NPS-AM-25-264

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Fraud in Afghanistan: Analysis of Internal Control Failures

December 2024

LTJG Hannah M. Wilson, USN

Thesis Advisors: Dr. Juanita M. Rendon, Lecturer
Dr. Michael E. Freeman, Professor

Department of Defense Management

Naval Postgraduate School

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943

Disclaimer: The views expressed are those of the author(s) and do not reflect the official policy or

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Department of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact the Acquisition Research Program (ARP) via email, arp@nps.edu or at 831-656-3793.

Acquisition Research Program
Department of defense management
Naval Postgraduate School

ABSTRACT

This thesis examines instances of fuel fraud schemes in U.S.-funded reconstruction projects in Afghanistan, hypothesizing that failures in internal controls enabled these fuel fraud schemes. Applying the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control Framework, this study analyzes documented cases of prosecuted and convicted military members involved in fuel theft. This research utilizes a case study methodology to identify systemic weaknesses in internal controls and recurring patterns of failure within the fuel management systems. The findings demonstrate that the lack of an effective internal control system contributed to fuel fraud. The results highlight the need for robust internal controls and improvements to enhance accountability and reduce vulnerabilities in the fuel management systems. This study also provides actionable recommendations to strengthen financial governance in conflict areas.

THIS PAGE INTENTIONALLY LEFT BLANK

ABOUT THE AUTHOR

LTJG Hannah Wilson is a Medical Service Corps Officer. She was commissioned through the United States Naval Academy, where she received a Bachelor of Science. After graduating from the Naval Postgraduate School she will be reporting to Financial and Materiel Management Training Course (FMMTC) in Bethesda, Maryland. She has follow-on orders to Naval Hospital Camp Pendleton.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am grateful to God for providing me with the strength, resilience, and opportunities to pursue my goals and complete this work. I would also like to thank my family for their support, encouragement, and love. Their belief in me has been a constant source of motivation throughout this journey. Special thanks go to my advisors, Dr. Rendon and Dr. Freeman, whose expertise, guidance, and patience has been vital to my success. Their mentorship and insight have helped shape the direction of this study, and I appreciate their support.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-AM-25-264

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Fraud in Afghanistan: Analysis of Internal Control Failures

December 2024

LTJG Hannah M. Wilson, USN

Thesis Advisors: Dr. Juanita M. Rendon, Lecturer
Dr. Michael E. Freeman, Professor

Department of Defense Management

Naval Postgraduate School

Approved for public release; distribution is unlimited.

Prepared for the Naval Postgraduate School, Monterey, CA 93943

Disclaimer: The views expressed are those of the author(s) and do not reflect the official policy or

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AICPA	American Institute of Certified Public Accountants
ANA	Afghanistan National Army
ANDSF	Afghan National Defense and Security Forces
ANP	Afghanistan National Police
ANSF	Afghan National Security Forces
ASFF	Afghanistan Security Forces Fund
CERP	Commander's Emergency Response Program
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CSTC-A	Combined Security Transition Command-Afghanistan
DLA-E	Defense Logistics Agency-Energy
DoD	Department of Defense
DoD OIG	Department of Defense Office of Inspector General
DP	Diplomatic Program
ECC-A	Expeditionary Contracting Command-Afghanistan
ERM	Enterprise Risk Management
ESF	Economic Support Fund
FBI	Federal Bureau of Investigation
FCPA	Foreign Corrupt Practices Act
FPDS	Federal Procurement Data System
FOB	Foreign Operating Base
GAO	Government Accountability Office
INCLE	International Narcotics Control & Law Enforcement
INL	Bureau of International Narcotics and Law Enforcement Affairs
MOD	Ministry of Defense
MOI	Ministry of Interior
NAT	National Afghan Trucking
NATO	North Atlantic Treaty Organization
NSPA	NATO Support and Procurement Agency
OIG	Office of Inspector General
OMB	Office of Management and Budget

PACER	Public Access to Court Electronic Records
RMC	Risk Management Council
SIGAR	Special Inspector General for Afghanistan Reconstruction
SMW	Special Mission Wing
USAID	U.S. Agency for International Development
USDA	U.S. Department of Agriculture
WSP	Worldwide Security Protection

I. INTRODUCTION

The U.S. government conducts numerous overseas contingency operations, investing substantial funds in resources, including goods and services, with fuel being a primary expense. The reconstruction efforts in Afghanistan, particularly in relation to fuel management, were plagued by systemic fraud, mismanagement, and internal control failures, which ultimately undermined the success of U.S. operations in the region. This research study examines the prevalence of fuel theft within the Afghanistan reconstruction program, with a specific focus on cases involving U.S. military members. By analyzing these cases through the lens of the COSO Internal Control Integrated Framework (hereafter referred to as the COSO Framework), this research aims to identify the primary and secondary control failures that allowed fraud to persist. The findings of this research highlight the importance of robust internal controls and oversight mechanisms to help prevent future mismanagement in complex operational environments.

This chapter provides an overview of the foundational aspects of this study. The Background section provides historical factors influencing this study. The Purpose of Research section provides insight into the reason behind this study, followed by the research questions this study will answer. The Methodology section explains the steps taken in this research and the way in which the research questions are answered. This chapter also highlights the importance of this research and limitations to the research conducted in this study. This chapter concludes with a Summary section. The next section addresses the background of aid issues in Afghanistan.

A. BACKGROUND

The influx of international aid to Afghanistan since 2001, particularly from the United States and its allies, has been substantial and aimed at supporting reconstruction and development in the post-Taliban era. Despite the United States investing over $2.261 trillion from 2001–2021 in various sectors ranging from security to infrastructure, pervasive issues of financial mismanagement and corruption continuously undermined these efforts (Crawford & Lutz, 2021). Numerous fuel theft cases illustrate the deep-

rooted challenges in managing these funds effectively (Special Inspector General for Afghanistan Reconstruction [SIGAR], 2014). These incidents underscore a systematic problem that extends far beyond single events, affecting numerous reconstruction projects funded by international aid, particularly from the United States. In 2012, 20 U.S. service members were convicted of participating in fraud schemes in Afghanistan reconstruction efforts (Harte, 2015). The volume and frequency of these cases highlights the need to identify internal control weaknesses over financial management within conflict areas, such as Afghanistan.

Due to the problems addressed previously, the United States and its international partners employed a variety of strategies for detecting and deterring financial mismanagement and corruption in Afghanistan. Key institutions such as SIGAR and the Department of Defense Office of Inspector General (DoD OIG) monitored and audited the allocation and use of funds while also participating in joint efforts with multi-agency task forces specifically targeting corruption in aid projects (SIGAR, 2009). The U.S. Agency for International Development (USAID) had its Office of Inspector General (OIG) conduct rigorous audits and investigations into the use of aid dollars (OIG, n.d.). These measures were critical for ensuring that funds and resources meant for development and reconstruction were not siphoned off through corrupt practices. Stringent auditing standards and investigative procedures were applied consistently to maintain integrity and accountability in financial management.

SIGAR was established in 2008 "to provide independent and objective oversight of Afghanistan reconstruction projects and activities" (SIGAR, n.d., para. 1). Headquartered in Arlington, VA, SIGAR also had multiple field locations throughout Afghanistan and a second office in Kabul, Afghanistan (SIGAR, n.d.). Quarterly reports given by SIGAR to Congress highlighted all audits and investigations that SIGAR was currently working on (SIGAR, n.d.). SIGAR produced hundreds of reports on fraud, corruption, waste, and abuse in Afghanistan. These reports were released following a lawsuit brought by *The Washington Post* citing the Freedom of Information Act (Whitlock et al., 2019). SIGAR repeatedly highlighted deficiencies in how funds were managed and monitored and identified multiple fraud incidents that impacted the United States' efforts to aid Afghanistan (Whitlock et al., 2019). The complexity and urgency of

the Afghanistan reconstruction effort often outpaced the establishment of effective financial controls, leading to financial losses.

Given the critical need to safeguard these investments, understanding the intricacies of financial mismanagement in such a challenging context is vital to ensure proper use of government funds. This research aims to examine failures of internal control systems related to fuel incidents that allowed losses to occur. By applying the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Integrated Framework (COSO, 2013), this study seeks to identify key vulnerabilities and provide recommendations to strengthen financial oversight of fuel in conflict areas. This research aims to provide recommendations to enhance accountability and efficiency in international aid use and to provide valuable insights.

B. PURPOSE OF RESEARCH

The purpose of this research is to examine fuel fraud incidents involving U.S. officials and military personnel in Afghanistan from 2001–2021 through the lens of the COSO Framework. This research aims to identify the mechanisms used in fuel fraud and provide recommendations for strengthening internal controls and oversight procedures to mitigate corruption in future reconstruction efforts. The findings of this research study may inform military leadership on fraud-conducive conditions and offer recommendations for enhancing internal controls and deterring fraud.

C. RESEARCH QUESTIONS

This research answers the following questions:

1. Which internal controls were most frequently bypassed or compromised in cases of fuel theft and/or fraud in Afghanistan?
2. Which COSO internal control components had the most fuel control failures?
3. What were the primary methods used in fuel theft and/or fraud activities?

D. METHODOLOGY

This research reviews publicly available court documents of fuel theft/fraud in Afghanistan to identify patterns of internal control failures by analyzing cases through the

lens of the COSO Framework. The type of financial mismanagement or fuel fraud and the corresponding weaknesses in the internal control system that allowed for these failures to occur are systematically examined to better understand the underlying issues. This methodology involves compiling the incidents of fuel theft cases into an Excel database to identify fuel control failures and their alignment to internal control components. The research in this study was reviewed by the Institutional Review Board and the conclusion was reached that it was not human subject research.

E. IMPORTANCE OF RESEARCH

An analysis of fuel fraud cases may identify any potential weaknesses in internal control frameworks when funds are allocated to a conflict area, which will inform military leadership on fraud-conducive conditions. By focusing on fuel cases specifically, this research aims to uncover how and why internal controls failed, leading to significant losses. The significance of this research lies in the possibility that identifying trends in internal control failures, along with recommendations based on the research study findings, may assist both policy-makers and government officials in enhancing measures to prevent financial mismanagement in conflict areas.

F. LIMITATIONS OF RESEARCH

This study has two primary limitations that may affect the comprehensiveness and generalizability of the findings. The first limitation is the scope of the cases examined. The cases of fuel theft/fraud analyzed in this study do not encompass all instances of fuel theft/fraud that occurred in Afghanistan during U.S. military operations there. The cases reviewed are those that have been documented in publicly available government reports, audits, and legal proceedings. However, many cases of fraud may remain unreported, undetected, or classified, especially given the complex and often unclear nature of military operations in conflict areas. Additionally, some prosecutions may have occurred without publicly accessible outcomes, leaving gaps in the dataset. As a result, the analysis may not capture the full extent of fuel fraud, potentially limiting the broader applicability of the findings. While the cases selected are representative of key fuel fraud incidents,

they may not reflect the entirety of fraudulent activities, and the patterns identified may be incomplete.

The second limitation is the subjectivity involved in identifying specific internal control failures for the fuel incidents. The alignment of the fuel control failures to the COSO internal control components are inherently interpretive. Although the study relies on established evidence in the form of court documents, the application of the COSO Framework to each case requires judgment. This subjectivity arises from the complexity of the fuel fraud cases and the often-ambiguous nature of the internal controls in place at the time. Multiple factors may contribute to a single fraud incident, and it can be challenging to isolate the failure of one specific control from broader systemic issues. Furthermore, the available documentation may not always provide explicit evidence of control failures, requiring inferences to be made based on the circumstances of the fraud. This interpretative nature introduces an element of bias, which may affect the consistency of internal control component identification across cases.

G. ORGANIZATION OF REPORT

The organization of this research paper begins with Chapter I, which introduces this study by providing a brief background, the purpose of research, the research questions, and methodology. Chapter II is an in-depth literature review starting with three academic theories: the Fraud theory, Auditability theory, and the COSO Framework theory. The Fraud theory section covers the theory's elements and the evolution of the Fraud Diamond from the Fraud Triangle. The section on Auditability theory addresses its history and components. The COSO Framework section of the literature review addresses the components, creation and evolution, government application, and limitations of internal controls. The literature review also examines government agencies, reports, audits, and investigations, which provide an in-depth look at the funding and fuel oversight issues during the United States' 2 decades in Afghanistan. Chapter III addresses the methodology utilized throughout this study and describes the creation of the database used to track internal control failures in the fuel cases researched.

Chapter IV presents the findings of the research, identifying specific COSO internal control failures in the documented cases of fuel fraud involving U.S. military

members. This chapter includes an analysis of how these control failures facilitated fraudulent activities and highlights common patterns across the cases. It also discusses the implications of these failures for future fraud prevention and control measures within military operations. It offers recommendations for strengthening the COSO Framework's application in military operations to prevent future fuel fraud. Chapter V concludes the research by summarizing the key findings and their implications for improving internal controls within the U.S. military. The chapter also provides suggestions for areas of further research, particularly in examining internal control failures in other high-risk areas of military logistics and procurement.

H. SUMMARY

This chapter provided an introduction and background to fuel fraud involving U.S. military personnel in Afghanistan, internal controls, and the COSO Framework. It explained the rationale for analyzing fuel fraud cases through the lens of the COSO Framework to identify internal control failures and to propose improvements to prevent future fuel fraud incidents. Additionally, this chapter outlined the research questions guiding this study, described the methodology for creating a database of fuel fraud cases, and discussed the significance and limitations of the research. Lastly, it provided an overview of the structure of the thesis. The following chapter presents a literature review that covers the evolution of academic theories of auditability, fraud, and internal controls as well as information on agencies and reports responsible for oversight and management of U.S.-funded Afghanistan reconstruction.

