Why COSO's Internal Control Framework Can't Give You Confidence

Abstract

The Big Four and cohorts promote the COSO integrated internal controls framework and COSO ERM integrated framework as "*best practice*". Billions of dollars are spent on advisory fees to public accounting firms to assist in providing assurance in financial reporting and audit attestations. Diverse industries have adopted COSO's guidance on compliance, risk, and audit practice but there is one thing missing – *confidence*. COSO and its internal and external auditors don't provide confidence, audit can only provide "reasonable assurance". COSO can't provide any level of confidence and that is a problem! Why does confidence matter? Confidence matters if you or your organization believe cybersecurity is a challenge. Confidence matters if operational risks and inefficiency is a concern. Confidence matters if the risk of anticipating how effective your strategic plans will be executed and your primary tool to manage risk is reliance on COSO's framework. Confidence matters if you want more than assurance that your organization is prepared for the challenges in a complex global marketplace.

The Big Four can't provide levels of confidence because COSO does not provide confidence they only provide *assurance*. COSO can only give you an opinion not confidence and not even absolute assurance. Auditor's deal in *degrees of satisfaction*? How is this measured? No one really knows or understands it because it is as subjective and ambiguous as it sounds.

Should the board of directors and senior executives put their confidence in these definitions? The real question is why hasn't anyone ever challenged how COSO has sold its framework as a risk management solution? Best practice? What scientific evidence does COSO provide that its framework works? How does COSO measure risk reduction after implementing its framework? Auditors are not even required to examine the full scope of evidence to come to a conclusion in their audit opinion.

You may not have ever asked these questions, but you should. The organizations who provide guidance to internal and external auditors don't mince words in their standards that define the limits of what an auditor provides in services and nowhere does the guidance include the term risk beyond audit risk of financial misstatement. See for yourself below from the Public Company Accounting Oversight Board and AICPA, the two bodies that oversee audit services.

Here is the highest level and scope of COSO's (public and internal audit's) assurance services:

PCAOB: "Reasonable assurance refers to the *auditor's degree of satisfaction* that the evidence obtained during the performance of the audit supports the assertions embodied in the financial statements. The auditor's standard report on the audit of financial statements explicitly asserts in the scope paragraph that the audit was conducted in accordance with professional standards and

states that "those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement."

AICPA: "Audit evidence is all the information used by the auditor in arriving at the conclusions on which the *audit opinion* is based and includes the information contained in the accounting records underlying the financial statements and other information. *Auditors are not expected to examine all information that may exist.* Audit evidence, which is cumulative in nature, includes audit evidence obtained from audit procedures performed during the course of the audit and may include audit evidence obtained from other sources, such as previous audits and a firm's quality control procedures for client acceptance and continuance."

AUDIT STANDARD NO#8: "In an audit of financial statements, *audit risk* is the risk that the auditor expresses an inappropriate audit opinion when the financial statements are materially misstated, i.e., the financial statements are not presented fairly in conformity with the applicable financial reporting framework. *Audit risk is a function of the risk of material misstatement and detection risk*."

- *Risks of material misstatement at the financial statement level* relate pervasively to the financial statements as a whole and potentially affect many assertions. Risks of material misstatement at the financial statement level may be especially relevant to the auditor's consideration of the risk of material misstatement due to fraud.
    - *Inherent Risk*
    - *Control Risk*
    - *Detection Risk*

Performance-based risk analysis is an enterprise-wide approach. The ESG movement is changing how organizations perceived their impact on the environment. Metrics are being gathered to demonstrate sustainable processes across the organizational footprint but what metrics are being gathered for the impacts on people? Few of the ESG goals will be met without proactivity influencing the right behaviors in employees, customers, suppliers, and more. The common denominator in all organizations is people and governance plays the biggest role in driving the right behaviors and influencing good decision-making to achieve corporate and environmental goals for sustainable operations. But are we asking the right questions?

Where are the biggest pain points to people - employees and customers? How can we reduce or remove friction and costs in back office? What are the strategies to enhance uncertainty management through better people management? Do we invest in the right skills and expertise to retain top talent who know how to build high performing teams? How best to create an

environment of competitiveness in excellence and support for growth? The two biggest organizational risks are performance and expectations. The tools for managing performance and expectations require a human-centered approach.

Tone at the Top is often mentioned as the key to successful outcomes, but really, a positive tone is needed at all levels of the organization. Business leaders often quote sports analogies focused on individual talent, "Best athlete", "Team player". Yet many fail to create an environment that allows all people to succeed. Teams, win or lose in team sports, not individuals, and teams with talent disappoint when the "chemistry" created by management is poorly managed. Teams have both superstars and position players all who contribute to success. When organizations under-appreciate the role position players contribute to success the wrong kind of tone is set. Setting the right tone across an organization enhances performance in profound ways.

Setting the right tone is about is creating an environment of excellence in execution and the right tools to solve problems. One of the key tools is organizational behavior. However organizational behavior is in flux today. The Great Resignation is signaling trouble in organizational behavior that has been ignored for decades.[1] Part of the problem is organizational hierarchy and 19th century risk governance practices that have made organizations risk averse, less innovative, and bureaucratic.[2] To examine how organizations became rigid and inflexible we must first consider corporate governance.

Confusion in Enterprise Risk Practice – Part 1

In 1985, the Committee of Sponsoring Organizations was formed to sponsor the National Fraudulent Financial Information Commission (the Treadway Commission). The Treadway Commission was sponsored and jointly funded by five major professional accounting associations and institutes based in the United States: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and Institute of Management Accountants (IMA).

The Treadway Commission recommended that the sponsoring organizations of the Commission work together to develop an integrated guidance on internal control. These five organizations formed what is now called the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.[3][4][5]

In the mid-1970's the U.S. experienced widespread questionable corporate campaign finance and corrupt foreign practices which caused the Securities and Exchange Commission to enact the Foreign Corrupt Practices Act (FCPA) of 1977.[6] FCPA was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government

[1] https://www.cbsnews.com/news/great-resignation-60-minutes-2022-01-10/
[2] https://www.cnbc.com/2022/01/14/the-great-resignation-expert-shares-the-biggest-work-trends-of-2022.html
[3] https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission
[4] https://www.sec.gov/news/speech/1989/012689grundfest.pdf
[5] https://www.sec.gov/rules/final/33-8238.htm
[6] https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act

officials to assist in obtaining or retaining business. The anti-bribery provisions of the FCPA have applied to all U.S. persons and certain foreign issuers of securities. With the enactment of certain amendments in 1998, the anti-bribery provisions of the FCPA now also apply to foreign firms and persons who cause, directly or through agents, an act in furtherance of such a corrupt payment to take place within the territory of the United States.

The FCPA also requires companies whose securities are listed in the United States to meet its accounting provisions. These accounting provisions, which were designed to operate in tandem with the anti-bribery provisions of the FCPA, require corporations covered by the provisions to (a) make and keep books and records that accurately and fairly reflect the transactions of the corporation and (b) devise and maintain an adequate system of internal accounting controls.

Congressional hearings on the causes of the failures focused on what could have been avoided by, among other things, *better audit practice*. Concerns about independent public accounting and audit practice is a recurring theme in corporate financial malfeasance, a topic to be returned to later. David S. Ruder, the Chairman of the Securities and Exchange Commission, emphasized "the role of internal audit in deterring, detecting, and reporting financial frauds*"* however the Commission Report went further.

