or near real-time access to the most accurate, current, and topically-relevant information that he / she needs to advance business objectives, it is just as important that the outcome or result of the use of that information (i.e. deal closed, project milestone reached) is fed back through the intelligence loop and disseminated to the individuals who can use that intelligence to gain advantages in other areas.

Sean Lyons: Looking back on the trends and developments which have occurred in this area over the past 5-10 years, what in your opinion have been the most significant advances in intelligence technology in this space?

Stephen Walker: I think the most significant advances in intelligence technology have been made in two critical areas: scope and configurability. Outside of the remarkable innovations in the technologies themselves, what they have enabled has fundamentally shifted the intelligence paradigm. Realizing the market's fatigue with "technology for technology's sake" implementations, and understanding that any potential benefits stemming from technology is substantially dependent upon the manner and level to which it is used, vendors have been devoting a lot of time and resources towards the configurability and customization of their tools. Corporate intelligence is being driven to the masses by both embedding / linking intelligence technologies into established and familiar procedures and applications and giving discrete intelligence technology the configurability sufficient to ensure that an employee can customize it enough that it becomes familiar and will use it. From integrating intelligence tools into daily business and operational processes to data collecting web applications, top performing companies are using technology advances as a vehicle to expand the scope of information input, and as a result their corporate intelligence output is more accurate, detailed and timely.

Sean Lyons: Corporate intelligence represents a very broad spectrum, extending to areas such as business, market and competitive intelligence, as well as knowledge management and communication etc. Effectively coordinating these areas can therefore be quite a challenge for any organization. Are there particular best practice frameworks which you consider most suitable for an organization when implementing its intelligence program?

Stephen Walker: Organizations with the most effective and efficient corporate intelligence frameworks don't necessarily gravitate towards one best-practice framework over another. Rather, realizing that the core function of corporate intelligence involves advancing business goals, and that each individual organization has a unique set of current and future business objectives, a developing trend is to incorporate portions of several established frameworks. Data collected from hundreds of global organizations [by the Aberdeen Group] for July's 2008 benchmark study, "Is Your GRC Strategy Intelligent? Analytics for Accurate, Real-Time Visibility and Decision Making", revealed that internal policies and best practices was the top methodology / framework (by a factor of about 4x) driving company's budgetary investments to increase visibility and intelligence.

Sean Lyons: The adoption of a more holistic approach to intelligence involves developing appropriate integrated strategies across the enterprise in order to help address intelligence issues. Is there a particular maturity model which best reflects the phases of development that organizations can expect to go through?

Stephen Walker: From a general perspective, Carnegie Mellon's Capability Maturity Model (CMM) is a good template that organizations can use as a jump-off point. A few frameworks emerging from the Governance, Risk management, and Compliance (GRC) space, particularly OCEG's GRC capability model, offer a more detailed and strategic view. The rise of the GRC market as a whole is exciting for a number of reasons; one of the most important and business-relevant being that a comprehensive GRC initiative offers the opportunity to integrate, converge, and streamline critical, yet historically siloed and discrete, functional areas. When holistically derived, these initiatives directly facilitate and advance embedding the communication channels, escalation procedures, and monitoring and measuring capabilities that embeds consistent and accurate intelligence on an enterprise wide basis. Having said that, the majority of organizations are relatively low in the maturity curve. Embedding intelligence throughout the organization is particularly challenging for companies competing in multi-regulatory industries. Errors stemming from inaccurate, incomplete, or conflicting information from multiple sources is an even bigger concern if the company has an expansive footprint with multiple, disparate operations. Oftentimes they lack visibility or even a common risk and compliance vocabulary, leading to redundant, costly, and inefficient activities. The most recent study published in September 2008, "Continuously Compliant: Ensuring Proactive, Comprehensive Compliance" revealed that the number one action top performing companies are taking to improve their maturity and performance is to establish, implement, maintain, and monitor consistent policies and procedures across geographies and lines of business. These companies understand that any operational performance improvements flow from an effective approach based on consistency and mapped back to the company's overall business goals. By embracing this strategy companies are able to focus more resources on strategic actions that generate sustainable operational advances.

Sean Lyons: Business intelligence (BI) in particular involves an appreciation of an organization's strategic, tactical and operational intelligence objectives. From your

experience what do you consider to be the most successful approach to aligning these multi-level objectives?

Stephen Walker: Organizational buy-in is critical to not only aligning the different levels and departments within a company, but also in realizing the goals of the overall initiative. One of the most important steps in achieving alignment and fostering organizational buy-in is to have a responsible executive take primary ownership of the project. In addition to being able to take a top-down look at the current organizational structure and identify where tweaks and adjustments need to be made to establish the required communication channels, protocols, and decision-making hierarchies, the executive has the wherewithal to make these changes happen. Once established, strategically focused monitoring tools and procedures must be implemented. Focusing on this strategy offers organizations some key benefits that continue to pay dividends well into the future. At the onset, comprehensive monitoring allows for the establishment of "current performance" risk, compliance, and intelligence baselines. The initial frequency and scope of monitoring activities is typically based on variables unique to the individual organization (i.e. company size, industry, geography, internal and external corporate objectives, business and growth goals, etc.). Once this baseline has been established, the incorporation of analytics provides companies with the opportunity to:

- Adjust corporate activities and strategies to ensure that pre-determined thresholds remain intact
- Escalate the identification, prioritization, and remediation of problem areas
- Track improvements in risk, compliance, and intelligence functions by mapping current performance against the established baselines to validate ongoing budgetary allocations

July's GRC & BI report clearly highlighted the business advantages to converging risk, compliance, and intelligence objectives. Understanding the importance of supplementing consistent monitoring of these processes with relevant analytic tools allowed top performing organizations to increase visibility and knowledge into risk and compliance activities by an average of 34%; an average increase 2.5-times greater than all other organizations.

Sean Lyons: The intelligence conversion process involves not only sourcing data, but also converting data into information, information into knowledge, and knowledge into intelligence so that it can be used in decision making in order to produce end results. Are there particular technology solutions which you feel best facilitate addressing these challenges?

Stephen Walker: The intelligence conversion process has become substantially more difficult over the last few years as the sheer volume of information that is now collected has grown exponentially. The surge in web-based applications has resulted in enormous collections of both structured and unstructured data. The amount of internal resources devoted to the conversion process, however, has not grown anywhere near apace with data and information collection. Recognizing this, a number of technology solutions have emerged to address this challenge. A good example of how technologies are helping

companies overcome these hurdles is tools that facilitate both structured and unstructured data compilation and analysis. Reminiscent of the old west tradition of “panning for gold”, these technologies help sift through the mountainous volumes of collected data and information to glean the important and relevant from the useless and unnecessary. Especially valuable when mapped back to corporate objectives and overall business goals, companies are increasingly finding value in incorporating analytic tools like dashboards to relay the pertinent knowledge to the individual who can capitalize on its availability. These BI tools are bridging the transitional gap that exists between the collection of relevant information and the ability to make actionable decisions based on the knowledge. Recent research from Aberdeen’s Business Intelligence Practice, highlighted in May 2008’s study, “Predictive Analytics: The BI Crystal Ball”, found that the use of analytics is helping companies to find and address problem areas *before* they negatively impact the business.

Sean Lyons: Effective intelligence requires investment. What advise would you give to those with responsibility for putting forward the business case for intelligence in their organization?

Stephen Walker: Too often the value of intelligence is described from an IT-centric approach. This is particularly relevant in times of economic uncertainty when budgetary allocations are being held in iron-fisted grips. While the memory of an individual or a single organization is often fleeting, as a whole, the market's memory is characterized by both its longevity and clarity. Upper-level decision makers and CxO budget holders have become fatigued with "technology for technology's sake" and burned too often in the past by high-tech hype-cycles and "over-promised, under-delivered" solutions. These stakeholders must be convinced of the *business* value of any solution implementation or service contract, and intelligence-enabling solutions are no exception. While the technologies, tools, and IT policies do indeed play a critical role in the overall success of corporate intelligence, the fact is that the IT budget is the mouse next to the business’ elephant. Selling into the business side of the company is the most effective way to gain budgetary support. However, to a substantial degree, that is dependent on tailoring the presentation of the potential value proposition in such a way that it heavily emphasizes how business goals will be advanced. Once an initial budgetary allocation is approved incorporating analytics and tools that monitor Key Performance Indictors (KPIs) on the achievement of enterprise-wide objectives helps to consistently prove the business case for corporate intelligence in at least two important regards:

- Providing managers and executives with visibility into how the various projects are progressing, thus enabling them to more quickly adjust project parameters, plans, and timelines to accommodate shifts in economic or market conditions
- Allowing the C-Suite and Board of Directors to more confidently and precisely determine forward thinking strategic plans by arming them with current and accurate updates.

July’s GRC & BI report revealed that incorporating KPI monitored analytic tools allowed the Best-in-Class to realize a 15% increase in the translation of collected risk assessment

data into actionable recommendations; one of several powerful business-focused metrics that help to continually validate the importance of the initiative.

Sean Lyons: In your opinion where should the position of CIO and/or the intelligence function ideally be positioned within an organization's corporate framework in order to be most effective?

Stephen Walker: One of the most effective ways to ensure the comprehensiveness and success of the intelligence function is to have an executive manage and take ownership of the overall project. However, merely positioning the overall management of corporate intelligence high in the organizational structure does not ensure its acceptance and use. Ineffectively communicating strategic corporate goals to daily process owners is a common problem in small and mid-size companies, and is even more common in large companies. The companies that are seeing the largest performance improvements are those that have an executive who routinely communicates corporate goals to the daily process and business-unit owners. By acting as a conduit between the executive team and the intelligence-tasked employees, the "Intelligence executive" enables full-circle communication characterized by affected employees knowing and proactively working towards the achievement of strategic business goals. Additionally, this role also assists upper-level "trigger-pullers" who can more efficiently focus and adjust current decisions and future engagements based on an enhanced understanding of how risk, compliance, and intelligence activities affect corporate goals.

Sean Lyons: Intelligence represents a critical aspect of other defense related activities such as governance, risk management, compliance, security, resilience, controls and assurance etc. In your view, to what extent does intelligence need to become embedded into these processes and why?

Stephen Walker: The success or failure of other critical corporate activities like governance, risk management, and compliance is, to a large extent, based on how pervasive intelligence is within the company's structure. To get beyond the "check-the-box" mentality and approach towards these activities that is so prevalent in many organizations, and to start driving sustainable business advantages, intelligence needs to essentially infect itself into the corporations DNA. Embedding intelligence into critical business processes, particularly risk and compliance, cannot be viewed as an option, but must be considered compulsory. A great example illustrating the importance of intelligence in critical processes and activities has been unfolding for the last few months; the rising regulatory storm brought about by the tumultuous and disastrous events unfolding in the financial sector. How can companies even hope to address the regulatory challenges without a mature intelligence framework? September's compliance-focused report details two important steps on the path to achieving and maintaining compliance that are all but impossible without proper intelligence:

- **Identify and monitor all regulatory information required for auditing and reporting.** By first understanding not only which regulations apply to the company's activities, but also the type and frequency of information and documents that must be produced to ensure compliance, companies can then evaluate the entirety of their

information streams, data repositories, and assets to identify which are applicable to a given regulation. Then, through establishing monitoring procedures on the relevant regulatory information, if questioned by outside auditors and regulatory bodies (which will almost certainly happen), the organization can supplement its "yes, I am compliant" statement with auditable documentary attestation.

- **Establish and implement process prioritization assessments and filtering mechanisms**. To ensure that internal resources are most effectively allocated, the initial prioritization assessment must look at compliance processes in the aggregate and their connections to core business activities. After identifying the compliance processes that have the greatest affect or potential impact on current and future business objectives, frequent monitoring procedures must be established to ensure the integrity and accuracy of these business-determinative processes. Additionally, filtering mechanisms can be put in place so that as the company's objectives and priorities adapt to business changes, (i.e. mergers, acquisitions, market fluctuations, and re-vamped product penetration strategies) the most frequent and comprehensive monitoring procedures are always directed towards the compliance processes that are most relevant to current and future, rather than past, business goals.

Sean Lyons: What in your view are the main challenges currently facing those responsible for intelligence in terms of getting the business buy-in on the importance of embedding intelligence into day to day activities?

Stephen Walker: Corporate intelligence is in a continual state of evolution and innovation as the market as a whole matures in its knowledge and understanding of the benefits of such initiatives. Additionally, given the uncertain economic climate and the fact that the decision-making authority for intelligence-enabling activities like risk and compliance has increasingly moved up the organizational food-chain to the C-Suite and Board of Directors, budgetary dollars are less accessible than in the past. From a strategic perspective, one of the most critical roles intelligence plays is informing these upper-level decision makers about the powerful ROI opportunity that exists when holistic strategies are mapped back to, and aligned with, that companies overall business goals and objectives. To surmount the above-mentioned budgetary and economic issues and the resulting, for lack of a better expression, “wait and see” mentality that some companies have taken to make sure intelligence [as a whole and GRC specifically] isn’t another vendor-driven hype-cycle, a number of organizations are winning by developing a penetration first, expansion later strategy. These companies employ risk, compliance, and intelligence tools to alleviate an urgent top-of-mind problem (i.e. achieving compliance with a specific and pressing regulation, more effectively managing and mitigating a high-priority operational risk, etc.) to show immediate value. Especially successful when paired with analytic tools like executive dashboards, this up-front win can not only validate the initial investment, but can also gain the executive support needed to ensure on-going budgetary allocations. The companies that initially took this approach and are now further along on the maturity curve are finding significant value from implementing solutions possessing the ability to address issue-specific problems while having the scalability to expand across various segments to a truly enterprise-wide level. The success or failure of an intelligence initiative is also significantly impacted by whether or not the

solutions feature customizable and easy to use functionality so that employees will actually use it.

Sean Lyons: BI appears to be playing an increasingly important role in business performance management. In your opinion which BI tools do you consider can be of most benefit when addressing the performance management of defense related activities?

Stephen Walker: Given the top-of-mind issues and challenges facing companies both today and in the near future, BI will be playing an increasingly important role in the Business Performance Management (BPM) space overall. Specifically, I feel incorporating targeted BI tools has the potential to address two very real challenges many companies are facing in the performance management of defense related activities. The first challenge, effectively monitoring, measuring, and reporting on business-focused performance metrics and objectives, can be substantially aided by incorporating analytic tools that enable sufficient visibility so that the processes, policies, and procedures that govern these defense related activities (especially relevant for risk and compliance activities) are consistently mapped back to the company's overall business goals. Especially important in a "measure twice, cut once" economic climate, this helps guarantee that all budgetary allocations are directly related to achieving business-driving objectives, while helping to ensure that all company resources are effectively allocated. As a corollary, employ tools that enable self-audit metrics for each business unit, to measure financial and operational risk and compliance activity on a more granular basis, provides two unique advantages; especially important to large, multi-national companies:

- Self-auditing the disparate business units conveys to individual staff members that there work is important and valuable to the overall company
- Self-auditing instills a sense of responsibility that leads to unit pride and enhanced performance

The GRC & BI and the Continuously Compliant reports underscored the importance of these activities. For example, by prioritizing risk and compliance related intelligence investments and focusing on their ability to enhance core business functions, Best-in-Class organizations were able to increase the integration of other enterprise applications (ERP, CRM, etc.) into their GRC framework by 14% while improving the effectiveness of risk management activities by 31%.

The second challenge that BI tools can have a profoundly positive impact on is the translation of data into actionable recommendations. One of the primary ways to help enable this transition is to incorporate BI tools that assess, monitor, and report on the most business-critical processes. The development and implementation of a prioritized, ongoing assessment plan offers a wide array of benefits. Identifying and ranking mission-critical processes will significantly decrease the odds of business activity being slowed or halted, and allows management to focus on the most important items and not be distracted by lower-level issues. Consistently monitoring key processes provides the organization greater visibility into the processes' inevitable vulnerabilities and "soft spots" prone to attack or degradation. This allows the organization to proactively repair or

replace potential weaknesses and ensure that critical process risk levels are kept within predetermined parameters.

Sean Lyons: In your view where does intelligence currently fit into the broader concept of an organization's program of self-defense and how do you see the role of intelligence developing going forward?

Stephen Walker: Currently, the maturity level of intelligence initiatives is rather low and still primarily approached from an ad-hoc or siloed basis, rather than an enterprise-wide perspective. Going forward, intelligence needs to be integrated into every aspect of a company's broader self-defense program. A prerequisite for the success of these overall programs is ensuring and maintaining the breadth, depth, and comprehensiveness of intelligence-enabling capabilities at all levels of the organizational structure. More specifically, given the magnitude of recent events, companies should consider how intelligence can aid and advance two vital areas that essentially serve as the gateway to the development of sound corporate governance and business integrity: internal audit and operational risk management. The seemingly overnight collapse of formerly billion-dollar blue-chip companies resulting from the economic turmoil in the financial services sector sent shockwaves into the upper echelons of government and corporate hierarchies in company's of all sizes from every industry segment. Given the uncertain economic landscape and the general public's virtually non-existent tolerance for questionable corporate ethics in the name of profit, companies must re-vamp internal frameworks and re-invest in targeted internal audit and operational risk management technologies and services to form a solid foundation for the establishment of sound corporate governance. The internal audit function, one of the fundamental checks and balances for sound corporate governance, is more important than ever given the changing and tightening regulatory landscape. Operational risk management, critical to streamlining inefficient operations, is increasingly important as corporate margins shrink and competitive pressures escalate. Embedding intelligence into these two areas can help companies to expand their intelligence initiatives into an enterprise-spanning framework that can benefit them in all aspects of the business.