II. LITERATURE REVIEW

A. INTRODUCTION

The purpose of this chapter is to discuss the academic frameworks of the Fraud theory, the Auditability theory, and the COSO Framework theory. In addition to these theoretical models, this chapter also provides an examination of government documents and government agencies that were instrumental to the Afghanistan reconstruction. These documents and agency reports also shed light on the pervasiveness of fraud and failure of internal controls, both of which undermined the effectiveness of the Afghanistan reconstruction.

B. FRAUD THEORY

This section of the literature review includes an exploration of the development of the Fraud Diamond from the original Fraud Triangle. The Fraud Diamond emphasizes the addition of a fourth element, capability, to the original three: pressure, opportunity, and rationalization. This section also provides an assessment of how this framework enhances fraud detection and prevention, its key elements, and its relevance in both detecting and preventing fraud.

1. Background on the Fraud Diamond

The Fraud Diamond theory, introduced by David T. Wolfe and Dana R. Hermanson (2004) in the journal article, "The Fraud Diamond: Considering the Four Elements of Fraud" expands on the well-known Fraud Triangle by incorporating a fourth element of capability. This advancement was built on the foundational work of Donald R. Cressey in his 1953 book, *Other People's Money: A Study in the Social Psychology of Embezzlement* (Machado & Gartner, 2018), which laid the groundwork for his theoretical framework on fraud now known as the Fraud Triangle. Cressey's research included a study of 200 inmates in prison for white collar crimes and the reasons behind their criminal actions (Cressey, 1953, as cited in Machado & Gartner, 2018). This research led him to revise his thesis multiple times and ultimately outline the three elements as opportunity, pressure, and rationalization (Cressey, 1953, as cited in Machado & Gartner,

2018). All three elements, which are shown in Figure 1, present the ideal conditions for fraud to occur, according to Cressey (Cressey, 1953, as cited in Machado & Gartner, 2018). Cressey's research on fraud laid the foundation for understanding the elements behind why people commit fraud and provided a roadmap for companies to better protect themselves from fraud.

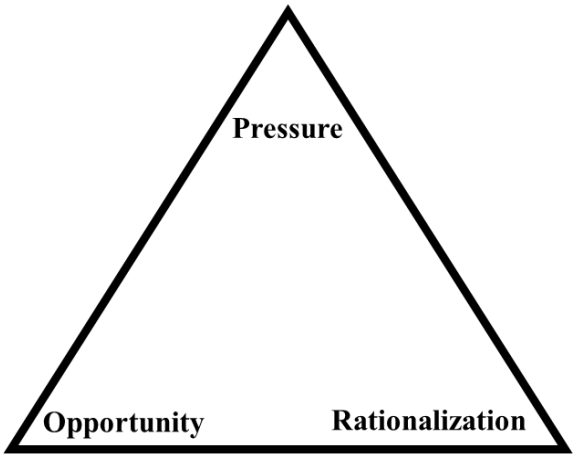

Figure 1. Fraud Triangle. Adapted from Machado and Gartner (2018).

Wolfe and Hermanson (2004) determined that there was a missing element, capability, which they argued was crucial to understanding why people commit fraud. By adding capability to the existing Fraud Triangle elements of pressure, opportunity, and rationalization, the Fraud Diamond provides a more well-rounded perspective on the conditions that can lead to fraudulent behavior. Wolfe and Hermanson (2004) determined that these four elements provide "a different way to think about fraud risks" (p. 38). This section provides an examination of the key components of the Fraud Diamond and details of its effectiveness in fraud detection and prevention.

2. Elements of the Fraud Diamond

The Fraud Diamond has been used as an analysis tool in a wide range of industries since it was introduced in 2004 in a publication of *The CPA Journal* (Hermanson & Wolfe, 2024). The four elements of the Fraud Diamond theory, which are shown in Figure 2, are pressure or incentive, which is the motivation behind committing fraud; opportunity, which is the circumstances that allow fraud to occur; rationalization, which involves the mindset that justifies fraudulent behavior; and capability, which is the

individual's traits and abilities that enable them to commit fraud (Wolfe & Hermanson, 2004, pp. 38–39).

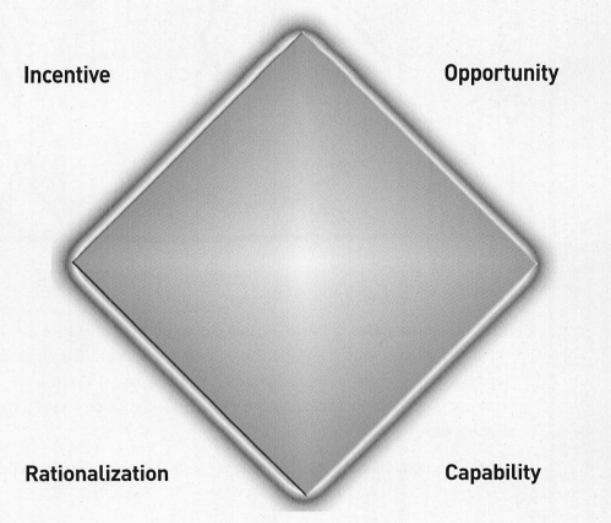

Figure 2. Fraud Diamond. Source: Wolfe and Hermanson (2004).

a. Pressure/Incentive/Motive

Wolfe and Hermanson (2004) emphasized that pressures can arise from either "I want to, or have a need to, commit fraud" (p. 39). This element considers both external and internal pressures, incentives, or motives that might compel someone to participate in fraudulent actions. For example, an employee facing personal financial crises may feel pressured to steal funds to cover overwhelming personal debts or an expensive medical bill. Also, corporate pressure at all levels can create unrealistic targets, leading individuals to commit fraud to meet these expectations (Accounting Insights, 2024). Understanding the various forms of pressures, incentives, or motives is crucial for organizations aiming to identify and mitigate potential fraud risks.

b. Opportunity

Weak internal controls, lack of oversight, and poor governance create environments where fraudulent activities can thrive. Wolfe and Hermanson (2004) argued that "fraud is possible" if "there is a weakness in the system that the right person could exploit" (p. 39). Without opportunities to commit fraud, even individuals under significant pressure are unlikely to do so because no opportunity means there is a lack of weaknesses in the system to exploit. Effective internal controls, such as segregation of

duties, regular audits, and appropriate amounts of oversight, are essential in reducing opportunities for fraud (Accounting Insights, 2024). Strong internal controls significantly decrease the likelihood of fraudulent activities by closing gaps that people could manipulate.

c. Rationalization

Perpetrators often convince themselves that their actions are justified, necessary, harmless or for the greater good. According to Wolfe and Hermanson (2004) rationalization means, "I have convinced myself that this fraudulent behavior is worth the risks" (p. 39). This element addresses the cognitive processes that enable individuals to overcome ethical boundaries and engage in fraud. Common rationalizations include beliefs that the act is temporary, the benefits outweigh the risks, it is for the greater good, or that the organization can afford the loss. Due to the many reasons that people can create to rationalize or justify fraud, companies must place emphasis on developing trainings and environments that foster moral behavior (Accounting Insights, 2024).

d. Capability

The addition of capability as the fourth element distinguishes the Fraud Diamond from the Fraud Triangle (Wolfe & Hermanson, 2004). Wolfe and Hermanson (2004) argued that without the necessary skills and confidence, even motivated individuals with opportunities and rationalizations may not commit fraud. This element underscores the importance of considering a person's competence and access to exploit vulnerabilities. For instance, according to Wolfe and Hermanson (2004), a high-level executive with extensive insight into the company's financial systems and access to critical information poses a greater risk of committing complex fraud schemes than a lower-level employee does. Assessing capability involves evaluating employees' roles, access levels, and technical skills, which can help in identifying potential fraud risks within the organization (Wolfe & Hermanson, 2004).

Wolfe and Hermanson (2004) also highlight the importance of personality traits when considering an individual's capability to commit fraud. They determine that there are six specific markers that should be watched for when considering people's capability

(Wolfe & Hermanson, 2004). The first marker is "the person's function within the organization" (Wolfe & Hermanson, 2004, p. 39). The higher or more specialized someone's position is in a company, the more unique position they are in to exploit weaknesses in the system. The second marker of an individual capable of fraud is, "the right person for a fraud is smart enough to understand and exploit internal control weaknesses and to use position, function, or authorized access" (Wolfe & Hermanson, 2004, p. 40). This means that people in those positions to commit fraud have the intelligence to understand their unique positions and exploit it for their personal benefit. The third marker is that the individual "has a strong ego and great confidence that he will not be detected, or the person believes he could easily talk himself out of trouble if caught" (Wolfe & Hermanson, 2004, p. 40). This highlights that people in these unique positions are often overly confident in their own abilities and underestimate the intelligence of those in charge of watching for discrepancies. The fourth marker identified is that "a successful fraudster can coerce others to commit or conceal fraud" (Wolfe & Hermanson, 2004, p. 40). This demonstrates the fact that these people are convincing enough that they not only commit fraud themselves but can get other people on board with their fraudulent activities. The fifth marker of someone capable of fraud is, "a successful fraudster lies effectively and consistently" (Wolfe & Hermanson, 2004, p. 40). This means that fraud does not involve someone who can stomach lying a single time; these people must lie continuously to cover their tracks and remain undetected. Stress is a part of many different job fields; therefore, the sixth and final marker is that "a successful fraudster deals very well with stress" (Wolfe & Hermanson, 2004, p. 40). The type of stress the sixth marker is addressing is the additional high-level stress that comes with defrauding people on a constant and daily basis. The six markers identified by Wolfe and Hermanson are shown in Figure 3 as the components of capability.

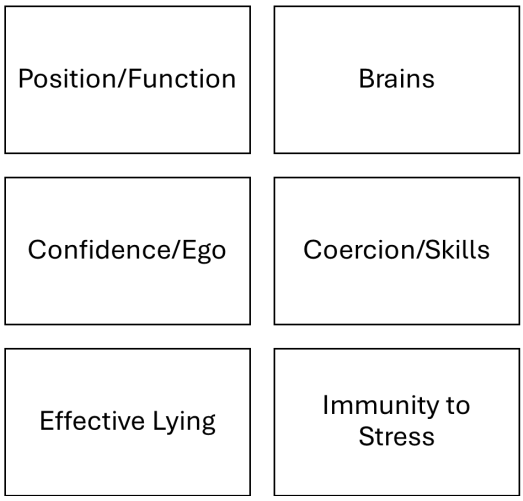

Figure 3. Components of Capability. Adapted from Wolfe and Hermanson (2004).

This section addressed the Fraud theory, highlighting its significance in understanding and preventing fraudulent activities within organizations. The four elements, pressure, opportunity, rationalization, and capability, provide a robust framework for organizations to assess and mitigate fraud risks. The next section addresses Auditability theory and the components of the Auditability Triangle.

C. AUDITABILITY THEORY

This section highlights the development of Auditability theory, which emphasizes the importance of creating systems and processes that allow for transparent and reliable accounting. This section also includes an assessment of how this theory enhances oversight and control by making entities more auditable.

1. Background on Auditability Theory

Micheal Power, in his 1996 journal article "Making Things Auditable," challenges the traditional view that auditing is a passive process of merely verifying pre-existing data. Instead, Power introduces the notion that auditing is an active process that involves the creation and shaping of environments to make them auditable. He states that an "audit is an active process of 'making things auditable,'" highlighting that auditability is not an inherent characteristic of financial data but a constructed one (Power, 1996, p. 289). Power's argument centers on the idea that auditing does not simply assess a static reality but participates in the creation of that reality. He asserts that in many cases,

"accounts and audits get co-produced," meaning that financial reports and the audits themselves are both shaped through the auditing process by one another (Power, 1996, p. 290). This co-production challenges the conventional belief in the independence of financial reporting and auditing, suggesting instead that the two are interdependent and evolve together.

The process of making something auditable, as Power (1996) continues to explain, involves "two components: the negotiation of a legitimate and institutionally acceptable knowledge base" and "the creation of environments which are receptive to this knowledge base" (p. 289). The knowledge base Power is addressing is the foundational base upon which audits are conducted. That foundational base is built because of discussions, compromises, and agreements among various stakeholders throughout the industry (Power, 1996, p. 305). The creation of environments involves designing and implementing systems, controls, and practices within organizations that can generate the data and evidence required by auditors to perform their assessments. Changes in a sector are necessary to ensure accountability as well as to create a clear and auditable trail that could satisfy the requirements of external auditors (Power, 1996). An internal control system is essential for establishing a strong environment, where internal controls can be clearly followed by employees and effectively audited by auditors.

This notion is further expanded by Weigand et al. in their 2013 article "Conceptualizing Auditability," in which they introduce a structured approach to auditability. They define auditability as a complex concept involving not only the verification of accounting data but also the creation of a verifiable, robust framework within the data (Weigand et al., 2013). They state that "the task of the auditing service (Auditor) is to give independent assurance that these statements are reliable" and that the organization's management has "delegated a certain level of control over the value object" to further support the assurance provided by the auditor (Weigand et al., 2013, p. 3).

