ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Enterprise Risk Management & Assessments Add to Legal Department Arsenal

Compliance and Ethics


▪ See the full spectrum.
▪ Spot the intangibles.
▪ A canny investment.
▪ An ultra-wide lens.
FAST ACTION
ERM®
NEW AND IMPROVED RISK MANAGEMENT


▪ See the full spectrum.
▪ Spot the intangibles.
▪ A canny investment.
▪ An ultra-wide lens.
FAST ACTION
ERM®
NEW AND IMPROVED RISK MANAGEMENT

CHEAT SHEET

- ***See the full spectrum.*** Enterprise Risk Management (ERM) takes a holistic approach to appraising risk.
- ***Spot the intangibles.*** ERM quantifies external factors, such as labor markets and global economic conditions, which cause business uncertainty.\
- ***A canny investment.*** While investing in risk management may not seem attractive, a robustly managed risk profile is crucial in today's regulatory environment.
- ***An ultra-wide lens.*** ERM takes into account financial, operational, reporting, compliance, governance, and strategic areas of organizational exposure.

Risk management is often identified as a discipline associated with the legal department. Protecting the business enterprise and its shareholders from legal and regulatory risk has always been a vital role of the general counsel's office and its staff. As such, it is most often thought of as a compliance program and management process of prescribed reporting structures and risk mitigation techniques designed to motivate, measure, and monitor a company's legal and ethical performance around complex business practices.

However, the rapidity of changes businesses face due to globalization, increased technology, and constant regulatory adjustments require transformation to many of the traditional compliance risk management ideologies, processes, and tools commonly used by most companies to achieve its risk management objectives. Because many of the typical techniques and procedures included in the conventional oversight of compliance risk fall short, legal department leaders are turning to Enterprise Risk Management (ERM) efforts that include greatly expanded risk assessments.

Compliance risk management

The full potential of ERM and risk assessments can be best understood by examining the history and changes impacting traditional compliance risk management. Compliance risk is the possibility that something damaging or unpleasant will happen as it relates to exposure from legal penalties, financial forfeitures, damage to brand and other material losses that an organization faces when it fails to obey criminal, civil, and industry laws, as well as industry regulations. Compliance risk is sometimes referred to as integrity risk because many compliance regulations are created to make certain business organizations operate fairly and ethically. Compliance risk management has typically been included in the collective corporate governance, risk, and compliance definitions because of the interdependencies between the three components.

Compliance-related risk is most often associated with the various government agencies and bureaus that are established to enforce regulations and statutes. It is not only the government regulatory bodies that are increasingly scrutinizing company risk management policies, but also investors. In an increasing number of industries, such as aero-defense, energy, and oil and gas, the board of directors is required to review and report on the adequacy of risk management processes in organizations they administer. Investors are looking for more assurance that the company is carefully considering risk.

One thing we have learned is that past experiences are not always a reliable indicator of what to expect in the future. The most recent global financial crisis was a wakeup call, a time when both compliance risk and other traditional risk management methodologies were failing. Many of the traditional financial risk assessments, indicators, and control mechanisms focused on historical financial failures. The integrity of the risk assessment process was impaired by the over-reliance on historical indicators.

For example, there was a heavy reliance on banking and financial performance indicators to signify an economic downturn, but those indicators typically focused on measuring historical activity. They failed to predict the dire consequences of a housing ownership spree based on new indicators, such as relaxed credit terms, increasing default rates of subprime borrowers, and the heavy investment and involvement of the largest investment and commercial banks in subprime origination activities.

Even today, most of the software currently used for monitoring risk and detecting potential fraudulent activities used by audit and risk management departments is designed to analyze historical data found in financial systems. This type of software does not identify and develop forward-looking key indicators that may offer insight into emerging market trends where there are no relevant historical performance statistics.

Enterprise risk management

Many business strategists and risk management associations advocate that what the general counsel’s office needs is a new theoretical roadmap to assess and manage risk. The solution we advocate is ERM.

Compared to traditional risk management, ERM elevates the focus on managing risks from tactical to more strategic objectives. In the ERM environment, risk management is integrated with strategy setting, business planning, performance measurement, and other business disciplines that leading general counsel are proactively using today.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established ERM as a comprehensive strategic business methodology that endeavors to do the following:

- Recognize the full spectrum of a company’s risks;
- Manage the collective influences of those risks as an interconnected group analogous to a risk portfolio; and,
- Provide reasonable assurance regarding the achievement of the organization’s objectives.