Originally published at the RiskCenter (www.riskcenter.com) *on the 22nd October 2008*

SECURITY

Prof. Stephen Northcutt

President of the SANS Technology Institute

About Stephen Northcutt

Stephen Northcutt is the President, Ex-Officio Director on the Board of the SANS Technology Institute, a post graduate level IT Security College. Stephen is an acknowledged expert in training and certification and is the founder of Global Information Assurance Certification (GIAC) which he founded in 1999 to validate the real-world skills of IT security professionals. GIAC provides assurance that a certified individual has practical awareness, knowledge and skills in key areas of computer and network and software security. He is the author/co-author of numerous books including the seminal book on intrusion detection. These books include:

- Computer Security Incident Handling: Step-by-Step
- Intrusion Signatures and Analysis
- Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPN's, Routers, and Intrusion Detection Systems
- IT Ethics Handbook: Right and Wrong for IT Professionals
- SANS Security Essentials with CISSP CBK
- Management 512 SANS Security Leadership Essentials for Managers now NIST SP800 Compliant, and
- Network Intrusion Detection: An Analyst Handbook

He was the original author of the Shadow Intrusion Detection system before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College.

The SANS Technology Institute

SANS is a thought leader in information security making the SANS Technology Institute one of the nation's leading security graduate schools that grants Masters degrees in information security. Students are taught to be leaders with a demonstrated track record of leadership, knowledge and expertise in information technology and security. At SANS, the wisdom of industry and business, college academia and practical skills merge as students are taught by leaders with a demonstrated track record of leadership, knowledge and expertise in information technology and security.

For more information visit: **www.sans.edu**

SECURITY AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Professor Stephen Northcutt, the President of the SANS Technology Institute shares his insights on the importance of security and its role in corporate defense with Sean Lyons.

Sean Lyons: Could you please describe why it was that you choose security as a career and what was is that initially attracted you to the security profession?

Stephen Northcutt: In 1996, I was a network designer and had switched to a Sun 3 workstation, instead of a tricked out Intel 386 with a 5k graphics board, in order to make Autocad wait for me rather than the other way around. One day, before a very long and involved session, I was brewing a pot of coffee and looked down and my Sun workstation was really busy, the disk light was blinking like crazy. Why is my Sun working so hard while I am making coffee, I wondered. So I typed a ps command and it was compiling software. An IP address from Australia had made use of the Sendmail pipe to shell vulnerability and I was compromised. I reached over and pulled the network cable from the wall. It took a few months for my job title to be changed, but from that moment on, I was a security guy; I felt so violated.

Sean Lyons: In your view, what are the security leadership essentials that organizations in general should focus on in their security mission or vision statements?

Stephen Northcutt: I like the original watchwords of British Standard 7799, to develop a culture of security. However, that is a bit broad, so organizations should focus on two basic things: configure systems and networks correctly (and keep them that way), and detect when bad events occur. If you can do those two things, you are a long way down the road towards information assurance.

Sean Lyons: In your opinion where should the position of CSO and/or the security function ideally be positioned within an organization's corporate framework?

Stephen Northcutt: When you say CSO most people feel that you are talking about logical or information assets as well as facilities or physical security. That position should report to either the CEO or COO. The folks that have a CSO report to a CIO are creating a conflict of interest situation.

Sean Lyons: Unfortunately in many organizations security only appears on the radar as a top priority after a serious incident has occurred. Generally speaking how important is security to an organization and what do you see as the main benefits which an organization can expect to get from implementing a comprehensive security program?

Stephen Northcutt: A security program's benefits vary depending on how it is implemented. Unless you have an architecture that is purpose built to allow the business logic to operate in a risk managed manner, you probably have "Security Theater" - the appearance of security. Way too many organizations do not build security from the

ground up, but rather treat it like an add-on, so they waste their money and do not achieve their goals. On the other hand, organizations that pursue a culture of security can operate with a much higher risk appetite and pursue business opportunities that elude poorly run organizations. At the end of the day, security should be a business enabler; it should allow you to move quickly, knowing the bases are covered.

Sean Lyons: Effective security requires investment, however tangible returns on security investment is not always that obvious to those involved in the business side of the organization. Firstly, what advice would you give to CSO's when preparing to put forward the business case for security within their organization? Secondly, what in your view is the most critical aspect of presenting the business case for security to the stakeholders?

Stephen Northcutt: Metrics, metrics, metrics. You can only truly manage what you can measure. Security is not voodoo, it is engineering. You can measure the amount of non-business related network traffic you send and receive (and some of that is very high risk stuff). You can measure how many dangerous attachments are dropped. You can measure incidents. You can decide what behaviors you want to modify with your awareness programs and measure the level of success. But if you are a CSO and you do not have a metrics focus, you probably are not very successful at presenting the security business case.

Sean Lyons: What do you consider to be the biggest challenge currently facing CSOs' in terms of getting business buy-in on the importance of security to an organization?

Stephen Northcutt: We are all on a journey and the level of maturity of organizations varies. In the beginning of the journey a CSO has to focus on awareness, getting the rest of the organization to understand that their assets are vulnerable to exfiltration and if the competition can steal the know-how that took us years to develop, they can potentially outcompete us, especially if they pay employees less per hour. After awareness, we tend to see organizations that "get it" and start acting in ways to protect their valuable intellectual property. Sometimes in this phase the security program gets a little too much power and you start to see a decrease in buy-in because of the cost of security. Hopefully, the organization will settle on an architecture and overall approach for security that allows for a balance between the needs of security and the needs to accomplish business.

Sean Lyons: Over the years you have no doubt seen many different trends occurring in the area of security in general, what in your opinion have been the most significant advances in security over the last 5-10 years and why?

Stephen Northcutt: Ubiquitous computing, always online, is by far the most significant technical change. The security impact of that is the need for endpoint security. Every endpoint, by definition, is its own firewall, its own perimeter. Unless your building is a Faraday cage, wimax and cousins will make non-corporate networking available to every endpoint in most urban areas

Sean Lyons: It has been said that IT security represents an asymmetric challenge to an organization and this is compounded by the fact that IT security threats by their very nature are continuously evolving and mutating. IT security management therefore also requires continuous improvement and innovation just to keep pace with these changes. Where do you see the major threats coming from in the next 5-10 years and what can be done to address these threats?

Stephen Northcutt: We can't see ten years down the road, the proof of that is what will the desktop computer be like in five years? No one knows. However, we can see three years pretty clearly. Malware will continue to advance and, as long as people continue to click on attachments and URLs, will infect an increasingly greater number of systems. The malware is controlled by central points, "botherders", and the primary mission of the malware is to collect information from the system and the user of the system. They take screenshots, they collect passwords and accounts, they look for sensitive information to exfiltrate. Over the next few years, you will see identity theft rise to new levels as the criminals know your mother's maiden name, where you lived five years ago, and so on. You will also see the countries that support these botnets in a large way do well economically as they have the advantage over the countries whose information is being systematically looted.

Sean Lyons: Certain analysts seem to believe that due to developments in technology it is increasingly likely that a convergence of physical and logical security will take place in the not too distant future. What are your views on the pros and cons of such a convergence?

Stephen Northcutt: Alarms and surveillance cameras run over IP so the convergence is happening quickly. The problem is that it is a lot easier to train a techie to manage an alarm console than it is to train a former law enforcement officer to manage a complex system. However, former law enforcement officers understand a lot about practical security and the psychology of the criminal mind, techies do not. So, there will be some interesting power struggles, and the definition of CSO may be altered somewhat over the next five years.

Sean Lyons: Traditionally many organizations tended to allow security specialists in different areas (e.g. client, application, operating system, database, network, gateway etc) operate in isolation, the view being that these multiple layers of defense represented defense in depth. In recent times the increasing use of terms such as enterprise-wide security, unified security and integrated threat management etc would suggest that there is a move towards a more strategically aligned approach to security in general. What do you see as the main merits and demerits of such an approach?

Stephen Northcutt: I am reminded of Daniel 12:4, people will travel back and forth and knowledge will increase. The amount of security knowledge you need to be effective is exploding. These days, no one can master the entire security domain, even someone working on this full time. So, we are starting to have to specialize. You are seeing people that are full time penetration testers or full time web security specialists. I like the idea of

unified threat management, but my concern is that it will be like the IPS disaster, we trusted these appliances to protect us; they didn't and we lost the capability to detect attacks, one of the two most crucial security activities. You can save a lot of money with unified threat management, but that is easily at the cost of security. If you are giving proper configuration of systems and networks and detection of attacks the attention they deserve, a unified threat management device is probably a decent tradeoff. However, except in the smallest of organizations, you need a couple of truly technically capable experts for your critical exposures.

Sean Lyons: Other defense related activities such as governance, risk management, compliance, intelligence, resilience, controls and assurance are increasingly becoming core elements of the security management framework. What impact has this had on security management as a discipline and do you see developments which would indicate that security itself is similarly becoming embedded into other areas throughout the enterprise?

Stephen Northcutt: If an organization has adopted a culture of security, do they need an information security department? Possibly not; they would be fielding proper configurations, systems designed to withstand attack. The operations folks would be alert for signs a negative event has occurred and can react. The audit folks would be checking that things are being done as they ought to be done. That said, such an organization would need to be very careful to make sure they did have the required expertise for critical exposures. This will be even more true as organizations roll out service oriented architectures because they expose so much business logic.

Sean Lyons: In your view where does the role of security management currently fit into the broader concept of corporate defense and how do you see its role developing going forward?

Stephen Northcutt: It all comes back to risk. The first question an organization needs to ask is how much of their total value is comprised of information assets. If you are a software company or an intellectual property holding company, it is probably 99%. If the majority of employees in an organization use computers daily to do their work, it is probably 80% or higher. Next, we need to understand that the focus of both nation state attackers and identity theft motivated attackers is to locate and steal your information. If they can steal 99% of the value of your organization, what is your organization worth? In terms of the role of security management, the greater the percent of value our information assets are, the closer to the top the information security leadership needs to be. It seems like the value of information in an organization is not decreasing, so this may be even more true in five years.

Originally Published at the RiskCenter (www.riskcenter.com) *on the 25th June 2008*

RESILIENCE

Kathleen Lucey

President of the Business Continuity Institute (BCI) USA Chapter

About Kathleen Lucey

Kathleen Lucey, FBCI, is the President of the Business Continuity Institute (BCI) United States Chapter. She has more than 25 years of experience in information security and business continuity planning in a wide variety of industries. Kathleen was appointed as Chair of the Contingency Planning & Management (CPM) Advisory Board in 2007, and was inducted into the CPM Hall of Fame in 2005 which was instituted in 1998 to recognize and acknowledge the significant contributions of select individuals and businesses dedicated to the pursuit of business continuity. She became a Fellow of the BCI in 2000, and was named Business Continuity Practitioner of the Year in 1998 by IBM, in recognition of the business continuity program she developed during a five-year period at a multi-national pharmaceutical and chemical manufacturing firm. She is a frequent speaker at business continuity conferences, and has also spoken at conferences and seminars sponsored by AmeriVault, the New York City Bar Association, ISSA, ISACA, IFMA, 7x24, Cingular, the American Banking Association, and the SIA. Kathleen has published articles in *Continuity*, *The Journal of the Business Continuity Institute*, *Continuity Central*, *Continuity Planning and Management*, *Communications and Continuity 2002*, among many others. She is also an adjunct professor at the New York University, School of Continuing Studies. Kathleen founded Montague Risk Management Inc. in 1996. The company specializes in all aspects of risk management, including risk identification, avoidance and mitigation, information security and continuity planning for the protection and continuous operation of critical business functions and information technology services, as well as reliability engineering for building and support systems. She has designed and delivered projects all over the United States, including nationwide projects, as well as in Europe, Southeast Asia, Canada and Mexico.

The Business Continuity Institute (BCI)

The Business Continuity Institute (BCI) was established in 1994 to enable individual members to obtain guidance and support from fellow business continuity practitioners. The wider role of the BCI and the BCI Partnership is to promote the highest standards of professional competence and commercial ethics in the provision and maintenance of business continuity planning and services.

For more information visit: **www.thebci.org**

RESILIENCE AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Kathleen Lucey, President of the Business Continuity Institute (BCI) in the United States, shares her insights on resilience and its role in corporate defense with Sean Lyons.

Sean Lyons: The term resilience is an evolving concept which perhaps in its simplest form could be said to refer to an organization's ability to withstand, rebound or recover from the direct and indirect consequences of a shock, disturbance or disruption. Is there a particular definition of resilience which you feel best describes its objectives?

Kathleen Lucey: We need to be careful to distinguish resilience from recovery. For me, resilience is a designed-in capability that will automatically or nearly automatically switch on upon failure of a part of the enterprise, and is a part of normal operations. Splitting of key critical functions and their location at a reasonable degree of geographic separation, is such a resilience measure. Load-balanced IT systems with synchronous or close to synchronous data mirroring and automatic re-routing of all transactions to the surviving system are another good example. "Withstand" is not appropriate because it does not contain this concept of designed-in automatic switching and contains no concept of the degree of damage, although it conceivably could be used in a physical sense, such as the wind resistance of a structure. "Recovery" implies the triggering of a set of highly specialized, generally quite elaborate procedures to re-create a defined pre-event capability, and would require activities that are not part of normal operations, being invoked only when the normal operational procedures and facilities have failed.

Sean Lyons: Looking back on the trends and developments which have occurred in this area since the early fire fighting days of emergency operations and crisis management, what developments most stick out in your mind and why?

Kathleen Lucey: Fault tolerant systems were the first step. Load-balanced systems in the same location were the second. Load-balanced systems remote to each other with data mirroring were the third. This is all in IT, which has made considerable progress. Very little has been done to assure continuity of critical business operations that is automatic. Little has been done to strengthen either the culture of the enterprise or to revise its hierarchical model. Exercises are conducted infrequently and are often quite artificial. Exercises that perform realistic simulations of emergency and crisis management functions are extremely rare outside of the military. Not a lot of progress there, although there are a very few.

Sean Lyons: What do you believe are the main characteristics of a resilient organization and what are the main component parts which an organization should focus on?

Kathleen Lucey: Splitting of critical operations with co-heads of departments in different geographic areas. Assuring reserve capacity to absorb interrupted operations in each of these. This provides automatic management backup and operations backup. Other than this, the organization should carefully map its dependency chains, including

equipment, people and specific skill sets, equipment, suppliers. Dependence should be reduced as financially appropriate through cross-training, maintenance of critical spares on-site, duplication of suppliers where possible, and other measures.

Sean Lyons: In terms of a best practice framework which an organization should adopt, are there any particular frameworks which you consider most suitable when implementing a resilience program in the corporate world?

Kathleen Lucey: I have not heard of any formal framework that adequately addresses this issue. But I do not know everything. The Resilience work being done at Carnegie Mellon's SEI may apply.

Sean Lyons: Unfortunately for many organizations their approach to resilience is a business continuity plan which is often no more than a slightly upgraded disaster recovery plan which gets dusted down once a year for a pre-arranged off-site test. What in your view are the main challenges currently facing those responsible for resilience in terms of getting the business buy-in on the importance of embedding resilience into day to day activities?

Kathleen Lucey: Knowledge, skills, and budget. Testing is a particular challenge: a 3-year rolling testing structure should be implemented that demonstrates progress to a more realistic scenario with each exercise. And the concept of "passing the test" should be outlawed, especially for auditors. We test to discover what is wrong, not what is right. A primary objective of every test should be to discover shortcomings or inadequacies in programs, plans, and knowledge.

Sean Lyons: As corporate social responsibility assumes greater priority, a reactionary approach to disaster and other contingency scenarios is no longer considered acceptable if organizations are to protect their people, operations and shareholder value. In your opinion does the corporate world need to undergo a change of paradigm in order to take sufficient proactive measures to protect not only the continuity of the business but also the health and safety of its stakeholders?

Kathleen Lucey: Definitely yes. The markets will punish those who do not protect employees and communities, and shareholders and customers (remember just how much dependency there is on third parties for critical functions now) at least in the developed world. This will not be simple, however, because the governing model in the corporate world, with certain exceptions, is still fundamentally a military hierarchy designed to assign accountability to individuals rather than to empower all.

