Corporate Compliance

vs.

Enterprise-Wide Risk Management

Brent Saunders, Partner

(973) 236-4682

November 2002

Agenda

- **Corporate Compliance Programs?**
- **What is Enterprise-Wide Risk Management?**
- **Key Differences**
- **Why Will Your Organization Benefit From Enterprise-Wide Risk Management?**
- **A Suggested Process for Imlementing EWRM**

COMPLIANCE DEFINED

A compliance program is a management process comprised of formal reporting structures and risk mitigation systems designed to motivate, measure, and monitor an organization's legal and ethical performance around complex business practices.

-- For manufacturers…it's More Than GXP

Elements of Model Compliance Program Initiatives

1. Written Standards of Conduct
2. Written Policies and Procedures
3. Designate a Chief Compliance Officer
4. Education and Training for All Employees - At Least Annually
5. Audit to Monitor Compliance
6. Discipline Employees Who Have Engaged in Wrongdoing

Elements of Model Compliance Program Initiatives

7. Investigate and Remediate Identified Problems
8. Promote Compliance as an Element in Evaluating Managers and Supervisors
9. Policy to Include Termination as an Option for Sanctioned Individuals
10. Maintain a Hotline to Receive Complaints and Ensure Anonymity of Complainants
11. Create and Maintain Required Documentation

U.S. Sentencing Commission Vice Chair, John R. Steer

"I think the guidelines may need to say something more about the need to have ongoing auditing and testing of a compliance program on paper to ensure that it is effective in practice."

What is Enterprise-Wide Risk Management?

- Best-in-class organizations are looking beyond the basic objective of implementing effective internal controls to satisfy financial and other reporting obligations, when designing their control structures
- They recognize that a company must have a dynamic risk management process that covers significant risk exposures, which augments the financial reporting process and enables the company to identify and respond quickly to changing conditions
- To be highly effective, risk management is being built into a company's infrastructure as an integral part of doing business and is tailored to address the company's critical risk exposures The resulting process is efficient, effective, and non-bureaucratic in nature, as it aligns existing risk management processes, thereby eliminating duplication of efforts

This integrated approach is commonly referred to as enterprise-wide risk management

What is Enterprise-Wide Risk Management?

- **Approached this way, compliance moves away from being viewed as a reactive, activity intensive process and towards being viewed as an active program to help an organization manage a broad range of changes to help it achieve a variety of business objectives in an efficient and effective manner**

- **Enterprise-wide risk management is anticipatory, flexible, and proactive. Enterprise-wide risk management is not reactive**

- **An enterprise-wide risk management framework emphasizes the need for processes to**
  - **Identify risk,**
  - **Assess risk, and**
  - **Monitor and manage changes of all types (financial, operational, legal, etc.)**

- **It is implementable at any level of the organization in whole or in part (i.e. business unit, functional process, geography)**

- **Enterprise-wide risk management helps mitigate surprises and ensures all organizations are aligned with key objectives**

What is Enterprise-Wide Risk Management?

Building in an Enterprise Wide Risk Management program: Current best practice

Most Organization's Today?

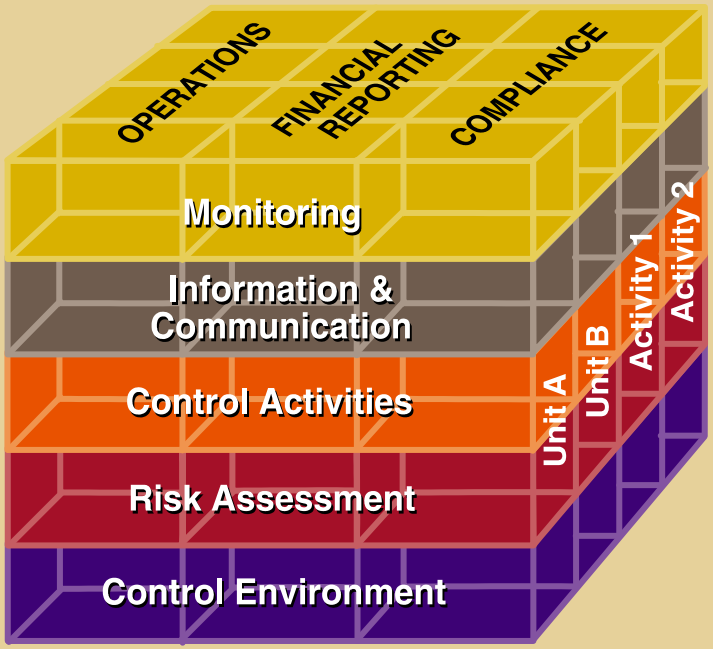
*Pulling together the disciplines that address both sides of risk – minimizing uncertainty and maximizing opportunities – the concept pushes an organization to address risks and their management explicitly – **as part of everyday business***

Enterprise-wide Risk Management is Supported by the COSO Framework

Internal Control is defined (in COSO and US auditing standards – AU 319) as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- *Effectiveness and efficiency of operations*
- *Reliability of financial reporting*
- *Compliance with applicable laws and regulations*

COSO identifies five components of internal control that need to be in place and integrated to ensure the achievement of each of the objectives.