For some companies, the interest in ERM is the result of experiencing one or more avoidable significant business failures or catastrophes. For others, the investment is the result of heightened focus of new legislative statutes and increased enforcement of existing laws and industry regulations such as the Affordable Care Act, Sarbanes-Oxley, Dodd-Frank, and the Foreign Corrupt Practices Act.

Whatever the reason or driving force, there is now an inherent understanding that success in business depends on the balance between improving bottom line profits and managing risk. The investment in ERM is becoming a top consideration for many business leaders as lack of processes and oversight can lead to detrimental economic and brand implications for a company.

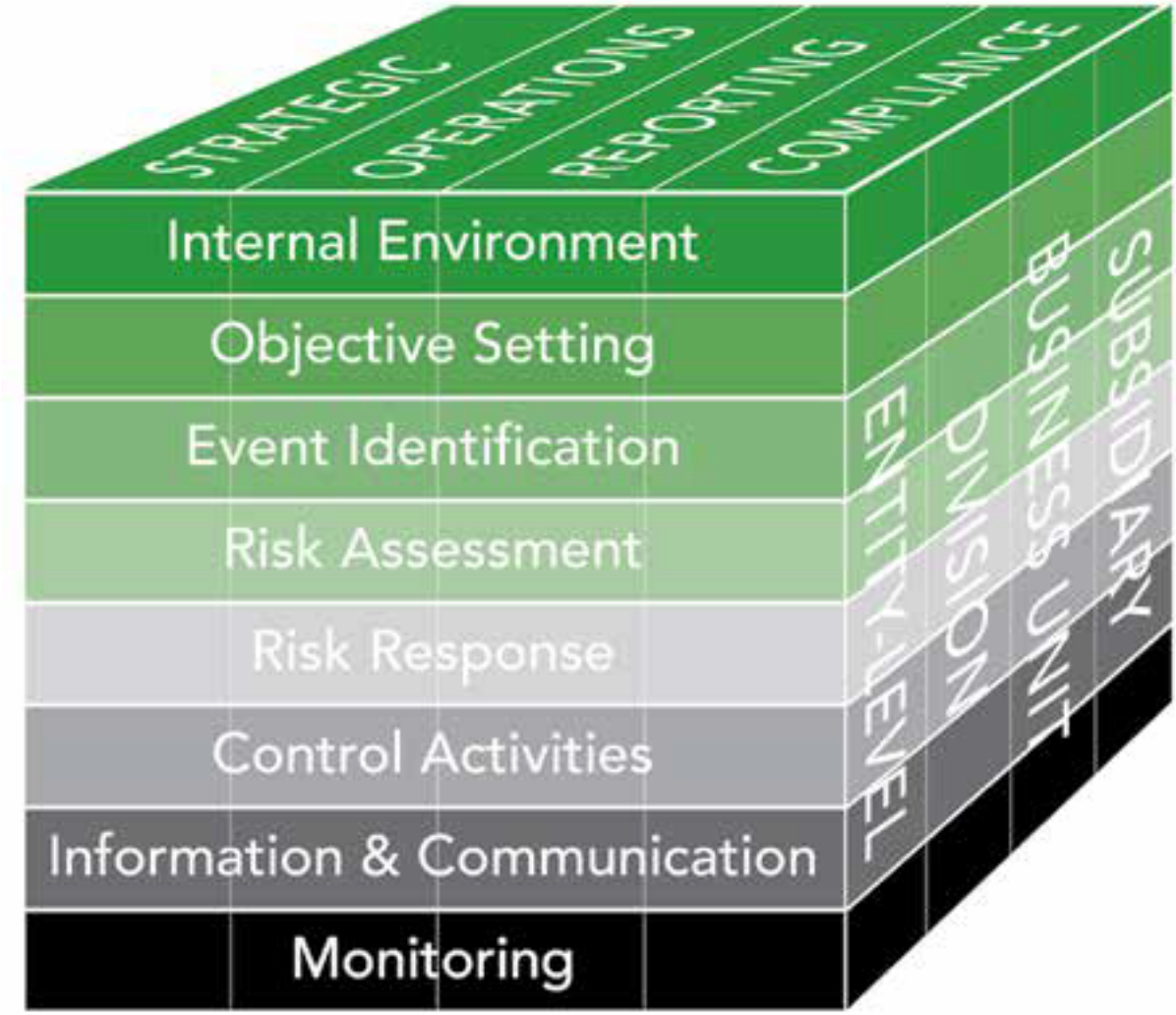
ERM takes a holistic approach to risk mitigation as all sources of value, both tangible and intangible,