Sean Lyons: In order to ensure resilience is appropriately prioritized within an organization those responsible for resilience must have appropriate status and authority within their organizations. In your opinion where should the responsibility for resilience ideally rest in the corporate framework in order to be most effective?

Kathleen Lucey: All control disciplines should report to the Chief Risk Officer, who then reports to the Risk Committee of the Board. See attached presentation entitled "Aligning BCM into the Firm's Overall Governance Model: From Shared Principles to Shared Governance" for an organization chart which includes the following:

- Business Continuity
- Crisis Management
- Emergency Management / Facilities
- Information Security
- Physical Security
- Records Management
- Safety
- Insurance

It is essential that these functions not reside within corporate or divisional silos.

Sean Lyons: Resilience is concerned with addressing not only high impact low probability threats but also focusing on low impact high probability threats, even though the nature of these threats is continuously evolving. Where do you see the major corporate threats coming from in the next 5-10 years, and what can be done to address these threats?

Kathleen Lucey: [As follows]

A. Supplier failure: Diversify suppliers.

B. Lengthy equipment replacement times: Maintain spares or additional equipment used for less critical operations.

C. Knowledge loss: Create loyalty, not fear, among employees. Cross-train.

D. Insider attacks, particularly within IT: Control of privileged accounts. Careful and continuous monitoring of behavior. Appropriate use of encryption to protect confidential data.

E. Infrastructure failures: Appropriate levels of maintenance and enhancement.

All of these are considerably more probable than a catastrophic terrorist attack or a natural disaster.

Sean Lyons: Effective resilience requires investment. What advise would you give to those with responsibility for resilience when putting forward the business case for resilience in their organization?

Kathleen Lucey: The key is to demonstrate the usefulness of resilience for the more probable and less catastrophic interruptions by measuring cost savings, which equates to higher profitability. The "insurance against total failure" argument has been used for a

long time and is not effective. It is, however, absolutely critical to measure the benefit of resilience measures when an event occurs in order to demonstrate the cost savings.

Sean Lyons: Traditionally responsibility for disaster recovery and/or business continuity was seen as being the task of IT or operational risk. Evolving views of resilience such as enterprise and operational resilience suggest that resilience consists of a number of imperatives which include risk management, compliance, security, continuity and IT. What are your views in terms of resilience as an interdisciplinary concept?

Kathleen Lucey: All of the control disciplines are doing the same things, just in different areas. It is wholly incorrect for resilience to be seen as part of the IT responsibility. It will fail each time that this is the case. Please refer to attached presentation which addresses the convergence of corporate control disciplines into an overall governance model, for more details.

Sean Lyons: How can organizations adopt a more holistic approach to resilience and create the appropriate integrated strategies and mechanisms across the enterprise in order to help address resilience issues?

Kathleen Lucey: This answer is relatively simple: reorganize its control disciplines into an integrated organization reporting outside of divisional or corporate silos. Only when the professionals can speak to each other and when best practices can be applied universally will we be able to see what is correct, what is insufficient, and begin to address inter-disciplinary difficult issues.

Sean Lyons: In your view where does resilience currently fit into the broader concept of an organization's program of self-defense and how do you see it developing going forward?

Kathleen Lucey: All control disciplines should be integrated:

- Information Security (computer security, data security)
- Records Management
- Emergency Management
- Crisis Management
- Business Continuity Management (disaster recovery, contingency planning, resilience)

All of the control disciplines work to minimize the probability and severity of incidents and all are concerned with controls to reduce incident-related effects: injuries and/or damages. This includes corporate officer protection and physical security, as well as public relations and employee protection. The benefits of the convergence of these disciplines include:

- The cross-pollination of control cultures erodes knowledge and jargon barriers
- Missing or ineffective controls are easier to see when all are grouped together
- Duplication of efforts can be eliminated

- Risk Management budgets can be allocated across the company, instead of competing for resources within department or silo-level organizations

See attached presentation for more details on how this integration of corporate control disciplines can be achieved.

Originally Published at the RiskCenter (www.riskcenter.com) *on the 6th November 2008*

INTERNAL CONTROLS

Jim Kaplan
Founder & CEO of AuditNet®

About Jim Kaplan

Jim Kaplan is the Founder and CEO of AuditNet® the largest free Internet portal for the audit, financial and compliance community. He has a Master of Science in Accounting from the American University in Washington, D.C. He is an active member of the Institute of Internal Auditors (IIA), the National Association of Local Government Auditors (NALGA) and the Association of Certified Fraud Examiners (ACFE). He is the 2007 recipient of the IIA's Bradford Cadmus Memorial Award and the 2005 Association of Local Government Auditors Lifetime Membership Award. Jim was a contributing editor for The Internal Auditor, the professional journal of the IIA. His column covered the different ways that auditors used computers and software. His writing has appeared in the Internet Bulletin for CPA's and Internal Auditing Alert. He is the author of The Auditor's Guide to Internet Resources 2nd Edition, published by the IIA. Jim developed an interest in electronic communications for audit professionals in the early 1990's through the use of bulletin boards and online commercial information services. As the founder and principal of AuditNet®, he developed an Internet Web site that links auditors around the world with over 1,300 audit related resources and over 2,000 audit work programs. Jim, a volunteer seminar leader for the Institute of Internal Auditors, is an accomplished speaker. He has presented at National and International conferences for the IIA, as well as conferences for ACUIA, AHIA, AICPA, ISACA, MIS Training Institute. He has spoken at local IIA chapters across the United States on various technology topics for auditors. He developed a course for the Graduate School, USDA Government Audit Training Institute called: Integrating the Internet into the Audit Process. As a writer, journalist, educator, lecturer and dedicated local government auditor, Jim has promoted and encouraged the use of technology and the Internet for audit productivity.

AuditNet®

The AuditNet® Web site is considered the premier digital resource for auditors around the world searching for audit-related information.

For more information visit: **www.auditnet.org**

INTERNAL CONTROLS AND THEIR ROLE IN CORPORATE DEFENSE

In this dispatch from the front line author Jim Kaplan the Founder and CEO of AuditNet® shares his insights on the importance of internal controls and their role in corporate defense with Sean Lyons.

Sean Lyons: The COSO Integrated Controls Framework has been with us since 1992 and during this time there have been many changes and developments in the way in which organizations are managed. In your view is such an approach still relevant in 2008?

Jim Kaplan: In my opinion the COSO approach is as relevant in today's environment as it was when the sponsors met and agreed on a common framework for evaluating controls in organizations. COSO is dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices. Control framework and standards must be able to adapt to changes in the environment and COSO has done just that. While the original charter examined the causal factors leading to fraudulent financial reporting, they subsequently examined enterprise risk management and internal controls over financial reporting for small companies. The most recent draft document covers guidance on monitoring internal control systems. This demonstrates the commitment of the sponsoring organizations to ensure that changes in the business environment take into consideration control frameworks.

Sean Lyons: Section 404 of the Sarbanes Oxley act of 2002 requires organizations to report on the effectiveness of their internal control over financial reporting. From your experience what impact has this act had on how US companies view controls and the responsibility for controls within an organization?

Jim Kaplan: In my opinion companies have reached a point where they recognize the importance of controls and where responsibility has been assigned within the management structure. While the method of getting companies to this point may not have been ideal it has had the impact of ensuring compliance through evaluation and reporting. Companies have implemented different approaches to reach the compliance mandate but the important thing is that they are getting there. Controls are no longer viewed as a necessary evil but rather as a part of doing business and an effective control system actually aids in achieving operating objectives.

Sean Lyons: Traditionally in many organizations internal controls have been fragmented throughout the organization with the operational responsibility lying with individual business units. Where do you think responsibility for ensuring that the organization has an integrated internal controls framework in place should ideally be positioned within an organization's corporate structure?

Jim Kaplan: This is an area where each company needs to examine where oversight for an integrated internal control framework needs to be positioned. As senior management

and the Board will ultimately be responsible then they should decide on an entity wide approach to this issue and assign responsibility accordingly. Some companies have set up compliance officer functions while others have assigned the responsibility to internal auditors. The assigned unit should have the full support of management, the Board and the Audit Committee.

Sean Lyons: An organization's internal control requirements should reflect the organizations profile in terms of risks, threats and vulnerabilities. As these can obviously change over time, how can an organization ensure that their internal control environment is adaptable and flexible enough to address the changing nature of this profile?

Jim Kaplan: This is one of the reasons that there needs to be periodic reviews of the control environment. Through the natural course of events there will be new risks, threats and vulnerabilities over time and the control structure must adapt to changes in the overall risk environment of the company. There should be a coordinated effort by the internal as well as the external auditors to monitor the controls environment and adapt to changes that take place in the course of business maturity. As the business experiences paradigm shifts that impact risk factors then the control environment must be reevaluated and modified to reflect changes.

Sean Lyons: Clearly control objectives should be aligned with business objectives at all levels, including strategic, tactical and operational. In your opinion what are the main obstacles which organizations are faced when attempting to address this challenge?

Jim Kaplan: While it may be clear regarding the alignment of control objectives with business objectives this is an area where conflicts can sometimes arise. Organizations can no longer look at these areas in a vacuum based on the legal and regulatory requirements (Sarbanes-Oxley, Foreign Corrupt Practices Act etc.) that are now in place. Organizations therefore need to have a strategy in place that ensures a coordinated effort aligning the two. There should be a strategic plan in place that addresses business objectives in terms of compliance with control objectives. The reporting status of the Internal Audit function to the Audit Committee and Board can assist in ensuring that control objectives are closely aligned with business objectives.

Sean Lyons: Business process control objectives should focus on such issues as integrity (e.g. validity, accuracy, completeness), confidentiality or timeliness etc and the resulting control measures (e.g. preventative or detective) required to be put in place should be based on these control objectives. Can you suggest how organizations can best address this process in a systematic manner?

Jim Kaplan: The most obvious answer to this question is that a strong and disciplined internal audit function is the means to ensuring that control objectives and the control measures are in place and operating as intended. The organization's management is responsible for establishing and maintaining controls. The established policies and procedures should be clearly written and communicated to all personnel. Management needs to conduct periodic assessments of the control objectives and determine whether

the control measures are reasonable and address risk exposures. The internal audit group should be examining and evaluating the control environment as part of their audit plan to identify and report on control weaknesses in the systems.

Sean Lyons: The control measures selected for implementation should reflect the level of comfort or confidence required by the organization while also considering the potential impact on the business process in terms of efficiency and effectiveness. This can often lead to disputes between the business and those responsible for controls. In your experience what is the best way of addressing this issue?

Jim Kaplan: There is a fine balance between the need for controls and the cost and impact of those controls on the business. When evaluating the control environment auditors must consider the risk exposure of the organization and the cost benefit of the control to cover that risk. Obviously if a control will significantly increase cost or impede the organization from operating in an efficient and effective manner then the auditor needs to consider the efficacy of recommending such action. However there are some situations in which the risk is so great that that, in the auditor's opinion, the absence of a control could impact the continuation of the business. The best way to ensure that controls are necessary and reasonable is for the auditors to discuss with management the risk exposures and possible control solutions that will meet management's objectives while minimizing the business impact.

Sean Lyons: Improving technological solutions has resulted in many organizations replacing traditional manual controls with automated control processes. A strong case can be made for this in terms of cost savings however some commentators suggest that moving towards complete automation can create its own new set of risks which can potentially out-weight any cost savings. Do you have a view on this, or do you think it possible to achieve a happy medium?

Jim Kaplan: Obviously there will be risks associated with automated control solutions. This merely highlights the importance of a strong IT audit presence. Technology advances mean that auditors can no longer look at reviewing systems and transactions from a historical perspective. The advent of continuous auditing or monitoring of automated systems is a necessity in the current environment. So the answer is yes there are new risks that could out weigh potential cost savings. Mitigation of these risks can be accomplished by organizations having a strong audit function with auditors having the necessary skills to operate in this environment. Additionally these auditors need to have the appropriate automated tools, such as ACL, Caseware IDEA and other advanced data monitoring tools to identify and detect control weaknesses and prevent, or at least minimize significant losses.

Sean Lyons: We have seen many organizations address risk and compliance issues by setting up centralized functions requiring specialist skills in these areas. Some believe that in general there is not a sufficient appreciation of the specialist skills and expertise required in order to manage the required control infrastructure. In your view does the

importance of internal controls warrant the set-up of a specific internal controls function within an organization similar to a risk or compliance function?

Jim Kaplan: In my opinion the responsibility for reviewing and evaluating internal controls rests with the internal audit function within the organization. By design external auditors will also review controls as part of the assurance function. When organizations set up multiple centralized functions it raises the possibility of internal conflicts. If organizations chose to go this route then there needs to be coordination between the units to ensure that there are no duplication of efforts. Obviously there are costs associated with setting up multiple units for compliance and oversight and to do so without coordination does not make good business sense.

Sean Lyons: Effective controls require investment however tangible returns on control investment are difficult to calculate. What advice would you give to those responsible for internal controls when preparing to put forward the business case for control investment within their organization?

Jim Kaplan: When making the business case for control investments within their organizations, I would advise managers to take into consideration both the actual as well as the intrinsic costs and values of control investments. The risk criteria must include both financial and non-financial items. For example here is a list of risk factors used by one internal audit function:

*IMPACT RISK FACTORS *

1. Volume and Dollar Value of Transactions
A measure of exposure from the volume and/or dollar value of transactions. Select the higher value of either the annual volume or annual dollar value when scoring the risk factor. (Weight 10%)

2. Financial Statement Significance
A measure of exposure arising from the entity's relationship to the asset, liability and revenue accounts. (Weight 5%)

3. Proprietary Nature of Information
A measure of the degree of loss or embarrassment from the misuse of information produced or collected by the entity's operations. (Weight 10%)

4. Impact on Reputation
A measure of the reputation effect on the organization, the business entity and/or customers resulting from a process or control breakdown. The greater the potential negative effect, the greater the impact scoring. (Weight 20%)

5. Impact on Customers
A measure of the effect on customer services resulting from a process or control breakdown. Activities performed incorrectly or inefficiently that

result in disruption, delay or slow down of delivering services to customers will have a high impact score. (Weight 20%)

6. Failure to Meet Organizational Goals and Objectives
The greater the effect that a business unit or process has on organization or department strategic objectives and goals, the greater the related impact score. (Weight 15%)

7. Regulatory Scrutiny and/or Penalties
The greater the extent that activities are covered by enforceable standards, regulations and/or legal requirements, the greater the possibility of noncompliance. (Weight 20%)

As mentioned before the cost of the control should not exceed the benefits derived from implementing that control. But managers must be mindful of the difficulties in assigning dollar values to risk criteria.

Sean Lyons: What do you consider to be the biggest challenge currently facing those responsible for internal controls in terms of getting business buy-in on the importance of controls to an organization and generally speaking from the business perspective how important are controls to an organization?

Jim Kaplan: In the current business environment controls are perhaps more important than ever. When the economy turns south there is enormous pressure levied on individuals and business managers. According to research conducted by the Association of Certified Fraud Examiners (ACFE), U.S. organizations lose an estimated 5 percent of annual revenues to fraud. When the economy suffers, organizations with weak internal controls could see an increase in fraud for the benefit of the individual as well as fraud perpetrated by managers seeking to mask poor performance. Also as businesses retrench and layoff employees the ability to segregate duties becomes an increasing challenge. When this happens it is important that managers initiate controls to mitigate the risk of fraud and misappropriation due to inadequate segregation of duties.

Sean Lyons: Other defense related activities such as governance, risk management, compliance, intelligence, security, resilience and assurance all heavily rely on the quality of the internal controls in place. In your view where do internal controls currently fit into the broader concept of corporate defense and how do you see its impact developing going forward?

Jim Kaplan: Internal controls are an important component of the corporate defense scheme and will continue as long as a business exists. Organizations must also implement other initiatives such as employee fraud awareness programs to highlight that fraud and internal controls are the responsibility of each and every employee within an organization. In a recent survey conducted by AuditNet (www.auditnet.org) 62.3% of the individuals responding indicated that their organization did not have a fraud awareness training program. This goes to the basic premise as to who is responsible for internal

controls within the organization. Managers have the responsibility to establish and maintain adequate controls to minimize risk. Every employee should also be aware of situations where controls are not working. Organizations need to have a program such as a fraud reporting hotline in place to handle employee reporting of control weakness. There also needs to be an effective internal audit function in place that ensures that internal controls are in place and operating as intended. The internal control framework has many components and they must all be considered by corporate management.