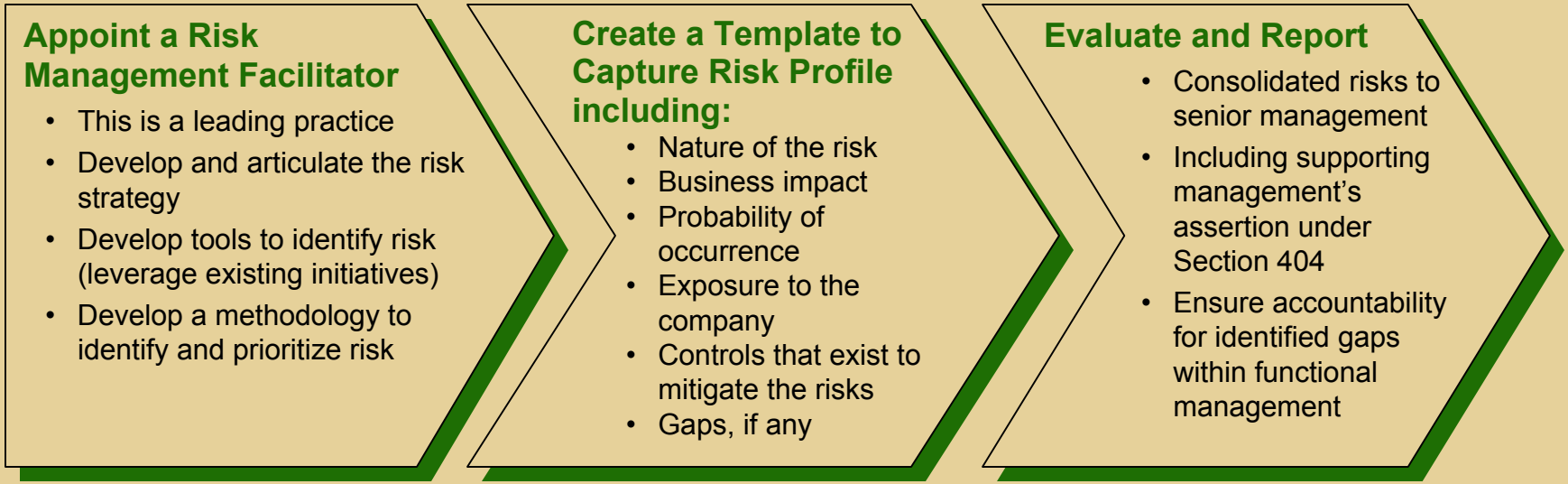


A Suggested Process

- **Assess your organization's current techniques, tools and approaches for evaluating risk across the organization and consider appropriate level of opportunity**
  - **High level view at an enterprise level, or**
  - **Detailed level view at Business Unit level (Sales, R&D, etc.)**
- **Conduct a gap analysis of current risk management practices against leading practice models, identifying existing internal best practices and potential opportunities for improvement**
- **Develop recommendations for developing an enterprise-wide risk management framework specific to your organization including an execution plan to not only identify risks but mitigate them with controls**

Sample Approach for EWRM

- **Once the assessment is complete, design and implement an Enterprise-wide risk management program for your organization**



- **Facilitate decision making and monitor program effectiveness**
- **Functional management will take the lead, with counsel from the risk management facilitator to identify, assess and decide how they will mitigate risks**
- **More structure will be built into the existing processes which will facilitate your organization's ability to be more proactive in the identification, assessment and curtailment of risks**

In Summary, Enterprise-Wide Risk Management Provides:

- **An integrated, dynamic display of business objectives, key risks, and controls that are aligned with supporting policies, procedures, and operating principles**
- **A robust, flexible structure that can deal systematically with both external and internal changes affecting the company**
- **An aligned and supportive infrastructure that facilitates early identification of new risks, communication, training, incident identification, issues management, and internal and external reporting**

Key Difference between Compliance Programs and EWRM

1. Scope - the EWRM program will be designed to proactively identify, assess and manage all risks (strategic, operational, regulatory, and ethical risks) faced by your organization, rather than just fraud & abuse in sales and marketing.

2. Approach to Risk Identification - the EWRM program will formalize the risk identification process. The EWRM program will incorporate a risk identification process into the formal strategic planning process and everyday business activities.

3. Proactive Risk Management - An EWRM program embeds responsbility for risk management at divisional and functional levels enabling your organization to quantify and analyze risk in a more proactive fashion.

4. Results Orientation - EWRM holds managers accountable for identifying and mitigating risk. A formal process for monitoring and reporting progress is established under EWRM.

5. Reduces Cost - EWRM aligns all existing risk management processes (including existing comliance programs) thereby eliminating duplication of efforts