are deemed vital to the business and they are subject to influences that must be understood and managed. Just as the sources of value can be internal and external, the influences to business enterprises can also be internal and external. For example, labor risk can present uncertainty that is both internal and external to the enterprise and can affect the viability of achieving business goals. As another example, global economic conditions are an external influence that can adversely affect financial markets, which in turn drives uncertainty in capital that may be needed to achieve business goals.

Eight ERM components

The ERM model consists of eight interrelated components according to COSO's September 2004 report, "Enterprise Risk Management- Integrated Framework."

1. **Internal environment –** The general character or attitude towards risk, management's risk philosophy, risk appetite, integrity, and ethical values.
2. **Objective setting –** Business objectives, goals, and direction must exist before risk and events can be identified that can affect their accomplishment.
3. **Event identification –** Internal and external events that can prevent a company from achieving its goals and objectives. It is important the events are distinguished between risks and opportunities.
4. **Risk assessment –** A process that identifies potential hazards and obstacles to prevent achieving goals. Hazards are identified along with the likelihood of occurrence and potential impact.
5. **Risk response –** Appropriate responses are developed for risks. The responses could vary between avoidance, accepting, or reducing the risks. The responses are developed and aligned in accordance to the company's risk appetite and risk tolerances.
6. **Control activities –** The policies and procedures are determined and set forth to help make certain the risk responses are carried out.
7. **Information and communication –** Information is recorded and communicated in a structure and timeframe that will make it possible for individuals to carry out their respective responsibilities.
8. **Monitoring –** The fullness of the ERM is monitored and adjustments are made as necessary.



ENTERPRISE RISK MANAGEMENT - INTEGRATED FRAMEWORK, EXECUTIVE SUMMARY, © 2004 COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). ALL RIGHTS RESERVED. USED WITH PERMISSION.

Of the eight ERM components, there are two key components that are addressed below.

Component two: Objective and strategy setting

The second of the eight ERM components is objective or strategy setting. The ERM model is not a simple streamlined sequential process where one element affects the next in a series. Rather, it is a dynamic, strategic, multi-directional process where virtually any part can have an influence on the other parts.

A strategic ERM approach that protects the business enterprise includes incorporating skills to shield enterprise value. This approach is more comprehensive and preferred more so than simply focusing attention on systems of controls or relying on external protection from insurance companies or the judicial system to mitigate loss. ERM stimulates management's confidence in seeking business prospects and incites management's intellectual capacity for understanding risks and being savvy enough to manage those risks.

The emphasis on strategy setting most often starts from the organization's board of directors and senior management and then filters down through the business units to the functional managers.

Although senior leadership may have initiated the topic of a more comprehensive risk management approach beyond compliance risk assessments, it will take a combined effort of strategic planning across all of the business units, including legal, to evaluate the long-term business goals and to integrate a risk management plan that mitigates an array of risks so the company can achieve all of its long-term goals.

Much like senior management and directors coming together to establish the vision and goals for the business, the same approach is taken with risk. As outlined by Protiviti Independent Risk Consulting in a “Guide to Enterprise Risk Management,” a working group of business executives establishes the role of risk management in the organization. Based on the group’s understanding of the key business units and their respective risks, a big picture view of how to organize the company’s risk management is developed and aligned with the organization’s objectives and strategies.

Once the shared vision has been defined, the overall risk management goals and objectives need to be established. They simply describe what is to be accomplished. The goals and objectives are defined in accordance with the company’s business strategy. Again, Protiviti Independent Risk Consulting has provided several examples of goals and objectives in its “Guide to Enterprise Risk Management” as follows:

- Achieve a better understanding of risk for competitive advantage;
- Build safeguards against earning-related surprises; and,
- Build and improve capabilities to respond effectively to low prospect, critical, catastrophic risks.