The Treadway Commission set forth three major objectives: (excerpts are summarized here)

(1) Understand how the extent to which fraudulent financial reporting damages the integrity of financial reporting, determine how fraud can be prevented, deterred, or detected sooner, and assess whether fraud is a product of a decline in professionalism of corporate financial officers and internal auditors; and whether the regulatory and law enforcement environment unwittingly tolerated or contributed to these types of fraud.
(2) Examine whether the role of the independent public accountant in detecting fraud had been negligent or lacked sufficient focus and determine whether changes to independent public accounting and internal audit practices can be enhanced through changes in audit standards and procedures to reduce the extent of fraudulent financial reporting.
(3) Identify attributes of corporate structure that contribute to fraudulent financial reporting or to the failure to detect such acts promptly.

The Treadway Commission recommendations targeted three groups: (a) public companies; (b) independent public accountants, and the (c) the SEC.

(1) Public companies were recognized as accountable for preparing accurate financial statements, setting tone at the top, oversight of internal accounting and audit, establishment of a board audit committee, preparing management and audit committee reports, seeking out second opinions from independent public accountants, and preparing quarterly reporting.

(2) Independent public accounting was recognized for playing a "crucial" role in detecting and deterring fraud, improving the effectiveness of the independent public accountant, and recommended changes in auding standards, changes in procedures that enhance audit quality, improving communications about the role of the independent public accountant, and changes in the process of setting audit standards.
(3) The Treadway Commission suggested to the SEC that improvements could be made in the area of fraudulent financial reporting including:
    a) increased deterrence using new SEC sanctions,
    b) greater criminal prosecution,
    c) improvements in regulation of the public accounting profession, and
    d) improvements by state boards of accountancy

The Treadway Commission also referenced two final recommendations related to the perceived liability and insurance crisis to be addressed. Additional recommendations suggested that individuals involved in the financial reporting process could benefit from "education to enhance the knowledge, skills, and ethical values that potentially may prevent, detect and defer fraudulent financial reporting." Accordingly, the Report recommended changes in business and accounting curricula, professional certification examinations, and continuing professional education to achieve the goals of the Commission.

The final report is only 37 pages long which included 49 specific recommendations by the Treadway Commission.[7] The Treadway Commission study was published in 1987, and in the fall of 1992, a four-volume report entitled, "internal control: integrated framework" was completed. The Treadway report presented a common definition of internal control and provided a framework against which internal control systems can be evaluated and improved. This report is guidance that US companies use to assess their compliance with the FCPA. This last statement is instructive and confirms the narrow scope of the COSO internal control integrated framework (ICIF). However, according to a survey conducted by online magazine CFO *published in 2006, 82% of respondents said they used the COSO framework for internal controls, supposedly to comply with FCPA.*

It is reasonable to assume that expanding internal controls more broadly beyond FCPA would occur to include other areas of financial reporting as well. COSO's audit and internal controls guidance has remained unchanged for 36 years, a focus on financial reporting and gathering evidence to attest to management's statements in financial reports. However, a 2020 study found

[7] See COSO, Internal Control-Integrated Framework (1992) ("COSO Report"). In 1994, COSO published an addendum to the Reporting to External Parties volume of the COSO Report. The addendum discusses the issue of, and provides a vehicle for, expanding the scope of a public management report on internal control to address additional controls pertaining to safeguarding of assets. In 1996, COSO issued a supplement to its original framework to address the application of internal control over financial derivative activities.

that only 20% of respondents used COSO's guidance, and of those firms only partial implementation is conducted.[8]

COSO published an addendum to the Reporting to External Parties volume of the COSO Report. The addendum discusses the issue of, and provides a vehicle for, expanding the scope of a public management report on internal control to address additional controls pertaining to safeguarding of assets. In 1996, COSO issued a supplement to its original framework to address the application of internal control over financial derivative activities.

The COSO Framework defined internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in three categories--effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. COSO's integrated internal controls framework includes the following components – "*the control environment, risk assessment, control activities, information and communication, and monitoring. The scope of internal control therefore extends to policies, plans, procedures, processes, systems, activities, functions, projects, initiatives, and endeavors of all types at all levels of a company*."

The COSO ICIF is definitional in nature, neither procedural nor prescriptive, which leads to confusion and disparate results in implementation. There was vigorous debate and confusion surrounding the definition of internal control over financial reporting. The guidance COSO issued on ICIF was clarification to assist with the scope of compliance. Notwithstanding the confusion, management has sole responsibility for adhering to this interpretation and public accountants are responsible for audit attestations in evidence to management's statements in financial statements.

A source of confusion has been the use of the term "*risk assessment*" in the COSO definition of internal controls over financial reporting. COSO's guidance includes risk language but fails to clarify the meaning of the term. For example, risk assessment as defined by COSO*, "risk are analyzed, considering likelihood and impact, as a basis for determining how they should be managed. Risk are assessed on an inherent and residual basis*." The definition leaves room for wide and varied interpretation which is a real weakness of the COSO framework.

How should internal control risks be analyzed? Who should analyze the risks? What methods are most effective at analyzing risk of internal control failure? What is an acceptable level of risk in internal controls? COSO fails to address these relevant questions nor define what is an "*ineffective*" or "*effective*" control. As a result, no training or expertise is needed to follow the guidance leading to disparate and varied results. Some risk professionals like the vagueness of

[8] https://www.academia.edu/45682001/The_Future_of_Risk_Management

COSO's guidance however a troubling increase in fraudulent financial reporting and corporate failure is the ultimate legacy of its framework.

A statutory requirement did not come into effect until 2002, after another series of financial accounting scandals in late 1990's and early 2000's, in the Sarbanes-Oxley (SOX) Act of 2002. SOX holds both registered public accounting firms and management of public companies ultimately accountable for the accuracy of financial statement reporting.[9] Section 404 of the Sarbanes-Oxley Act established a new rule that required management to include in their annual reports a certification of management's assessment of the effectiveness of the company's internal control over financial reporting. [10]

The annual report of management on the company's internal control over financial reporting has several key requirements: (only summaries provided): (a) a statement of management's responsibility to establish and maintain adequate internal controls; (b) a statement of management's assessment of the effectiveness of internal controls; (c) a statement identifying the framework used by management to assess the effectiveness of internal controls; and (d) a statement that the registered public accounting firm that audited the firm's financial statements include in management's annual report an attestation report on management's assessment of the company's internal controls over financial reporting. The COSO framework is not a requirement, and many executives are not aware of the type of framework used to assess the effectiveness of internal controls.

The Treadway Commission recognized the root cause of fraud as the behavior of independent public accountants, internal audit, and corporate executives in fraudulent financial reporting. The final Treadway Report documented the debates and finger-point that ensued afterwards ensuring that many of the recommendations were delayed or watered down until 2002 when Congress enacted the Sarbanes-Oxley Act. Many of the Treadway Commission's recommendations were codified into new legislation in SOX 2002. Ten years after the Treadway Commission, fraud grew exponentially worse, not better! Counterintuitively, COSO has benefited from increasing frequency in fraud by pivoting to consulting on failure in internal controls over financial reporting.