Originally published at the RiskCenter (www.riskcenter.com) *on the 23rd July 2008*

ASSURANCE

Michael J. A. Parkinson

Director at KPMG

About Michael J. A. Parkinson

Michael J. A. Parkinson CIA, CISA, joined the Board of the Institute of Internal Auditors - Australia (IIA-Australia) in 1996, was elected Vice-President in 1998 and became National President of IIA-Australia in 1999, serving until 2001. He continued to serve on the Board of IIA-Australia until 2005. From 2001 until 2004, Michael worked as the Host Committee chair for the IIA International Conference held in Sydney in 2004 and served on the International Conference Committee during that period. Michael is the Australian nominee Director on the Board of IIA Global for the period 2008-2010. In 2005, Michael joined the IIA Global International Relations Committee and was appointed its chair in May 2007. During 1994-97 and 2000-01 Michael represented Australia and New Zealand as the International Vice-President of the Information Systems Audit and Control Association (ISACA). During 2003-2006 he also served as the Chair of the ISACA International Education Board. Michael has been the prime motivator and coordinator of a number of technical publications issued by IIA Australia and recently worked with the Global Vision Taskforce to revise the Professional Practices Framework. He currently serves on the Standards Australia OB-007 Risk Management Committee. In 2007 he was presented with the Bob McDonald Award for contribution to the profession. He served as the Honorary Secretary of the Asian Confederation of Institutes of Internal Auditors for 2006-07 and as President of ACIIA from September 2007 to November 2008. He is currently a Director in the government services practice of KPMG Canberra. After 10 years in Information Technology and Government Finance he became an IT internal auditor in the early 1980s. He has worked as a government internal auditor for the last 20 years. Whilst working as a government employee he was the Chief Audit Executive of three different government agencies.

The Institute of Internal Audit (IIA)

The IIA is the internal audit profession's global voice, chief advocate, recognized authority, acknowledged leader, and principal educator. The IIA sets the *International Standards for the Professional Practice of Internal Auditing (Standards),* and provides other timely guidance related to internal control, information technology auditing, risk management, and internal auditing's role in organizational governance.

For more information visit: **www.theiia.org**

ASSURANCE AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Michael J. A. Parkinson, Director on the Board of the Institute of Internal Audit (IIA) Global, shares his insights with Sean Lyons on the importance of assurance and its role in corporate defense.

Sean Lyons: In its broadest sense corporate assurance could be said to represent how an organization obtains a level of comfort or degree of confidence, by what ever means, that everything is operating as expected, and if not, investigating exceptions in order to take appropriate remedial action. Is there a specific definition of assurance which you feel best describes the term and its objectives?

Michael Parkinson: I think the best definition of assurance comes from the dictionary. It is about one individual providing comfort to another. A level of independence in the provision of this comfort is useful but it is not essential.

Managers should be getting their primary assurance from their subordinates; boards should be getting their primary assurance from senior management. Because of the universal tendency to edit the full story when accounting for ones own actions, different levels of independent assurance have developed. The internal auditor is independent of the area being reviewed and is objective but has their primary interest directly associated with the well-being of the organization they serve; the external auditor is completely independent of the organization being examined.

While the (external) audit and accounting bodies have developed definitions for their own purposes, attempting to impose these on management or internal audit is counter-productive.

Sean Lyons: An organization's assurance program can include a combination of assurance options including its executive sub-committees (including its audit, compliance and risk, committees etc), its internal and external auditors, its line management and other external 3rd parties. In your view what level of reliance should ideally be placed on these individual assurance components?

Michael Parkinson: There is an old saying: "trust but verify". In an ideal world, management reporting would be comprehensive and accurate. Quality assurance systems and management supervision would ensure this and, after all, management have the bulk of the resources of the organization at their disposal. If the organization trusts the processes whereby management reports are created it should be able to rely on them – it gains this trust by questioning the managers concerned and asking independent reviewers (such as internal audit) to verify the processes.

External reviewers are usually not subject to the direction of the organization, but their commentary can be accepted as accurate and as indicators of where the organization should apply management attention.

In the usual hierarchy of reliance, the audit committee (or the board) relay on the reports of all the assurance providers and on the basis of these reports and of their own enquiries come to their own conclusions. Management assurance is a critical part of this and is essential in a well run organization. Internal audit assurance might rely on management assurance in some circumstances but will make its own enquiries and will form an independent view. Similarly the external assurance bodies might rely on the work of management and internal audit but will always form an independent view based upon their own work.

It is wasteful to repeat work that has been well done by another body, but it is foolish to simply accept its results.

Sean Lyons: In terms of a best practice framework which an organization should adopt, are there any particular frameworks which you consider most suitable when implementing an assurance program in the corporate world?

Michael Parkinson: There are many models for frameworks and I do not believe that any one of them should be singled out. The critical point to make here is that an assurance framework must be tailored to the organization to which it applies; whatever the model that forms the basis for the framework, it must not be applied blindly.

Even in the corporate world, accountability structures, legal structures and reporting requirements vary widely from jurisdiction to jurisdiction. There is no one best framework. The principles underlying COSO (1992) or CoCo are still applicable and organizations would do well to consider the principles of risk management set out in ISO/IEC 31000 when it is published in mid 2009.

Sean Lyons: What have been the main trends and developments which you have seen over the last 5-10 years in the area of assurance which have impressed you most?

Michael Parkinson: I am not sure that "impressed" is the word I would use, but I have noted a tendency for audit committees to swing between over-emphasis on compliance and over-emphasis on efficiency at the expense of compliance. I think this is sometimes driven by the desire to be different – by this I mean that new players like to be able to say something different from their predecessors – and as a consequence anything that makes a change is favoured. In my view neither one extreme nor the other is desirable. Overemphasis on compliance with procedure, often without questioning the purpose of the procedure, is as harmful as allowing managers to take unnecessary risks. While basic risks to the organization and their associated controls may not be exciting to review it is usually failures in the management of basic risks that causes organizations to fail.

In those places where risk management is properly recognized as a discipline for all managers, it is also recognized that not all risk is a bad thing. The outcomes that can arise from some uncertain situations can be positive. Controls should therefore be about promoting desirable outcomes as well as preventing undesirable ones. When internal audit and management recognize this, they are on the path to a strong organization.

Sean Lyons: In your opinion to what extent has the introduction of legislation such as the Sarbanes-Oxley act 2002 been successful in modifying corporate behavior and in contributing to the introduction of a more robust system of checks and balances in the corporate framework?

Michael Parkinson: Legislation of this kind is well intentioned but, in my view, it has led to an industry of compliance rather than a culture of conformance. Much of the impact of S-Ox has arisen from rules laid down by PCAOB and these rules are complex. In any society where the general attitude is that form is more important than substance will require complex rules to specify the form. We have already seen that these rules have not stopped unscrupulous or foolish behaviour: people are still putting a gloss on bad performance; people are still making poor choices on too little information; people are still taking risks well beyond what the long-term reward warrants.

Sean Lyons: The existence of an audit committee is generally considered an important component in an organization's assurance program. What do you see as being the specific role of the audit committee and how important is the composition of its membership?

Michael Parkinson: The audit committee is critical to the supervision of governance and risk management processes. The audit committee is the agent for the board in ensuring that the risks of the organization are identified and managed and that the reporting (both operational and financial) of the organization is timely and accurate.

The audit committee does not manage the organization, but it is responsible for ensuring that the management processes are in place and functioning.

The committee should be small and should have diverse membership that as a whole understands the organization, the economic sector in which the organization operations, the legal and financial obligations of the organization and the principles of control.

Sean Lyons: What do you consider to be the primary roles of both internal and external audit in the assurance process?

Michael Parkinson: Internal audit has (should have) an organization-wide remit. Its interest is in the long-term health of the organization rather than having any specific loyalty to current management or current owners. Its task is to consider the risks of the organization and, by investigation and testing, provide assurance that the control processes are appropriate to the risks and are operating effectively and efficiently. It has a parallel function of assisting or advising the organization in response to risks that are not adequately managed or risks that might arise from proposed changes to the nature of operations. Internal audit assurance covers the full range of operations and proposed operations of the organization and is directed at all areas of risk.

The external auditor has a statutory obligation to examine certain aspects of the organization. These aspects may vary depending on legislation, but they will never

encompass the same scope as the internal auditor. The form of reporting from the external auditor is also quite limited so the assurance provided is highly specific.

Sean Lyons: In many organizations the business units themselves will claim to be closer to their business and therefore better placed to give comfort or assurance on issues relating to their area. To what extent should the requirements for an independent, objective and impartial opinion out-weigh this on-the-ground experience and expertise?

Michael Parkinson: Business units should be required to provide assurance on their own operations as a part of normal organizational accountability. This does not mean that they should be exempt from review. Independent, objective review can question unstated assumptions and will not have the same blind-spots as on-the-ground management. The best run organizations welcome this form of examination.

Unfortunately, individuals are not always completely honest or transparent in their reporting – especially if there are powerful personal rewards associated with the contents of reports. In such circumstances, the presence of an independent and objective review function will be a motivator to honesty and a potential detector of inaccurate reporting.

Sean Lyons: In recent years the IIA has inserted the term consulting into its definition of internal auditing in an attempt to increase the added-value of internal auditing as a service. In your opinion how can an internal audit function best provide consultancy services while at the same time ensuring that they avoid any potential conflicts of interest?

Michael Parkinson: There are long and complex arguments here. Internal audit has always had a dual function – identifying weaknesses and suggesting improvements. The change in the definition in 1999 did not really change this fact: it brought the definition into line with existing practice.

Internal audit has an assurance program that is determined by the audit committee and it must protect the resources that provide this – that is it cannot allow the, sometimes more interesting, consulting activity limit the achievement of the assurance program. At the same time it has talented resources who may have developed a very deep knowledge of the organization and using those resources in an advisory capacity can be in the long-term interests of the organization.

The *International Standards for the Professional Practice of Internal Auditing* and other parts of the *International Professional Practices Framework* address this issue. In short, however, the suggested mechanisms involve ensuring individual auditors do not review their own work or, where this is not practicable, declaring the conflict and imposing additional quality review on the work.

Sean Lyons: An increasing number of audit conferences and seminars are now referring to an integrated assurance framework as addressing the practicalities of bringing together risk, compliance, governance and audit so that values and synergies can be unlocked and

a more dynamic and sustainable assurance model can be created. What are your thoughts on such an approach?

Michael Parkinson: There are lots of "integrated" frameworks around. In 1992, COSO published an internal control integrate framework. An integrated assurance framework is a subset of an integrated risk management framework – assurance being a component of the risk management process.

Certainly it is a good idea to consider all relevant activity and the extent to which it can be coordinated. Frameworks can be valuable guides for thinking though the issues – identifying objectives, marshalling resources, planning and executing activity and checking the outcomes. Frameworks can also be a vehicle for consulting and sales organizations to repackage old ideas without necessarily improving the result.

Sean Lyons: In many organizations assurance functions are unfortunately seen in a negative light whereby they are considered a necessary evil rather than a strategic asset? What advice would you give to those with responsibility for assurance when putting forward their business case and what do you consider to be the main challenges which need to be overcome?

Michael Parkinson: Controls improve an organization's performance. The addition of brakes to a motor vehicle enables it to go faster and the knowledge that those brakes are functioning gives confidence to the driver and the passengers. While it is theoretically possible for an organization to be over-controlled, the natural tension between line staff and review staff tends to limit the possibility of this.

A well designed system of controls address the risks of an organization – promoting desirable outcomes and limiting potential damage. The purpose of the assurance function is to systematically review these controls to keep them adequate, appropriate, effective and efficient. This is something that line-management will never find sufficient time to do and which the internal auditor has training to undertake.

Sean Lyons: In your view where does assurance currently fit into the broader concept of an organization's program of self-defense and how do you see it developing going forward?

Michael Parkinson: The assurance processes are like an instrument panel. They are not the controls, but they tell the organization's board and top management how the organization is performing and whether the controls are operating correctly. While more effective ways of reporting may be developed, the basic controls and the knowledge that they are working will always be required.

Originally published at the RiskCenter (www.riskcenter.com) *on the 30th December 2008*

GOVERNANCE, RISK & COMPLIANCE (GRC)

Scott L. Mitchell

Chairman and CEO of the Open Compliance & Ethics Group (OCEG)

About Scott Mitchell

Scott L. Mitchell serves as the Chairman and CEO of the non profit think tank called the Open Compliance & Ethics Group (OCEG). He is a recognized leader in corporate governance, risk management, compliance, ethics, eLearning and information technology. Mr. Mitchell was recently appointed to the Committee of Sponsoring Organizations (COSO) Task Force and was recognized two years in a row by Business Finance Magazine as one of the "Top 60 Influencers" in corporate finance. Treasury & Risk Magazine named him to the list of "Top 100 Most Influential People in Finance" and he was recognized two years in row by Human Resource Executive Magazine as one of the top 20 thought leaders regarding the future of human resource management. Mr Mitchell and OCEG have been featured on USA Today, The Wall Street Journal, Compliance Week, Institutional Investor Magazine, Inside Counsel, Inc. Magazine, and other leading publications. His monthly column in Compliance Week Magazine "GRC Illustrated" is recognized as one of the most innovative ways to visually describe the complex issues associated with corporate governance, risk management, compliance and ethics. He has delivered keynotes in several countries including the United States, Canada, Australia, United Kingdom, The Netherlands, Norway, and Singapore. He has also served as a guest lecturer at a number of universities including Arizona State University, University of Michigan and Northern Illinois University. Mr. Mitchell began his career by using his education in both accountancy and computer science at the Small Business Administration, Arthur Anderson, and Anderson Consulting (Accenture). Throughout his career, he has spent equal time in the board room, in the c-suite, and in the trenches consulting Fortune 500 clients.

The Open Compliance & Ethics Group (OCEG)

The Open Compliance & Ethics Group (OCEG) is a nonprofit organization that uniquely helps organizations drive "Principled Performance™" by enhancing corporate culture and integrating governance, risk management, and compliance processes. OCEG currently has 19,000 members.

For more information visit: **www.oceg.org**

GRC AND ITS ROLE IN CORPORATE DEFENSE

In this dispatch from the front line Scott L. Mitchell, Chairman and CEO of the Open Compliance & Ethics Group (OCEG), shares his insights on governance, risk and compliance (GRC) and its role in corporate defense with Sean Lyons.

Sean Lyons: The acronym GRC is becoming an increasingly recognized term. Do you have a preferred definition of GRC which you consider best describes the relationship between governance, risk and compliance and the objectives of GRC?

Scott Mitchell: Yes, I do – OCEG has recently stated our formal definition of GRC, because we have seen a lot of confusion about this relatively new but critical term.

We define GRC as a system of people, processes and technology that enables an organization to:
* understand and prioritize stakeholder expectations;
* set business objectives congruent with values and risks;
* achieve objectives while optimizing risk profile and protecting value;
* operate within legal, contractual, internal, social and ethical boundaries;
* provide relevant, reliable and timely information to appropriate stakeholders; and
* enable the measurement of the performance and effectiveness of the system.

And OCEG has defined 8 Universal Outcomes for a GRC system:

- Achieve Business Objectives
- Enhance Organizational Culture
- Increase Stakeholder Confidence
- Prepare & Protect the Organization
- Prevent, Detect & Reduce Adversity
- Motivate & Inspire Desired Conduct
- Improve Responsiveness & Efficiency
- Optimize Economic & Social Value

We base this definition on the premise that an organization implements a GRC system to provide a pathway to what we call Principled Performance®, so let me explain that for you as well.

Principled Performance® is the clear articulation of an enterprise's objectives, both financial and non-financial, and the methods by which it establishes and stays within the boundaries it will observe while driving toward those objectives. Principled Performance goes beyond ethical performance, economic performance or corporate social responsibility.

It's important to note that Principled Performance® means defining "right" for an individual company, then doing the "right" things the "right" way -- not only to create value, as in the traditional view of an organization's purpose, but to protect value, address

uncertainty and help the organization stay within its customized boundaries of conduct as well.

So, back to GRC. A number of key business processes help organizations achieve Principled Performance®. While there are many activities and functions that contribute -- such as internal controls, audit, assurance, quality, IT, HR and others -- 13-letter acronyms just don't catch on. So GRC stands in for all of those critical functions and represents the synergistic effect of an integrated approach, the creation of a whole that is far more than merely the sum of its parts. Within the context of the integrated GRC system, all the individual functions share a mutuality of interest, a common need for information and contribution to the organization's efforts to achieve Principled Performance®.

Sean Lyons: GRC as a concept has been described in many different ways. It has been described as a technology, a methodology, a philosophy, a discipline and even a federation of professional roles. This has led some to say that it is almost easier to describe what it is NOT. How would you describe GRC?

Scott Mitchell: This is an issue tackled recently by our President, Carole Switzer, in response to a blogger who was challenging the validity of GRC as a concept, and who mistakenly identified it as nothing more than a term created by technology vendors. So let me share her comments with you.

GRC is not a dashboard, a technology solution, or a buzzword for compliance at all cost. Nor is it just ERM on steroids, as some would say. Nor is it a fad - just another acronym to drive consulting engagements.

GRC represents a paradigm shift in approach to business management and governance of an enterprise. It is a philosophical and structural view of how an enterprise can use its resources (human, technological and financial) to ensure that the organization meets its objectives while staying with the boundaries set by both law and choice of the board and the C-suite.

