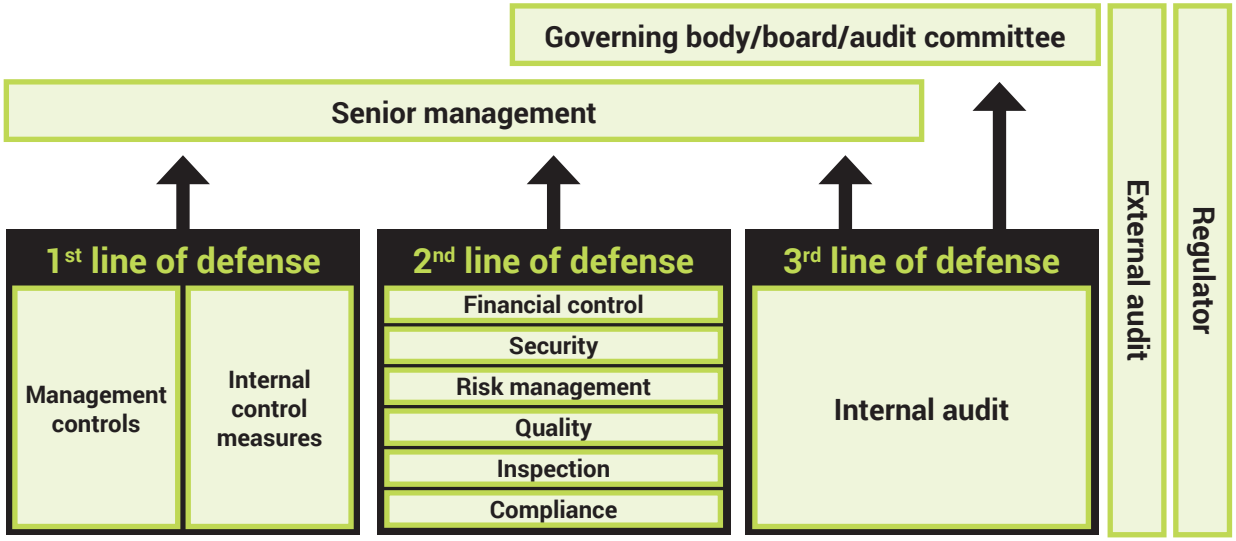
bakertilly
now, for tomorrow.

Reduce fraud and other enterprise risks with internal audit procedures

In a previous insight, we discussed the importance of an effective internal control structure to reduce the risks of fraud, errors and irregularities. So what if your organization now has an effective internal control structure with the critical tone at the top, segregation of duties and an effective system of reviews, authorizations and approvals? Are you now fully protected from fraud risks? Are you protected from other enterprise risks to your law firm? Unfortunately, the answer is "no, fraud and enterprise risks still exist." For example, fraud may occur due to the lack of compliance with well-designed control policies and procedures.

The "three lines of defense" model is a commonly accepted risk management framework used to manage risk and controls as follows:

- First line of defense: operational management
  - Owns and manages risks; performs day-to-day risk management activity
- Second line of defense: oversight
  - Finance, human resources, risk management and compliance functions; set direction, define policy and provide assurance
- Third line of defense: internal audit
  - Provides assurance that the other lines of defense are functioning effectively



Adapted from ECIIA/FERMA Guidance on the 8th EU Company Law Directive, article 41

The American Lawyer magazine noted in a March 2019 article that one of the largest law firms in the world inadvertently transferred millions of dollars in client funds to a fraudster. It is likely this large law firm has a rather effective overall internal control structure; however, diligent compliance may have been lacking. Similarly, an audit committee member of a public company recently noted a similar fraud instance where wire transfer instruction changes from a seemingly appropriate source were not properly verified. To further complicate the need for diligent compliance with all procedures, the individual noted that, upon investigation, the public company determined that their information systems had been breached and monitored for a year while the fraudsters waited for an ideal time to strike.

Along with fraud risks, every organization faces additional enterprise risks. For law firms some of those enterprise risks include compliance with laws and regulations, cybersecurity and data protection threats, conflicts and professional practice requirements, security procedures over client escrow accounts, and increasingly important operational risks to effectively plan and manage legal matters that are more closely monitored by client demands. Many of these additional enterprise risks fall outside the scope of typical financial controls; however, they are generally controlled through a series of policies and procedures, as part of the second line of defense.

As a result, along with an effective internal control structure, internal audit procedures, acting as a third line of defense, are valuable additions for an organization to manage fraud and other enterprise risks. The mission of internal audit stated by The Institute of Internal Auditors is "to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." A fully functioning internal audit department is atypical in most law firms due to the costs of dedicated internal audit personnel. Typically, performance of various periodic internal audit procedures do not necessitate the addition of dedicated full time staff. Limited testing procedures can be assigned to internal support staff or outsourced for occasional support. We recommend that law firm management (be that a management committee, audit committee, managing partner, executive director or firm administrator depending on the size and structure of the firm) periodically review and evaluate overall enterprise risks across the organization.

1. Evaluate potential risks to determine higher risk areas and its sources
2. Evaluate the consequences of the risks and the likelihood of occurrence
3. Determine resources to appropriately mitigate the risk and establish controls without an overburdening cost

Then, based on that evaluation and ranking of risks, the organization should consider the use of internal audit procedures to reduce such risks, maximize performance and improve governance.

For example, potential internal audit procedures might include:

- A periodic review of adherence to practice procedures to reduce malpractice risks
- Testing of IT security measures and phishing attempts to improve sensitivity to cyber risks
- Review of compliance with partner succession and transition plans to enhance the preservation of client relationships
- Review adoption of best practice project management initiatives or approval of pricing alternatives to improve efficiency and client satisfaction
- Test adherence with purchasing policies that may range from travel, corporate credit card usage or other cost management programs, to vendor selection and contract compliance
- Testing of potential anomalies to minimize fraud risks that may include review of transactions just below approval thresholds, querying for duplicate payments, and review of manual rush checks processed outside of normal payable cycles

These are far from all-inclusive examples as they represent a small sample of potential procedures that may help a law firm manage risks and improve performance.

The range of issues to address are also impacted by the unique characteristics of each law firm. For instance, smaller firms often allow attorney-wide discretion and authority that might be beneficial for speed of decision making while lacking in optimal effectiveness. Very large firms may have numerous offices around the country and the world, subjecting those firms to more complex sets of laws and regulations, not to mention more challenges to monitor local procedures and maintain familiarity with local vendors. And while every firm faces new client/matter intake risks, the complexity of the conflict check, or evaluation of matter expertise, or the credit worthiness of the client, or the engagement letter terms, or the pricing alternatives will all vary depending on the size and type of legal practice.

Accordingly, firm management is in the best position to assess its unique risk characteristics and consider internal audit procedures to mitigate problems. The review of enterprise risks, including fraud, should occur on at least an annual basis. This may be accomplished with one comprehensive annual review, or the evaluation of individual risks may be spread over the course of the year.

The key is to recognize that along with establishing a strong internal control structure (first line of defense), every organization needs to evaluate fraud and other enterprise risks on a regular basis and consider what methods can be employed to mitigate risks (as part of the second line of defense). For some risks, insurance products are available to control exposure or requirements for higher levels of approval may provide the desired comfort. For many other risks, the utilization of internal audit procedures (third line of defense), are valuable alternatives to provide assurance and insight to management.