The ERM framework is designed, aligned, and established to accomplish the company’s objectives set forth in four categories:

- Strategic — Company’s vision, mission, goals, and objectives.
- Operations — The effective and efficient use of resources to produce goods and services.
- Reporting — Disclosing the organization’s financial status to internal and external stakeholders.
- Compliance — Adhering to criminal laws, civil laws, industry laws, and industry regulations.

ERM is designed and built to supersede the traditional risk management model. There are plans and methodologies established to implement ERM, but several weaknesses have been noted:

- ERM framework — The ERM intent was to consolidate all activities, functions, and interests within the company in such a manner that their risks might be integrated, examined, and managed as a unit. Some have alleged there is no such process that provides 100 percent certainty that management of all risks has been achieved.
- Proactive vs. reactive — The tenet that all risks have already been identified seems unreasonable. Potential risks may appear to be illusive and non-threatening because they often are not obvious and are difficult to articulate. Management can only be proactive with risks that have been identified.

ERM cannot rank every risk correctly — management is not omniscient and without all information, knowledge is limited. There are never enough resources to mitigate every identified risk.

Although ERM can be an integral part of managing an organization, it does not govern everything management does. Management’s choices as to the relevant business objectives, the specific risk

responses, and the allocation of resources are management's decisions and are not part of ERM.

Component four: Risk assessments and appetite

After business leaders have developed the strategic risk management vision and aligned the risk management goals and objectives to the overall business goals and objectives, theoretically a risk framework has been established. The enterprise risk framework structure will include the risk appetite and the enterprise-wide risk assessment, which is the fourth component of ERM noted above.

Risk assessment begins with determining or confirming a company's risk appetite. According to the Institute of Risk Management, risk appetite is a core consideration in an ERM approach. Risk appetite can be defined as "the amount and type of risk that an organization is willing to take in order to meet its strategic objectives." Senior management and a company's legal counsel develop the company's risk appetite. The risk appetite reflects management's risk philosophy and risk tolerance. It signals the company's capacity to accept risk as well as a comprehensive understanding of the level of risk the company can safely endure and manage for long periods of time. As an example, a company with a high risk tolerance may be willing to invest more capital in emerging markets versus a more conservative approach of remaining heavily invested in stable, but less profitable, markets. To be sure, this risk appetite is influenced to some degree by the results of the enterprise risk assessment and a gap analysis of the organization's priority risks.

The risk assessment gap analysis is then conducted. This exposes the weaknesses and shortcomings of the current risk management environment and analyzes the processes and tasks that have been established to correct the revealed deficiencies. There are often various departmentalized silos of risk management involved in this process, such as internal audit, financial management, IT governance, and compliance. The traditional concept of risk is always present and often discussed, and the focus is on designing controls, systems, and mechanisms to mitigate or prevent threats. Those particular notions are not without merit. However, ERM may be the best breed in designing and implementing capabilities for managing the risks that matter most.

An enterprise risk assessment is quite different from traditional risk assessments that are often conducted within the various functional unit silos discussed above. Traditional assessments tend to focus on the individual risks that matter only to the particular departments such as internal audit, IT governance, or financial management.

Risk Assessment Checklist

- NAME OR TITLE OF RISK
- SCOPE OF RISK
- NATURE OF RISK
- STAKEHOLDERS
- RISK EVALUATION
- LOSS EXPERIENCE
- RISK TOLERANCE/ APPETITE
- RISK RESPONSE
- POTENTIAL FOR RISK IMPROVEMENT
- STRATEGY AND POLICY

Recall that an underlying tenet for ERM is the notion that virtually all risk events impacting corporations today are foreseeable and manageable. Therefore, before it analyzes gaps, an enterprise risk assessment seeks to identify and source all potential risks that, if occurred, would have a material impact on the company's ability to achieve its objectives and business goals.

To identify all potential relevant risks, the company must seek input from representatives of all functional areas that are directly impacted by the potential risks. The lack of participation by all stakeholders is likely to undermine the success of the risk assessment process.

By methodically assessing enterprise risks and analyzing the gaps within, the company should be capable of identifying the following:

- Key risks that can hinder the attainment of strategic objectives;
- A clear course for communicating significant risks to senior management and the directors;
- A foundation for strategic planning and decision making; and,
- Activities associated with managing risks.