Weigand et. al (2013) also built on Power's (1996) ideas regarding internal controls by offering a detailed breakdown of the levels of auditability, illustrating how internal control systems and IT infrastructure play crucial roles in creating environments

that are conducive to effective auditing (Weigand et al., 2013). The four main auditability levels, illustrated in Figure 4, show how the audit focus shifts with the different types of control infrastructure present (Weigand et al., 2013). They describe a four-level auditability framework, which ranges from "transaction-based" auditing to "governance-based" auditing, where the focus shifts from "operational process" to "management process" (Weigand et al., 2013, p. 5). This framework emphasizes that "moving to a higher level [of auditability] is assumed to be incremental" and that each level requires a more sophisticated integration of controls and transparency (Weigand et al., 2013, p. 5).

	AUDIT FOCUS	INFRASTRUCTURE	AUDIT TYPE	PRIMARY STATEMENT
1	operational process	physical environment, possibly IT-based	transaction-based	self-report
2	accounts	(a) tracing infrastructure (b) accounting information system	system-based	self-report
3	operational policy	(a) policy (GRC) information system (b) enforcement infrastructure	risk-based	accounting information system
4	management process	Management Information System	governance-based	accounting information system

Figure 4. Auditability Levels. Source: Weigand et al. (2013).

Weigand et al. (2013) assert that achieving higher levels of auditability not only increases audit effectiveness but also enhances the organization's capability to decrease risk and improve overall governance. They argue that increasing controls are a benefit because "at each auditability level, the organization becomes more transparent," which aligns with Power's (1996) claim that the creation of auditable environments involves significant improvements of internal controls (Weigand et al., 2013, p. 7). Achieving auditability requires an organization to establish and maintain appropriate controls. These controls are essential for ensuring that the auditing process can be carried out effectively.

Rendon and Rendon (2015) build on the theory of auditability in their article "Auditability in Public Procurement: An Analysis of Internal Controls and Fraud Vulnerability," by emphasizing the critical role of internal controls in fostering an environment in which effective audits can be conducted. As they state, "transformation occurs when organizations establish data collection practices and systems of documentation to make them auditable" (Rendon & Rendon, 2015, p. 713). The focus

should not be solely on the act of auditing but on the preparatory work that makes an organization auditable. Creating systems and processes that support auditability requires more than just policy adjustments; it necessitates substantial organizational changes. According to Rendon and Rendon (2015), this process begins with the organization's structure: "Auditability also reflects an organization's governance structure and that structure's management of procurement activities" (p. 713). Therefore, organizations must integrate auditability into their daily operations, ensuring that their practices are transparent and can withstand external scrutiny. Furthermore, they emphasize that enhancing internal controls is a critical component of this transformation. They explain that "this includes implementing an internal control management program overseeing internal control policies to ensure compliance with laws and regulations" (Rendon & Rendon, 2015, p. 724). Rendon and Rendon (2015) continue to explain that these steps can significantly improve an organization's ability to deter and detect fraudulent activities. This general approach to auditability confirms the organization is prepared to manage risks and prevent fraud successfully (Rendon & Rendon, 2015).

Rendon and Rendon (2015) further explain that the improvement of an organization's internal controls, personnel, and processes results in a more auditable organization, which is more likely to detect and deter fraudulent activities. Their theory emphasizes the link between internal controls and auditability: "organizations need to emphasize auditability in its [their] operations, and specifically, in its [their] internal controls" (Rendon & Rendon, 2015, p. 718). The connection between auditability and internal controls is shown in Figure 5, which depicts their conceptual framework, known as the Auditability Triangle, of the three elements of auditability theory: internal controls, personnel, and processes (Rendon & Rendon, 2015).

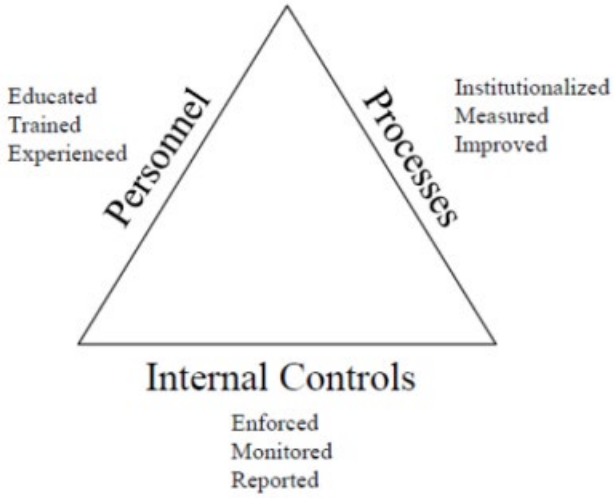

Figure 5. Auditability Triangle. Source: Rendon and Rendon (2015).

2. Auditability Triangle Components

This section of the literature review introduces the components of the Auditability triangle. It identifies and defines each component and explains its importance to effective audit practices. The next section addresses competent personnel and the role that personnel play in the success of a company's auditability.

a. Competent Personnel

The first component of the Auditability Triangle, competent personnel, refers to personnel who are adequately trained and have appropriate experience in their area of responsibility (Rendon & Rendon, 2015). Rendon and Rendon (2015) emphasize that "the organisation's contracting officers should be knowledgeable of internal controls" because without that knowledge, the internal controls are ineffective (p. 718). Competent personnel are necessary at all levels of an organization because fraud can occur at any stage throughout the process. Without component personnel, processes cannot be properly followed, and internal controls will not be enforced, thereby defeating the purpose of the other two components. Therefore, ensuring that the personnel within an organization have a clear and strong understanding of processes and internal controls is crucial to increasing auditability and decreasing fraudulent activities (Rendon & Rendon, 2015).

b. Capable Processes

The second component, capable processes, refers to the organization's ability to perform procurement-related activities effectively (Rendon & Rendon, 2015). Processes deemed capable are those "that are fully established, institutionalized, mandated, integrated with other organizational processes, periodically measured, and continuously improved" (Rendon & Rendon, 2015, p. 716). The capability of these processes is critical because without capable processes, there is no ability to ensure transparency within reporting and recording activities. Processes must be constantly proven capable because assessments and developments will require adaptation of those processes, which may affect their capability (Rendon & Rendon, 2015).

c. Effective Internal Controls

The third component of the Auditability Triangle is effective internal controls, which is the backbone of ensuring that an organization's activities conform to legal and regulatory requirements. According to Rendon and Rendon (2015), enforcing internal controls is meant to guarantee "compliance with laws and regulations, monitoring procedures to assess enforcement, and reporting material weaknesses" (p. 716). These controls are structured around the five components established by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (Rendon & Rendon, 2015). The COSO Framework, particularly its 2013 update, outlines 17 principles associated with these five components, offering a comprehensive guide to establishing effective internal controls within an organization (Rendon & Rendon, 2015). By adhering to these principles, organizations can mitigate risks, prevent fraud, and ensure that their processes are both transparent and accountable.

This section addressed the development of auditability theory and the creation of the Auditability Triangle and its three components: competent personnel, capable people, and effective internal controls. Auditability theory underscores the importance of creating an environment in which audits can be effectively conducted. As organizations continue to evolve, the principles of Auditability theory provide a critical framework for maintaining integrity and promoting effective and sensible utilization of organizational

resources. The next section provides a detailed background of internal controls, the five components of internal controls, and the 17 associated principles.

D. INTERNAL CONTROLS FRAMEWORK

This section introduces the COSO Framework, a widely accepted model for an organization creating effective internal controls. It also presents an examination of the framework's key components and the way in which those components strengthen overall internal control systems.

1. Background on Internal Controls Framework

The origins of the COSO Framework trace back to the mid-20th century, when the American Institute of Certified Public Accountants (AICPA) provided the first formal definitions of internal controls (Moeller, 2013). This first set of standards described by the AICPA, "called the Statement of Auditing Standards (SAS No. 1) defined the practice of financial statement external auditing in the United States for many years" and was primarily focused on safeguarding assets and ensuring accuracy and reliability of financial records (Moeller, 2013, p. 5). However, this first set of standards lacked a comprehensive and consistent approach to internal controls across different industries and sectors (Moeller, 2013). There were multiple changes and updates to the AICPA's first definitions of internal controls over the following years. In the 1970s, the United States experienced "an unusually large number of corporate accounting fraud and internal control corporate failures," which culminated in the enactment of the Foreign Corrupt Practices Act (FCPA) of 1977 (Moeller, 2013, p. 6). The FCPA introduced stringent requirements for companies to ensure accurate documentation of company financial documents as well as the implementation of strong and reliable internal controls. Although the FCPA was a significant step forward, it still did not provide a clear and universally accepted definition of internal controls, leaving companies and auditors without a standardized framework with which to guide efforts.

The lack of clarity and consistency in the definition and application of internal controls led to the formation of COSO, which sponsored the creation of the National Commission on Fraudulent Financial Reporting in 1985 (Division of Financial Services,

n.d.). Eventually known as the Treadway Commission, the commission's primary objectives were to identify the root causes of falsified monetary reporting and develop suggestions for improving the reliability of financial reports (Moeller, 2013). The Treadway Commission's final report emphasized the importance of a strong internal control environment and called for management to take greater accountability for the efficiency of their organization's internal controls (Moeller, 2013). In response to these recommendations, COSO started to develop a framework for internal controls (Moeller, 2013).

The COSO Framework, first published in 1992 and officially known as the *Internal Control–Integrated Framework*, was developed in response to a growing recognition of the importance of robust internal controls within organizations (COSO, 2023). The framework provided a comprehensive model for designing, implementing, and evaluating internal control systems within organizations. The framework introduced five key components of internal controls: control environment, risk assessment, control activities, information and communication, and monitoring (Moeller, 2013). In 2013, COSO released an updated version of the framework due to changing "business and operating environments" (Dickins & Fay, 2017, p. 119). The updated framework, shown in Figure 6, retained the original five components but added 17 principles to provide greater clarity and guidance for implementing effective internal controls in a modern business context (Dickins & Fay, 2017).

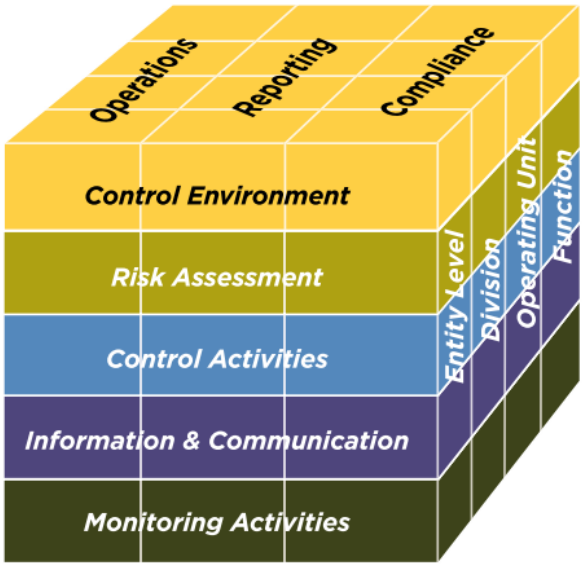

Figure 6. COSO Framework. Source: COSO (2013).

2. COSO Internal Controls Components

This section identifies each component of the COSO Framework. It also addresses the importance of the components by providing definitions and the impact each component has on the overall framework success and failure. The next section begins the in-depth look at these components with the control environment.

a. Control Environment

The first component, control environment, forms the foundation of the COSO Framework, setting the tone for how internal controls are perceived and implemented throughout an organization. According to COSO (2013), "The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization" (p. 3). As the basis for all other internal control components, control environment provides authority and structure which is essential for achieving an organization's objectives (Government Accountability Office [GAO], 2014, p. 21). Often referred to as the "tone at the top," this component emphasizes the critical role of senior management and the board of directors in establishing and promoting a culture of integrity, ethical values, and accountability (COSO, 2013, p. 3). Leadership's commitment to these values influences the overall control environment and is reflected in the entity's guidelines, procedures, and practices (COSO, 2013). This component also

directly influences the organization's approach to hiring, training, and retaining competent individuals who align with the entity's values and objectives (GAO, 2014). By promoting a culture of competence, the control environment ensures that employees are not only capable but also motivated to uphold the organization's ethical standards.

b. Risk Assessment

The second component, risk assessment, is a "dynamic and iterative process" within the COSO Framework, essential for identifying, analyzing, and managing risks that could impede the achievement of an organization's objectives (COSO, 2013, p. 4). COSO (2013) defines risk assessment as determining "the possibility that an event will occur and adversely affect the achievement of objectives" (p. 4). Therefore, this component emphasizes the need for organizations to establish clear objectives, which serves as the foundation for identifying and assessing risks. It also requires organizations to consider both internal and external factors related to risk (GAO, 2014). This process includes the identification of risks, the analysis of their potential impact, and the determination of appropriate responses (GAO, 2014). One critical aspect of risk assessment is the consideration of fraud risk (COSO, 2013). Organizations must evaluate where and how fraud might occur and implement controls to mitigate these risks (GAO, 2014). This process must be responsive to changes in the external environment and internal business processes (COSO, 2013). Risk assessment ensures that the organization remains agile and capable of managing new risks as they arise.

c. Control Activities

The third component of the COSO Framework is control activities. Control activities are the measures implemented to reduce risks identified during the risk assessment process. COSO (2013) defines control activities as "the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out" (p. 4). These activities are an integral part of the COSO Framework, ensuring that management's directives to address risks are implemented effectively (COSO, 2013). Control activities exist across all tiers within an entity and include a variety of protocols and processes designed to prevent or

detect errors, fraud, and other risks that could impact the organization's objectives (COSO, 2013). A vital aspect of the control activities component is segregation of duties across an organization (COSO, 2013). Control activities can be both preventive and detective, encompassing various types of actions such as authorizations, verifications, reconciliations, and performance reviews (GAO, 2014). The specific risks and objectives of the organization determine the design and implementation of these activities.

d. Information and Communication

The fourth component of the COSO Framework, information and communication, is critical to the effective operation of all internal control components within the COSO Framework (COSO, 2013). COSO (2013) emphasizes the importance of information by stating, "Information is necessary for the entity to carry out internal control responsibilities to support the achievement of its objectives" (p. 5). This component guarantees that essential information is recognized, collected, and shared in an appropriate manner and timeline facilitating individuals to perform their responsibilities effectively (COSO, 2013). The quality of information, as well as its relevance and reliability, are essential for making informed decisions that support the organizational objectives.

