WHITEPAPER

fidato partners

Absolute Assurance in a "Reasonable Assurance" World

Overview

It has been over 18 years since the Sarbanes-Oxley Act of 2002 ("SOX") created the Public Company Accounting Oversight Board ("PCAOB") to oversee the Accounting industry. During that time, the PCAOB has issued multiple Accounting Standards to guide the work performed by external audit firms. From 2004 – 2006, Auditing Standard No. 2 (AS 2) "established the requirements and provided directions that apply when an auditor is engaged to audit both a company's financial statements and management's assessment of the effectiveness of internal control over financial reporting." In 2007, Auditing Standard No. 5 (AS 5) superseded AS 2, providing a more "top-down" risk-based approach to the audit of internal control. Throughout the years, one definition in the SOX landscape has remained consistent. Specifically, an external audit's opinion related to the effectiveness of internal control over financial reporting includes the words "reasonable assurance." Recently, in response to ever changing and evolving pressures from the PCAOB, external audit firms have migrated from this concept to one which more closely aligns with absolute assurance. Downstream impacts have been felt most by public companies which are having trouble adjusting to the ever-changing needs from an evidence and review standpoint. This has resulted in an increase in material weaknesses noted in year-end filings as compared to previous years. That said, companies have an opportunity to prevent deficiencies from escalating in severity by implementing certain safeguards noted below.

Defining Reasonable Assurance

Paragraph 17 of PCAOB Auditing Standard No. 2, An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements, describes reasonable assurance as follows: "Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of reasonable assurance . . . Reasonable assurance includes the understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance."

The PCAOB and external audit firms have always taken comfort in the last part of the definition – that reasonable assurance is a **high** level of assurance. Historically, reasonable assurance was obtained by reducing audit risk to an appropriately low level through applying due professional care, including obtaining sufficient appropriate audit evidence. However, in recent audit periods, external audit firms seem to have moved the bar more towards an

absolute assurance standard. This shift has been in direct response from heightened pressures from the PCAOB and an increase in non-compliant audits rendered to the Big-4 external audit firms in recent years.

As a result, we have seen an increasing number of material weaknesses within the past year's (2019) 10k filings compared to any other year of recent memory. Having been involved in several debriefs with clients on these 2019 findings, it appears as if certain severity conclusions could have been downgraded if safeguards as the ones detailed below were implemented.

How Companies Can Fight Back

Proximity to financial statements / Cycles with a high propensity for fraud

As part of internal control over financial reporting, companies must ensure that the "softer side" of COSO is contemplated within their organizations. An effective control environment, risk assessment, information and communication protocol, and monitoring process are important to establishing the basic structure for internal control over financial reporting. These items, while indirectly impacting a company's financials, nevertheless provide an important foundation for controlling a company.

The implementation of control activities rounds out the COSO framework. As it relates to internal control over financial reporting, certain control activities are naturally more critical than others to mitigate material misstatement to financial statements. These control activities are ones with a higher proximity to the financial statements (i.e. controls within the Period-End Financial Reporting business process) and controls supporting business process cycles with a higher propensity for fraud (i.e. controls within the Revenue cycle). In turn, a failure in these control activities (and more often than not weaknesses in multiple control activities in the aggregate) are typically the only areas which should ever escalate from a severity standpoint. If your external audit provider is concluding a significant deficiency / material weakness exists in an area with a low proximity to the financial statements (i.e. an upstream sub-process) or with a low propensity for fraud (i.e. Fixed Assets), there more than likely are compensating controls which can be pointed to which would not merit that deficiency / combination of deficiencies to elevate in severity. Companies should ensure they are showcasing such fact patterns (specifically related to issues with a low proximity to the financials or with a low risk of fraud) when evaluating deficiencies related to internal controls.

fidato partners

Information Technology General Controls ("ITGCs")

ITGCs create the foundation of a company's control environment which is IT-dependent. Placing safeguards into operation to restrict access to only authorized individuals, prevent unauthorized changes from being migrated to the production environment of financially significant systems, and validating the completeness and accuracy of data flowing through systems provide the building blocks for business process control activities in a company's control environment. These controls are typically seen as pervasive and not able to be directly assessed a magnitude of potential misstatement to the financial statements during the deficiency evaluation process at year-end. As a result, even if a combination of ITGCs were to fail at the end of the year, a material weakness should not be assessed to a company's control environment if business process controls (especially those with a high proximity to the financials which are manual in nature) are deemed to be operating effectively. Weaknesses in multiple ITGCs, by themselves, would not be concluded by a well-informed, competent, and objective individual to be a material weakness.

Service Organizations

The control environment of a public company is typically not fully contained within the boundaries of the company itself. Companies utilize service organizations for various functions supporting internal control over financial reporting. A common (and necessary) practice for companies is to review a service organization's SOC 1 report and determine whether appropriate controls have been placed in operation and are suitably designed and operating effectively at the service organization for the financially significant process(es) which has been outsourced. In certain instances, service organizations will refer to subservice organizations within their SOC 1 reports for functions which are outsourced to a separate third-party. In almost all cases, subservice organizations referenced in SOC 1 reports either a) perform functions which are operational in nature and are not in-scope for purposes of internal control over financial reporting or b) have such a low proximity to the financial statements of the company under audit that the chance of material misstatement is extremely remote. We have seen some external audit firms begin to request subservice organizations referenced in service organization reports in their never-ending quest for absolute assurance. Other than in one-off cases (i.e. a company has multiple products each with their own SOC 1 report and a "centralized" ITGC SOC 1 referenced as a subservice organization report), companies should not have to evaluate subservice organization reports in connection with internal control over financial reporting procedures.

