Six Stages to Addressing Section 404

1. Plan and scope the evaluation.
2. Document your controls.
3. Evaluate the design and operating effectiveness of your controls.
4. Identify and correct deficiencies.
5. Prepare management's report on internal control over financial reporting.
6. Prepare for the independent auditor's report on management's assessment of internal control over financial reporting.
Risk From The CEO And Board Perspective

CH. II

1: ASSESS
- Evaluate risk
- Rank
- Categorize

2: SHAPE
- Assess probability
- Model/quantify
- Impact
- Avoid/accept
- Transfer/market

3: OPTIMIZE
- Analyze and
- Correlate
- Execute

4: ANTICIPATE
- Monitor
- Refine
- Lead

Centralized risk management tends to focus on risks that affect the achievement of key corporate objectives and strategies and significantly affect most if not all functions and processes (e.g., reputation management). These risks may be referred to as enterprisewide (EW) risks. Accountability for EW risks may reside with the CEO and the board of directors (although responsibility for EW risks may be dispersed throughout the organization). Other risks that may be managed centrally include those that require specialized skill sets that cannot be duplicated at the division level or those that require partnering or contracting at the corporate level.

Decentralized risk management pushes the responsibility for risk management to those who live with it day to day. Risks that may be best managed in this way are division or process-level risks, which are those that are significant only within a particular process but nonetheless affect the organization's ability to successfully implement its strategies overall.⁵
Risk Officers

As we discussed in Chapter 3, *Risk in a Modern Global Business Context*, several corporations have created the role of Chief Risk Officer. Others have assigned similar responsibilities to an existing corporate officer, often the CFO. Regardless, the responsibilities typically include:

- Establishing ERM policies, defining roles and responsibilities, and setting implementation goals
- Assigning accountability and authority for ERM in the business units
- Improving ERM competence and helping managers align risk responses with risk tolerances
- Overseeing integration of ERM with other business planning and management activities
- Overseeing development of enterprise and business-unit-specific risk tolerances
- Helping managers establish control activities
- Helping managers develop reporting protocols and monitoring the reporting process
- Reporting to the CEO on progress and problems, and recommending needed remedies
Ironically, companies are now more predisposed to ERM in large part because of the data gathering and compliance disciplines imposed by it. But we believe ERM merits another cost-benefit evaluation, and among the benefits evaluators should include are:

- Aligning business strategy with risk appetite
- Relating growth with risk and return
- Improving risk-response decisions
- Reducing operational risk surprise and loss
- Identifying and managing risks that go cross-enterprise
- Integrating responses to multiple risks
- Identifying and responding to positive risk opportunities
- Improving capital rationalization
RISK CULTURE:

- Use common risk language and concepts.
- Communicate about risk using appropriate channels and technology.
- Develop training programs for risk management.
- Empower managers with defined risk boundaries.
- Identify and train risk experts.
- Align risk management techniques with company culture.
- Develop a knowledge sharing system.
- Include risk management activities in job descriptions.
Embed. Measure. Monitor:

- Identify key performance indicators and critical success factors related to risk.
- Establish success measures for risk strategy and activities.
- Provide a periodic process for measuring risk and return.
- Identify and implement monitoring processes and methods of feedback.
- Establish a feedback loop and replace outmoded systems as needed.