

**SORMS**

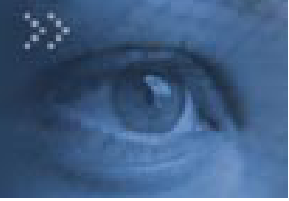
Strategic Operational Risk Management Solutions



# **Operational Risk Management: The Difference between Risk Management & Compliance**

**Bill Sharon, CEO and Founder, SORMS**

Copyright SORMS 2005



There seems to be a good deal of confusion about the role of the compliance function vs. the role of the risk management function. In many organizations risk management has been subsumed into the audit organization and there are a growing number of “risk management” consultancies that are offshoots of external auditing firms. Has audit become risk management and if not, what’s the difference?

In October, 2004, COSO issued its framework for managing Enterprise Risk. A slide in the downloadable PowerPoint summary on the COSO site states:

***“Internal Auditors...play an important role in monitoring ERM, but do NOT (emphasis provided by COSO) have a primary responsibility for its implementation or maintenance.”***

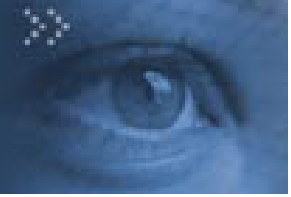
Despite this authoritative statement, we seem to have lost the distinction between risk management and the audit/assurance/regulatory/compliance function. Senior risk management positions listed in the classifieds are defined as “managing the process to meet all regulatory and legislative requirements”. The only arena in which the management of risk in complying with a legal or regulatory requirement would be appropriate is organized crime. Where else would the assessment of whether or not to break the law or be in compliance with established regulatory requirements be considered an exercise in managing risks? Certainly, there may be room for interpretation of a statute or regulation, but if that interpretation puts a company in jeopardy, one might want to find a new set of lawyers and accountants.

That said, the confusion between the two roles continues. Let’s look at what these functions are really about and how, although different, they are inextricably linked.

The operational disciplines which support a business process (IT, HR, Facilities, Finance, Legal, Tax, etc.) all have professional standards, are benchmarked by best practices and are subject to laws and regulations that govern their activities in part or in whole. Comparing the level of adherence to these regulations, laws and best practices is an essential compliance activity and one that the audit organization is best skilled to undertake. A strategy for examining the conformity to required regulations is essential and is often supplemented with control self assessments. This is fundamental to good business practice; it is not risk management.

For example, at its core, Sarbanes Oxely requires transparency in financial processes and establishes standards for executive loans, the timing of trades of company stock, auditor independence, etc. These are all requirements for the functioning of the finance discipline within the company. As the guardians of established financial practices, financial professionals are the primary people responsible for maintaining these standards. The audit function is there to ensure that they are doing their jobs. Is there risk involved if the finance department does not do its job or if they are aware of non-compliance on the part of other individuals and do nothing about it? Absolutely, but the risk is confined to non-compliance, not the management of situations that are either generated through the activities of 3<sup>rd</sup> parties or through the active decision of management to pursue a business strategy.





Risk management, on the other hand, is inherently a process of assembling relevant information upon which the leadership of an organization can make considered judgments about strategic direction, investments, acquisitions, divestitures etc. Certainly the identifications of hazards or weaknesses in the operating environments of companies contribute to the risk profile of an organization and have impact on its ability to achieve business objectives, but these weaknesses are but one component of assessing risks.

For example, if a business wanted to penetrate a new market it would look to risk management to provide an assessment of the likelihood of success of the venture. The HR organization might identify a constricted labor market along with alternatives for addressing the problem. Risk management has the responsibility of coordinating the risk assessments of all of the operational disciplines along with options to address the identified issues. In our HR example the solutions could range from transferring existing employees to paying a premium for local talent to the acquisition of a local company that already has the required talent. With these options identified, business managers can make educated decisions on the course of action that is best aligned with their goals.

We seem to have lost sight of the fact that taking calculated risks is the driving force behind all successful business activities. Managing risk is not just about assessing and quantifying all the things that could go wrong, but, perhaps more importantly, understanding all the things that need to go right for the enterprise to be successful. Somehow we have descended into a culture focused on ferreting out all the issues that could contribute to failure to the point where risk management has become marginalized as overhead to the business process, not a contributor to its success.

How did this happen. Certainly, the excesses of the recent past by a handful of executives have contributed to a demand for transparency and accountability in the business process. This is a good thing. As the application of Sarbanes Oxely matures we can expect that common sense will again prevail and compliance will become a matter of course rather than an expensive pre-occupation.

