Use of an ERM Map to Implement or Enhance Your Compliance Program

For some time I have wanted to write about an Enterprise Risk Management (EMR) Map that I came across. It is put out by a company called MetricStream. This ERM Map is designed to assist the compliance practitioner in either designing or reviewing a company's Governance, Risk and Management (GRC) by providing a visual representation of the *best practices* in compliance business processes. It allows a company to either develop a gap analysis or classify gaps in its GRC program by better understanding overall system requirements. The ERM Map lays out these *best practices* in a visual format; identifying sub-processes within the specific disciplines involved in ERM; and finally separating such practices in Leadership, Organization, Process and Technology. This post will focus on Leadership and Process and I will discuss these in only some of the areas which are identified by discipline on the ERM Map.

I. Chief Compliance Officer

a. Leadership-the Chief Compliance Officer (CCO) is responsible is the model for ethical behavior and should link ethics to business success. The CCO should be a part of the Executive Leadership Team and work to create a formal compliance program including a Code of Conduct, Compliance Policy and Compliance Procedures to detail how the program should be conducted throughout the company.
b. Process-the CCO should develop processes for monitoring of compliance so that if there is a violation, it can be detected and then remedied. There should be some type of ethics certification and creation of an anonymous reporting or helpline. There should be a formal measurement of compliance and ethics risks and a follow-up analysis of compliance failures to determine lessons learned going forward.

II. Chief Risk Officer

a. Leadership-this role should lead through visibility on the full spectrum of enterprise and operational risk. As risk management is a value generating business process; the role should be a part of the Executive Management Team.
b. Process-this role is responsible for creating the formal process for analyzing and managing enterprise risk across the company. It assists to ensure that the Internal Audit process is risk driven and that financial processes are risk-based.

III. Chief Financial Officer

a. Leadership-the Chief Financial Officer (CFO) should focus the department's efforts on business risk when conducting internal audits. This is broader than simply general audit, Sarbanes-Oxley (SOX) or Foreign Corrupt Practices (FCPA) audits; it should include all business risks. There should be accountability to the company's Board of Directors.

Process-initially it should be noted that ERM should drive audit priorities and the overall audit process should be repeatable and systematic. There should be consistent processes in place between operational and internal audit. In the area of findings, a summary of findings should be reported to the Board of Directors and there should a collaboration of findings with and recommendations to the persons or departments which are audited.

IV. Chief Operating Officer

a. Leadership-the Chief Operating Officer (COO) should be responsible for operational risk and should lead the effort to impart that quality and safety are at the core values of the company. This office should be accountable to regulators, industry and legal standards. The COO should lead to achieve consistent compliance and minimize exceptions.
b. Process-the CCO should lead in the collaboration between quality and regulatory affairs. If there is decentralized accountability, the CCO must consolidate the reporting through centralized record keeping and document control. This role should enhance the collaboration between quality and regulatory affairs.

V. Chief Information Officer

a. Leadership-with a nod towards my "*This Week in the FCPA*" partner Howard Sklar who routinely lists data security as a key compliance concern, I will discuss the role of the Chief Information Officer (CIO) within the ERM Map. The role should begin with expertise on the integration of technological controls into business applications. The CIO should be charged with the centralized management of IT governance and should ensure that the IT environment is secure. This would include protection of information security. Finally as a leadership function, the CIO should ensure that data security is a Board of Directors agenda topic.
b. Process-here the CIO should work to have an overall IT framework assist to drive business processes. There should be a centralized document management and approval system and there should be end-user identity management.

I have but scratched on the surface of the information readily available on the ERM Map. I would urge the compliance practitioner to go to the company's website and order a complimentary copy of the map. It will give you a very good visual road map to create or enhance a complete company-wide GRC structure or allow you to think through any of the departments I have discussed and several others on the ERM Map which I have not discussed. It is a very valuable and free tool.

This publication contains general information only and is based on the experiences and research of the author. The author is not, by means of this publication, rendering business, legal advice, or other professional advice or services. This publication is not a substitute for such legal advice *or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified legal advisor. The author, his affiliates, and related entities shall not be responsible for any loss sustained by any person or entity that relies on this publication. The Author gives his permission to link, post, distribute, or reference this article for any lawful purpose, provided attribution is made to the author. The author can be reached at tfox@tfoxlaw.com.*