GRC is about ensuring that the organization has clearly established objectives and the means to meet those objectives efficiently and effectively - identifying risk and ensuring compliance with both external requirements and internal policies and procedures. It is not just about ensuring compliance; it is about achieving what OCEG calls Principled Performance.™

The IT tools being created to help in that effort - the GRC solutions or parts thereof — are an essential piece of this puzzle but they are not the puzzle. Having integrated GRC requires establishing the strategy, controls, policies/procedures, measures AND technologies to ensure that consistent and accurate information flows up, down and across the organization, enabling true governance.

Sean Lyons: GRC is a relatively new term and appears to be still evolving as a concept. Could you tell us something of the history of GRC, its origins and what have been the main developments to date?

Scott Mitchell: OCEG began to drive the discussion about integrated GRC and develop the process model that details GRC structure more than 5 years ago. The acronym GRC, which had been used for a few years by PwC in regard to their consulting services, was adopted more broadly by OCEG and then others starting in 2003, when thought leaders in the ranks of OCEG's charter members began discussing how the areas of governance, risk and compliance are interrelated. Since then, hundreds of experts (legal, audit, risk, compliance, ethics, finance, quality, IT, and others) have contributed to creation and ongoing refinement of the OCEG Framework and thousands more have reviewed it when in public exposure drafts and used it since it became final three years ago. August 11th, OCEG will be releasing Version 2.0 of its GRC Capability Model, which is at the heart of the OCEG Framework. Anyone register at www.oceg.org can download it and provide comments to us.

Sean Lyons: In terms of best practice frameworks which an organization may wish to adopt, are there any particular frameworks or maturity models which you consider most suitable when addressing the GRC challenge?

Scott Mitchell: Most countries don't have any clear framework to offer to their businesses to build investor confidence and attract additional capital in the areas of governance, risk, or compliance. However, you look at any one of the functions that contribute to GRC in isolation (like HR, IT or audit) and globally, there are plenty of best practice frameworks and, in some cases, maturity models. The OCEG GRC Capability Model™ serves as a meta-framework pulling this information across disciplines into one integrated framework. And given that hundreds of experts from all of the relevant areas of expertise have participated in its development, we are pretty confident that it is the essential tool for anyone developing, improving or evaluating a GRC system.

Sean Lyons: Traditionally in many organizations the responsibility for governance, risk and compliance has been somewhat fragmented throughout the organization. In your opinion where should the responsibility for implementing a GRC initiative ideally rest in the corporate framework? Who should be the driving force behind GRC?

Scott Mitchell: Because GRC involves a variety of functions, the responsibility for execution has to be cross-disciplinary, but it shouldn't be undertaken in a siloed or fragmented approach. Who should drive integration? What should it look like? To realize a high-performing GRC system, several key players must be actively involved in the design, implementation and management of the system. Let me summarize the more detailed discussion that we have in the Red Book.

The Board or whatever oversight authority you have must be charged with oversight of the GRC system. The Board must:

* direct the purpose and desired outcomes of the system;
* set a charter for its involvement in the system;
* vet business objectives and ensure they are congruent with values and risks;
* be knowledgeable about the design and operation of the system;
* obtain regular assurance that the system is effective;
* provide reasonable assurance that management's representations are sound; and
* operate aspects of the system that require Board perspective and independence.

Some of those aspects are:
* monitoring any control activities conducted by senior management;
* monitoring senior management's override of control activities;
* selecting, evaluating, compensating and terminating senior management; and
* addressing long-term issues that may exceed senior executive tenure.

Management must undertake strategic planning and implementation of the GRC system. Taken as a whole, management must:
* design, implement and operate an effective system or some aspect of a system at the direction of the Board;
* provide regular assurance about the effectiveness of the system;
* communicate with stakeholders about the effectiveness of the system; and
* evaluate and optimize the performance of the system.

Management should obtain and provide regular assurance about the effectiveness and performance of the GRC system. An independent review can open up a view of the system that reveals not only weaknesses in design or operation, but also opportunities for further integration and exchange of best practices from one area of the organization to another. For its part, the Board is required to obtain regular assurance about the effectiveness of the system and to use information developed independently of management to form impressions of the system's effectiveness. Independent review is required; internal or external personnel can conduct independent reviews.

Assurance personnel must:
* provide assurance that risks are correctly identified, evaluated, managed and monitored;
* provide regular assurance to the Board and management that the GRC system or some aspect of it is effectively designed to address identified risks and requirements in light of the organization's culture and objectives;
* provide regular assurance to the Board and management that the system or some aspect it is effectively operating as designed.

Sean Lyons: The distinction between GRC and ERM has been the subject of much debate. GRC has been described by some as ERM plus the integration of governance and compliance, while others argue that ERM already addresses governance risk and compliance risk. What are your views in relation to this debate?

Scott Mitchell: In a sense, anything can be re-characterized as a risk, but that can turn things on their head. We have governance structures to efficiently make sound decisions throughout the organization to conduct operations and generate value not because lacking structures poses a "governance risk". We've heard people argue that governance already includes risk management and compliance. We've heard compliance professionals characterize governance and risk as compliance activities. What all of these perspectives have in common is the fact that GRC activities do fit together and have critical relationships to one another. This is why OCEG is helping organizations approach GRC with an integrated capability, defining process interactions and information flows.

Sean Lyons: In your opinion, what are the GRC leadership essentials that organizations in general should focus on in the achievement of their GRC vision?

Scott Mitchell: We see the idea of leadership and champions existing at any number of levels within the organization. Essentially the role of a leader or champion has to include breaking down barriers to change, developing buy-in for the GRC system, and communicating how the desired GRC outcomes are being achieved and contributing to organizational objectives. It is essential for any GRC leader to demonstrate strong character ethics and be role models of normative values to the organization and its stakeholders. As such, they must be competent in their respective areas of responsibility and should demonstrate personal integrity.

Beyond this general notion of leadership, there are three key leadership roles in achieving GRC outcomes: the Board (or governing authority), management and assurance. Combining these roles in a system of checks and balances that aligns with the culture, structure and processes of the organization is the key for the execution of their respective responsibilities contributing to the realization of verifiable GRC outcomes.

Sean Lyons: Introducing a GRC approach within an organization obviously requires a certain level of investment. What advise would you give to those with responsibility for GRC when putting forward its business case in terms of a value proposition for their organization?

Scott Mitchell: Frankly, the top three drivers for investment in the three years before 2007 were all "compliance" related. Our community of practice told us through our 2007 GRC Strategy Study that the most important element to their business case was a "specific problem that involved significant payout". That history has jaded the perspective on what it should take for the value proposition. Once you get past compliance as a historical justification, the mandates for a business case are pretty standard: i) clear alignment to business objectives and ii) clear articulation of value. The good news was that there is a plethora of ways to demonstrate the benefit side of the equation whether you focus on stakeholder benefits, financial benefits, process benefits, or workforce and cultural benefits.

Fundamentally, the biggest challenge is that organizations don't know what their current approaches are already costing them so they can't assess the value that could be

generated by GRC over the current state. So, start defining the total cost of current approaches and start getting those measures in place. One of the great skill sets within GRC is risk analytics, leverage that skill set in building the business case so your organization is properly allocating capital and resources.

Sean Lyons: What do you consider to be the biggest challenge currently facing GRC in terms of getting business buy-in on the importance of GRC to an organization?

Scott Mitchell: We asked our community of practice several question in our 2007 GRC Strategy Study to understand this dynamic. They told us that they knew their organization was adversely affected by process redundancies and that they could create efficiencies by standardizing approaches. They even knew that the greatest impacts were increased operating expenses and the costs of reconciling disparate information. However, an overwhelming majority said they'd either be guessing or quite simply couldn't estimate the current level of resources used pursuing governance, risk, compliance or enabling technology. Since there are in fact so many potential entry points into GRC, even if you take the easiest point of entry (i.e., where you have a compliance issue), as long as you take the right approach, you can then leverage that investment to demonstrate the value and create a series of business cases to perpetuate the approach throughout the organization, building grass roots buy-in.

Sean Lyons: In terms of GRC market segmentation, business analysts in this space have yet to agree on accepted market categories. In your opinion how important is it that this issue be addressed?

Scott Mitchell: What we have been seeing is that the clarity of OCEG's message around GRC is cutting through the confusion created by enterprising professionals equating their background in one area of compliance to full GRC experience hoping to capture more market share. OCEG's GRC Capability Model™ delineates what constitutes core capabilities from risk area specific domain content. Our experience is actually that the major multi-national organizations that would be providing consulting services in the area of GRC are not really segmenting the market as between GRC facets. Instead, they are addressing the unique perspectives and needs that the particular buyer with whom they are speaking has into the larger GRC picture.

On the technology front, there has been significant debate on how to characterize solutions. For a period of time, the label "GRC" was slapped onto almost every technology offering out there. OCEG's Technology Council has embraced and engaged in that debate, ultimately identifying 60 "technology components" inclusive of hardware, applications, and information services. The new Red Book identifies how and where discrete Technology Components can be used to enable GRC. We have those Technology Components categorized across business applications, GRC core applications and infrastructure and we have done so without any bias toward a build versus buy or a cohesive versus composite approach to delivering these components. Each Technology Component is linked to each of the elements (series of practices) in the Model that they enable and they serve as a bridge into OCEG's GRC Blueprint™ which further delineates

architectures and case studies. The OCEG Technology Council is also aiding the IT community by creating the GRC IT Roadmap as a means of helping them get started in the process of implementing a GRC technology strategy.

Sean Lyons: The GRC territory appears to be expanding beyond governance, risk and compliance and certain GRC vendors have extended their product features to include additional components such as controls, assurance and indeed other defense related activities. Do you think that the term GRC may prove somewhat restrictive when attempting to bring these related but distinctive activities together, given it appears to prioritize governance, risk and compliance ahead of these other components?

Scott Mitchell: From its inception, GRC has never just been those three things. We've always embraced the fact that GRC involves multiple processes and disciplines and is more than the sum of its parts. So, perhaps since the market is still fairly young in the integrated GRC perspective, we have to do a little more messaging around its breadth. But, the fact that there are multiple pathways simply means more opportunities to communicate how all these disciplines come together to deliver GRC outcomes.

Sean Lyons: In your view where does GRC currently fit into the broader concept of an organization's program of self-defense and how do you see it developing going forward?

Scott Mitchell: It's safe to say a strong GRC system is *essential* to self-defense. In the Universal Outcomes – where we started this conversation – you'll note that *protecting* value is in only a quarter of the outcomes. Three-quarters is focused on *creating* value. But even though GRC eclipses the concept of self defense and extends beyond that notion to driving Principle Performance®, you simply cannot say your are well protected without it. Without an integrated approach to risk, consistency of approach to compliance efforts across silos, and an ability to gather and parse the same information for multiple purposes, as we like to say, its not "good governance", its only guessing governance.

Originally published at the RiskCenter (www.riskcenter.com) *on the 12th August 2008*

INFORMATION TECHNOLOGY

Lynn Lawton

International President of the Information Systems Audit and Control Association (ISACA)

About Lynn Lawton

Lynn Lawton, CISA, FBCS CITP, FCA, FIIA**,** is the International President of the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). Previously, she was a vice president on ISACA's International Board from 1999 to 2002, and returned to the International Board as an appointed director of ISACA in 2006. A member of ISACA for the past 19 years, Lawton has served on the North of England UK Chapter Board for 10 years, including six years as chapter president. She also served on ISACA's global Standards Board for four years, prior to chairing it for two years, and set up and chaired ISACA's Governmental and Regulatory Agencies Board for three years and its Assurance Committee for one year. Lynn is a director at KPMG LLP in London, UK, where she is responsible for risk management for KPMG UK's Performance and Governance services at KPMG's UK Advisory Services function. She has more than 20 years of experience providing IT assurance services and security advice across a range of industries. She has led teams of IT audit and security specialists engaged in activities including the IT aspects of financial statement audit and internal audit, as well as improving business and IT processes and controls and system security, system testing, benchmarking of information security, IT strategy implementation and outsourcing implementation.

The Information Systems Audit and Control Association (ISACA)

The nonprofit, independent ISACA® is a global leader in IT governance, security, control and assurance. Founded in 1969 as the EDP Auditors Association, ISACA is the single, leading international source for information technology controls. ISACA is dedicated to serving the needs of IT governance professionals.

For more information visit: **www.isaca.org**

I.T. AND ITS CORPORATE DEFENSE REQUIREMENTS

In this dispatch from the front line Lynn Lawton, the International President of the Information Systems Audit and Control Association (ISACA) shares her insights on information technology (IT) and its corporate defense requirements with Sean Lyons.

Sean Lyons: Information Technology (IT) is increasingly becoming an invaluable part of business in the 21st century however with this the task of defending the IT environment has also become an increasing challenge. What in your opinion have been the most significant developments in this area in recent years?

Lynn Lawton: Information and the technology that supports it have become some of the most valuable assets of all types of organizations, yet at the same time, they are often the most intimidating and misunderstood. One of the most important developments in defending the IT environment is the dominance of mobile technology and the complete thought-change needed to continue to protect IT. Security experts previously focused on firewalls and controlling the perimeter of an organization, but the perimeter is now boundless and many organizations are actually reducing expenses by allowing customers and vendors access to their systems. Privacy is another growing issue for organizations, with increasing governmental regulations and public interest in what organizations do with information and how it is being protected. There is an increased risk with outsourcers and the potential, for example, for them to sell credit card numbers. Wireless and miniaturization need to be addressed because people now have the ability to walk away with sensitive information on small devices such as thumb drives. In light of these developments, defense must move beyond an IT issue and be the responsibility of all stakeholders.

Sean Lyons: The requirement for good corporate governance has traditionally been restricted to the boardroom however IT governance is now also receiving a great deal of attention. What specific aspects should an organization consider when selecting and implementing an IT governance framework?

Lynn Lawton: More people are getting involved in governance over IT, and that has tremendous commercial benefits for the organizations concerned. According to the *IT Governance Global Status Report 2008* (www.itgi.org), three-quarters of respondents indicated that a C-level executive (CEO, CFO or CIO) is the champion for IT governance, and 68 percent of business managers participate in, or lead, IT governance decision-making. The survey also showed that IT governance maturity and the importance an organization puts on risk management follow a linear growth pattern. Just like corporate governance, effective governance over IT is a boardroom issue. When considering an IT governance framework, such as *Control Objectives for Information and related Technology* (COBIT), important attributes are that it links to business requirements, organizes activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered. The *Board Briefing on IT Governance* advises that boards should, among

other activities, measure performance by defining and monitoring measures and leveraging a system of balanced business scorecards that are maintained by management.

Sean Lyons: In recent years the introduction of a multitude of laws and regulations has meant that IT compliance is now an increasingly onerous element of IT management. In your opinion what specific compliance requirements have had the most significant impact on IT management?

Lynn Lawton: IT compliance should no longer be viewed as a sunk cost, but rather as a value-adding activity. Even compliance with regulations such as Sarbanes-Oxley and Basel II, which have had tremendous impact on enterprises around the world, can improve controls and security, which affect the bottom line. The goal is to integrate requirements into the enterprise as a whole. The maturity of IT governance risk and compliance (GRC) practices for managing reward and risk has a direct impact on organizations. Enterprises with the most mature practices have been found to deliver the best business results, according to *Annual Report 2008* from the IT Policy Compliance Group.

Sean Lyons: Managing IT risk is increasingly complex given the potential cascade of consequences which can result. IT risk is not only concerned with direct 1st order consequences to IT assets etc, but also with the knock-on indirect 2nd and 3rd order consequences which can occur further down the line on the business process side. Have you seen examples of organizations which have been able to successfully integrate the management of IT risk with other enterprise risks?

Lynn Lawton: Education and communication among all levels of an organization are vital to ensure that risks are recognized and addressed. While the impact of an IT failure can be devastating to an organization, there is also the risk of failing to take advantage of an opportunity to use IT in a way that further benefits the organization. Improving competitive advantage or operating efficiency are two examples of this. Sanjay Bahl, CISM, chief security officer of Tata Consultancy Services (TCS), India, was named the winner of the second annual Excellence in Security Convergence and Contribution to Enterprise Risk Management (ERM) Award because of his expertise in the growing fields of ERM and security convergence. At TCS, an IT services, business solutions and outsourcing organization with a presence in 50 countries, Bahl established an enterprise-wide converged security environment and effectively addressed risk management and security across the organization. By adopting a model of security convergence covering all physical, informational and human aspects of the organization, he achieved multiple benefits for the company, including layered security measures, multiple regulatory compliances and a lower cost of ownership by involving multiple stakeholders and putting in place initiatives to ensure continuous improvement.

Sean Lyons: Information is increasingly regarded as one of an organization's most valuable assets and hence the task of securing this asset is also considered important. What are your views on the value of security management now including the convergence of both physical and IT security in order to manage enterprise risk.