But the confusion between the audit function and risk management has a more insidious origin. As companies moved to become more efficient over the past 10 -15 years the mantra of “adding value” was preached up and down the corporate corridors. Operational disciplines moved aggressively to position themselves as aligned and essential to achieving corporate objectives. Failure to do so could result in outsourcing or even elimination. The position of the audit function began to gain a reputation as not “value added”. After all, what’s the point of having someone looking over your shoulder to ensure that you are following sound business practices when business is booming?

So auditors became “risk managers” based on the argument that a failure to comply with legislative and regulatory requirements posed risks to the organization. From the standpoint of a dictionary definition there is truth to that argument, but functionally in the organizational environment, it creates serious problems. Risk management is about assessing, both



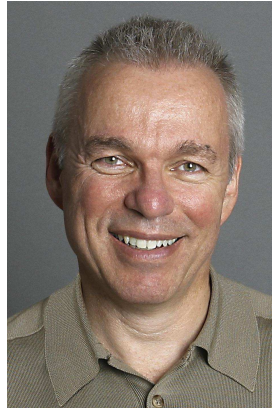
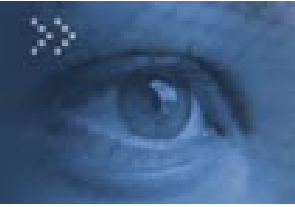


quantitatively and qualitatively the opportunity for success of business initiatives. It is composed of methodologies and processes which are designed to develop information critical to achieving the strategic objectives of the organization. The compliance function is essential to ensure that those methodologies and processes are being followed in the manner intended. Merging the two together essentially means that there is no oversight of the risk management function. Loosing the compliance function in an activity that has become as complex as risk management is not an acceptable outcome.

More importantly, risk management is loosing the relevance battle. We are rapidly achieving risk overload where legions of people are being employed internally and externally to document, categorize and analyze all the things that can and have gone wrong. While increasing the sophistication of the tools designed to avoid the hazards implicit in the business process is useful, the current question is one of balance. We need to position risk management as an aid to business managers in making decisions, not as a check-list of all the things that have and might go wrong. It is human nature to see the failings of the efforts of others as irrelevant to one's own abilities. If risk managers want to be "value added" they need to provide information about the activities that must be undertaken for success rather than only serving up examples of failures.

The unexpected will always happen. Progress is dependent on solving problems that were not anticipated. These events need to be embraced as opportunities to learn and to improve, not as proof that Chicken Little was right. Risk management needs to be a separate and independent function form the audit organization. Compliance is an extremely important a function in today's regulatory environment and risk management is an essential discipline for a complex organization. Clouding the boundaries between the two reduces their value and is ultimately dangerous.





Bill Sharon, CEO and Founder of Strategic Operational Risk Management Solutions (SORMS) has 25 years of experience in the Financial Services and Marketing/Communications industry in a variety of “C” level positions and consultancies. The consistent thread throughout his career is a focus on streamlining operational environments in the service of the business strategy.

At JP Morgan as the COO of Corporate Real Estate, he was a key player in the transformation from a commercial bank to an investment bank through the development and construction of high tech offices in 23 markets that reflected the new organizational culture. He went on to develop cross functional processes for penetrating new markets and establishing new products. He also created the first proactive operational risk management process designed as a vehicle to communicate opportunities as well as issues on a real time basis.

At Price Waterhouse, he established the North American Operational Risk Management practice which focused on the “upside” of risk – the choices an organization needs to make to stay competitive. His clients included American Express where he assisted the organization in evaluating their operational readiness to issue bank sponsored cards in the US and Corning where he evaluated the operational environments of acquisition targets.

Over the last six years he has worked primarily in the marketing services industry, initially as a consultant to McCann Erickson in professionalizing the wholly owned subsidiary that provided IT services and then as a consultant to Interpublic as they began to centralize operational services. Most recently, as the CIO of McCann Worldgroup, Bill developed a global collaborative system as the foundation for supporting the cross-discipline business strategy of Demand Creation. He is featured in the two recent articles on in CIO Magazine and has authored an executive briefing on managing risk in marketing services published by the Cutter Consortium in May 2005.

Bill holds a clinical degree and, for the first ten years of his professional life worked with adolescents in the South Bronx and East Harlem, an experience that taught him the very difficult skill of how to listen. He can be contacted at [bsharon@sorms.com](mailto:bsharon@sorms.com).