WHITEPAPER

fidato partners

Targeted Restricted Access Controls

Almost every company has a periodic review of user access as part of their ITGC environment. Typically, on a quarterly or semi-annual basis, management will produce a listing of users with access to the financially significant application and perform a review to validate access of the individuals remains commensurate with job responsibilities. These reviews typically operate as "management review controls" in organizations, requiring a heightened level of audit precision from both internal and external audit groups. This extra level of scrutiny focuses on various areas of design of the control activity:

- Has the process for extracting the user listing from the system been documented to showcase completeness and accuracy?
- Are all users being extracted from the system or are certain users not included (and is that appropriate due to them not impacting ICFR)?
- Do reviewers understand the level of access (i.e. roles) assigned to users they are reviewing?
- Are reviewers recertifying their own access to systems?
- Is there evidence to showcase how management is comfortable that any changes to user's access were actually made?
- How does management gain comfort that reviewers are not "rubber stamping" reviews which come across their desks?

These areas (among others) are various points in the user access reviews where the design or operation of the control activity can be called into question by audit firms. Deficiencies in these reviews combined with other control weaknesses in a company's environment could lead, in the aggregate, to a significant deficiency or greater.

However, there is a way for companies to combat this risk. In addition to performing a user access review, companies have been implementing targeted user access reviews on users who specifically have more sensitive access from a financial standpoint. Validating a subset of users on a periodic basis is a potential way to combat control deficiencies related to user access reviews for applications with high numbers of users. These reviews typically have a smaller quantity of users in-scope; as such, successful operation is easier to achieve.

fidato partners

Manual / Disaggregated Control Environments

Companies are continuously attempting to automate their control environments through the use of system workflows and segregating duties within key financially significant systems. However, in most cases, companies still rely on a fair amount of manual business process controls to mitigate the risk of material misstatement to their financial statements. Within such manually focused control environments, the risk related to segregation of duties is substantially reduced. Companies requiring such reviews (either via workflows within systems or manual, paper-based signoffs) mitigate risks of unauthorized transactions moving further downstream to the financial statements. These manual reviews assist greatly with reducing the "could" factor evaluated when control deficiencies are identified.

Additionally, while many companies have moved to an Enterprise Resource Planning ("ERP") solution to manage a majority of their financially significant processes, "legacy" systems supporting certain in-scope functions remain in some capacity at almost all companies. The ability to segregate access to only certain applications drastically reduces the risk of cross-application segregation of duties conflicts. This setup from an IT perspective, combined with manual control environment considerations noted above, helps companies inherently mitigate the risk of material misstatement to the financial statements due to fraud or error.

Timely Performance of Procedures

Companies pay high prices for internal and external audit fees. Internal Audit departments, whether staffed fully in-house or outsourced to a third-party provider, are typically multiple people in size. External audits are extremely expensive from a blended rate per hour perspective, even with the Shared Service model many of those firms currently employ. Given the cost of these services (and the potential negative effects to stock price from a material weakness), the one thing all companies should mandate is that audit teams plan and perform an interim round of procedures early in the year. Phasing the work and performing procedures prior to the middle of Q3 can allow companies to identify any weaknesses in their controls and implement remediation procedures with enough iterations for controls to operate prior to the as of controls opinion date. One of the easiest safeguards for companies to implement is to obtain an objective view of its control environment early in the year to allow for sufficient time for any necessary enhancements or remediation efforts.

WHITEPAPER

fidato partners

Final Thoughts/Conclusion

Do you feel like you are in a never-ending, uphill battle with your external auditor? Do you feel like these organizations are always asking for more, but never for less (even in areas of low risk)? Fidato can assist you navigate these conversations, utilizing some of the solutions identified above. We can help companies design safeguards which provide a high level of targeted assurance for not much effort. Additionally, as an independent, co-sourced or outsourced controls assessor, we can perform these procedures early in the audit period. This provides companies with an independent lens into their control environment and enough time to remediate any findings prior to required filings.

****

Please look for future updates on other risk management matters at www.fidatopartners.com

Contact
Justin DiGaetano, CRMA, CISA | Principal, Risk Management

1001 Old Cassatt Road | Suite 200 | Berwyn, PA 19312
Two Commerce Square | 2001 Market Street | Suite 3230 | Philadelphia, PA 19103
jdigaetano@fidatopartners.com | 609 315 7186 (c)

www.fidatopartners.com
https://www.linkedin.com/in/justin-digaetano-08a953/

About Fidato Partners, LLC

Fidato Partners is the leading service provider of consulting and recruiting in accounting, risk management, and information technology in the Mid-Atlantic region, enabling companies to achieve greater growth and performance by filling critical resource and knowledge gaps. From emerging growth to global organizations, we are dedicated to providing the highest level of service to our clients. For more information, visit www.fidatopartners.com.