COSO's member firms began promoting integrated internal controls as a *risk* framework with other Big Four Accounting firms, selectively chosen academics, and external consultants to promote risk-based audits. The risk communications has always been troublesome and fraught with a variety of conflicting definitions and meanings. Depending upon one's point of view, one person's perception of risks can mean different things to different people. COSO's generic risk language means that anything can be a risk without rigorous probabilistic confidence levels or

[9] https://corporatefinanceinstitute.com/resources/knowledge/other/top-accounting-scandals/
[10] https://www.sec.gov/rules/final/33-8238.htm

rules-based guidance. Subjectively-defined assessments of risk have led unintended rigidity under the guise of risk management leading to a culture of risk aversion as opposed to a culture of compliance.

Auditors are responsible for managing *audit risks*, not business risks. The biggest risk to registered independent public auditors is a failed audit; fraud, misstatements of financial reports, and failure to identify accounting malfeasance. The AICPA defines an auditor's role in assessing audit risk.[11]

"This Audit Risk Assessment Tool (ARAT) is designed to provide illustrative information with respect to the subject matter covered and is recommended for use on audit engagements that are generally smaller in size and have less complex auditing and accounting issues. It is designed to help identify risks, including significant risks, and document the planned response to those risks. The Audit Risk Assessment Tool should be used as a supplement to a firm's existing planning module whether in a firm-based or commercially provided methodology. The Audit Risk Assessment Tool is not a complete planning module.

The AICPA recommends the Audit Risk Assessment Tool be completed by audit professionals with substantial accounting, auditing and specific industry experience and knowledge. For a firm to be successful in improving audit quality and efficiencies, it is recommended that an auditor with at least five years of experience complete the Audit Risk Assessment Tool, or the engagement team member with the most knowledge of the industry and client (often Partner in small or medium firms) provide insight to whomever is completing the Audit Risk Assessment Tool. The AICPA recommends this should not be delegated to lower-level staff and just reviewed—it should be completed under the direction of the experienced auditor (if you delegate to inexperienced auditor, you will be at risk for less effectiveness and efficiencies because the tool is intended to be completed by an experienced auditor).

The Audit Risk Assessment Tool does not establish standards or preferred practices and is not a substitute for the original authoritative auditing guidance. In applying the auditing guidance included in this Audit Risk Assessment Tool, the auditor should, using professional judgment, assess the relevance and appropriateness of such guidance to the circumstances of the audit. This document has not been approved, disapproved, or otherwise acted on by a senior committee of the AICPA. It is provided with the understanding that the staff and publisher are not engaged in rendering legal, accounting, or other professional service. All such information is provided without warranty of any kind."

The AICPA is clear that audit risks is the primary role of auditors and only "experienced" auditors should use the audit risk assessment tool. The ARAT is not a rigorous risk assessment tool to be used beyond the scope of an audit and guided by experienced senior auditors. It is however easy to see why there has been confusion about the role of audit in risk assessment and

[11] https://www.aicpa.org/resources/download/aicpa-audit-risk-assessment-tool

risk management as the scope of work auditors are asked to do has expanded. The problem is that the tools auditors have at their disposal are inadequate to an effective risk assessment and is recognized in the AICPA guidance above. Misinterpretations of this guidance and the misuse of risk language has resulted in unnecessary costs and poorly inadequate risk programs.

SOX added further confusion in its requirement on the formation of an audit committee on corporate boards. The Sarbanes-Oxley Act of 2002 mandates that audit committees be directly responsible for the oversight of the engagement of the company's independent auditor. Securities and Exchange Commission (the Commission) rules were designed to ensure that auditors are independent of their audit clients.[12] Guidance from the Securities and Exchange Commission is clear cut:

> "The Commission's general standard of auditor independence is that an auditor's independence is impaired if the auditor is not, or a reasonable investor with knowledge of all the facts and circumstances would conclude that the auditor is not, capable of exercising objective and impartial judgment on all issues encompassed within the audit engagement. To determine whether an auditor is independent under this standard an audit committee needs to consider all of the relationships between the auditor and the company, the company's management, and directors, not just those relationships related to reports filed with the Commission. The audit committee should consider whether a relationship with or service provided by an auditor:"
>
> (a) creates a mutual or conflicting interest with their audit client.
> (b) places them in the position of auditing their own work.
> (c) results in their acting as management or an employee of the audit client; or
> (d) places them in a position of being an advocate for the audit client.

Confusion in the interpretation of the guidance above has extended to the role of the audit committee. The S.E.C. guidance for the audit committee did not intend it to become a *de facto* "risk committee". The role outlined by the S.E.C. as described above, is to ensure independence in the auditor's duty.[13] However, the audit committee's role is impaired by an increase in advisory and consulting relationships between the auditor and the company." The lines have been blurred to the extent that conflicts in the relationship between external auditors and the firm have become difficult to untangle.

The risk of "*mutual and conflicting interests*" is widespread when independent auditors are consulting on risk management, the sole responsibility of management, or providing other services that lend itself to place the audit firm in a position of being an advocate for the audit client. The rules are intended to limit and prevent conflicts, yet these same conflicts continue to be the cause of financial fraud and business failure. The extent of the damage in misaligned

[12] https://www.sec.gov/info/accountants/audit042707.htm
[13] https://www.sec.gov/info/accountants/audit042707.htm

interpretations of the rules created by auditor role expansion has become substantial in material loss in shareholder value and jobs when companies fail, and litigation ensues.[14]

The original mandate given to the Treadway Commission was completed in 1992 when its report was issued. The report was designed to ensure *compliance* with the Foreign Corrupt Practices Act, a very narrow remit. Typically, when a Blue Chip panel has completed its task the group is dissolved however the COSO group has persisted for 36 years. A detailed review of deliberate actions taken by the COSO board will demonstrate how the nonprofit remains a platform for generating consulting fees for independent public accounting firms.

The role of corporate risk functions were nonexistent or newly forming in the early-1990's and 2000's. Large financial services firms implemented market, financial, and credit risk departments but operational risk management did not take shape until much later in the Basel Capital Accord formulated by Central Bankers. Many of these risk functions operate as silos without active engagement between the different disciplines but recent changes have shown that enterprise risk functions are slowly evolving. Enterprise-wide risk management (ERM) is a process of coordinated risk management that places greater emphasis on co-operation among departments to manage an organisation's range of risks as a whole. Enterprise wide risk management is still an aspirational goal for most organizations with some progress noted. While COSO's ERM integrated framework (IF) is has captured public attention as the most popular the reality is that few organizations adhere to COSO's guidance and instead use a hybrid of risk practices to achieve an enterprise view of risks.

Several industries still do not have formal risk programs. Public accounting firms benefit from covering a broad swath of industries and internal operations. This perspective gives its members a ringside view of risk practice across diverse firms along with insights on management's expectations about the lack of leadership in risk practice broadly. COSO filled a gap in uncoordinated efforts in risk practice given its position on the audit committee of corporate boards.

Congressional legislation in Sarbanes-Oxley was designed to clarify the narrow scope of audit and public accounting firms after Enron, WorldCom and Tyco revealed the complicity of audit behavior in fraudulent financial reporting.[15] Title I of Sarbanes-Oxley established the Public Company Accounting Oversight Board to monitor and inspect registered public accounting firms, evaluate audit quality, and administer discipline if necessary. Title II of SOX mandated auditor independence to avoid conflicts of interest, among many other requirements.