The COSO Framework highlights the importance of the dual role of communication by outlining the expectations for both internal and external communication within an organization (COSO, 2013). Internal communication within an organization is vital for ensuring that information flows freely and effectively between different levels and functions (COSO, 2013). This communication includes not only the dissemination of information from top management to employees but also the upward communication of information, such as reports on the effectiveness of internal controls. External communication is equally important, as it involves sharing relevant information with external parties (COSO, 2013). Another aspect of external communication is the accounting systems used within an organization to ensure the financial reporting that an organization produces about itself is accurate and reliable (COSO, 2013). Clear information and communication fosters transparency and trust with those who rely on the

organization's internal control system to ensure the accuracy and reliability of information (COSO, 2013).

e. Monitoring Activities

The fifth and final component of the COSO Framework, monitoring activities, is accountable for assessing the effectiveness of the internal control system over a period of time (COSO, 2013). This component involves the continuous or periodic evaluation of the five components of internal control to ensure that they are "present and functioning" as intended (COSO, 2013, p. 5). Monitoring is integrated into daily operations or includes separate evaluations conducted periodically. The results found from the monitoring activities must be communicated thoroughly and efficiently to the proper channels. Those findings are then evaluated against standard regulations, and management makes decisions based on those regulations (COSO, 2013). Effective monitoring activities help organizations identify deficiencies within their internal control systems so that they can take actions to correct those deficiencies before the issues get worse.

3. GAO Green Book

In 1983, the GAO published the original "Green Book," which is officially known as the *Standards for Internal Control in the Federal Government* (Yellowbook-CPE, 2021). The GAO adopted the COSO Framework (GAO, 2014). The Green Book provides federal employees with detailed information regarding the COSO Framework components: control environment, risk assessment, control activities, information and communication, and monitoring (GAO, 2014). Following an update of the COSO internal controls model in 2013, the GAO published an updated version of the Green Book in September 2014 (Yellowbook-CPE, 2021). The updated Green Book maintains detailed information regarding COSO internal control components and aligns the framework components with 17 principles, as shown in Figure 7. GAO has published another revision of the Green Book and has the 2024 Exposure Draft posted on its website (GAO, 2024).

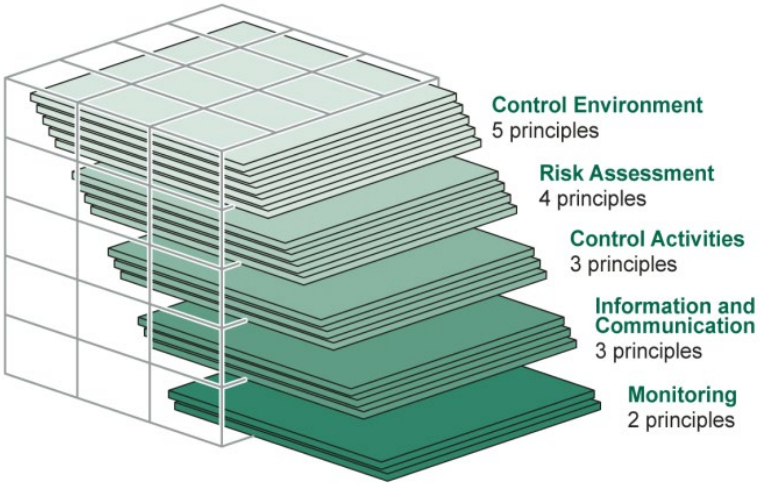

Figure 7. COSO Principles. Source: GAO (2014).

The 17 principles provide detailed guidance on the implementation and operation of an internal control system. They also provide information regarding reporting and documentation requirements (GAO, 2014). These 17 principles, combined with the internal control components, provide comprehensive guidance for federal agencies to achieve their organizational objectives while complying with laws and regulations (GAO, 2014).

4. Office of Management and Budget Circular A-123

The Office of Management and Budget (OMB) Circular No. A-123 defines the responsibilities of federal agencies in implementing enterprise risk management (ERM) and internal controls to improve accountability, effectiveness, and efficiency in government operations (Executive Office of the President, 2016). The circular emphasizes the integration of ERM practices with internal control processes, providing federal managers with a framework to identify, assess, and manage risks that could hinder the achievement of their strategic objectives (Executive Office of the President, 2016). According to the circular, "Each Federal employee is responsible for safeguarding Federal assets and the efficient delivery of services to the public" (Executive Office of the President, 2016, p. 2). This statement underscores the collective responsibility within federal agencies to maintain strong internal controls and manage risks proactively.

The circular is structured to guide agencies through several key processes, beginning with the establishment of ERM within management practices. Agencies are

encouraged to develop a Risk Management Council (RMC) to oversee risk management activities and ensure that risks are identified, assessed, and addressed at all levels of the organization (Executive Office of the President, 2016). As the circular states, "ERM provides an enterprise-wide, strategically-aligned portfolio view of organizational challenges" (Executive Office of the President, 2016, p. 10), which helps agencies prioritize resource allocation and enhance mission delivery. A significant aspect of OMB Circular No. A-123 is its alignment with the GAO Green Book (Executive Office of the President, 2016). The circular instructs departments to incorporate internal control activities with their risk management processes, ensuring that controls are designed to provide "reasonable assurance that the objectives of an entity are achieved" (Executive Office of the President, 2016, p. 22). This integration is critical for maintaining compliance with laws and regulations while also addressing risks related to operations, reporting, and compliance.

Furthermore, the circular outlines the necessity for agencies "to continuously monitor, assess and improve the effectiveness of [their] internal controls" (Executive Office of the President, 2016, p. 8). It states that "Agency managers must continuously monitor, assess, and improve the effectiveness of internal control" (Executive Office of the President, 2016, p. 29). This ongoing assessment process is essential for identifying deficiencies and implementing corrective actions to strengthen the internal control environment (Executive Office of the President, 2016). The circular also highlights the importance of transparency in reporting on internal controls, requiring agencies to provide annual assurance statements that include details on any identified material weaknesses and the corrective actions taken to address them (Executive Office of the President, 2016). Overall, OMB Circular No. A-123 serves as a foundational document for federal agencies, providing them with the necessary guidelines to implement effective risk management and internal control systems.

5. Limitations of the Internal Controls

Internal controls, while essential, are not infallible and possess inherent weaknesses. They are designed to provide reasonable assurance in supporting an organization's objectives but cannot guarantee complete assurance (COSO, 2013). The

first limitation within an internal control framework is its dependency on the individuals responsible for overseeing and implementing the controls. As noted in the COSO Framework, "internal control cannot prevent bad judgment or decisions," which underscores that human factors, whether intentional or unintentional, can lead to failures in internal controls (COSO, 2013, p. 9). In his journal article "Controlling Internal Controls," Phillip Candreva (2006) discusses findings from two GAO investigations into the management practices of three federal departments. He emphasizes that the human element is often the most significant vulnerability within internal control systems, stating "The most frequently cited problem was employee training" (Candreva, 2006, p. 465). Candreva's (2006) claim highlights the critical importance of proper training, education, and ongoing monitoring of employees to ensure that internal controls are not only implemented but also effective. Without these measures, the strength of an organization's internal controls can be significantly compromised, leading to potential failures that undermine the organization's objectives.

The second limitation of internal controls is the inadequate monitoring of their implementation and effectiveness. As Candreva (2006) highlights, "Although each department established what appeared to be well-designed internal controls, all lacked sufficient monitoring and assessment of the efficacy of those controls" (p. 465). This deficiency in oversight undermines the assurance that internal control processes are functioning as intended. Without robust monitoring mechanisms, the internal control framework is vulnerable to breakdowns, as there is no reliable verification that the controls are being effectively executed. This gap in monitoring can lead to a compromised system in which potential issues go undetected, ultimately weakening the organization's overall control environment.

The third limitation of internal controls is the vulnerability to management override by individuals with the authority to manipulate them. The American Institute of Certified Public Accountants (AICPA) identifies various reasons that management might choose to override established controls, including "powerful incentives to meet accounting objectives" (AICPA, 2005, p. 2). Whether driven by personal or professional reasons, management override poses a significant risk to the effectiveness of an organization's internal control system. Even a well-designed system can fail if

management circumvents controls to achieve specific outcomes, emphasizing the importance of external oversight and regular audits to mitigate this risk (AICPA, 2005).

6. Importance of Internal Controls

A complete and comprehensive internal control system provides entities with reasonable assurance that the organization's objectives will be achieved in accordance with laws and regulations (COSO, 2013). These controls enhance the organization's ability to adapt to both internal and external changes in the business and operational environments (COSO, 2013). When effectively implemented and maintained, internal controls significantly improve organizational performance (COSO, 2013). They also play a crucial role in mitigating risks, ensuring they are kept within acceptable levels (COSO, 2013). Additionally, internal controls provide critical support for sound decision-making and governance within the organization, while also delivering valuable feedback on how effectively the organization is operating (GAO, 2014).

A comprehensive internal control system provides entities with the necessary assurance that their objectives will be achieved in accordance with established laws and regulations (COSO, 2013). This assurance is particularly significant, as it increases the likelihood that an organization will reach its strategic goals (Executive Office of the President, 2016). Internal controls also strengthen management's confidence in the organization's ability to meet these objectives, offering a reliable foundation for effective decision-making and governance (GAO, 2014). The COSO Framework further underscores the importance of internal controls in supporting sound governance practices, which are essential for aligning organizational actions with long-term objectives (COSO, 2013).

Internal controls are crucial for enhancing an organization's ability to adapt to both internal and external changes in business and operational environments (COSO, 2013). This adaptability is key to sustaining performance, as it allows organizations to respond effectively to emerging challenges and opportunities. When implemented and operated effectively, internal controls contribute significantly to improving organizational performance by ensuring that operations are efficient and aligned with strategic goals (COSO, 2013). Moreover, these controls provide valuable feedback on how effectively

an entity is functioning, enabling continuous improvement and refinement of processes (GAO, 2014). Internal auditors also recognize the importance of the control elements within the COSO Framework, viewing them as critical to "increasing the effectiveness of internal control systems" (Fourie & Ackerman, 2013, p. 510).

Effective internal controls are instrumental in managing and mitigating risks within an organization, ensuring that these risks remain at acceptable levels (COSO, 2013). By reducing the potential for errors and irregularities, internal controls help "reduce risks affecting the achievement of the entity's objectives" (GAO, 2014, p. 19). One of the most significant aspects of internal controls is their role in deterring fraud (Fourie & Ackerman, 2013). A strong internal control system is widely regarded as one of the most effective protections to prevent fraudulent activities, providing a framework of oversight, accountability, and preventive measures (Fourie & Ackerman, 2013). Strong internal controls make it more difficult for individuals to abuse the system for personal gain and easier to detect fraudulent activities when they occur.

Fraud theory, auditability theory, and the COSO Framework are important to understand as they provide the theoretical foundation for this research study related to Afghanistan reconstruction projects and fuel procurement in Afghanistan. The next section introduces important government agencies related to the Afghanistan reconstruction and the oversight of projects in the area.

E. SPECIAL INSPECTOR GENERAL FOR AFGHANISTAN RECONSTRUCTION

Congress established the Special Inspector General for Afghanistan Reconstruction (SIGAR) under Section 1299 of the National Defense Authorization Act for Fiscal Year 2008 (SIGAR, 2009). The purpose of SIGAR is to provide independent and objective oversight of U.S. reconstruction efforts in Afghanistan (SIGAR, 2009). According to SIGAR's (n.d.) website, the organization, headquartered in Arlington, VA, is responsible for billions of dollars that "[have] been appropriated for Afghanistan relief and reconstruction since 2002" (para. 1). SIGAR (2009) was created to focus on auditing, inspecting, and investigating the use of funds to "prevent and detect [instances of] waste, fraud, and abuse" (p. 1). The agency has broad jurisdiction, encompassing all U.S.

agencies and organizations involved in the Afghanistan reconstruction effort (SIGAR, 2009). A successful Freedom of Information Act lawsuit by *The Washington Post* against SIGAR resulted in interviews with senior officials over Afghanistan reconstruction efforts, failures, and successes being released to the public (Whitlock et al., 2019). Those released interviews, along with SIGAR's other reports, have often revealed systemic issues, such as poor planning, inadequate oversight, and rampant corruption. Since its creation, SIGAR (n.d.) has issued many audits, investigative reports, and quarterly reports to Congress that have highlighted oversight issues and resulted in numerous criminal prosecutions. Reporting directly to the secretary of state and secretary of defense, SIGAR (2009) continued to have a critical role in monitoring U.S. involvement in Afghanistan, ensuring the lessons learned from this endeavor are fully documented and addressed. The U.S. has since stopped all reconstruction efforts in Afghanistan following the full withdrawal of U.S. military forces on August 30, 2021 (Zeidan, n.d.). However, SIGAR continues to publish reports on Afghanistan and the lessons learned from U.S. operations in the country (SIGAR, n.d.).