The risk assessment process then consists of an evaluation of available data, information, and the likelihood and significance of the event's occurrence. The most effective risk assessments then lead to a reconsideration of the risk appetite and the preparation of risk responses. Hence, the assessment activity itself is conducted with some degree of expectation toward making proactive decisions and determining the necessity for further actions.

Legal department proposal for enterprise risk management:

A value proposition summarizes why a service or feature is intended to make a product or service attractive to customers. So what is the value proposition for implementing ERM? What is the value proposition for CEOs or general counsel to exchange the traditional risk management approach for ERM?

The CEO's challenge for a large enterprise is to capitalize on business opportunities and stay ahead of its competitors by being innovative and establishing a vision and direction that will inspire management, employees, and investors. The CEO must manage the company in the presence of changing business conditions. All of these endeavors must be accomplished and still provide assurance to investors, directors, and stakeholders that the company knows how to protect and enrich the enterprise value.

Here are examples of the value provided by ERM:

- Align risk appetite and business strategy.
- Implement more robust risk assessment process.
- Improve regulatory compliance and risk responses.
- Improve capital deployment and resource allocation.

ERM is intended to help CEOs and general counsel achieve these goals by enhancing the company's risk management capabilities in an everchanging operating environment. Jim Kreiser of Clifton Larson Allen highlighted several benefits of ERM:

Enhanced risk-focused culture for the organization — The increased focus of risk integrated with

senior management and legal counsel results in more discussion of risk at all management levels. This cohesive approach within the most senior level of the company is analogous to the concept of “Tone at the Top.” This cultural shift helps to breakdown the management silos with respect to how risk is managed. The result is communication of risk and sharing risk information across all parts of the company, which encourages better insights and decision making concerning risk at all levels.

Standardized risk reporting — ERM supports a more comprehensive framework and structure to manage risk across the organization resulting in standardized reporting that tracks and reports risk to directors and executives. Some other specific reporting improvements are timeliness, conciseness, and collection of the right risk information. Collectively, standardized reporting enables better risk mitigation decisions.

Heightened concentration and perspective on risk — The enhanced risk focus and standardized reporting helps develop better and more timely indicators of potential risk which provides early warning signs notifying management to changes in their risk profiles. ERM expands the viewpoint of risk beyond mitigation to an evaluation of risk as it may identify opportunities to increase competitive market positions.

More efficient use of company resources — In organizations without ERM, individuals operating in risk management silos are most likely approaching risk assessments and risk management using many different methods. The framework and tools used in an ERM model to assess, report, and manage risk will be more consistent and most likely eliminate redundant and unnecessary procedures. This will improve efficiency by utilizing the right amount of resources, consistent procedures, and reporting mechanisms, which will result in a more effective risk management model.

Effective coordination of regulatory and compliance matters — ERM will not eliminate regulatory and compliance matters that have to be monitored, controlled, and reported to various external government regulatory and financial agencies. However, since ERM develops and integrates a consolidated and standard risk framework, using standard assessment procedures and standardized reporting, the process of providing information to regulatory bodies will be much more complete, effective, and efficient. The proponents and pioneers of ERM indicate that not only will ERM enable better management of market, competitive, and economic conditions, but it will also increase the leveraging and consolidation of disparate risk management functions.

At this point, few companies have fully implemented ERM and replaced the traditional forms of risk management. The gulf between ERM and traditional risk management is quite overwhelming and too much for most companies to entertain. There are many ingrained behavioral changes that would need to be addressed and overcome in the various risk management department silos.