Fraud, executed through the manipulations of systems, people and processes is a significant risk to organizational survival but it is one risk among many shared in all organizations. A financial

[14] https://www.telegraph.co.uk/business/2022/01/12/kpmg-auditor-uses-minority-ethnicity-defence-forged-carillion/
[15] https://corporatefinanceinstitute.com/resources/knowledge/other/top-accounting-scandals/

risk exists if the principals of a firm choose to commit fraud. The risk of not detecting, deterring, preventing, and correcting this one risk, which can take many forms, is a significant business risk. However, fraud is a business risk the Treadway Commission and the SEC delegated to management, internal audit, independent public accountants, and the SEC to address. COSO's framework works only when people are committed to ethical behavior and follow acceptable accounting practice. One of the key concepts in the COSO integrated internal control framework is, "Internal control is carried out by "people." It is not simply about policies, manuals, and forms, but about people at all levels of an organization.

However, in the same guidance the limitations of COSO's framework are described here, "Internal control involves human action, which introduces the possibility of errors in prosecution or trial. Internal control can also be overridden by collusion among employees (separation of duties) or coercion by senior management.

The magazine `` CFO *reported that companies are struggling to apply the complex model provided by COSO. "One of the biggest problems: limiting internal audits to one of the three key objectives of the framework. In the COSO model, these objectives apply to five key components (control environment, risk assessment, control activities, information and communication, and monitoring "Given the number of possible matrices, it is not surprising that the number of audits can get out of control." CFO magazine continued to state that many organizations are creating their own risk and control matrix by taking the COSO model and modifying it to focus on the components that relate directly to Section 404 of the Sarbanes-Oxley Act.*

In fact, a 20-year COSO study of fraud, since the enactment of COSO's ICIF, found that the occurrence and magnitude of fraud exploded over the twenty years since the enactment of COSO's ICIF.[16] In fact, the detection of fraud is more likely than not from an internal whistleblower than from internal audit or independent public accounting firms. Fraud risk is one of many financial risks inherent in all for profit and nonprofit organizations alike. Human behavior is the risk not internal controls.

The fact that COSO's framework is not a risk management framework does not minimize the importance of this work. Naming ICIF a risk framework has created significant confusion in the emphasis placed on compliance versus the analysis of risk in the business broadly. The confusion created in audit's role should be settled to allow for advancements in both regulatory compliance and business risk analysis, separately and in collaboration. The attention and resources spent on compliance risks has created organizational rigidity, bureaucracy, and risk aversion.

It is important to understand how COSO and public accounting firms grew into a dual role: on the one hand, providing assurance services to external stakeholder on the accuracy of financial reporting; and on the other hand, acting as advisers and consultants on enterprise risk and other advisory services. These dual roles create inherent conflicts the S.E.C. warns boards to be

[16] https://www.coso.org/documents/FraudStudyOverview_000.pdf

cognizant of and proactively address. Confusion, complexity, and complacency has led to the adoption of a framework designed to address a very narrow compliance mandate (bribery) became adopted as a "*one-size-fits all*" risk solution without any substantive evidence of efficacy in risk mitigation.

COSO's guidance points out these weaknesses, "*although business risk management provides significant benefits, there are limitations. Business risk management depends on human judgment and, therefore, is susceptible to decision making. Human failures, such as simple errors or errors, can lead to inadequate risk responses. In addition, controls can be voided by collusion of two or more people, and management can override business risk management decisions. These limitations prevent a board and management from having absolute security regarding the achievement of the entity's objectives."*[17]

Philosophically, COSO is more oriented towards controls [compliance]. Therefore, it has a *bias* towards risks that could have a negative impact instead of the risk of missed opportunities.[18] The bias of negative outcomes create risk averse behavior while ignoring upside opportunities in informed risk seeking behavior. To better understand the performance of COSO's guidance on the mitigation of fraudulent financial reporting, I reviewed the results from internal studies COSO published in 2010.[19][20].

In 2010, COSO published a nine-year study called "Fraudulent Financial Reporting – 1998-2007: An Analysis of U.S. Public Companies".[21][22] A summary of the 2010 report was published by the North Carolina State Poole College of Management. The 2010 study was the last of only two studies conducted by COSO. The first study covered the years 1987 – 1997 and included a small sample of 294 cases of fraud. The 2010 study sample size included 347 cases of alleged fraudulent financial reporting.

Excerpts of the summary are presented here:

- "The dollar magnitude of fraudulent financial reporting soared in the last decade, with total cumulative misstatement or misappropriation of nearly $120 billion across 300 fraud cases with available information (mean of nearly $400 million per case) This compares to a mean of $25 million per sample fraud in COSO's 1999 study. While the largest frauds of the early 2000s skewed the 1998-2007 total and mean cumulative misstatement or misappropriation upward, the median fraud of $12.05 million in the present study also was nearly three times larger than the median fraud of $4.1 million in the 1999 COSO study.

- Companies allegedly engaging in financial statement fraud had median assets and revenues just under $100 million. These companies were much larger than fraud

[17] https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission
[18] https://en.wikipedia.org/wiki/Committee_of_Sponsoring_Organizations_of_the_Treadway_Commission
[19] https://corporatefinanceinstitute.com/resources/knowledge/finance/financial-engineering/
[20] http://guide.berkeley.edu/graduate/degree-programs/financial-engineering/
[21] https://erm.ncsu.edu/library/article/coso-fraud-study/
[22] https://pcaobus.org/oversight/inspections/firm-inspection-reports

companies in the 1999 COSO study, which had median assets and revenues under $16 million.

- The SEC named the CEO and/or CFO for some level of involvement in 89 percent of the fraud cases, up from 83 percent of cases in 1987-1997. Within two years of the completion of the SEC's investigation, about 20 percent of CEOs/CFOs had been indicted and over 60 percent of those indicted were convicted.
- The most common fraud technique involved improper revenue recognition, followed by the overstatement of existing assets or capitalization of expenses. Revenue frauds accounted for over 60 percent of the cases, versus 50 percent in 1987-1997.
- Relatively few differences in board of director characteristics existed between firms engaging in fraud and similar firms not engaging in fraud. Also, in some instances, noted differences were in directions opposite of what might be expected. These results suggest the importance of research on governance processes and the interaction of various governance mechanisms.
- Twenty-six percent of the fraud firms changed auditors between the last clean financial statements and the last fraudulent financial statements, whereas only 12 percent of no-fraud firms switched auditors during that same time. Sixty percent of the fraud firms that changed auditors did so during the fraud period, while the remaining 40 percent changed in the fiscal period just before the fraud began
- Initial news in the press of an alleged fraud resulted in an average 16.7 percent abnormal stock price decline in the two days surrounding the news announcement. In addition, news of an SEC or Department of Justice investigation resulted in an average 7.3 percent abnormal stock price decline.
- Long-term negative consequences of fraud were apparent. Companies engaged in fraud often experienced bankruptcy, delisting from a stock exchange, or material asset sales following discovery of fraud – at rates much higher than those experienced by no-fraud firms."

The term *evidence-based* is used by research analysts to describe efficacious outcomes in studies to determine the effectiveness of methodology or practice. Using the above outcomes as evidence, COSO's ICIF would be referred to as the *null hypothesis* of financial fraud or risk mitigation.[23] In the 20 years after the formation of the Treadway Commission financial fraud was materially worse. Considering the small sample size, the results were likely gross understatements of fraud. The COSO report did not break out which public accounting firm fared worse than other firms, but the aggregated nature of the findings suggest the weakness was broad.