The GAO executed an audit in 2021 of 424 of its unclassified reports to give a summary of internal control issues plaguing the Afghanistan reconstruction efforts (GAO, 2021). These reports have identified critical issues, such as poor planning and management of funds, which have resulted in numerous suggestions for improvement. One aspect of this investigation included an examination of SIGAR's contribution to the improvement of management and oversight of funds in Afghanistan.

The GAO's (2021) investigation revealed that SIGAR's reports have also led to identification of fraud vulnerabilities. According to the GAO (2021), "SIGAR also conducts… forensic reviews of reconstruction funds managed by DoD [Department of Defense], State and USAID to identify anomalies that may indicate fraud" (p. 4). SIGAR's audits covered reviews of entire programs and more detailed reports, which addressed specific aspects of contracting at select locations to identify areas of fraud, waste, and abuse (GAO, 2021). The GAO's investigation highlights SIGAR's comprehensive efforts since 2008, which have resulted in informed recommendations for future reconstruction efforts in Afghanistan and other countries.

This section introduced the SIGAR agency, the purpose and creation of the organization, and some important reports that highlight some of the issues about which the organization produced reports. The next section addresses U.S. funding for Afghanistan and which programs received most of the funding.

F. U.S. FUNDING FOR AFGHANISTAN RECONSTRUCTION

The United States appropriated approximately $2.261 trillion from 2001–2021 on the war, reconstruction efforts, and humanitarian aid in Afghanistan, according to research from the Watson Institute (Crawford & Lutz, 2021). This number includes $530 billion worth of interest charged on money borrowed by the United States for the Afghanistan War (Crawford & Lutz, 2021). The total cost of the war and reconstruction over the 2 decades the United States was in Afghanistan, according to SIGAR, was $145 billion for rebuilding Afghanistan and $837 billion for warfighting costs (SIGAR, 2021c). The SIGAR number does not include costs associated with humanitarian aid projects the U.S. invested in Afghanistan. Appropriations for reconstruction efforts are the focus of the majority of SIGAR (2021c) investigations and are shown in Figure 8 by funding category and year. These funds include training and equipping Afghan security forces, building infrastructure, strengthening credible democratic processes, investing in education, stimulating economic growth, and conducting counternarcotics activities (SIGAR, 2021c).

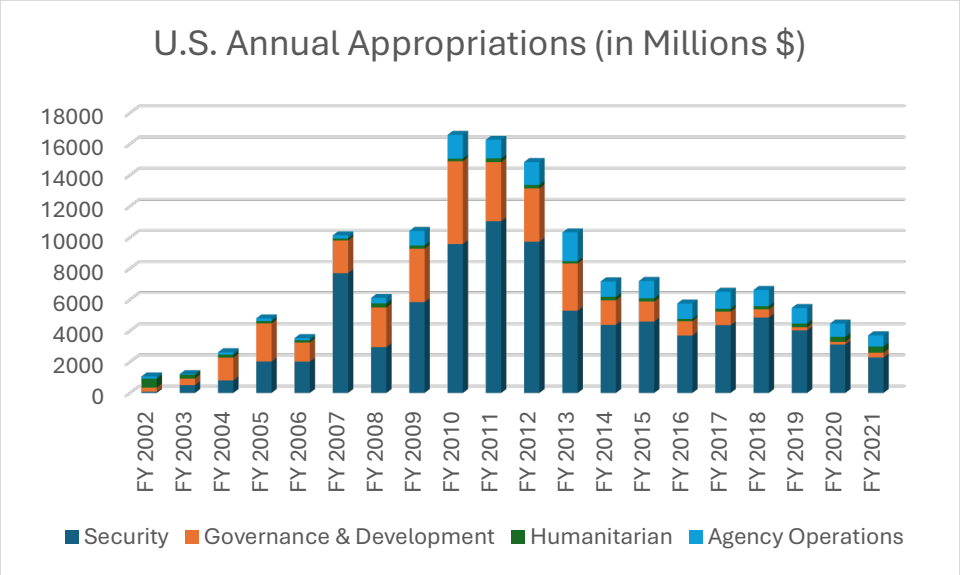

Figure 8. U.S. Annual Appropriations. Adapted from SIGAR (2024).

1. Key Funding Programs

The funding appropriated between 2002–2021 was allocated to a wide array of programs and projects; however, based on data from funding tables provided by SIGAR (2024), 83% of the funding was provided to five programs: the Afghanistan Security Forces Fund (ASFF), Commander's Emergency Response Program (CERP), Economic Support Fund (ESF), International Narcotics Control & Law Enforcement (INCLE), and Diplomatic Programs (DP), specifically the Worldwide Security Protection (WSP) Program. Of the total funding provided, $80,744.25 (66%) was given to ASFF. Figure 9 shows the breakdown of spending for those five highest-funded programs.

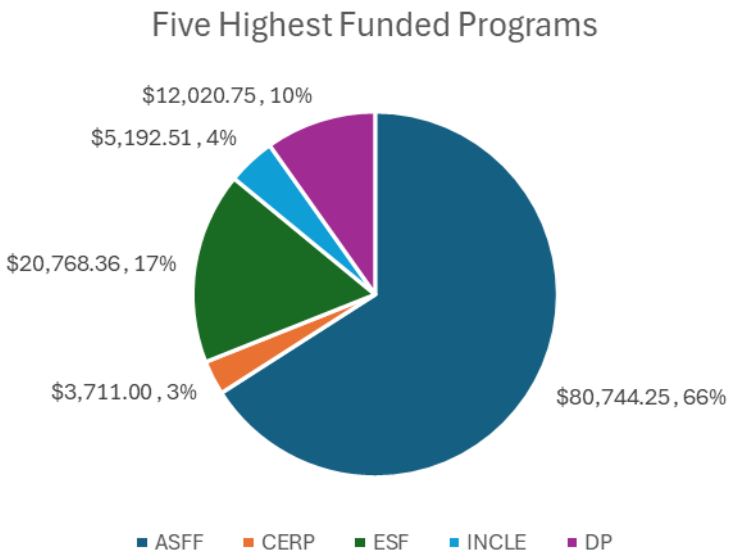

Figure 9. Five Highest Funded Programs. Adapted from SIGAR (2024).

This section provided data and figures that highlight which programs received the highest amount of funding throughout Afghanistan reconstruction. The next section provides an overview of these five programs for context on which programs received the majority of U.S. funding.

a. Afghanistan Security Forces Fund

The ASFF accounts for a significant portion of the funding provided to Afghanistan; these funds were used to provide support to Afghanistan's security forces. The purpose of funding the ASFF was to support the development of a professional and self-sufficient Afghan security force to "combat a resilient insurgency and be a reliable counterterrorism partner with the United States" (Office of the Secretary of Defense, 2017, p. 1). The funds provided to the ASFF were used to support the Afghan National Defense and Security Forces (ANDSF) as well as the Afghanistan National Army (ANA) and the Afghanistan National Police (ANP) (Office of the Secretary of Defense, 2017). These funds included "the provision of equipment, supplies, services, training, facility, and infrastructure repair," according to the Defense Security Cooperation Agency (n.d.). The ASFF was focused on shifting the ANDSF from defending Afghanistan to offensively protecting the nation (Office of the Secretary of Defense, 2017). While the United States provided financial oversight over most of the funds provided to the ASFF, a portion of the money was provided directly to the Afghan government with specific

conditions for use of those funds to promote fiscal discipline and accountability within the government (Office of the Secretary of Defense, 2017).

b. Economic Support Fund

The purpose of the ESF was to improve Afghanistan's "political, economic, and security needs" (InterAction, n.d., para. 1). The ESF supported programs aimed at rebuilding critical infrastructure such as roads, schools, and medical facilities (Department of State, n.d.-a). This fund also was spent on strengthening Afghan governmental institutions to make them more accountable, transparent, and capable of serving and protecting their citizens (InterAction, n.d.). ESF funds were also spent on initiatives designed to improve economic relations between Afghanistan and neighboring countries, promote economic growth, and provide jobs for Afghan citizens (Department of State, n.d.-a). Lastly, these funds were used to decrease the narcotics production and trade throughout Afghanistan by providing alternative job options for Afghan farmers and strengthening the national law enforcement's ability to combat the drug trade (Department of State, n.d.-a).

c. Diplomatic Programs

The United States funded many diplomatic programs in Afghanistan aimed at stabilizing the country and promoting long-term stability. These programs included substantial resources to build a more cohesive Afghanistan government by focusing on improving public administration and oversight programs (SIGAR, 2015). Human rights programs, security improvements, economic growth, education, and diplomacy programs with other nations were some of the other diplomatic programs the United States funded. One specific diplomatic program, which received a large amount of funding throughout the years of Afghanistan reconstruction, was the Worldwide Security Protection (WSP) program (Department of State, n.d.-b). The WSP program provided funding for the protection of people, property, and global information (Department of State, n.d.-b). The program also included supporting security programs and managing diplomatic missions to achieve peace and security in Afghanistan (Department of State, n.d.-b).

d. International Narcotics Control & Law Enforcement

The INCLE fund is controlled by the Bureau of International Narcotics and Law Enforcement Affairs (INL) within the Department of State (Office of Inspector General, 2023). The INCLE program, under the INL, is focused on counternarcotics programs, law enforcement training and education, judicial system reform, and combatting trafficking of persons and wildlife (Office of Inspector General, 2023). In Afghanistan, these efforts were also focused on the people and ensuring at-risk groups were protected and provided increased opportunities (Bureau of International Narcotics and Law Enforcement Affairs, n.d.). The INL had updated monitoring and evaluation of the programs funded under INCLE in Afghanistan; however, there were significant issues with the internal control systems over these programs (Office of Inspector General, 2023). These issues led to inefficiencies in achieving program goals and ensuring effective use of funds. There were also significant issues with tracking the success of programs and creating and maintaining system standards for the INCLE programs (Office of Inspector General, 2023).

e. Commander's Emergency Response Program

The purpose of CERP was to provide commanders in theater with the approval to undertake projects that directly benefited the local population, specifically the areas of "water and sanitation, food production and distribution, agriculture/irrigation, electricity, healthcare, education," and many more (DoD, 2009, p. 27–5). The program was aimed at improving the living conditions of local people and in turn fostering goodwill toward U.S. forces. The intent was to start small-scale projects, which the local government could sustain and improve upon using the funds provided (DoD, 2009). Initially funded by millions of dollars that the U.S. seized from the Ba'athist Party in Iraq, CERP then became funded by appropriations funded by the U.S. government (Martins, 2005). According to a report from RAND on CERP usage in Afghanistan, CERP was "a valuable tool in improving the lives of Afghans but also in protecting the lives of American soldiers" (Egel et al., 2016, p. 55). CERP provided commanders with the ability to fund programs without having to work through bureaucratic processes, and due to the added flexibility, the program was initially highlighted as a major success (Martins, 2005). Despite the benefits, the program also faced challenges with oversight of the

funds, resulting in concerns about potential misuse and abuse (Egel et al., 2016). The significant issues identified included inconsistent documentation and "inadequacy of CERP financial control processes," which prevented effective tracking of the funds (Egel et al., 2016, p. 65). The GAO, in a 2009 report on CERP in Afghanistan, found that personnel at all levels had inadequate or no training regarding the use of CERP funds (GAO, 2009c). These issues highlight that CERP was another program with a lack of needed internal control systems in place to properly manage U.S funds in Afghanistan.

This section addressed the five programs that received 83% of all the funds provided by the United States to Afghanistan from FY 2002–2021. The next section introduces reports, special project investigations, and audits that highlight the complexities and challenges with the management of funds provided for Afghanistan reconstruction.

2. Funding Management Issues

This section highlights the persistent financial management issues that impacted U.S. reconstruction efforts in Afghanistan from 2001–2021. Numerous reports from SIGAR, GAO, and other government entities documented systematic weaknesses in oversight, financial controls, and management. These reports show how mismanagement, corruption, and poor internal controls led to significant inefficiencies in the management of funds and equipment allocated for Afghanistan.

The financial management and oversight of U.S reconstruction efforts in Afghanistan have been consistently highlighted as areas of concern by various government investigative agencies, specifically SIGAR and the GAO. A report published by the GAO in January 2021 outlined years of shortcomings in the DoD's response to audit recommendations made by the GAO and SIGAR starting in 2002. Of the more than 400 GAO reports on Afghanistan since 2002, 105 were focused on reconstruction activities, and of those 105 reports, 50 of those reports identified significant internal control deficiencies (GAO, 2021). The 50 reports found deficiencies in a range of areas, to include human resources, monitoring, contracting, information quality, coordination, policy or guidance documentation, planning, evaluation, risk assessment, and more (GAO, 2021). This GAO report summarizes 20 years of reports by multiple government

agencies addressing the glaring concerns about internal control systems in Afghanistan. The following paragraphs address some of the repetitive issues with internal control systems, which negatively hindered reconstruction efforts in Afghanistan.