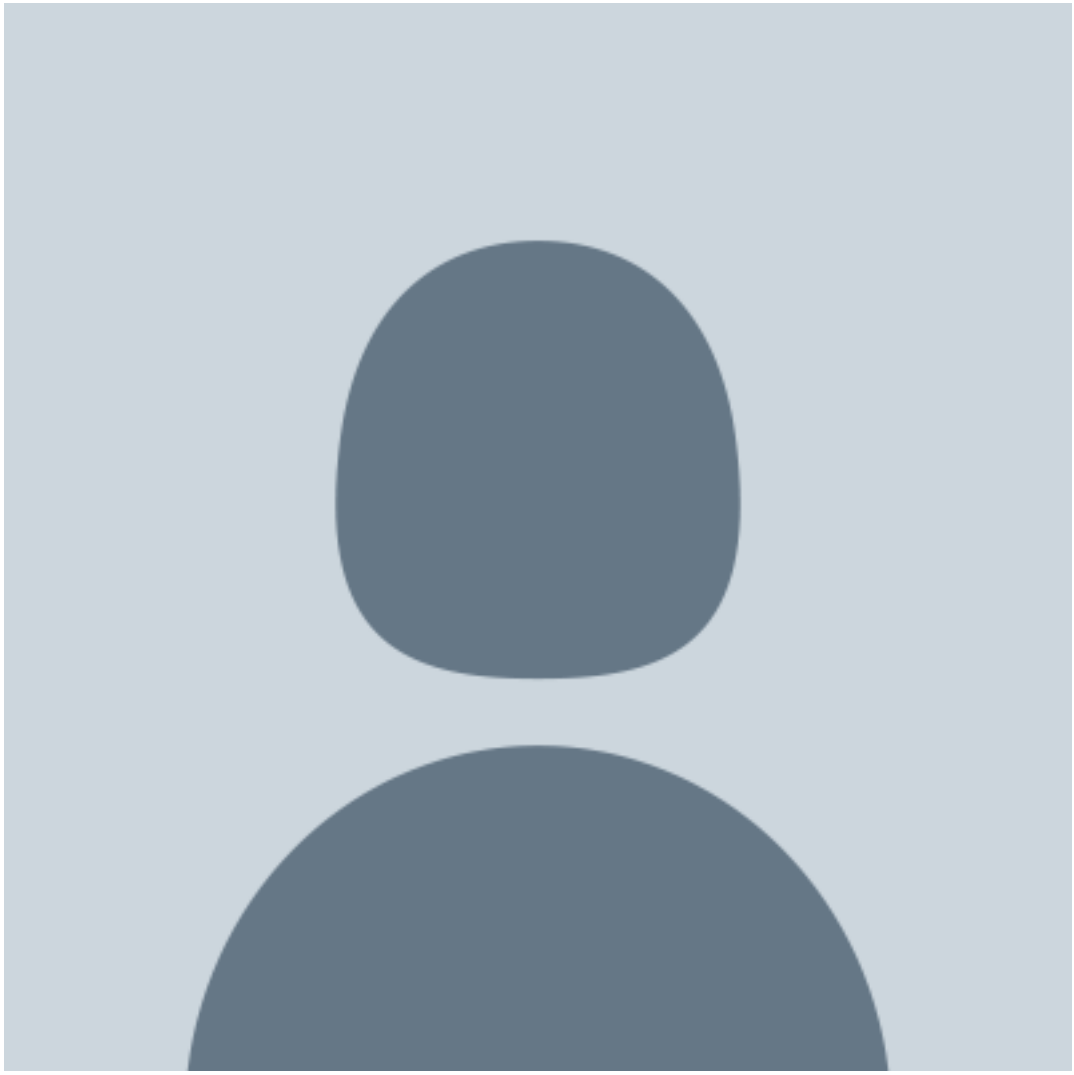
The very same behavioral changes were required when companies were considering adopting Kaizen, Six Sigma, and Lean Manufacturing. Consider that it was a historic moment in 2009 when Toyota surpassed GM in number of vehicles sold. It marked the end of a 77-year reign as the world’s number one automaker. One of the most critical reasons for the shift was Toyota’s adoption of Kaizen, the concept of continuous improvement.

Behavioral changes in business can occur and the results can be measured. In 1984, GM and Toyota entered into an agreement to work together at a car factory in Fremont, California. As part of the arrangement, GM workers went to Japan and worked on a Toyota auto assembly line. When the

Americans returned to the Fremont plant, the changes that they implemented were monumental. Within three months, a union workforce that was notorious for being one of the worst in America was achieving near perfect quality ratings.

It is not certain the same outstanding results can happen, but ERM adopts the same concepts as Kaizen and other lean manufacturing concepts — like Six Sigma — by continuously improving the risk management capabilities that really matter. The results have been proven and are measurable in the companies that adopted and changed to ERM and a model of continuous improvement.