[23] https://en.wikipedia.org/wiki/Null_hypothesis

COSO has never published follow up reports after the 2010 study, however more recent headlines provide further evidence fraudulent financial reporting has gone global.[24][25][26] "In the 20 years that followed, after the Enron fraud faded into history, the Big Four Accounting firms rebuilt their consulting empires, advising on everything from insolvency to cybersecurity. But now a fresh stream of scandals has again raised concerns that firms selling services like merger advice cannot also function effectively as auditors." (Michael O'Dywer and Kaye Wiggings, London, Financial Times, "*Insurgents take on the scandal-hit Big Four*")[27]

"That has forced Deloitte, EY, KPMG and PwC to rein in the cross-selling that helped bring them a combined $157 billion in annual revenues last year – opening the door for nimble competitors to lure away star performers with generous pay cheques."

"Smaller insurgents, many of them private equity-backed, are bidding for the most lucrative divisions of the Big Four's business without the drag of the low margin, highly regulated and potentially reputation-damaging audit operations."

In an odd twist of irony, independent public accounting firms have benefited from fraud by raking in billions in consulting fees. When a company fails because of financial malfeasance one of the other big four firms take over to clean up the mess. Due to the lack of competition and the global reach of the largest public accounting firms, audit has become too *Big to Fail*, or has it?

Cognitive Map: The Unintentional Consequences of a global ERM Framework – Part 2

The COSO ERM Integrated Framework has garnered global acceptance as a standard in some circles by leveraging confusion in the public. So how did public accounting firms and internal auditors who use COSO's guidance to leverage the credibility of the five participating organizations and make billions in consulting fees. We can find clues to the answer in COSO's own research. In a research study commissioned by COSO, we can begin to see how the organization orchestrated ERM IF into an international phenomenon. The findings were presented in a 2013 Alternative Accounts Conference.

[24] https://amp.ft.com/content/a8c60322-3e56-4889-b346-e34d3c5f1e97
[25] https://www.ft.com/content/57e0ff80-de17-48b1-9da7-5bdbaaad8898
[26] https://amp-ft-com.cdn.ampproject.org/c/s/amp.ft.com/content/548f99ff-1815-4af1-a7ef-e631cf9c720a

The COSO board participated in a set of workshops sponsored by the Queen's School of Business and the University of New South Wales with financial support provided by the CPA-Queen's Centre for Governance. The title of the study: "*Hybridized Professional Groups and Institutional Work: COSO and The Rise of Enterprise Risk Management*." The authors of the report were Christie Hayne, School of Business, Goodes Hall, Queen's University, Kingston, ON, Canada and Clinton Free, Australian School of Business, University of New South Wales, Sydney, Australia.
(Excerpts from the report are presented below):

"This study specifically aims to examine the emergence and institutionalization of COSO's ERM-IF. Adopting a qualitative research design, we interviewed a range of individuals directly involved in COSO's Board and Project Advisory Council at the time the ERM-IF framework was devised, as well as the principal authors of the framework. We also interviewed individuals outside of the COSO groups (e.g., consultants, executives) that we felt would offer valuable insights into the process of diffusion. In total, we conducted 15 interviews with individuals important to COSO and the ERM-IF. We also consulted a large body of secondary materials to provide further evidence and substantiate findings."

"This study makes two key contributions. First, it presents an account of the mechanisms and processes that gave rise to the formation of COSO's ERM model, which has become the dominant risk management model in North America and beyond. We detail how COSO engaged in a comprehensive project of institutional work comprised of political, cultural, and technical activities (Lawrence & Suddaby, 2006; Perkmann & Spicer, 2008). Drawing upon taxonomies developed in the area of institutional work, we illustrate the varied and overlapping forms of agency that enabled COSO's ERM-IF to successfully institutionalize."

"Recent research in the area of institutional work augments and extends institutional theory, a perspective which has wide currency in accounting research. While others have focused on categories of institutional work (e.g., Goretzki, Strauss & Weber, 2013), we adopt a holistic approach to illustrate the wide ambit of work required to successfully diffuse a new managerial technology. We demonstrate that COSO's institutional work was marked by non-sequential, often serendipitous, actions that acted to overlap and reinforce each other. To the best of our knowledge, this article is the first to fully elaborate the notion of institutional work in accounting research."

"Second, we present a more fully articulated conception of the actors involved in the supply side of a management innovation. Specifically, we draw attention to the notion of *hybridized professional groups*, reflecting the way that COSO was able to draw importantly from the social and cultural capital, networks, and resources of its members in disseminating the emerging model. Miller, Kurunmaki and O'Leary (2008) argue that existing literature has largely neglected

the hybrid practices, processes and expertises that make possible lateral information flows and coordination across the boundaries of organizations, firms, and groups of experts or professionals."

COSO's research suggests that its ERM integrated framework (IF) did not emerge from the rigors of scientific testing or statistical analysis but instead was an orchestrated effort coordinated by its Board members who leveraged the "cultural capital" of its five professional organizations reinforcing credibility through its members in accounting, auditing, academics, researchers and select consultants. The actions taken by the COSO Board was a deliberate effort undergirded by the credibility of forming a nonprofit group of professional associations which grew out of the Treadway Commission. Notwithstanding the fact that its framework is not designed to withstand the rigors of a robust risk framework.

"*Scarbrough (2002) argues that professional groups tend to fulfill theorization roles in the shaping of a management fashion while consultants fulfill the diffusion side), we demonstrate that a more distributed but cohesive group of actors – comprised of accountants, auditors, academics, researchers and consultants – was able to perform multiple roles and effectively support both the development and preservation of the concept*."

The researchers compared the emergence of COSO's ERM to past fads in management. "*Many researchers have observed that management innovations – including ISO standards (Corbett & Kirsch, 2001), product development management control systems (Davila et al., 2009), activity-based costing (Malmi, 1999), total quality management (Sharma et al., 2010), performance-based incentives (Bol & Moers, 2010) and the balanced scorecard (Busco & Quattrone, 2009; Qu & Cooper, 2011) – have swept across a broad range of industrial sectors in the past two decades (Abrahamson & Fairchild, 1999; Alcouffe, Berland & Levant, 2008; Bort & Keiser, 2011; Jackson, 2001*)."

"*The diaspora of associated entities provided a key platform for advocating and promoting the ERM technology and provided a stable and influential network of support. Our analysis suggests that, as a large, multi-faceted hybridized professional group, COSO was able to bridge conventional diffusion categories of disruption, creation and maintenance."*

This study sheds light on the deliberate steps COSO took to create a platform for commercial growth under the auspices of an independent nonprofit to reap billions in consulting fees for public accounting firms. The study is interesting in what is not included in its analysis:

(1) There is no due diligence provided on other existing risk frameworks for comparison to their own ERM IF.

(2) None of the academics or consultants provided detailed empirical evidence of the effectiveness of COSO's principles or guidance in real-life settings even though it had been in use for approximately twelve years after the Treadway Commission's Report had been issues.
(3) The public accounting firms had twelve years to gather extensive data on the performance of COSO's ICIF to help inform how to extend its framework at the enterprise level and chose not to do so.
(4) If COSO had conducted such an analysis the findings were not shared with researchers who conducted an extensive literature review in preparation for the study.
(5) Why did COSO not address the initial gap (human failures) identified in its own guidance? Extensive academic literature from Paul Slovic, Dan Kahneman, Amos Tversky, Frank Knight, Herbert Simon, and many other giants in psychology and economic theory was available to provide guidance for human behavior and decision-making under uncertainty?