The GAO issued a report in 2009 addressing a lack of oversight and tracking of U.S.-supplied weapons to the Afghan National Security Forces (ANSF). These weapons were supplied beginning in 2002, and there were not sufficient tracking programs to ensure proper accountability of the weapons, resulting in "87,000 or about 36 percent of the 242,000 weapons that the United States procured and shipped to Afghanistan" being unaccounted for by the Combined Security Transition Command-Afghanistan (CSTC-A) (GAO, 2009b, p. 4). Other U.S.-supplied equipment, such as night vision devices and other sensitive equipment, was also not tracked, and when audited, the CSTC-A could not provide records for many other types of equipment (GAO, 2009b). A second GAO report from 2009 addressed a lack of oversight personnel for construction projects (GAO, 2009a). The lack of qualified personnel to oversee construction projects was not a new issue in Afghanistan. For example, "in September 2007, the State Inspector General found that State had neither clearly defined authority and responsibility nor developed standard policies and procedures for" contractors and oversight employees (GAO, 2009a, p. 29). The DoD and USAID were both facing a lack of oversight personnel for construction projects for years according to this GAO report; however, proper training for personnel was slow to be mitigated after initial reports years prior to the 2009 GAO report.

The *Report on Progress toward Security and Stability in Afghanistan*, issued by the DoD to Congress in 2008, identified key financial management issues, starting with widespread corruption that "undermines internal reconstruction and development efforts" (Executive Services Directorate, 2008, p. 10). This report also highlights that due to inaccurate accounting and tracking systems, there was no reliable data detailing the amount of internal assistance provided to Afghanistan since 2001 (Executive Services Directorate, 2008). A special project report from SIGAR in 2015 addressed internal control issues identified during the spending of over $66 billion of appropriations from 2002–2014 (Office of Special Projects, 2015). One issue was the failure to track contracts properly in the Federal Procurement Data System (FPDS) before 2010, resulting from the

DoD not reporting treasury account codes for contracts; therefore, it was not possible to link contracts to their funding sources (Office of Special Projects, 2015). The report also highlighted the lack of oversight with inter-agency fund transfers, which increased the potential for fraud and corruption and decreased investigative agencies being able to track and prosecute fraud (Office of Special Projects, 2015).

Despite numerous reports and audits of management, oversight, and internal control issued during the first decade of Afghanistan reconstruction, these challenges continued throughout the following decade. A 2020 SIGAR evaluation report highlights internal control issues within the DoD's Afghanistan operations. From 2014–2019, SIGAR issued hundreds of reports containing 219 recommendations for the DoD to improve internal controls and oversight; however, due to "high staff turnover" and other reasons cited by the DoD, less than 40% of SIGAR's (2020) audit recommendations were implemented. The lack of implementation of recommendations resulted in "$240 million in questioned costs" due to reoccurring oversight and contracting issues (SIGAR, 2020, p. 4).

Following the 2020 report from SIGAR addressing the lack of implementation of recommendations by the DoD, SIGAR issued a report in 2021 regarding $494 million of spending that could not be supported with required documentation (SIGAR, 2021b). The spending was done by USAID and the U.S. Department of Agriculture (USDA) for Afghanistan, as well as the DoD, between 2012 and December 2020. The questioned costs were incurred because "the implementing partner lacked sufficient supporting documentation to support costs incurred, costs charged to the funding agency did not comply with federal laws and regulations, and cost charged did not comply with award terms" (SIGAR, 2021b, p. 6).

Twenty years of Afghanistan reconstruction spending documented in a lessons learned report by SIGAR reaffirmed the widespread internal control failures (SIGAR, 2021c). Billions of dollars were invested in projects that ultimately proved unsustainable for the Afghan government (SIGAR, 2021c). Weak monitoring and evaluation systems failed to identify these problems in a timely manner, and slow responses from U.S. agencies further exacerbated the situation. Projects were often rushed, focusing on

temporary political goals rather than permanent stability, which further strained Afghan institutions' ability to manage the efforts put in place (SIGAR, 2021c). The lack of coordination, both within U.S. agencies and between the United States and Afghan government, allowed inefficiency, fraud, waste, and abuse to persist (SIGAR, 2021c). These systemic weaknesses illustrate persistent challenges in managing reconstruction funds and ensuring accountability.

This section addressed ongoing financial monitoring issues throughout the 2 decades the United States provided reconstruction funds to Afghanistan and the difficulties in maintaining accountability of those funds. The next section addresses the fuel procurement programs in Afghanistan and identifies the oversight mechanisms each program utilized to prevent fraud.

G. FUEL PROCUREMENT IN AFHGANISTAN

The process of fuel distribution to the U.S. military, coalition military forces, and the Afghanistan National Defense and Security Forces (ANDSF) in Afghanistan involved several key stages, starting from procurement and ordering, continuing through delivery, and ending with usage by U.S. military, coalition military forces, and the ANDSF (SIGAR, 2018). This supply chain was managed through a collaboration of U.S. agencies, contractors, and Afghan ministries, ensuring operational readiness for both U.S. and Afghan forces.

1. U.S. Military Fuel Supply Process

Fuel procurement for the U.S. military was primarily handled by the Defense Logistics Agency-Energy (DLA-E), which secured fuel through competitive contracts with suppliers. As the primary provider of fuel, DLA-E delivered fuel to all 13 U.S. military bases in Afghanistan (SIGAR, 2018). DLA-E used two types of contracts: direct delivery, where contractors retained ownership of the fuel until it reached the U.S. military bases, and transportation contracts, where contractors transported fuel owned by DLA-E (SIGAR, 2018). The control mechanism in place for direct delivery contracts was that the contractor was responsible for fuel lost during transportation. For transportation contracts, DLA-E retained ownership of the fuel in transportation, but if more than 0.5%

of the fuel was lost during transportation, the contractor paid $15 per gallon of fuel that was lost above the limit (SIGAR, 2018). Besides the previously mentioned financial deterrents for fraud, there were no other control mechanisms in place to deter or prevent fraud and theft of fuel being transported to U.S. military bases.

The secondary method of fuel procurement for the U.S. military was by the U.S. Army Expeditionary Contracting Command-Afghanistan (ECC-A) under a contract with the National Afghan Trucking (NAT) (SIGAR, 2018). Fuel contracts delivered under ECC-A were a significant source of fuel for the U.S. military in the first decade of operations in Afghanistan, with 5,000 fuel missions being carried out between September 2011 and January 2012 (SIGAR, 2018). The number of contracts significantly declined in later years, with only 16 fuel missions between March and June 2017. The significant decline resulted in the discontinuation of ECC-A in October 2017 (SIGAR, 2018). Prior to ECC-A being dissolved, control mechanisms had been implemented to decrease fuel theft, "including decreasing the acceptable fuel loss rate from 5 percent to 1 percent" as well as installing transponders in NAT contractors' trucks to allow for live position monitoring (SIGAR, 2018, p. 3).

In addition to ECC-A fuel, U.S. military forces would occasionally receive fuel from the North Atlantic Treaty Organization (NATO) Support and Procurement Agency (NSPA) due to their alignment with the international coalition operating in Afghanistan (SIGAR, 2018). For example, the U.S. military provided NSPA-donated fuel to the Special Mission Wing (SMW), which was commissioned by the Afghan government in 2012 (SIGAR, 2018). Once fuel was delivered from any source, it was transferred to U.S. military control and stored in secure tanks managed by military personnel. The fuel process for the U.S. military is shown in Figure 10.

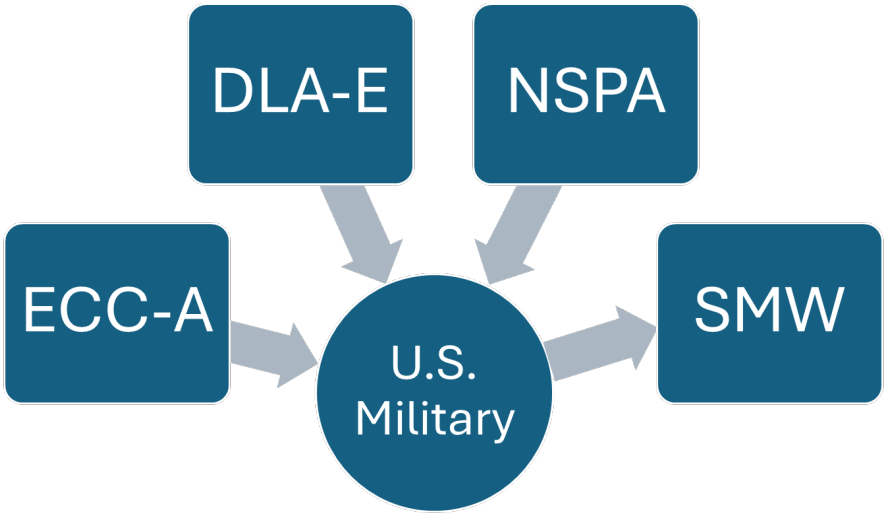

Figure 10. U.S. Fuel Supply Process in Afghanistan. Adapted from SIGAR (2018).

2. Coalition Military Forces Fuel Supply Process

Fuel distribution for coalition forces in Afghanistan was managed by the NSPA which was responsible for delivering fuel to all 21 coalition forces locations throughout Afghanistan as well as the Afghan SMW (SIGAR, 2018). Coalition forces relied on the NSPA to manage the total fuel supply chain, beginning with procurement through delivery, using oversight and monitoring mechanisms. The NSPA contractors retained accountability for the fuel up to the receipt by the intended location; therefore, contractors were accountable for any fuel lost during transportation (SIGAR, 2018). The NSPA's fuel distribution process included checks at various stages throughout the process and various staff throughout the contracting, logistical, technical, and financial places in the process to ensure controls were working as designed (SIGAR, 2018). The NSPA utilized a system in its delivery trucks that allowed for live location tracking, location history, and checks on both the amount of fuel in trucks as well as the chemical configuration of the fuel in the container to ensure fuel was not watered down or switched with a lesser quality fuel (SIGAR, 2018). After fuel was delivered to coalition sites, the NSPA also utilized devices to monitor the amount of fuel in storing containers, electronic cards to identify which personnel accessed fuel, and handheld tools to

electronically receive receipts and delivery data (SIGAR, 2018). Figure 11 shows the role of the NSPA in the fuel process in Afghanistan.

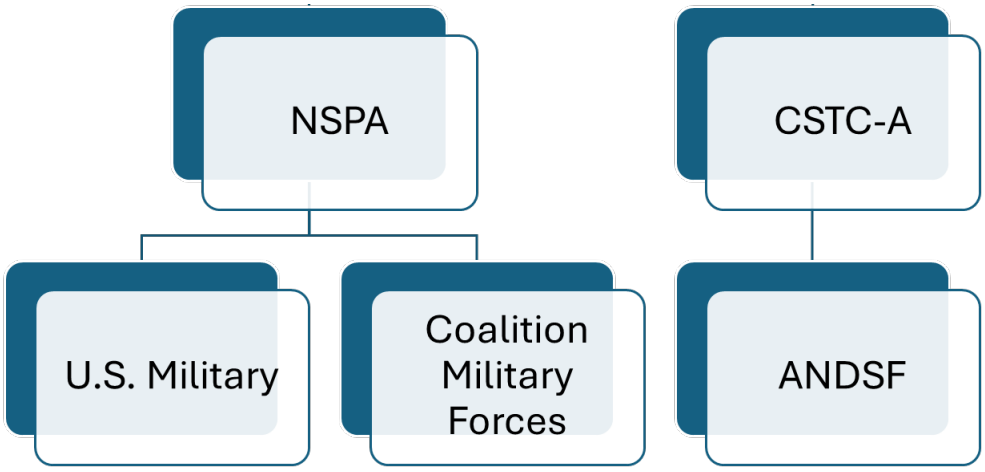

Figure 11. Coalition Fuel Process in Afghanistan. Adapted from SIGAR (2018).

3. Afghanistan National Defense and Security Forces Fuel Supply Process

The organization predominately liable for providing fuel to the ANDSF was the Combined Security Transition Command Afghanistan (CSTC-A), which was a DoD organization (SIGAR, 2018). CSTC-A used funds from the ASFF to purchase the fuel for ANDSF in two different ways, off-budget and on-budget. Both methods of fuel support involved CSTC-A working with the Afghanistan Ministry of Defense (MOD) and the Ministry of Interior (MOI) to strengthen Afghan government oversight departments' abilities to manage their own government processes and operation (SIGAR, 2018).

Off-budget fuel support involved the CSTC-A using ASFF funds to pay for fuel contracts managed by ECC-A. For this method of fuel delivery, the MOD and the MOI estimated the fuel need based on equipment that was operational and previous fuel usage rates for that amount of equipment. CSTC-A then used this estimation to order fuel, except ground and aviation fuel, for ANDSF on a monthly basis (SIGAR, 2018). To prevent issues with contract expiration dates, CSTC-A ordered ground and aviation fuel for ANDSF on a yearly basis (SIGAR, 2018).

After CSTC-A ordered the fuel, contractors would deliver it to the specified ANDSF locations and receive payment after successful receipt of the fuel at those

locations (SIGAR, 2018). The contractors were accountable for the fuel until it was successfully received by the ANDSF location; therefore, any fuel missing throughout the transport process was the liability of the contractor. The financial deterrent of the contractor being responsible for any unaccounted-for fuel was the main oversight control for the delivery process of off-budget fuel to ANDSF (SIGAR, 2018).

On-budget fuel support involved the Afghanistan government receiving funding from international donors to aid the Afghan government in procuring fuel and other essential items for operations (SIGAR, 2018). ASFF funds were also provided directly from the DoD to the Afghan MOD and MOI to support fuel and operational costs of the ANDSF. Through this process, the MOD and the MOI submitted their fuel consumption reports to CTSC-A. After CSTC-A reviewed the reports, the requested funds for the amount of fuel used were transferred to the Afghan Ministry of Finance, which purchased the fuel (SIGAR, 2018). Usage of on-budget procurement for fuel was increased to one-third of the requested fuel in 2013 and 100% in 2014 to enable the Afghan government to take more control of the oversight of fuel operations (SIGAR, 2018). On-budget fuel procurement was completely stopped in February 2017 "due to concerns about the ministries contract management, fuel quality issues, and corruption" (SIGAR, 2018, p. 6).