Lynn Lawton: Because of many factors, including the increase in terrorism and security breaches, the convergence of physical and IT security is inevitable and brings many benefits. It is a natural evolution that enables businesses to protect all of their assets more effectively and efficiently operationally, and to achieve financial efficiencies too. Information is a critical, yet intangible, asset and even traditional physical assets now rely greatly on information, for example a smart card verifies a person's identity while also tracking his/her physical location. The whole organization should be involved in security because all departments need to combine efforts to detect, prevent, respond to and recover from incidents. Organizations benefit by integrating strategic planning and risk management in a consistent and holistic manner. Ensuring consistency of risk assessment across physical and logical security increases efficiency and cost effectiveness and reduces duplicate investments.

Sean Lyons: Many IT professionals believe that in order to achieve an effective IT control environment there is a requirement for a consistent application of standards, guidelines, and procedures throughout the enterprise. Others would argue that there is no such thing as a "one size fits all" solution and that requirements need to be tailored to suit the prevailing circumstances encountered. What are your views in relation to this debate?

Lynn Lawton: Actually, both sides of the debate make good points and fortunately there is guidance that directly addresses this issue. Enterprises need to have consistent policies in place, but the implementation needs to be customized for each environment. I am somewhat biased because I have been involved for many years, on a volunteer basis, with the nonprofit IT Governance Institute (ITGI) and its development of COBIT, which is a globally accepted set of tools for governance over IT. COBIT was specifically designed as a framework that can be customized for all sizes and types of organizations, be they businesses, nonprofits, academic institutions, governmental agencies or other entities. COBIT provides the over-arching structure that harmonizes with more specific guidance, such as ITIL, ISO 27002, and CMM. Basically, COBIT helps ensure an organization's IT is helping it achieve its goals and objectives. It helps reduce IT-related risks and increases confidence in the information provided by IT. COBIT has a business orientation that links business goals to IT goals, providing metrics and maturity models to measure their achievement. It also has a process focus that clearly subdivides IT into four domains and 34 processes. Developed and refined over the years by teams of international experts—all highly respected business people who have volunteered their time and expertise to ITGI—COBIT is freely available for download from *www.itgi.org*. Case studies showing how organizations around the world have utilized COBIT are at *www.isaca.org/cobitcasestudies*.

Sean Lyons: IT assurance is a critical aspect of the enterprise decision making process as reliance on IT is increasingly becoming a core element of business decision making. To this end IT audit is central to any IT assurance framework and therefore is the focus of an increasing amount of interest. In your view what are the core issues which differentiate an IT audit function from other types of audit functions?

Lynn Lawton: IT audit is a critical function in today's enterprise. Technology-based systems have replaced many formerly manual and clerical activities, and regulators worldwide require increased control and reporting. One issue that differentiates IT audit is the rapid change of the technical expertise required to be effective. New technology is brought onboard all the time and each advance has a great impact on the organization, often introducing new weaknesses and loopholes. IT audit needs to stay a few steps ahead to prepare for these advances and mitigate any new risks. Another issue is the need for excellent business communication skills. IT auditors need to speak in terms that executives relate to about what problems may exist and how they may be fixed. They also need to communicate with technical specialists about what is needed to get the job done. In addition, since most organizations rely on networked systems, IT auditors can perform their work from a central location, even if the equipment is distributed around the world. This allows for the potential for near continuous auditing.

Sean Lyons: We are seeing that various defense related activities such as governance, risk management, compliance, intelligence, resilience, controls and assurance are increasingly becoming core elements of the IT management framework. Traditionally in many organizations these activities have operated in isolation of each other even within the IT department. What guidance can you give to organizations hoping to integrate these activities in order to help ensure that they are all in alignment?

Lynn Lawton: COBIT is focused on aligning all of these disparate facets of an organization into a cohesive program of governing IT for a variety of enterprises. It has been recently updated to include more executive management-level guidance and a common language to communicate goals, objectives and expected results.

Sean Lyons: Defending an organization's IT environment requires further investment however tangible returns on this additional investment are difficult to calculate. What advice would you give to those responsible for IT defense when preparing to put forward the business case for IT defense investment within their organization?

Lynn Lawton: Organizations traditionally have a less than stellar record of capturing value from intangible assets such as information and IT. People responsible for IT defense need to show clearly that the IT investments are not specifically about technology, but rather should be viewed as investments in enterprise change, security and improvement. Everyone in an organization will have a different viewpoint of what constitutes value. The goal is to address these differences and focus on what will propel the organization closer to its goals. The business case should include answers to the "Four Ares,"[2] based on relevant business-focused information: Are we doing the right things, Are we doing them the right way, Are we getting them done well, and Are we getting the benefits. The process of developing a business case should be owned by the business sponsor and involve all key stakeholders. Expected business outcomes—including lead and lag indicators—should be identified. Details on the six steps of business case development are explored in *Enterprise Value: Governance of IT Investments, The Business* Case, popularly known as Val IT, which is available as a free download from

[2] Reference to the "Four Ares" concept by John Thorp, author of "The Information Paradox".

www.itgi.org. Other research also supports the business case. The *2008 Annual Report* from the IT Policy Compliance Group shows that protecting customer data pays organizations back by supporting higher revenues, larger profits, increased customer satisfaction and retention, reduced financial loss and risk, lower spending on regulatory compliance, and providing better alignment between business objectives and IT capabilities.

Sean Lyons: What do you consider to be the biggest challenges currently facing IT functions in terms of getting business buy-in on the importance of IT defense to an organization?

Lynn Lawton: Senior executives respond to strong business cases that benefit shareholders and focus on achievable ROI. Do the research and clearly outline in non-technical language the potential risks (including to the organization's finances, personnel and reputation). Also build the business case by outlining expenditures, resources needed, outcomes (financial and non-financial) and how the project aligns with enterprise goals.

Sean Lyons: What do you predict will be the most serious threats facing IT over the coming years and how can organizations prepare to address these threats?

Lynn Lawton: I agree with the findings of the *IT Governance Global Status Report 2008*, which showed that insufficient IT staff availability, service delivery issues, and difficulty proving the value of information technology (IT) will continue to plague executives at organizations around the world. On a good note, 93 percent of respondents said that IT is somewhat to very important to the overall corporate strategy—an increase of 6 percent from 2005. In addition, IT is always on the board agenda, according to 32 percent of respondents—up from 25 percent in 2005, and 8 percent of respondents said the IT department always informs the business about potential business opportunities, up from 14 percent in 2005. Technology is changing so rapidly right now, we have to stay constantly updated and become involved in industry groups to monitor and prepare for future advancements.

Sean Lyons: In your view where does the role of IT management currently fit into the broader concept of corporate defense and how do you see its role developing going forward? Do you think that responsibility for IT defense should reside within the IT management function?

Lynn Lawton: IT management and defense need to be aligned with the enterprise's overall goals and objectives. In fact, 72 percent of general management members agree strongly that IT investments create value for the organization. Executive management holds the overall mandate for ensuring IT defense of the enterprise, but at the same time, it also is every stakeholder's responsibility. The weakest link is not the central server, but the mouse (and mouth) of the user.

Originally published at the RiskCenter (www.riskcenter.com) *on the 3rd of July 2008*

SUMMARY REVIEW

Sean Lyons

Series Editor and Producer

About Sean Lyons

Sean has been described as a leading pioneer within the contemporary corporate defence movement, being a firm advocate of the requirement for corporate defence to play a more eminent role in corporate strategy. He is the resident contributor in the field of corporate defence for the RiskCenter, a New York financial risk management media company, based on Wall Street. He is also the architect of the related cross-functional discipline of Corporate Defence Management (CDM) and has already had a number of papers published internationally on this and other defence related topics. His work has been published by such publishers as the RiskCenter, the Bank Director, the Corporate Board Member, the Journal of Operational Risk, the Business Continuity Journal, StrategicRISK, Information Management (formerly the DM Review), GTNews and by organizations such as the Global Association of Risk Professionals (GARP), the Risk and Insurance Management Society (RIMS), the Risk Management Association (RMA) and the Open Compliance & Ethics Group (OCEG). Sean has lectured and spoken on these topics at seminars and conferences relating to Corporate Defence and Corporate Defence Management (CDM), Enterprise Risk Management (ERM), Governance, Risk & Compliance (GRC) and Business Resilience, in both Europe and North America including Canada, the United States, the United Kingdom, the Netherlands and Portugal. Since graduating from the University of Limerick (Ireland) with a Bachelor of Business Studies (BBS) degree in 1988, he has amassed two decades of experience in the banking and financial services industry, working as an Operational Trouble-shooter, Internal Auditor and Management Consultant. He has previously worked with, held senior management positions with, and/or been a professional advisor to, a number of leading financial organizations in the Republic of Ireland, United Kingdom and Australia. Employers and clients have included HBOS, KBC, INVESCO, CIGNA and Saudi International Bank. He is currently operating as an independent management consultant and corporate defence advisor, where he offers professional services in the emerging area of corporate defence management.

For more information on his published work visit: **http://ssrn.com/author=904765**

CRITICAL COMPONENTS WHICH MAKEUP AN ORGANIZATION'S PROGRAM FOR SELF-DEFENSE

In the final dispatch of this series Sean Lyons provides a summary review of the insights shared by our expert commentators on the critical components which makeup an organization's program for self-defense. The series included features on governance, risk, compliance, intelligence, security, resilience, controls, and assurance, and their perceived roles in defending an organization. He also considers the extent to which the management of these activities needs to be fully appreciated by all those presiding over the necessary changes now required to help ensure the development of more robust corporate frameworks going forward.

APPRECIATION

Throughout this series we have been very fortunate to have received extremely insightful views and opinions from established experts in their specialist disciplines. The Q&A sessions featured respected and emerging commentators with outstanding credentials and well qualified to impart their knowledge relating to their respective fields. I would therefore like to begin by publicly thanking each of the participants for sharing their experience and expertise with us throughout this series.

SUMMARY REVIEW

During this dispatch I will be providing a abstract summary of some of the key insights expressed by our learned guests which particularly resonated with me. This summary review addresses the series from an overview perspective, with a high level corporate defense focus in mind. Please refer to the individual features for more detailed analysis.

CORPORATE DEFENSE

This series focused on the term "corporate defense" as an umbrella term used to represent the management of those critical activities which constitute an organization's program for self-defense. During the series we saw how each of these defense related activities represent a critical component, and has an essential role to play in helping to defend an organization, and indeed the interests of its various stakeholders. As there are a large number of stakeholders who rely on these activities to operate effectively, every organization requires that these activities are managed in an appropriate manner. The following in my own view represent some of the key issues which were highlighted during the series.

GOVERNANCE

Richard M. Steinberg, CEO of Steinberg Governance Advisors, Inc.
In our feature on governance and its role in corporate defense Richard Steinberg was of the view that the term "governance" used in context of a business organization, is best preserved for the workings of the board of directors, however he acknowledged that it is

also used much more widely, getting into what management does to run a company. He described corporate governance as the allocation of power between the board, management, and shareholders, placing specific emphasis on the board of directors as the central point in governing a company, and its relationship with management and the company's owners. He explained that from a legal perspective, this involves directors carrying out their duties of loyalty and care, and acting in good faith. He went on to state that good corporate governance comes down to the board providing effective advice, counsel and where necessary direction to the CEO and senior management team – along with carrying out its required monitoring activities. Management's responsibilities must be subject to oversight at the board level, therefore one key board responsibility is to oversee what management is doing to identify, analyze, and manage risk, and understanding to what extent agreed limitations on the company's risk appetite are being met. Management must establish appropriate business processes to deal with risk, ensure compliance, secure its information and resources, and the like, and provide sufficient information to the board so it can become comfortable with these activities. At the board level, he suggests focusing on guidelines that, while covering the basic fiduciary responsibilities, emphasize where and how the board can add real value to the organization to grow share value. He acknowledged that scandals tend to provide the impetus for boards to take the necessary steps to become comfortable that management has set the right "tone at the top," through not only words but also actions that permeate the culture of the organization. He went on to explain that an organization's culture is shaped by management's philosophy and operating style, the company's organizational structure, and its policies, processes and people. The culture is established over the history of a company, and has a profound effect on how it responds to internal and external events. He noted that corporate culture should be about embracing integrity and ethical values which means doing the "right thing", and may require sacrificing short term gains in order to enhance long term share value. This means ensuring that performance measures align with both the strategy and compensation metrics for the CEO and top management team. He pointed out that compensation today is a lightening rod for institutional investors and should be in line with long term performance. An area too often overlooked is having a sound plan for CEO succession – both in an emergency and longer term – and being prepared in advance for a crisis situation that may suddenly arise. He stated that communications with shareholders, including transparency in financial reports and maintaining an open channel for major shareholders, also require attention. Finally he concluded that effective governance at the board level, and what's done throughout the management structure, is critical to defend against a broad range of challenges and threats. Processes and related activities at all levels must be established and executed effectively to avoid harm.

RISK

Dr. David M. Rowe, Director of PRMIA

In our feature on risk management and its role in corporate defense David Rowe explained that he viewed risk management as the process of assuring that risk versus return decisions are made on a well informed basis with as much insight as possible into possible adverse events. He stated that risk management is vital to long-term success and

that the value of a firm is driven largely by two fundamental factors, the market's expected growth in a firm's earnings and the discount rate it applies to those future earnings. In his view risk management's role is to enhance long-term value by reducing the risk-based discount rate applied by the market to its expectation of a firm's future earnings. The task of the business side of an organization is primarily to raise the expected growth in earnings (subject to a constraint on risk). He explained that it is important for risk managers to recognize that the goal is not to eliminate risk but rather to assist their organizations in judging whether prospective returns warrant assuming the risks involved, leavened with the recognition that some risks are necessary for a business to survive and prosper. He noted that it is the breadth of the potential dangers that makes the emerging role of the chief risk officer (CRO) especially challenging and expects the role of the CRO to grow to encompass broader responsibility for strategic and business risk in addition to narrower risk measurement, monitoring and management functions. He went on to explain that one requirement for long-term corporate success is constant vigilance and the will to act when threats emerge. By its nature, risk management always must react to innovations on the business side of an organization, creating an inevitable lag in the ability to deploy comprehensive assessments of the risks. The key challenge is to manage the gap between ideal risk management information functionality and the reality of risk systems actually in place and operational to assure it does not grow dangerously large. He suggested that as in politics so it is in risk management, there are no final victories as management of all kinds is a constant challenge of making decisions under uncertainly. It also requires thinking holistically so that some thought has been given to how certain events might play out in practice. He points out that this enhances the ability to respond quicker to an emerging crisis, since some of its implications will have been reasoned out in advance. Specific areas of risk require a wide range of detailed idiosyncratic indicators that are appropriate to issues of a particular type. The challenge at the enterprise level is to capture how these risks may interact if things go wrong. He suggested that integrated risk management should not mean trying to distill risk down into some single summary metric but rather it is the continuous process of evaluating how specific risks in different areas may accumulate or reinforce each other in especially damaging ways. He noted that historically too much reliance was placed on technical quantitative modeling without questioning the underlying data and assumptions involved, and suggests that what is required is blended econometric modeling with seasoned judgment. By building a sound risk assessment process, based on both technical quantitative analysis blended with judgmental inputs from a wide range of sources, a firm can gain a reputation for avoiding the most damaging mishaps. He predicts that the painful consequences of the subprime mortgage crisis will serve to accelerate the transition to a blend of quantitative analysis and judgment. He noted that in the end, risk management needs to involve a process that regularly incorporates feedback from macroeconomists, country risk specialists, lawyers, accountants, operations managers and others into a continuing dialog around large emerging risk issues. Finally he states that in his view risk management is effectively synonymous with the corporate defense function

Philip Martin, Chairman of the Institute of Operational Risk (IOR)

In our feature on operational risk and its role in corporate defense Philip Martin noted that operational risk, unlike market or credit risk, is unique in that it touches all parts of a

company's business. He stated that it was worth considering that it is major operational risk events that destroy companies rather than credit or market risk events, however there is still a long way to go before operational risk management is on the same footing as credit or market risk management disciplines. He suggested that aspects of the current credit crunch can be put down to a failure to understand the effects on a product or a portfolio when the three risk categories collide. He stated that ultimately operational risk events are largely caused by two things, either it is an act of God (earthquake, windstorm, flood), or it is a person – doing something they should not be doing, or not doing something they should be doing. He was of the opinion that operational risk, because of its unique characteristics, makes a mockery of those who argue that "if you can't measure it, you can't manage it!" and went on to state that for a while, it seemed like the quantitative world was dominating and even controlling the operational risk management debate and that therein lay the road to madness! Attempting to place a number on a risk that depends on an individual's behaviour and then use that to drive a capital requirement made little sense. Further, some of the measurement approaches were so complicated that they could only be understood by the individual who designed the mathematical equation. He argued that companies have spent millions of dollars in developing such "black-box" approaches which have been of little use to those who run the business. However he also explained that recent conferences and workshops have focused very much on the practical aspects of operational risk management techniques rather than the theory. He noted that proactive risk management is about excellent communication across business lines so that all business units understand how their actions can impact on others and having the discipline to tackle potential obstacles. He viewed the concept of enterprise risk management (ERM) as an interesting one, noting that it's easy to say, but not easy to do. An ERM initiative can create considerable conflict as to who will be responsible for what and it takes strong leadership to make this work. In his view within the financial services industry, ERM is still a relatively new concept and there are few companies who are prepared to put their hands up and say that their ERM initiative has been a success. He also noted that it certainly makes sense for all risks to be proactively managed across a business rather than in silos. He pointed out that when the good times roll, profits can cover up a multitude of problems and argued that it is quite clear that the events of the last 12 to 18 months within the global financial services community have significantly moved the risk management goal posts. He concluded that going forward operational risk management ought to be front and centre in a company's program of self-defense.