Ultimately, the study was not conducted to determine if COSO's ERM integrated framework was effective in its mission. The study was designed simply to determine how effective COSO had been at creating a facade of legitimacy as a risk management framework with no efficacious outcomes from its guidance.

Many risk professionals and business executives are still surprised to learn that COSO ERM IF is not a risk standard and not required by legal mandate. COSO has been effective at "socializing" its principles as a best practice however COSO provides no metrics from which to measure the performance of its guidance. In other words, COSO simply filled a vacuum in risk management leadership that continues to prevail and created the appearance of a standard through the force of cohesion of its members collectively advocating for its guidance. Comments from researchers and participants on the COSO board exemplify their awareness of how confusion in organizational risk practice created opportunities for its integrated internal control framework.

"*As it [COSO ERM IF] emerged, it became apparent that risk management was a canvass with a host of aspiring artists. Within the broad area of financial management, management accountants, internal auditors, external auditors, management consultants as well as a new and increasingly visible body of risk managers (see Aabo, Fraser & Simkins, 2005; Hall, Mikes & Millo, 2013) all sought to stake a claim as the concept opened up opportunities for applied use.*

In effect, this made risk management different from other innovations in accounting such as activity-based costing, the balanced scorecard or risk-based auditing, which have generally been circumscribed to particular areas of management accounting, auditing, or financial accounting. In this sense, COSO's ERM-IF is an innovation that is remarkable in its breadth (contested by a range of sub-disciplines) and commercial penetration (applied throughout the world).

While there is no legal mandate for its use, it nevertheless has attracted normative force. While Olson and Wu (2008) claim that there are over 80 risk management standards across the globe[28], research has consistently identified COSO ERM-IF as the best known (Fraser et al., 2008) and most widely diffused risk management standard (COSO, 2010b). The institutional work that has facilitated this rise is thus an important object of scholarly attention."

COSO ERM, like other subjectively-defined risk management frameworks, is a prime example of the *rational man theory,* homo economicus, at play in enterprise risk practice. Economic theory of a rational man posits that humans innately possess all the skills and capabilities to always make rational choices. Research in economic theory and behavioral science has soundly refuted the fallacy in rational man theory by pointing out obvious examples of contradictions in rational behavior expressed in contemporary society. Homo periculum (*human risks or risk wo/man*) is a play on words like *homo economicus* in economics.[29] *Homo periculum* is introduced to define the fallacy of using subjectively-defined risk processes; a fallacy in judgment that an organizations' subjectively-defined pursuits in risk management are conducted optimally. The persistence of the fallacy in *homo economicus* continues in risk practice today leading to failed performance and expectations in risk governance. This is a cognitive risk, a blindness to heuristics and biases that limit our ability to recognize errors in judgment. A more detailed explanation of homo periculum will follow in Part 3.

The critique is not all negative. COSO was instrumental in focusing attention on the basic elements of a risk program for compliance. COSO's ICIF is foundational yet as we enter a digital age of innovation, smart systems, and hybrid work we must move forward with risk tools and technology equal to the task of a new digital operating environment. The "E" in ERM is no longer relevant. Risks are not contained by physical walls. Digital business models create digital risks that are not addressed or even contemplated in COSO's guidance.

COSO's research study also contained warnings about the dual role COSO has created as a trusted agent and an adviser on risk management. "*For some, however, accounts of institutional entrepreneurship have tended to be hagiographic and represent a bridge too far in asserting the heroic influence of individual agents (Delmestri, 2006; Lawrence, Suddaby & Leca, 2009; Suddaby, 2010). As Lawrence, Suddaby and Leca (2011, pp. 52-53) put it: "Missing from such grand accounts of institutions and agency are the myriad, day-to-day equivocal instances of agency that, although aimed at affecting the institutional order, represent a complex mélange of*

---

[28] Indeed, several international risk management standards pre-date the COSO framework including CAN/CSA-Q850-97: *Risk Management: Guideline for Decision*-Makers issued by the Canadian Standards Association in 1997 (62 pages); BS 6079-3:2000 *Project Management: Guide to the Management of Business-related Project Risk* issued by the British Standards Institution in 2000 (22 pages); JIS Q2001: 2001(E) *Guidelines for Development and Importance of Risk Management* Systems issued by the Japanese Standards Association in 2001 (20 pages); IEEE Standard 1540-2001: *Standard for Software Life Cycle Processes – Risk Management Standard for Software Life Cycle Processes – Risk Management* issued by the American Institute of Electrical and Electronic Engineers in 2001 (24 pages); and AS/NZS 4360:2004: *Risk Management* issued jointly by Standards Australia/Standards New Zealand in 2004 (24 pages). Based on a wide ranging analysis of several standards, Raz and Hillson (2005) conclude that there is "wide consensus regarding the main steps and activities of a generic risk management process" (p. 65) and that "where there are apparent differences in process, these are largely attributable to variations in terminology" (p. 64).

[29] https://en.wikipedia.org/wiki/Homo_economicus

forms of agency – successful or not, simultaneously radical and conservative, strategic and emotional, full of compromises, and rife with unintended consequences."

"*A wide range of studies have examined the factors that support the demand for management innovations. The phenomenon of management 'fads' and 'fashions' has inspired a large body of research, prompting some commentators to question whether management fashions research itself has become the next academic fad (Clark, 2004). The social and organizational functions of management innovations are generally related to reducing uncertainty, insecurity, ambiguity, and imperfection (Mazza & Alvarez, 2000) and providing managers with an image of innovativeness (Kieser, 1997) or even heroism (Clark & Salaman, 1998). Somewhat paradoxically, this is often achieved through the use of concepts that are of high linguistic ambiguity (Benders & Van Veen, 2001)."*

The warnings are prophetic and capture the risk of using COSO's ERM framework to address even mundane risks. The AICPA guidance above succinctly points out the risk of untrained auditors using their own audit risk tool inappropriately. Many risk and compliance professionals erroneously believe that the process of implementing COSO's framework is an act of risk management. The goal of risk management is *actively seeking to learn what you don't know about risks.* The real nature of risk management is reductions in ignorance about risk writ large. Knowledge of a risk is the first step of discovery followed by an understanding of root cause analysis in risk origination and finally risk treatments.

Researchers in the study provided extraordinary insights from participant's comments in individual interviews. The following commentary from board members, consultants and academics provide an intimate perspective in how COSO ERM was conceived and promoted as a risk management framework from an insiders' perspective:

"COSO is kind of an odd organization, not just in terms of being a virtual organization but, you know, what is it? It's not really a standard setter and yet it is kind of a standard setter. It's not a company; it's not a for-profit organization. And so, I think, when COSO comes out with guidance, it carries a pretty unique credibility because you can't attribute their actions to a profit motive per se. (Douglas Prawitt, Interview 5)"

"The cipher COSO itself is noteworthy. Described as "disarmingly mundane" by Consultant 3, COSO leaves unspecified the identity of the involved organizations and imparts an almost faceless proceduralism to COSO's activities."

Members of the COSO Board describe how confusion in public perception in COSO's not-for-profit status creates a shield from scrutiny into public accounting firm's profit motives.

What followed from these discussions was a recognition of the failure COSO's integrated internal controls framework and the need to move on to the next approach of promoting an enterprise-wide framework to replace ICIF.