This section addressed the fuel process for the U.S. military, coalition military forces, and the Afghan military forces. The next section addresses reports spanning the 2 decades the U.S. was operating in Afghanistan, which identified weakness with the oversight of the fuel program. These reports also highlight the high number of fraud cases related to fuel and the potential for more fuel-related fraud and theft.

4. Fuel Management Issues

This section highlights multiple reports, audits, and investigations conducted by key oversight bodies such as SIGAR, the GAO, and the DODIG. These documents provide in-depth reviews of systemic vulnerabilities and failures in Afghanistan's fuel management program, specifically those related to theft, fraud, and internal control issues.

Fuel theft and fraud were pervasive and persistent issues throughout the U.S. military's involvement in Afghanistan. Over the course of the 2 decades that the U.S. military was operating in Afghanistan, numerous investigations and reports from oversight bodies such as SIGAR, the GAO, and the DODIG documented extensive losses and systematic vulnerabilities that enabled fuel crimes to occur. These problems began with systemic failures in the early 2000s, shortly after U.S. operations in Afghanistan commenced. Over time, these vulnerabilities allowed corruption, theft, and mismanagement to become entrenched within Afghanistan's fuel supply chain, resulting in financial losses and operational inefficiencies. Key reports indicate that internal controls were insufficient, documentation was lacking or non-existent, and accountability mechanisms were either absent or not enforced (SIGAR, 2021b; GAO 2012; DODIG, 2017).

a. Lack of Accountability and Incomplete Records

Beginning in the early years of U.S. involvement in Afghanistan, accountability over fuel purchases and deliveries emerged as a problem. SIGAR and GAO reports noted the lack of proper record keeping, making it difficult to track fuel deliveries accurately. In 2011, SIGAR released its quarterly report highlighting that the "DoD could not accurately account for over $1.1 billion in fuel provided to the ANA," exposing the vulnerabilities of fuel to fraud and theft (SIGAR, 2012b, p. 18). These gaps in reporting were exacerbated by the destruction of critical financial documents related to ANA fuel purchases, with nearly $475 million worth of records shredded, further hindering accountability mechanisms (SIGAR, 2012b). SIGAR (2012b) also criticized the method CSTC-A used to calculate fuel requirements and determined the fuel estimates were inflated, leading to excess fuel that was being pilfered. The fuel estimation system, CSTC-A, often led to fuel being ordered for vehicles and equipment that were no longer operational or had been destroyed (SIGAR, 2012a). In a testimony on the fuel estimation and tracking issues to Congress, Special Inspector General John F. Sopko stated, "No single commodity is important to the reconstruction effort in Afghanistan as fuel, and no commodity is at such risk of being stolen" (SIGAR, 2012b, p. 20). This mismanagement often led to significant waste and made it easier for fuel to be stolen or diverted.

b. Widespread Theft and Investigations

Fuel became known as "liquid gold in Afghanistan" due to its high value, ease of theft, and sale on the black market (SIGAR, 2013, p. 36). A significant case in 2012 involved fuel theft at Forward Operating Base (FOB) Fenty. This incident involved three U.S. Army personnel conspiring with Afghan trucking contractors to steal approximately 180,000 gallons of fuel (SIGAR, 2018). The stolen fuel, valued at $765,000, was sold on the Afghan black market and generated an estimated profit of $2 million for the perpetrators (SIGAR, 2018). A separate investigation during the same years at Camps Jordania and Marmal revealed another significant fuel theft scheme. An influential Afghan official defrauded the U.S. government out of an unknown amount of fuel but well over 10,000 gallons of fuel. The Afghan official was providing payoffs to fuel depot staff in exchange for them overfilling fuel trucks. The same official was also forging documents to the U.S. government for fuel delivers that were not delivered and collecting payment for fuel that was later sold on the Afghan black market (SIGAR, 2018). The investigation involving the U.S. military and law enforcement agencies, "led to more than $1 million in contract cost savings and recovery of" some of the pilfered fuel (SIGAR, 2018, p. 40). The cost savings from uncovering the scheme does not include the amount that was lost prior to the theft being uncovered. Additionally, a 2015 SIGAR investigation found that fraudulent fuel cards had resulted in an estimated $1 million of losses for the U.S. government (SIGAR, 2018). An Afghan trucking business was drawing fuel from a U.S. military base's fuel depot and had used a separate trucking company's credentials to gain access to the base and steal fuel (SIGAR, 2018). The investigation resulted in the recovery of the entire amount of stolen fuel costs (SIGAR, 2018). These cases highlight only a few of the major cases of fuel theft in Afghanistan that continued for the entire 2 decades the United States was operating in the country. The pervasive nature of fuel theft and fraud in Afghanistan exploited weak oversight mechanisms and systemic corruption, resulting in millions of dollars of loss for the U.S. government. Despite efforts to address these issues, fuel's high value and liquidity made it a persistent target for theft.

c. Oversight Failures and Unimplemented Reforms

A 2012 report by the GAO revealed systemic issues with the DoD's fuel demand management in Afghanistan, highlighting gaps in visibility and accountability over fuel consumption at forward-deployed locations (GAO, 2012). While the DoD had made efforts to improve fuel demand management by developing more comprehensive guidance and initiating projects aimed at reducing fuel consumption, the lack of both collaborative efforts and a systematic approach to tracking initiatives hindered the full implementation of reforms. The report underscores that without a mechanism to track fuel demand management efforts, the DoD may continue to struggle to foster coordination, avoid duplication, and ultimately prevent waste and fraud in the fuel program (GAO, 2012). This report called attention to the significant issues with fuel tracking and monitoring early in the reconstruction efforts. However, many of these same issues remained throughout the entire 2 decades of reconstruction efforts in Afghanistan.

Despite large scale investigations, increased attention, and reports from earlier years on fuel vulnerabilities, systemic issues persisted in the oversight of fuel distribution in Afghanistan. A 2017 DODIG audit report revealed several issues with CSTC-A's ability to manage fuel contracts for the ANA (DODIG, 2017). While CSTC-A implemented some improvements, such as establishing Logistics Executive Steering Committee (ESC) meetings to enhance coordination between oversight bodies, significant gaps in oversight remained (DODIG, 2017). CSTC-A relied heavily on data provided by vendors and ANA personnel for fuel deliveries and consumption reports. The lack of independent physical inspections of fuel deliveries left CSTC-A unable to verify the accuracy of these reports, making the system vulnerable to fraud and theft (DODIG, 2017). Additionally, CSTC-A's reliance on commitment letters to assess fuel needs and consumption failed to ensure accurate fuel allocations. CSTC-A imposed financial fines on ANA corps for non-compliance with obligation letters, but these efforts did little to address the broader issue of inaccurate fuel data. As a result, U.S. direct assistance, valued at $174.7 million, was susceptible to fraud and waste (DODIG, 2017). CSTC-A also faced challenges in validating ANA's fuel usage, as there was no process in place to perform random inspections or verify fuel consumption on the ground (DODIG, 2017).

As previously stated, a 2020 SIGAR report provided further insight into the systemic failures in managing fuel for Afghan forces. Less than 40% of SIGAR's recommendations from earlier years were implemented, highlighting the persistent gaps in oversight (SIGAR, 2020). While earlier reports led to some changes, there were still significant issues the DoD did not implement or address in a timely manner. According to the report, some recommendations were not implemented or acted on at all (SIGAR, 2020). SIGAR (2021a) followed up on the lack of implemented recommendations addressed in its 2020 report the following year, and the results showed little to no improvement. In fact, CSTC-A reported that almost half of the fuel being provided to ANDSF was being stolen (SIGAR, 2021a). CSTC-A stopped utilizing recommendations that had been implemented, such as commitment letters to establish clear fuel requirements, and was once again seeing unreliable data for fuel requirements and a decrease in tracking the usage of fuel (SIGAR, 2021a). Additionally, the issues discussed in the 2017 DODIG report were still prevalent in 2021. There was a lack of accurate monitoring systems, fuel estimation methods, and systems to ensure fuel delivery (SIGAR, 2021a). Despite CSTC-A's efforts to train Afghan officials and improve procurement systems, the entrenched corruption within Afghan ministries meant that CSTC-A continued to manage the fuel supply process, which remained highly susceptible to fraud and theft.

H. SUMMARY

This section addressed reports highlighting the systemic failures, fraud, and corruption that plagued U.S.-funded fuel programs in Afghanistan. While significant cases of fraud were uncovered and some reforms were implemented, many of the core issues remained unresolved. This chapter discussed Fraud theory, Auditability theory, and the COSO and GAO internal control frameworks. In addition, this chapter addressed the Afghanistan reconstruction efforts, U.S. funding for Afghanistan reconstruction, and fuel procurement in Afghanistan. The next chapter addresses the methodology used in this research study and the development of the two databases used throughout this study.

III. METHODOLOGY

A. INTRODUCTION

This chapter outlines the methodology employed in conducting the research on internal control failures in fuel fraud cases in Afghanistan. The research method centers on the creation and analysis of a database detailing these control failures. The first part of this chapter provides an explanation of the process used to develop and compile the database. The primary source of information was Public Access to Court Electronic Records (PACER), a public court records website, which provided detailed case files related to fuel fraud incidents involving U.S. military personnel. These cases served as the foundation for the database. The next section provides an explanation of how the fuel fraud control failures within each court case were systematically analyzed and categorized. A set of predefined criteria was used to identify and separate key actions, decisions, and control failures in each case. This approach ensured that all significant events related to fuel fraud were captured in a structured manner, allowing for detailed analysis and comparison across cases. Finally, this chapter details how the resulting database was aligned with the COSO Framework. Each fuel fraud control failure was mapped to at least one of the five components of internal controls to identify specific control deficiencies. The next section of this chapter provides a detailed explanation of how the fuel fraud database was developed, including the criteria used to classify and organize the data.

B. DEVELOPMENT OF THE FUEL FRAUD DATABASE

The development of the fuel fraud database began with an evaluation of the necessary approvals for using publicly available court records. Since this research did not involve interviews or the collection of personally identifiable information, NPS IRB determined a full IRB protocol was not required. Additional publicly available sources were also utilized and are further discussed in the Sources section. These documents and records identified specific events, individuals, and processes relevant to the fraud cases. Following a review of the available court documents, a database was created to catalog each incident, the individuals involved, their roles, and the corresponding internal control

components that were compromised. For each court case, the fuel control failures were identified. Each fuel control failure was then aligned to one of the COSO internal control components, as either a primary control deficiency or secondary control deficiency. The next section provides a detailed overview of the sources used in this research.

1. Sources

The sources for this research were drawn from a combination of government reports, press releases, and publicly available court records. Key information about individuals involved in fuel fraud cases was initially obtained from Federal Bureau of Investigation (FBI) press releases, SIGAR reports, and news releases from other government agencies. These sources provided the names of military personnel and contractors implicated in fuel fraud. Once the individuals were identified, their court cases were accessed through the PACER system, which allowed for the collection of detailed case files. These case files served as the primary source for documenting the events, actions, and internal control failures related to fuel fraud. Together, these sources offered a comprehensive overview of the cases and enabled the creation of a robust database for further analysis.

2. Search Terms

The search strategy employed for this research was designed to systematically identify relevant cases and documents across the sources outlined in the previous section. Specific names of military personnel and contractors involved in the fuel fraud cases were used as search terms. Additionally, broader search terms were employed to capture comprehensive data related to the topic, including phrases such as “fuel fraud in Afghanistan,” “fraud in Afghanistan,” “military fuel fraud Afghanistan,” and “fuel theft Afghanistan.” These terms were used across multiple sources to ensure a comprehensive collection of cases and incidents related to fuel fraud. The next section provides an explanation of how each incident, individual, or process was categorized with respect to primary and secondary internal control components.

C. DATABASE COMPOSITION

The composition of the Excel database for this research involved assessing each court case document to identify incidents involving fuel control failures. Once fuel control failures were identified, each failure was aligned to one or more internal control components. The recorded fuel control failures were then tallied by internal control component to determine which components resulted in the highest number of fuel control failures in the cases used in this research.

D. ALIGNMENT TO FRAMEWORK

The COSO Framework served as the foundation for categorizing the individuals, processes, and events documented in the fuel fraud cases by their associated internal control failures. Based on the description of the fuel control failures, a primary alignment to one of the COSO internal control components was determined. Following this, the fuel control failures were aligned to one secondary COSO internal control component. This method of alignment allowed for a clear identification of which internal controls were most directly linked to the fraud and operational failures. By systematically associating each event with its respective primary and secondary components, the analysis provided a structured view of how internal control weaknesses contributed to fuel fraud.

