Capitalizing on the Convergence of Risk Management Functions: Maximizing the Value of the Compliance Program

2012 HCCA Conference

Joel Dziengielewski
Ken Zeko

Learning Objectives

1. Learn about recent trends related to the overall convergence of risk management

2. Learn how to strategically position Compliance and the Compliance Program in the overall risk management spectrum

3. Learn how to efficiently involve operational areas in the overall risk management process
Presentation Overview

1. Introduction – Increasing Importance of GRC Convergence
2. Single View of Risk
3. Benefits of GRC Convergence
4. A Holistic Approach to GRC
5. Positioning Compliance in the Risk Management Spectrum

1. Optimizing Compliance into the GRC Model

Introduction – Increasing Importance of GRC Convergence

- Companies are exploring new operating models and transforming their businesses to improve profitability and enhance value.
- Driven by the need to reduce cost and drive efficiencies, companies are reassessing their risk and control oversight functions to identify and break down silos.
- Forward-looking companies pursue business transformation activities with a strong focus on governance, risk management, and compliance.
- To ensure risk management strategies are addressing increased business complexity, heightened regulatory and government oversight, and enhanced shareholder and stakeholder expectations, organizations are focused on governance, risk, and compliance (GRC) convergence.
- GRC convergence takes a more strategic look at oversight functions, such as compliance, internal audit, SOX, or operational risk management, and creates a taxonomy and common risk and control language to improve risk coverage, while maximizing the leverage of information and resources.
Single View of Risk

- Risk mechanisms currently deployed by companies often lack a unifying vision and objectives and fail to implement a uniform enterprise risk management strategy.
- GRC convergence replaces this fragmented approach with a single view of risk that is articulated across the entire organization, providing a common language, approach, and methodology for risk management.
- The goal of GRC convergence is to create a centralized platform for monitoring, measuring, and managing risk.
- Such a platform strengthens governance processes and facilitates effective and inclusive risk reporting to management and the board, to help meet global compliance within the corporation’s risk management mandates.
- This single view of risk allows the oversight functions to better leverage risk information and rate issue using a common vision.

Benefits of GRC Convergence

- While benefitting all stakeholders, the advantages of GRC convergence are particularly beneficial to internal audit and other assurance functions due to the broad scope of their risk management mandate.
- Moving forward, effective GRC convergence is likely to be seen as a foundation for continued business success.
- With greater visibility and control over risk across their business, organizations can gain a real competitive advantage, enabling them to make business decisions in alignment with their strategic objectives and risk tolerance.

- Streamlined review and oversight processes
- Reduced burden on business personnel
- Enhanced risk management
- Increased ability to comply with new laws and regulations
- Increased efficiency by using a common language and structure on process, risk, and control
- Greater leverage among risk management and compliance functions
- Increased effectiveness and efficiency in risk management and compliance
- Improved cost rationalization and optimization of the company’s risk management investment
A Holistic Approach to GRC

Holistic Approach to GRC

Success Factors to Drive a GRC Holistic Model

PEOPLE

- An Holistic GRC Model should be designed to bring people, process, and data together for effective convergence.
- It offers a framework in which specific components of GRC can be approached in a methodological way. People are the most important factor.
- Because GRC convergence may impact multiple stakeholders, gaining early buy-in is important. Aligning goals and managing expectations of all key stakeholders is essential, along with clearly defining roles, responsibilities, and accountability.
- GRC convergence can provide organizations a holistic view of their risk skill sets and identify more efficient deployment of these resources.
- It can upscale risk and control capabilities and foster a risk-savvy culture across an enterprise through integrated training and development programs.
- Senior leadership sponsorship is also critical to ensure GRC convergence has broad impact over multiple risk and control oversight functions.
Success Factors to Drive a GRC Holistic Model

- Companies should build a common risk language or taxonomy across the organization that accommodates the unique responsibilities and mandates of all stakeholders.

- A well-defined organizational structure, down to the process level, becomes important when defining and articulating a single view of risk.

- Because many of the risk and control oversight stakeholders may operate at different levels in the organization (for example, SOX may evaluate controls at the process level, but ERM looks at enterprise-wide risk) the taxonomy must accommodate all and allow for risk and control information to be shared effectively by all relevant stakeholders.

- GRC convergence can improve the coordination and alignment of risk management and compliance functions, streamlining oversight processes and minimizing duplicative work.

- Extending beyond the risk assurance functions, GRC convergence facilitates global compliance with risk management mandates across the entire enterprise.

Positioning Compliance in the Risk Management Spectrum

What types of risk assessments are being conducted?

- ERM
- Operational
- Financial
- Compliance
- Fraud
- Quality
- Conflicts of Interests
- Strategic
Positioning Compliance in the Risk Management Spectrum (con’t)

Who is assessing risk?

• The Audit Committee
• Internal Audit
• An ERM function
• The Chief Risk Officer
• Compliance
• Finance
• Risk Management

Other considerations

• How are the risks reported and managed?
• How does the organization talk about risk?
• What is the Board’s involvement?
• Audit Committee, Audit and Compliance Committee, and/or Quality Committee?
• Are the various risk assessment activities spokes in a larger risk management umbrella or do they stop in their individual silos?
• How should risk information be aggregated?
Involving Operations in the Risk Management Process

- Minimize how often operational areas are interviewed regarding various risks.
- Is the organization using common definitions of risk and common descriptions of risk ratings (red, yellow, green vs. high, medium, low)
- Who is accountable for identifying and monitoring risks? And, do they know it?
- Does management have the appropriate tools to identify and monitor risk?
- Does management understand how to identify and monitor risk?
- Remember: Operations personnel have full-time jobs besides assisting with risk recognition and mitigation.

Success Factors for Optimizing the GRC Concept & Compliance

1. Secure support and endorsement from the executive leadership team.
2. Build a governing structure and develop a steering group comprised of leaders from each of the functions included in the convergence efforts, headed by a senior-level leader.
3. Consider all key internal stakeholders and regulatory regimes in the convergence effort and identify all requirements to be accommodated at the outset.
4. Establish guiding principles to ensure alignment with strategic objectives, cross-company buy-in, and consistent progress.
5. Begin with well-defined risk assessment processes.
6. Establish a clear change management plan and implement it throughout the program.
7. Be aggressive, but prudent, targeting achievable goals most meaningful to stakeholders.
8. Take an extended view across the organization to identify opportunities beyond converging control and compliance to other organizational and process changes that may benefit the organization.
9. Think people, process, and data: don’t let a tool or technology alone drive the convergence process.