"*Oliverio (2001) pointed to a number of failings including the absence of implementation guidance and clear allocations of responsibility as well as the imperative of an enterprise-wide approach. Furthermore, the competing frameworks were all motivated in some part by observations that COSO's IC-IF was no longer adequate in managing against diverse and growing risks. Where internal control was once seen as a valuable process for assuring the achievement of an organization's goals, it was seen to come under increasing scrutiny."*

"There were some people who were looking ahead and saying 'Okay, what's the next step?' We [COSO] have this internal control framework out here and now companies are using it, auditors are looking at internal controls…. What's the next step in the evolution of things? What are outside parties interested in? They are interested in how you're controlling things, but what's at the core of that control framework? First, it's identifying risk and then implementing controls to mitigate and control those risks…. So, in a way, the COSO internal control framework was a rudimentary risk management framework. (Douglas Prawitt, Interview 5)"

"In effect, what PwC was able to do was to position itself to roll out its framework as the international benchmark. Under the COSO badge, PwC was able to take the lead in consulting in the area. (Consultant, Interview 3)"

"What the profession needed was a comprehensive way to talk about risk. There are many ways of looking at risk but what we found is that people were talking and using the same terms in different fashions and so forth. And our view was that we needed a comprehensive framework on enterprise risk management, and it had to be across the enterprise and that if we could introduce

the framework, it could get more people talking about enterprise risk management-management and therefore moving to manage risk in a much more effective way. So that was the motivation behind starting with the ERM framework. (Larry Rittenberg, Interview 7")

"Because of that lack of a mandate [from a regulator, for example], organizations can sort of pick and choose pieces of it that work and not feel like they have to do a full blown implementation. We're in the early phases of ERM where people are just out there

picking, there's no mandate for anything and so I think people have found it helpful, but I guess it's good that they're not being forced into it at this point. ERM is so complex to really do, companies have realized if they try to go from A to Z, it will stall. (Mark Beasley, Interview 3)"

"I think part of it is because of the COSO consortium of organizations and frankly PricewaterhouseCoopers having been the author of the COSO ERM report – the names attached and the fact that COSO's internal control became a standard. The background and expertise of those organizations, and if I may say so also PwC, has caused people to look to it as the place to go in gaining insight, in gaining direction on how to build an ERM architecture in their organizations. (Rick Steinberg, Interview 9)"

This is an excellent time to introduce cognitive mapping.[30] The term was generalized by some researchers, especially in the field of operations research, to refer to a kind of semantic network representing an individual's personal knowledge or schemas. The cognitive map above provides a look into the "mind's eye" of participants as they deliberate the merits of adopting COSO ERM IF.[31]

"Part of it is probably, just the fact that it's a US framework, to be honest with you. I think that carries a lot of clout, probably decreasingly so the way the world is moving, but I think that it still does carry some impact. (Douglas Prawitt, Interview 5)"

"The whole US thing; it's what I call the McDonald effect: it's American, it's big, and it's what the New York Stock Exchange will accept. (John Fraser, Interview 1)"

"I was invited to speak in Tokyo, and I remember talking to the Minister of Economy … he said, "But you also have to understand that many Japanese businesses are already New York Stock Exchange traded and so whatever they hear is happening in the US, they want to do it". He said, "Many others are New York Stock Exchange wannabes. So, they're not on the New York Stock Exchange yet, but they want to figure out what the best practices are in the US and then get ready and say that they're already doing those practices … so that division is going to implement enterprise risk management or some COSO framework to make it look more relevant." (Paul Walker, Interview 8)"

"Some accounting firms were fairly responsive to it [COSO's ERM-IF] and kind of did similar to us [PwC], kind of developed methodologies and things to go deliver services around it. There

---

[30] *Ungar, Simon (2005). "Cognitive maps". In Caves, Roger W. (ed.). Encyclopedia of the City. Abingdon; New York: Routledge. p. 79. doi:10.4324/9780203484234. ISBN 9780415252256. OCLC 55948158.*

[31] https://en.wikipedia.org/wiki/Cognitive_map

was also some who felt that they could build a better mousetrap or already had a better mousetrap. (Frank Martens, Interview 14)"

"Most consulting firms want to have tools and frameworks that are branded their own so they can use them, even if it's just a slight change. I think everybody tries to come up with their own little process wheel, everybody tries to come up with their own framework for looking at it, everybody tries to come up with their own common risk language, it's just the way it is. (Consultant 1, Interview 10)"

"There are a lot of mouths to feed, and we were out hawking for work like everyone else. And COSO was a name that people knew ... Sure most of the big players refined this to develop their own proprietorial tools, but the COSO model opened the door if you like. (Consultant 3, Interview 12)"

The comments from board members, consultants and public accountants give you a real sense of the genesis of COSO ERM. There clearly was recognition that a singular focus on internal controls was no longer sufficient and a new approach was needed. One interviewee noted, *"ERM is so complex to really do"*. ERM is hard because the methods for analyzing disparate risks in aggregate requires different approaches than subjective-defined audit risk tools. It is unlikely that measures of "likelihood" and "impact" are sufficient analytical predictors of enterprise wide risks such as cyber, operational, human, technological and strategic risks in aggregate.

On the one hand, there is no longer a regulatory justification for COSO to continue to exist 36 years after the conclusion of the Treadway Commission. The Sarbanes-Oxley Act of 2002 has still not materially reduced fraudulent financial reporting. On the other hand, neither the SEC nor the Public Company Accounting Oversight Board has fully addressed the inherent conflicts of interest in the dual-role of consulting and audit advisory work. The firewalls that should exist have proven to be made of paper mâché, if they exist at all. Corporate boards must take back control of the audit committee's clearly defined scope to ensure audit independence. There is now a robust and thriving community of risk professionals and risk advisory firms to provide organizations with independent risk guidance or to supplement existing risk departments.

Auditors and public accounts have a value role to play in advancing internal controls over financial statements. More advanced guidance is needed on digital controls, connected devices, external third-party controls in the cloud and on vendor site inspections. As organizations continue the transition to digital strategies support to strengthen internal controls over financial reporting provide ample opportunity for public accounting firms. The SEC should also ensure and encourage an expansion of regulated public audit firms' eligibility and regulate independent risk advisory firms to enable competition for access to the global marketplace of ideas in financial accounting and risk management.

Researchers demonstrate the challenges in creating a competitive market in public accounting.[32] "Because public accounting is a regulated practice, the profession actively manages its relationship with the state. While prior studies have analyzed the profession's efforts to shape its regulatory environment, few studies have examined the profession's pointed attempts to influence a specific regulatory policy that affects the practice of auditing in the United States. Drawing on extant theories of regulation and political economy, this study investigates the rationality and effectiveness of political action committee (PAC) contributions paid to members of the US Congress by the US public accounting profession during the policy formulation period of the Sarbanes–Oxley Act of 2002.

Based on the results of empirical tests, we conclude that the US profession strategically manages its relationship with the federal government, in part, through direct involvement in the financing of political campaigns. Furthermore, the profession's pattern of contributions implies an ideologically conservative as well as a professional regulatory motivation for providing financial support to federal legislators. Thus, although the US profession continues to proclaim the primacy of its public interest orientation, it does not appear to be politically neutral when attempting to influence public policy."