Catherine Hilton

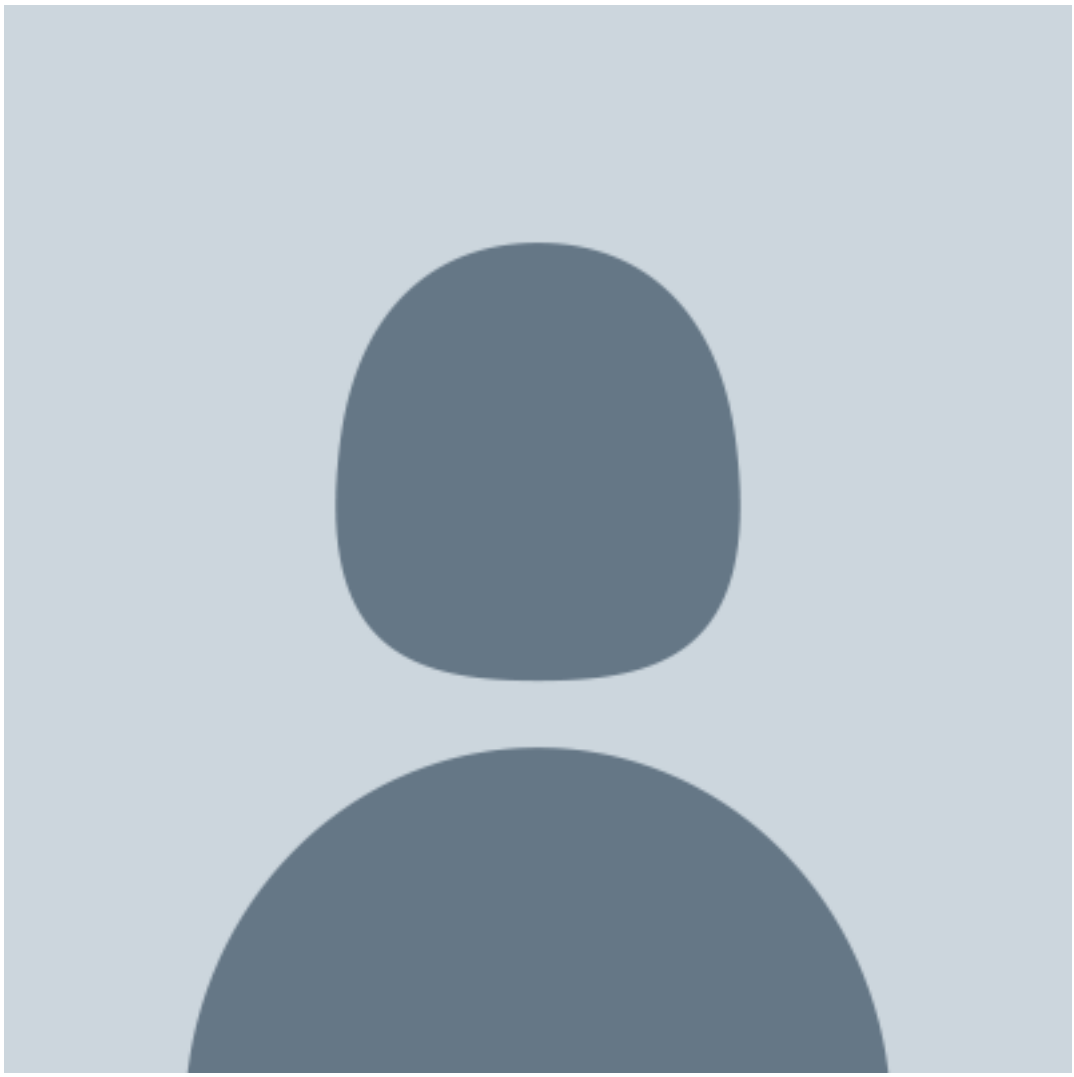


VP of Legal and Compliance

UPS Capital Corporation

The arm that provides financial, insurance, and payment solutions. She’s been with UPS Capital for 15 years and serves as its CLO and CCO. Hilton and her team strive to provide competent, timely, cost-effective, and solution-oriented legal advice and compliance related support for UPS Capital’s global business operations.

H. Glen Jenkins, CPA, CVA, CFE



Senior Manager in the Fraud and Forensic Services Practice

the Atlanta, GA offices of Warren Averett

Jenkins has more than 20 years experience assisting corporate counsel in complex commercial litigation, calculation of economic damages, fraud investigations, and business valuations of tangible

and intangible practices.