Steven J. Dreyer, Managing Director at Standard & Poor's

In our feature on ERM and its role in corporate defense Steven Dreyer described S&P's view as seeing ERM as an organizational commitment to manage risks holistically across the enterprise. While many firms can be successful at silo-based risk management, and be recognized for it favorably in the S&P ratings process, the idea of looking at managing risks more broadly is a new concept in their ratings process. He noted that their ERM analysis will focus initially on risk culture and strategic risk management as these elements are universally applicable and comparable across organizations of various sizes, sectors, and locations. S&P will be less concerned with drilling down to all levels of the organization to identify risk principles in action, but will focus more on understanding how senior management and the board sets and implements risk policy. He explained that

S&P are considering ERM to be a broader concept, not only downside risks but encompassing also the exploitation of risks on the upside. He suggested that companies with effective ERM avoid surprises but also optimize risk-adjusted returns. He pointed out that effective ERM can help firms avoid outsized, unexpected losses and those that achieve the full benefits of ERM may be able to optimize risk/return tradeoffs in making strategic decisions, which can lead to enhanced returns over a long period of time. At the same time he explained that S&P did not expect to see too many firms that demonstrate and advanced holistic approach. He emphasized that effective silo-based risk management is considered a minimal requirement for strong credit ratings, but would not by itself indicate that a firm was optimizing ERM as a tool for enhanced risk-adjusted returns, resilience in responding to adversity, and overall stability. He acknowledged that S&P are focusing on broad culture, strategy themes and consistency of communication, and that the CRO is of interest to S&P if that person is accountable for important risks the firm faces, has significant visibility with senior management, and has a direct line of communication with the board of directors. He noted that S&P view self-defense or resilience, focused as it is on the downside risks, as a key ingredient in ERM.

COMPLIANCE

Roy Snell, CEO of the Society of Corporate Compliance & Ethics (SCCE)

In our feature on compliance and its role in corporate defense Roy Snell stated that implementing the essential elements of a compliance program is a critical first step in any corporate defense activity. He outlined the key elements of a compliance program which he stated include auditing, monitoring, education, anonymous reporting mechanism, reporting to the board, discipline, investigations, and policies and procedures. He stated that a compliance program was very important in developing a culture of compliance within an organization and suggested that compliance is not complex, but it's hard because most people don't have enough courage to implement the basic elements of a compliance program. The elements of a compliance program are important and are what you need to be successful. He stated that organization's do way too much talking about doing the right thing and need to start auditing, monitoring, and enforcing the behavior we are looking for. He stressed that employees are tired of all the talk, they want to see leadership back up their words with action. He put forward the view that it is a very exciting time in compliance with the job of the compliance officer making the top ten lists of the hottest jobs in the country, as settlements drive the implementation of compliance programs and the hiring of compliance officers. He stated that the Sarbanes-Oxley act could go away tomorrow and nothing would change, as society is tired of corporate wrongdoing and the enforcement community is simply reacting to society's request for change. In his view an effective chief compliance officer (CCO) makes sure that each department implements and maintains the essential elements of a compliance program. His advise is to just try to keep things simple where possible, noting that successful people try to keep things simple. The intent is to find and fix regulatory compliance problems. He pointed out that if you want to eliminate the need to defend yourself, don't do anything that would require you to defend yourself, and he suggested that by finding and fixing your problems and you will reduce the need to defend yourself. He concluded that in relation to an organization's program for self-defense that

compliance (finding and fixing problems) is the single most effective use of an organization's time and money.

INTELLIGENCE

Stephen Walker, technology markets analyst at the Aberdeen Group

In our feature on intelligence and its role in corporate defense Stephen Walker noted that intelligence in the corporate world is fundamentally about driving improved business performance. He explained that intelligence was especially valuable when mapped back to corporate objectives and overall business goals. He suggested that effectively monitoring, measuring, and reporting on business-focused performance metrics and objectives, can be substantially aided by incorporating business intelligence (BI) tools that enable the processes, policies, and procedures that govern defense related activities to be consistently mapped back to the company's overall business goals. He stated that ineffectively communicating strategic corporate goals to daily process owners is a common problem in small and mid-size companies, and is even more common in large companies. Errors stemming from inaccurate, incomplete, or conflicting information from multiple sources is an even bigger concern if the company has an expansive footprint with multiple, disparate operations. He noted that BI analytic tools such as dashboards are bridging the transitional gap that exists between the collection of relevant information and the ability to make actionable decisions based on that knowledge. He suggested that by acting as a conduit between the executive team and the intelligence-tasked employees, the chief intelligence officer (CIO) enables full-circle communication characterized by affected employees knowing and proactively working towards the achievement of strategic business goals. He stated that intelligence is most effective as a full circle process characterized by not only ensuring that the right individual within the organization has real-time or near real-time access to the most accurate, current, and topically-relevant information that he / she needs to advance business objectives, it is just as important that the outcome or result of the use of that information (i.e. deal closed, project milestone reached) is fed back through the intelligence loop and disseminated to the individuals who can use that intelligence to gain advantages in other areas. He put forward the view that the success or failure of other critical defense activities like governance, risk management, and compliance is, to a large extent, based on how pervasive intelligence is within the company's structure. To get beyond the "check-the-box" mentality and approach towards these activities that is so prevalent in many organizations, and to start driving sustainable business advantages, intelligence needs to essentially infect itself into the corporations DNA. Embedding intelligence into critical business processes, particularly risk and compliance, cannot be viewed as an option, but must be considered compulsory. Finally he noted that going forward intelligence needs to be integrated into every aspect of a company's broader self-defense program.

SECURITY

Prof. Stephen Northcutt, President of the SANS Technology Institute

In our feature on security and its role in corporate defense Stephen Northcutt emphasized the importance of developing a culture of security. He recommended that organizations

should focus on two basic things: configure systems and networks correctly (and keep them that way), and detect when bad events occur. If you can do those two things, you are a long way down the road towards information assurance. In his view the position of the chief security officer (CSO) should report to either the CEO or chief operations officer and the folks that have a CSO report to a CIO are creating a conflict of interest situation. He explained that unless you have an architecture that is purpose built to allow the business logic to operate in a risk managed manner, you probably have "Security Theater" - the appearance of security. In his view way too many organizations do not build security from the ground up, but rather treat it like an add-on, so they waste their money and do not achieve their goals. He pointed out that in the beginning of the journey a CSO has to focus on awareness, getting the rest of the organization to understand that their assets are vulnerable. He noted that after awareness is achieved, we tend to see organizations that "get it" and start acting in ways to protect their valuable intellectual property. Hopefully, the organization will settle on an architecture and overall approach for security that allows for a balance between the needs of security and the needs to accomplish business. He suggested that organizations that pursue a culture of security can operate with a much higher risk appetite and pursue business opportunities that elude poorly run organizations. At the end of the day, security should be a business enabler; it should allow you to move quickly, knowing the bases are covered. He pointed out that the security impact of the trend towards ubiquitous computing, being always online, is the need for endpoint security, and that every endpoint, by definition, is its own firewall, its own perimeter. He stated that while the convergence of physical and logical security is happening quickly, as alarms and surveillance cameras run over IP, the amount of security knowledge you need to be effective is exploding. He pointed out that these days, no one can master the entire security domain, even someone working on this full time, so, we are starting to have to specialize. You are seeing people that are full time penetration testers or full time web security specialists. He said he liked the emerging concept of unified threat management (UTM) as a method of saving money on security, but warned that without giving configuration and detection the attention they deserve that it is easily at the cost of security itself. He stated that in the end it all comes back to risk. The first question an organization needs to ask is how much of their total value is comprised of information assets. In terms of the role of security management in the broader sense of corporate defense he explained that the greater the percent of value our information assets are, the closer to the top of the organization the information security leadership needs to be.

RESILIENCE

Kathleen Lucey, President of the Business Continuity Institute (US Chapter)

In our feature on resilience and its role in corporate defense Kathleen Lucey explained that we need to be careful to distinguish resilience from recovery. In her opinion resilience is a designed-in capability that will automatically or nearly automatically "switch on" upon failure of a part of the enterprise, and is a part of normal operations. Splitting of key critical functions and their location at a reasonable degree of geographic separation is such a resilience measure. Load-balanced IT systems with synchronous or close to synchronous data mirroring and automatic re-routing of all transactions to the

surviving system are another good example. “Recovery” implies the triggering of a set of highly specialized, generally quite elaborate procedures to re-create a defined pre-event capability, and would require activities that are not part of normal operations, being invoked only when the normal operational procedures and facilities have failed. She explained that in terms of resilience there had been considerable progress in IT but very little has been done to assure continuity of critical business operations that are automatic. In her opinion little has been done to strengthen either the culture of the enterprise or to revise its hierarchical model. Exercises are conducted infrequently and are often quite artificial and stated that exercises that perform realistic simulations of emergency and crisis management functions are extremely rare outside of the military. She points out that “testing” is a particular challenge and that the concept of “passing the test” should be outlawed, especially for auditors. We test to discover what is wrong, not what is right. A primary objective of every test should be to discover shortcomings or inadequacies in programs, plans, and knowledge. In relation to an organization’s corporate social responsibility she suggested that the markets will punish those who do not protect employees and communities, and shareholders and customers at least in the developed world. In her view organizations should focus more attention on issues such as supplier failure, lengthy equipment replacement times, knowledge loss, insider attacks and infrastructure failures as all of these are considerably more probable than a catastrophic terrorist attack or a natural disaster. She suggested that by splitting of critical operations with co-heads of departments in different geographic areas assures reserve capacity to absorb interrupted operations in each of these and provides automatic management backup and operations backup. Additionally an organization should carefully map its dependency chains, including equipment, people and specific skill sets, equipment, suppliers and that dependence should be reduced as financially appropriate through cross-training, maintenance of critical spares on-site, duplication of suppliers where possible, and other measures. In terms of a more holistic approach to corporate resilience she suggested that all of the organization’s control disciplines work to minimize the probability and severity of incidents and all are concerned with controls to reduce incident-related effects: injuries and/or damages. Finally in relation to an organization’s program for self-defense she stated that as all of the control disciplines are doing the same things, just in different areas, that all of these control disciplines should be integrated.

INTERNAL CONTROLS

Jim Kaplan, CEO of AuditNet®

In our feature on internal controls and their role in corporate defense Jim Kaplan explained that the internal control framework has many components and they must all be considered by corporate management. He explained that the organization's management is responsible for establishing and maintaining controls, and that the established policies and procedures should be clearly written and communicated to all personnel. He stated that management needs to conduct periodic assessments of the control objectives and determine whether the control measures are reasonable and address risk exposures. The internal audit group should be examining and evaluating the control environment as part of their audit plan to identify and report on control weaknesses in the systems. He noted

that the control framework and standards must be able to adapt to changes in the environment as through the natural course of events there will be new risks, threats and vulnerabilities over time and the control structure must adapt to changes in the overall risk environment of the company. He pointed out that this is one of the reasons that there needs to be periodic reviews of the control environment. There should be a coordinated effort by the internal as well as the external auditors to monitor the controls environment and adapt to changes that take place in the course of business maturity. As the business experiences paradigm shifts that impact risk factors then the control environment must be reevaluated and modified to reflect changes. He described how an organizations needs to have a strategy in place that ensures a coordinated effort aligning control objectives with business objectives. There should be a strategic plan in place that addresses business objectives in terms of compliance with control objectives. He pointed out that there is a fine balance between the need for controls and the cost and impact of those controls on the business. However there are some situations in which the risk is so great that that, in the auditor's opinion, the absence of a control could impact the continuation of the business. In his opinion the best way to ensure that controls are necessary and reasonable is for the auditors to discuss with management the risk exposures and possible control solutions that will meet management's objectives while minimizing the business impact. He did however state that controls are no longer viewed as a necessary evil but rather as a part of doing business and an effective control system actually aids in achieving operating objectives. He put forward the view that in the current business environment controls are perhaps more important than ever. When the economy turns south there is enormous pressure levied on individuals and business managers. He warned that when the economy suffers, organizations with weak internal controls could see an increase in fraud for the benefit of the individual as well as fraud perpetrated by managers seeking to mask poor performance. Also as businesses retrench and layoff employees the ability to segregate duties becomes an increasing challenge. When this happens it is important that managers initiate controls to mitigate the risk of fraud and misappropriation due to inadequate segregation of duties. He emphasized that internal controls are an important component of the corporate defense scheme and will continue as long as a business exists.

ASSURANCE

Michael J. A. Parkinson, Global Director of the Institute of Internal Audit (IIA)
In our feature on assurance and its role in corporate defense Michael Parkinson explained that assurance is about one individual providing comfort to another and that a level of independence in the provision of this comfort is useful but it is not essential. He noted that boards should be getting their primary assurance from senior management, that managers should be getting their primary assurance from their subordinates, and that business units should be required to provide assurance on their own operations as a part of normal organizational accountability. He pointed out that unfortunately, individuals are not always completely honest or transparent in their reporting – especially if there are powerful personal rewards associated with the contents of reports. In this context he referred to the old saying: “trust but verify”. If the organization trusts the processes whereby management reports are created it should be able to rely on them – it gains this trust by questioning the managers concerned and asking independent reviewers to verify

the processes. He suggests that in such circumstances, the presence of an independent and objective review function will be a motivator to honesty and a potential detector of inaccurate reporting. Independent, objective review can question unstated assumptions and will not have the same blind-spots as on-the-ground management. He also pointed out that because of the universal tendency to edit the full story when accounting for ones own actions, different levels of independent assurance have developed. In the usual hierarchy of reliance, the audit committee (or the board) relay on the reports of all the assurance providers and on the basis of these reports and of their own enquiries come to their own conclusions. The audit committee is the agent for the board in ensuring that the risks of the organization are identified and managed and that the reporting (both operational and financial) of the organization is timely and accurate. He stated that internal audit assurance covers the full range of operations and proposed operations of the organization and is directed at all areas of risk. Internal audit assurance might rely on management assurance in some circumstances but will make its own enquiries and will form an independent view. He suggests that it is wasteful to repeat work that has been well done by another body, but it is foolish to simply accept its results. He explained that the internal auditor is independent of the area being reviewed and is objective but has their primary interest directly associated with the well-being of the organization they serve. Its interest is in the long-term health of the organization rather than having any specific loyalty to current management or current owners. Its task is to consider the risks of the organization and, by investigation and testing, provide assurance that the control processes are appropriate to the risks and are operating effectively and efficiently. He states that internal audit has always had a dual function – identifying weaknesses and suggesting improvements. As it has talented resources who may have developed a very deep knowledge of the organization therefore using those resources in an advisory capacity can be in the long-term interests of the organization. This can include assisting or advising the organization in response to risks that are not adequately managed or risks that might arise from proposed changes to the nature of operations. In his view the external auditor is completely independent of the organization being examined and that while the external assurance bodies might rely on the work of management and internal audit they will always form an independent view based upon their own work. The external auditor has a statutory obligation to examine certain aspects of the organization and while these aspects may vary depending on legislation, they will never encompass the same scope as the internal auditor. The form of reporting from the external auditor is also quite limited so the assurance provided is highly specific. He noted that the purpose of the assurance function is to systematically review controls to keep them adequate, appropriate, effective and efficient. This is something that line-management will never find sufficient time to do and which the internal auditor has training to undertake. In terms of its role in an organization's broader program of self-defense he stated that the assurance processes are like an instrument panel, they are not the controls, but they tell the organization's board and top management how the organization is performing and whether the controls are operating correctly.