Decoding the Failure in Audit and Confusion in Enterprise Risk Management – Part 3

The unintentional *noise* in public accounting and auditing costs financial markets trillions of dollars in real and potential losses on a global scale – creating a massive cognitive risk and one that could have been mitigated had Congress, the SEC and the public understood the need to focus on the root cause of risk (human behavior) instead of internal controls over financial reporting. Herbert Simon pointed out this risk in 1947 in *Administrative Behavior* and introduced the concept of "bounded rationality".[33] *"Simon recognized that a theory of administration is largely a theory of human decision making, and as such must be based on both economics and on psychology.*

Simon presented arguments against the then prevalent theory that "humans as agents who are consistently rational and narrowly self-interested, pursue their subjectively-defined ends optimally." Even though academics have settled the fallacy of belief in perfect rationality, remnants of these beliefs and practices still operate in corporate boards, government, and other institutions whether we consciously realize it or not. Our inability to recognize these risks is what I call cognitive risks.

Cognitive risks exist in many forms but primarily manifest in inattentional blindness to risk in judgment, bias and impacts in human error.[34] Inattentional blindness *"occurs when an individual*

[32] https://www.researchgate.net/publication/223239550_Money_politics_and_the_regulation_of_public_accounting_services_Evidence_from_the_Sarbanes-Oxley_Act_of_2002
[33] https://en.wikipedia.org/wiki/Herbert_A._Simon
[34] https://en.wikipedia.org/wiki/Inattentional_blindness

fails to perceive an unexpected stimulus in plain sight, purely as a result of a lack of attention rather than any vision defects or deficits. When it becomes impossible to attend to all the stimuli in a given situation, a temporary "blindness" effect can occur, as individuals fail to see unexpected but often salient objects or stimuli." Examples include texting while driving, or decision-making while distracted by calls or deadlines. While we value multitasking we are lousy at doing it well. Counterintuitively, inattentional blindness occurs by blindly following what other organizations have adopted as "*best practice."*

Why is cognitive risk relevant? Behavioral economists and researchers have already identified similar risks in heuristics, bias, health, and safety issues; however, to date, their insights have not been applied to risk governance specifically. The idea became obvious to me as an area in need of attention and research after reading the insightful examples provided in the book, *Noise*. An entirely new and unexplored approach to thinking about risk has been revealed in the precepts in *Noise*. Kahneman, et al, present a simple approach, *decision audits*, to detect the presence and the magnitude of this hidden risk.

As an example, the global adoption of COSO ICIF and COSO ERM IF is noisy and biased on several fronts. Let me explain further. The process of implementing COSO ICIF is both *noisy* and *biased* in that no two organizations adopt the processes and principles in the same way. The definition of "noise" is variability (dispersion) in judgment(s). What that means in practical terms is two-fold: a) COSO lacks a verifiable target of performance for risk mitigation when a partial implementation is as satisfactory as a full implementation. b) COSO lacks any predictive value in how effective the framework would perform as evidenced by the variability in disparate implementation outcomes.

The second major problem with COSO's two frameworks is they are biased towards a focus on internal controls over financial reporting. This point was made clear by COSO itself in the creation and explanation of the ICIF. A biased framework is systemically incorrect in that no matter the means of implementation users will view risks in one way limiting one's view of the spectrum of risks that exist. This is a classic cognitive risk in inattentional blindness!

There are two kinds of error: ***Noise and Bias***. Consider a group of friends at their favorite pub playing a game of darts. The group is made up of four teams who play every Friday night. Team 1's darts consistently hits near the bullseye. The team 1's tightly clustered darts represent a perfect pattern. Team 2 is consistently off target to the left, but also in a tightly clustered pattern of darts. (*biased*) Team 3's darts are widely scattered with no discernable pattern (*noisy*), and Team 4's darts are off target but also widely scattered (*both noisy and biased*). Now convert the darts into business decisions. Bias has gotten more attention, but noise is a hidden culprit in the flaw of judgment….and more than expected.

A layman's explanation may also be helpful. Here is a practical example: If two dozen firms of the same size and risk profile adopt COSO's ICIF or its ERM IF in disparate ways there is no way to determine if COSO's framework is an effective tool to mitigate risks because of inherent noise and bias in how the framework is implemented. In practical terms, inconsistency in how COSO's framework is implemented creates a regulatory lottery. If a regulator finds deficiencies in one firm the same deficiencies or greater may exist in other firms creating a systemic risk within the industry. The evidence of this lottery effect has played out in fraudulent financial reporting across different industries after the partial adoption of different components of COSO's two main frameworks.

Fundamentally, COSO's ICIF and its ERM IF are flawed risk frameworks and the billions spent on implementation are the costs of error in judgment. COSO's own research is evidence of inherent flaws in its framework but the real damage in corporate governance is the expectation that COSO's framework is a best practice in risk management.

Over-reliance on subjectively-defined risk management programs is an example of the fallacy I call, cognitive risk, or *homo periculum.* Homo periculum is a fallacy in assuming frameworks like COSO's ERM IF are optimal approaches to achieving maturity in risk management programs. Compliance-oriented frameworks are helpful to ensure consistency in institutional behavior but are only the first step in a multidisciplinary process toward building a robust risk practice. This concept may be hard to grasp initially because many risk professionals are not familiar with the science of risk. But consider that all buildings rely on a good foundation based on ground and weather conditions the architect must consider for long-term sustainability, including maintenance and upkeep.

Or consider the analogy one senior executive frequently used. A race car needs good brakes, suspension system, and tires for different weather and road conditions to allow the race car driver to perform optimally to win while remaining safe. Weakness in any of the foundational areas of design create inherent vulnerability to the entire system. That is why the World Trade Center towers held after the planes hit allowing most of the participants to escape unharmed versus the catastrophic failure of the Condo towers on the beach in Florida. Attention to details matter because the details allow you to take informed risks after you have addressed the fundamentals.

Risk management is not solely about following someone else's script for what a risk program is, it is about understanding the proper design of a risk program to address your unique and specific risk needs.
Reimagining the organization is about designing new solutions for the needs of your firm not following the leader, especially when the self-anointed leaders know less about your risks than you do.

The merging of psychology and economics has resulted in a more robust understanding of judgment and decision-making under uncertainty and helps explain why this flaw has gone undetected and underrepresented in traditional risk frameworks like COSO ERM, ISO 31000 and most existing risk programs. It is premature to call any traditional risk framework *"mature"* without an extensive grounding in the science of risk whose root and branch is informed in psychology, behavioral economics, behavioral science, and decision science. Economists dubbed the rational man theory *"homo economicus",* I have dubbed the rational risk theory in traditional risk practice *"homo periculum"*, a fallacy I call cognitive risk, a fallacy that organizations' subjectively-defined pursuit of risk management is conducted optimally.

The noise in public accounting and audit that I referred to earlier is the same as those referenced in the prologue, *"wherever there is judgment, there is noise – and more of it than you think" ("Noise", p.12,* Kahneman, Sibony, Sunstein 2021*).* Public accounting and audit are predicated on judgment. Judgment is required in response to accounting for the complexity of today's business environment. A problem arises when attempting to overly rely on subjective judgment in the application of complex risk analysis without appropriate rules-based guidance.

We now know that noise is the variability of judgment. When business leaders and auditors differ on "the risk" of a course of action or the outcome of certain business practices these disagreements create bias and noise in judgment. When organizations lack the tools to minimize bias and noise the resulting residual risk is costly whether known or not. This risk is largely undetected until the accumulation of these unresolved judgments add up to an unexpected failure or operational inefficiencies.