GRC

Scott L. Mitchell, Chairman & CEO of OCEG

In our feature on GRC and its role in corporate defense Scott Mitchell defined GRC as being about people, processes and technology and added that it about ensuring that the organization has clearly established objectives and the means to meet those objectives efficiently and effectively - identifying risk and ensuring compliance with both external requirements and internal policies and procedures. He stated that from its inception, GRC has never just been about governance, risk and compliance and that OCEG have always embraced the fact that GRC involves multiple processes and disciplines and is more than the sum of its parts. He suggested that GRC stands in for all of those critical functions and represents the synergistic effect of an integrated approach, the creation of a whole that is far more than merely the sum of its parts. He explained that what all of these perspectives have in common is the fact that GRC activities do fit together and have critical relationships to one another. Because GRC involves a variety of functions, the responsibility for execution has to be cross-disciplinary, but it shouldn't be undertaken in a siloed or fragmented approach. He suggested that GRC represents a paradigm shift in approach to business management and governance of an enterprise. It is a philosophical and structural view of how an enterprise can use its resources (human, technological and financial) to ensure that the organization meets its objectives while staying with the boundaries set by both law and choice of the board and the C-suite. Having integrated GRC requires establishing the strategy, controls, policies/procedures, measures and technologies to ensure that consistent and accurate information flows up, down and across the organization, enabling true governance. He referred to Principled Performance® as defining "right" for an individual company, then doing the "right" things the "right" way -- not only to create value, as in the traditional view of an organization's purpose, but to protect value, address uncertainty and help the organization stay within its customized boundaries of conduct as well. He emphasized that protecting value is in only a quarter of the outcomes, that three-quarters is focused on creating value. He went on to say that even though GRC eclipses the concept of self defense and extends beyond that notion to driving Principle Performance®, you simply cannot say your are well protected without it. He stated that without an integrated approach to risk, consistency of approach to compliance efforts across silos, and an ability to gather and parse the same information for multiple purposes, as we like to say, its not "good governance", its only guessing governance. He suggested that it's safe to say a strong GRC system is essential to self-defense.

INFORMATION TECHNOLOGY

Lynn Lawton, International President of ISACA

In our feature on I.T. and its corporate defense requirements Lynn Lawton stated that just like corporate governance, effective governance over IT is a boardroom issue. She suggested that IT compliance should no longer be viewed as a sunk cost, but rather as a value-adding activity. Even compliance with regulations such as Sarbanes-Oxley and Basel II, which have had tremendous impact on enterprises around the world, can improve controls and security, which affect the bottom line. The goal is to integrate

requirements into the enterprise as a whole. In her experience enterprises with the most mature practices have been found to deliver the best business results. She noted that education and communication among all levels of an organization are vital to ensure that risks are recognized and addressed. She stated that while the impact of an IT failure can be devastating to an organization, there is also the risk of failing to take advantage of an opportunity to use IT in a way that further benefits the organization. She identified improving competitive advantage or operating efficiency are two examples of this. She noted that because of many factors, including the increase in terrorism and security breaches, the convergence of physical and IT security is inevitable and brings many benefits. It is a natural evolution that enables businesses to protect all of their assets more effectively and efficiently operationally, and to achieve financial efficiencies too. The whole organization should be involved in security because all departments need to combine efforts to detect, prevent, respond to and recover from incidents. She noted that organizations benefit by integrating strategic planning and risk management in a consistent and holistic manner. Ensuring consistency of risk assessment across physical and logical security increases efficiency and cost effectiveness and reduces duplicate investments. Enterprises need to have consistent policies in place, but the implementation needs to be customized for each environment. She stated that IT audit is a critical function in today's enterprise and that IT auditors need to speak in terms that executives relate to about what problems may exist and how they may be fixed. They also need to communicate with technical specialists about what is needed to get the job done. She suggested that COBIT is focused on aligning all of these disparate facets of an organization into a cohesive program of governing IT for a variety of enterprises. IT management and defense need to be aligned with the enterprise's overall goals and objectives. She concluded that executive management holds the overall mandate for ensuring IT defense of the enterprise, but at the same time, it also is every stakeholder's responsibility.

A number of other individual topics were touched on by the commentators which I feel are best addressed as single issues due to their commonality. In many cases the responses received were in my view relevant to all of the defense related activities covered and all involved in these activities could perhaps learn something from one another.

BEST PRACTICE FRAMEWORKS

Richard Steinberg stated that while there are many governance frameworks out there, each serving a somewhat different purpose his advice was to recognize the positives of what's available, and selectively draw from what's most useful to one's organization in developing a structure and supporting processes. He also stressed that so called "best practices" often portray what many boards do, rather than what a handful of the best boards are doing and others would do well to learn from. Michael Parkinson also noted that there are many models for assurance frameworks and that he did not believe that any one of them should be singled out. The critical point he wished to make was that an assurance framework must be tailored to the organization to which it applies; whatever the model that forms the basis for the framework, it must not be applied blindly. He stated that frameworks can be valuable guides for thinking though the issues – identifying

objectives, marshalling resources, planning and executing activity and checking the outcomes. In Stephen Walker's view each individual organization has a unique set of current and future business objectives and a developing trend is to incorporate portions of several established intelligence frameworks. Lynn Lawton stated that when considering an IT governance framework, important attributes are that it links to business requirements, organizes activities into a generally accepted process model, identifies the major IT resources to be leveraged and defines the management control objectives to be considered. Steven Dreyer pointed out that S&P are agnostic about particular ERM frameworks, other than to recognize that an organization that effectively employs a generally recognized framework such as COSO or AS/NZS 4360 would be supplying evidence that it has made a commitment to manage risks consistently across the enterprise. Roy Snell was of the view that too many people are developing complex frameworks that are overwhelming and so complicated people lose the whole point of compliance programs. He warned that unnecessarily complex frameworks can dilute compliance efforts and distract leadership from finding and fixing problems.

RESPONSIBILITY AND ACCOUNTABILITY

Richard Steinberg stated that in relation to corporate governance, at the board level, responsibility rests with the full board. A board's responsibility is to serve the interests of the company and its shareholders, centered on enhancing long term share value. With that said, many responsibilities can be and are best dealt with at the committee level, with many boards having established nominating/governance, compensation, audit, finance and risk committees. Certainly the corporate secretary can be an important support system, making the work of the board that much more effective and efficient. And the CEO of course has responsibility for establishing management structures to carry out the agreed strategy in light of his/her management philosophy and style. Philip Martin also felt that the responsibility for operational risk must rest with the board of directors. He stated that it is all about the "tone at the top". Senior management, starting with the chief executive, must support the involvement of the operational risk management function in the planning of new business initiatives. Roy Snell felt that in relation to compliance the key is independence. The CCO needs to be able to act without pressure to look the other way. The only way independence can be ensured is to have the CCO report to the board. He also stated that delegation is the key as compliance professionals are not responsible for regulatory compliance rather the entire organization is responsible for regulatory compliance. Jim Kaplan felt that this is an area where each company needs to examine where oversight for an integrated internal control framework needs to be positioned, as senior management and the board will ultimately be responsible. He added that managers have the responsibility to establish and maintain adequate controls to minimize risk and every employee should also be aware of situations where controls are not working. Scott Mitchell stated that by combining the roles of the board, management and assurance in a system of checks and balances that aligns with the culture, structure and processes of the organization, is the key for the execution of their respective responsibilities contributing to the realization of verifiable GRC outcomes. Kathleen Lucey explained that the governing model in the corporate world, with certain exceptions, is still fundamentally a

military hierarchy designed to assign accountability to individuals rather than to empower all.

PRESENTING THE BUSINESS CASE

Philip Martin felt that when presenting the business case for operational risk it was important to focus on the benefits to the business. Stephen Walker agreed that selling into the business side of the company is the most effective way to gain budgetary support. He also stated that to a substantial degree, that is dependent on tailoring the presentation of the potential value proposition in such a way that it heavily emphasizes how business goals will be advanced. Scott Mitchell said that the mandates for a business case are pretty standard: i) clear alignment to business objectives and ii) clear articulation of value. The good news was that there is a plethora of ways to demonstrate the benefit side of the equation whether you focus on stakeholder benefits, financial benefits, process benefits, or workforce and cultural benefits. He stressed that fundamentally, the biggest challenge is that organizations don't know what their current approaches are already costing them so they can't assess the value that could be generated by a new initiative. Roy Snell stated that the problem is most CEOs work strictly off of numbers, that they need proof. He warned that if you only measure financial success, you will not only negatively affect compliance efforts, you may encourage non-compliant behavior and suggested that he would try to get a top manager and a Board member to attend a compliance conference. Stephen Northcutt put it simply metrics, metrics, metrics. He explained that security is not voodoo, it is engineering which implies to me that everything can be measured in some shape or form. He explained that you can measure network traffic and incidents, and you can decide what behaviors you want to modify with your awareness programs and measure the level of success. But if you are a CSO and you do not have a metrics focus, you probably are not very successful at presenting the security business case. He expressed the view that you can only truly manage what you can measure. Kathleen Lucey felt that the key is to demonstrate the usefulness of resilience for the more probable and less catastrophic interruptions by measuring cost savings, which equates to higher profitability. She stressed that it is absolutely critical to measure the benefit of resilience measures when an event occurs in order to demonstrate the cost savings. Jim Kaplan noted that the risk criteria must include both financial and non-financial items and that it was important that the cost of the control should not exceed the benefits derived from implementing that control. He did however warn that managers need to be mindful of the difficulties in assigning dollar values to risk criteria. Richard Steinberg suggested that there is sufficient anecdotal information and first hand experience working with boards and senior managements evidencing that sound governance practices indeed do drive positive performance. Michael Parkinson expressed the view that controls improve an organization's performance like the addition of brakes to a motor vehicle which enables it to go faster, and the knowledge that those brakes are functioning gives confidence to the driver and the passengers. Lynn Lawton suggested that the business case should include answers to the "Four Ares," based on relevant business-focused information: Are we doing the right things, Are we doing them the right way, Are we getting them done well, and Are we getting the benefits.

CHALLENGES AHEAD

David Rowe noted that a major challenge is neutralizing the tendency to overvalue a dollar of profit coming in the front door relative to a dollar of profit prevented from leaving through the back door. In effect, profit that is easy to see in the accounting statements tends to be given greater weight than less explicitly visible achievements in loss prevention. Balancing these two contributions fairly is a constant battle and always will be. Making risk awareness part of a corporation's culture is a task of immense proportions and even interim success will only be possible if the board, the CEO and the senior management team, are actively and wholeheartedly insistent on its importance. Philip Martin stated that the well-worn cliché that everyone in an organization is a risk manager is absolutely true as each employee, from the chairman of the board to the security guard on your front door, has a role to play. Of course each employee will have a different role depending on their responsibilities, but it's almost like a neighbourhood watch scheme in your local community. If everyone participates in the effort to prevent crime, pretty soon the incidents of crime will reduce. So it is for operational risk. By building awareness across the company and training staff so that they understand what they are looking for and what is their required behaviour, a company goes a long way towards the development of a robust operational risk management framework. He stated that there is still an image issue in that the front office will frequently view risk as a business "disabler" rather than an "enabler". He suggested the objective was to be regarded as a "trusted advisor". Roy Snell stated that compliance training is not only important within an organization, but it is important that business schools begin to teach the essential elements of a compliance program and the role of the compliance officer. He noted that it's very simple, if you make compliance a part of the review process or the bonus calculation, you will see results. If you just talk about it and don't measure it or reward it, it won't happen. Richard Steinberg noted that he advises his clients to be careful of placing too much responsibility on a chief compliance officer, chief risk officer, general counsel, or chief audit executive etc. Those staff functions can and should provide important support and monitoring, but experience clearly shows that unless line leadership accepts responsibility for risk, compliance and related activities, there are likely to be problems. Jim Kaplan warned that when organizations set up multiple centralized functions there are associated costs as well as raising the possibility of internal conflicts. If organizations chose to go this route then there needs to be coordination between the units to ensure that there are no duplication of efforts and to do so without co-ordination does not make good business sense. For Kathleen Lucey this answer was relatively simple, companies should reorganize their control disciplines into an integrated organization reporting outside of divisional or corporate silos. Only when the professionals can speak to each other and when best practices can be applied universally will we be able to see what is correct, what is insufficient, and begin to address inter-disciplinary difficult issues. Stephen Walker noted that the rise of the GRC market as a whole is exciting for a number of reasons; one of the most important and business-relevant being that a comprehensive GRC initiative offers the opportunity to integrate, converge, and streamline critical, yet historically siloed and discrete, functional areas. When holistically derived, these initiatives directly facilitate and advance embedding the communication channels, escalation procedures, and monitoring and

measuring capabilities that embeds consistent and accurate intelligence on an enterprise wide basis. Scott Mitchell saw leadership and champions existing at any number of levels within the organization. Essentially the role of a leader or champion has to include breaking down barriers to change, developing buy-in for the GRC system, and communicating how the desired GRC outcomes are being achieved and contributing to organizational objectives. It is essential for any GRC leader to demonstrate strong character ethics and be role models of normative values to the organization and its stakeholders. As such, they must be competent in their respective areas of responsibility and should demonstrate personal integrity. Michael Parkinson warned that in any society where the general attitude is that form is more important than substance will require complex rules to specify the form. We have already seen that these rules have not stopped unscrupulous or foolish behaviour: people are still putting a gloss on bad performance; people are still making poor choices on too little information; people are still taking risks well beyond what the long-term reward warrants.

CONCLUSION

Each of the activities addressed in this series addressed the critical and inter-connected components of an organization's program for self-defense which need to be addressed at both macro (strategic and tactical) and micro (operational) levels. These activities are not new and have been in operation in some form or another for a considerable amount of time. Unfortunately as we have recently seen, in good times there can tend to be an imbalance between the focus on new business generation and safeguarding against potential liability. Over the past 12-18 months we have seen extreme examples of the knock on impact (direct and indirect) associated with this imbalance, be it at organization (e.g. Madoff and Société Générale scandals), national (e.g. the US subprime mortgage debacle) or international (e.g. the global economic crisis) levels. If organizations both individually and collectively are to restore stakeholder confidence then ensuring that each organization is committed to implementing a comprehensive and robust program for self-defense is perhaps a good starting place. Those responsible for presiding over the required changes to the existing corporate frameworks would also do well to focus their attention on this topic and perhaps identity a silver lining somewhere in this dark cloud. Rather than yet again introducing even more prescription legislation, perhaps by ensuring that corporate defense activities play a more eminent role in corporate strategy would help address the substance over form issues which currently prevail in many organizations. I would recommend that business schools focus not only on teaching the core elements of these defense related activities but also focus, not only on their critical inter-dependencies, but how these activities can be effectively managed in a more integrated manner. At this point previous suggestions of mine, made some time ago, that organizations should consider the appointment of a director with sole responsibility for corporate defense, and that a stint in corporate defense be considered as part of an organization's CEO succession planning, do not at this time seem at all outlandish. Such a position (i.e. Director of Corporate Defense) would of course carry great responsibility, but if approached in the correct manner should be viewed as a business enabler and trusted advisor to the board and not be as feared by many as, a business disabler. Such a role, rather than being stigmatized, would need to be aligned with corporate objectives in

order to help ensure that the organization is provided with a more balanced view, thereby creating a situation whereby the organization is in a position to make more informed decisions, which are in line with its agreed corporate strategy. The corporate world cannot continue to be drawn (like a moth to a light) to the business upside without fully understanding and appreciated the possible downside, as rewards and their associated risks come hand in hand. In every situation the potential downside exists whether we like it or not, to ignore it or not fully understand it is simply not good business in terms of long term sustainability. A final word of warning, any program for self-defense which is not purpose built and embedded into the corporate culture, as we have already learned to our cost, will end up being no more that what Stephen Northcutt referred to as "Theatre", the appearance and perhaps illusion of self-defense.

My own views on corporate defense as an inter-disciplinary concept and how the corporate world needs to tackle this challenge are already well documented. For those interested in my more recent thoughts in this area please refer to the attached link (The Changing Face of Corporate Defence in the 21st Century).

Feedback
If you would like to provide feedback on this feature, comment on the overall series itself or email suggestions on related topics to be covered in any future series I can be contacted at **sean.lyons@riscinternational.ie**

Originally published at the RiskCenter (www.riskcenter.com) *on 13th of January 2009*

Related Publications on Corporate Defense

By Sean Lyons

The Changing Face of Corporate Defence in the 21st Century

- *Originally published - StrategicRISK – May 2008*

Risk Management's Role in Corporate Defense

- *Originally published- ERM Symposium 2008 – April 2008*

Corporate Defence: Risk Management, Business Resilience and Beyond

- *Originally published - The Business Continuity Journal, Vol. Two, Issue Four, January 2008*

The Corporate Defence Continuum Series

Part (1): Governance, Risk and Compliance (GRC)

- *Originally published -The RiskCenter – 23rd January 2007*

Part (2): Intelligence, Security and Resilience

- *Originally published -The RiskCenter – 29th January 2007*

Part (3): Controls and Assurance

- *Originally published -The RiskCenter – 6th February 2007*

Part (4): The Quest for a Holistic Solution

- *Originally published -The RiskCenter – 13th February 2007*

An Introduction To Corporate Defence Management (CDM)

- *Originally published -DM Review / DM Direct - 15th December 2006*

Challenges Facing Contemporary Corporate Defense

- *Originally published -The RiskCenter – 12th December 2006*

An Executive Guide To Corporate Defence Management (CDM)

- *Originally published -The RiskCenter – 16th November 2006*

Corporate Defence Management: A Strategic Imperative

- *Originally published -The Bank Director – October 2006*

Corporate Defence: Are Stakeholders Interests Adequately Defended?

- *Originally published -The Journal of Operational Risk, Vol. 1, No. 2 Summer 2006*