E. SUMMARY

This chapter detailed the methodology used in this research, focusing on the creation of a database centered on fuel fraud cases in Afghanistan. It outlined the data sources employed, such as public court records accessed through PACER, FBI press releases, and SIGAR reports, and described the process for identifying and categorizing relevant events. This chapter also detailed how each incident was aligned to a primary and secondary COSO internal control component. Additionally, it covered the search terms and strategies utilized to compile the database. The next chapter includes an exploration of the findings of this research, an analysis of the internal control failures, and recommendations for strengthening internal controls to mitigate future fraud risks.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINDINGS, ANALYSIS, IMPLICATIONS, AND RECOMMENDATIONS

This chapter includes a thorough analysis, highlights findings, discusses implications of the results, and provides recommendations based on the findings of this research study. An examination of the findings focuses on involvement of military personnel by rank, the geographic distribution of fuel theft incidents, and internal control failures by component. The chapter presents an analysis of the databases developed for this research study, including the Primary Fuel Fraud (PFF) Database and Secondary Fuel Fraud (SFF) Database to determine trends in fraudulent activities across the court cases used in this study. Each incident identified in these databases is aligned to a COSO internal control component. The chapter addresses the broader implications of the results of this research study. The chapter provides recommendations based on the findings and analysis to address the weaknesses identified in this research. The following section discusses the findings of this research.

A. FINDINGS

Each incident identified from the court cases is related to fuel fraud incidents in the Army. The court cases were all found through the public site PACER. Based on the incident's description in the court case, each incident's control failure is aligned with one of the five components of the COSO Internal Control Integrated Framework: control environment, risk assessment, control activities, information and communication, and monitoring activities. For each incident, a determination was made as to whether the control failure in the incident was categorized as a primary internal control component type failure or as a secondary internal control component type failure.

This researcher compiled two fuel fraud databases of 118 events that corresponded with 17 different court cases focusing exclusively on the actions of military personnel involved in theft schemes during deployments to Afghanistan. All cases involved enlisted U.S. Army members. The cases were not chosen to only include enlisted Army members; however, the search terms returned cases that only included that specific group of military members. Some schemes are only partially represented, as

some individuals who were involved were either civilians or foreign nationals, and therefore excluded. Additionally, certain participants' actions are absent from the databases due to sealed records, limiting this study's scope. The cases collected in these databases do not represent all the cases of fuel theft in Afghanistan.

The databases document the criminal activities of military members by case. While these actions are documented once per court case, the fuel theft schemes involved the repetition of the actions multiple times. In some cases, a single scheme resulted in the theft of more than 100 truckloads of fuel from U.S. military bases. The databases provide concise summaries of the methods used to commit the theft, support fellow conspirators' actions, and outline steps taken to conceal the theft. Each incident is aligned with an internal control component of the COSO Framework, which was identified as the primary component followed by an analysis of the secondary component related to each of the incidents. The following sections provide the findings of this research study.

1. Involvement by Rank

The data from the cases all involve U.S. Army personnel. The data collected did not involve any cases of military members in other branches charged in the schemes nor did the data include any cases of Army officers convicted in these fuel theft schemes. The rank distribution of military personnel involved in the fuel theft schemes shows 49 incidents (42%) of convicted offenders were Army sergeants (E-5), 27 incidents (23%) were Army specialists (E-4), 22 incidents (19%) were Army staff sergeants (E-6), and 19 incidents (16%) were Army sergeant 1st class (E-7). Sergeants were the most frequently involved rank, including 42% of the offenders. The combined involvement of junior enlisted, sergeants, and specialists accounted for 76 (65%) of all incidents, while higher-ranked enlisted personnel, staff sergeants and sergeants 1st class, made up the remaining 41 incidents (35%). Figure 12 shows the involvement in these schemes by rank.

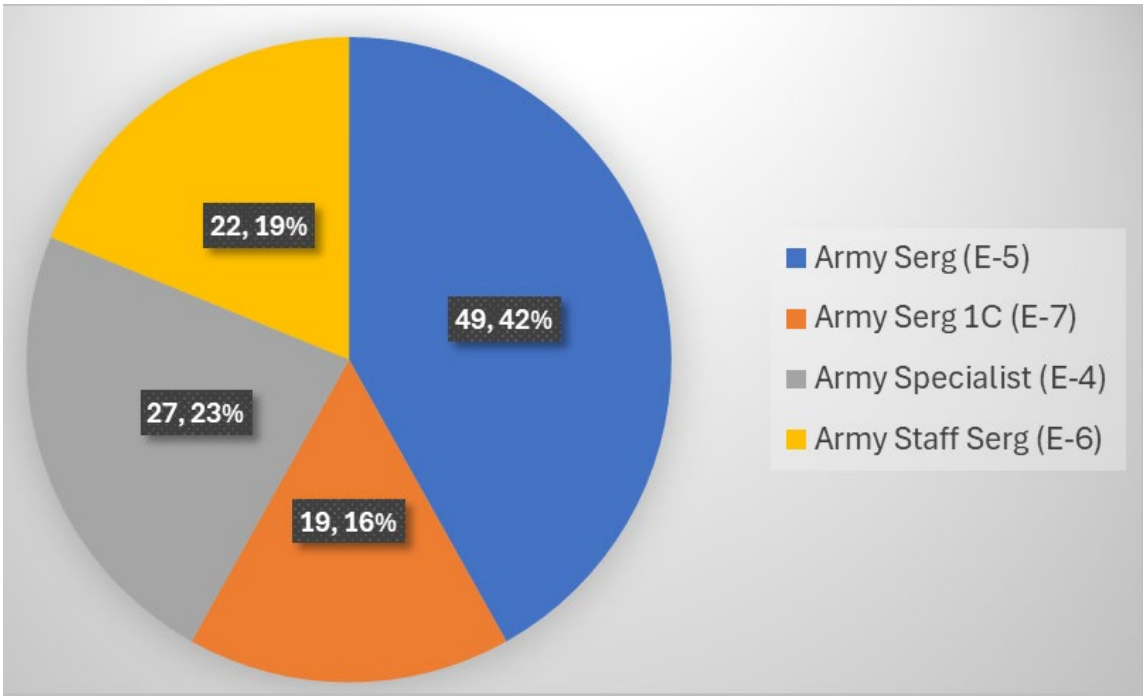

Figure 1. Incidents by Rank

2. Geographic Distribution of Incidents

The geographic distribution of incidents in this study calls attention to specific bases that had more fuel management issues than others. Foreign Operating Base (FOB) Fenty had 44 incidents (37%), Kandahar Air Field had 37 incidents (31%), FOB Gardez had 13 incidents (11%), FOB Sharana had 10 incidents (9%), FOB Shank had 9 incidents (8%), and FOB Salerno had 5 incidents (4%). FOB Fenty and Kandahar Air Field made up 81 (68%) of all the incidents recorded from the fuel theft cases in this study. Figure 13 depicts the breakdown of fuel fraud incidents by military base.

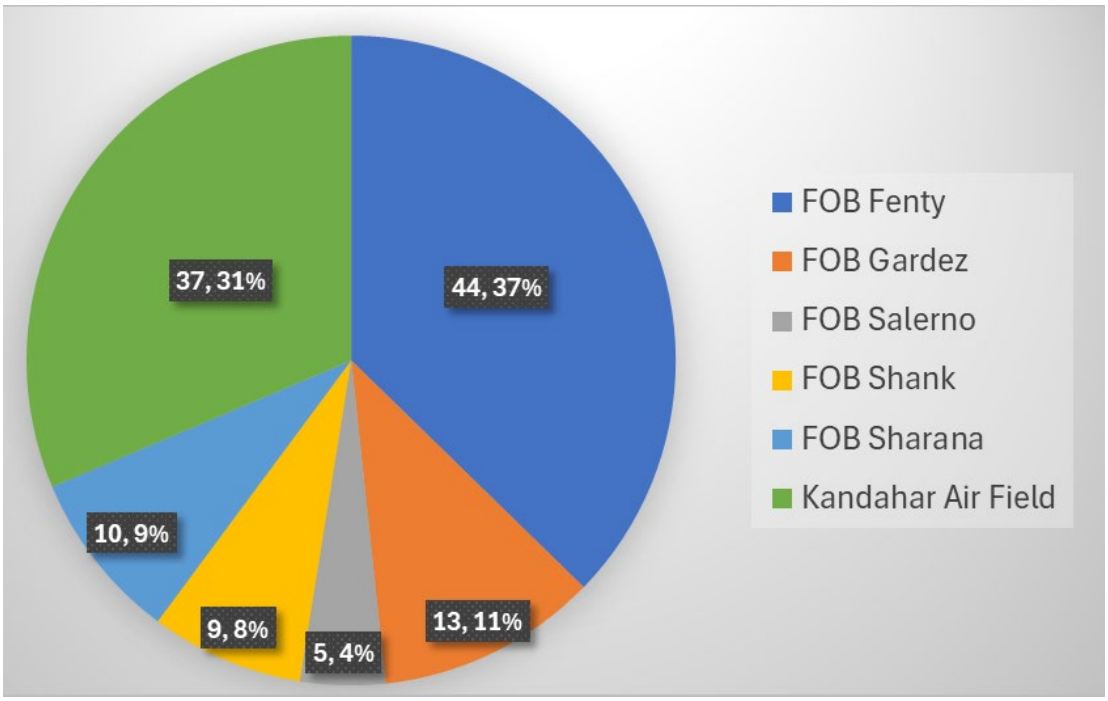

Figure 2. Incidents by Location

3. Internal Control Databases

The PFF Database and SFF Database align each incident of the fuel fraud schemes and actions taken to conceal fuel fraud and theft after it occurred to a primary and secondary internal control component. Determining the primary and secondary internal control component for each incident involved analyzing the incidents and actions that led to the fraud. Next, each incident and action were linked to the relevant COSO component. The primary component was identified as the one most directly responsible for the failure, meaning that if it had been functioning properly, the incident likely would not have occurred. The secondary component was the internal control that could have caught or mitigated the problem after it began.

Table 1 provides a breakdown of the primary, secondary, and total internal control failures within all the fuel fraud schemes investigated in this study. Control activities accounted for 73 (73%) of total component failures. Control environment comprised 57 (24%) of total component failures. Risk assessment component failures were 40 incidents (17%) of total component failures. Monitoring activities comprised 56 (24%) of total

component failures. Information and communication components accounted for 10 (4%) of total component failures.

	Primary Component Failure	Secondary Component Failure	Total Component Failures
Control Environment	**28 / 24%**	**29 / 24%**	**57 / 24%**
Risk Assessment	**25 / 21%**	**15 / 13%**	**40 / 17%**
Control Activities	**51 / 43%**	**22 / 19%**	**73 / 73%**
Information & Communication	**1 / 1%**	**9 / 8%**	**10 / 4%**
Monitoring Activities	**13 / 11%**	**43 / 36%**	**56 / 24%**

Table 1. Recorded Incidents Component Failures

Figures 14 and 15 show the breakdown of primary and secondary component failures across all incidents. Control activities had the highest number of primary control failures at 51 (43%) but was only responsible for 22 (19%) secondary failures. Control environment had the second highest number of failures for primary failures at 28 (24%) and secondary failures of 29 (24%). Risk assessment was the component with the third most primary failures at 25 (21%) but only 15 (13%) of secondary failures. Monitoring activities was not the component with a high number of primary failures at 13 (11%) but was the highest number for secondary component failures at 43 (36%). Information and communication had the lowest number of failures at 1 (1%) for primary and 9 (8%) for secondary failures.

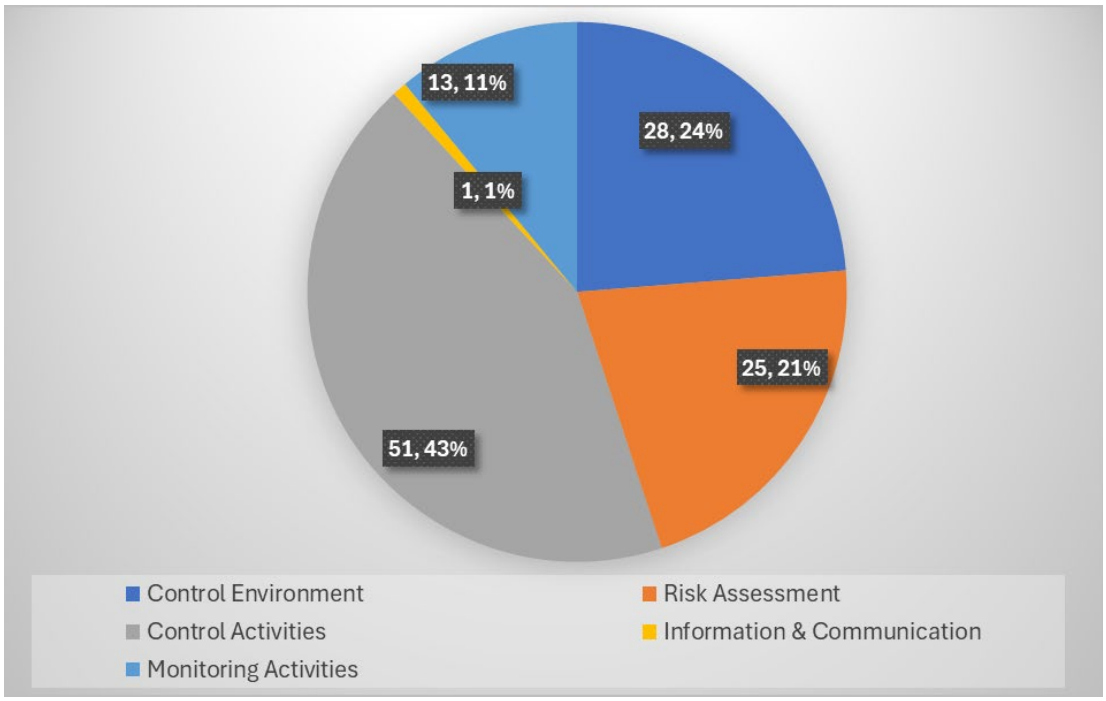

Figure 3. Primary Internal Control Component Failures

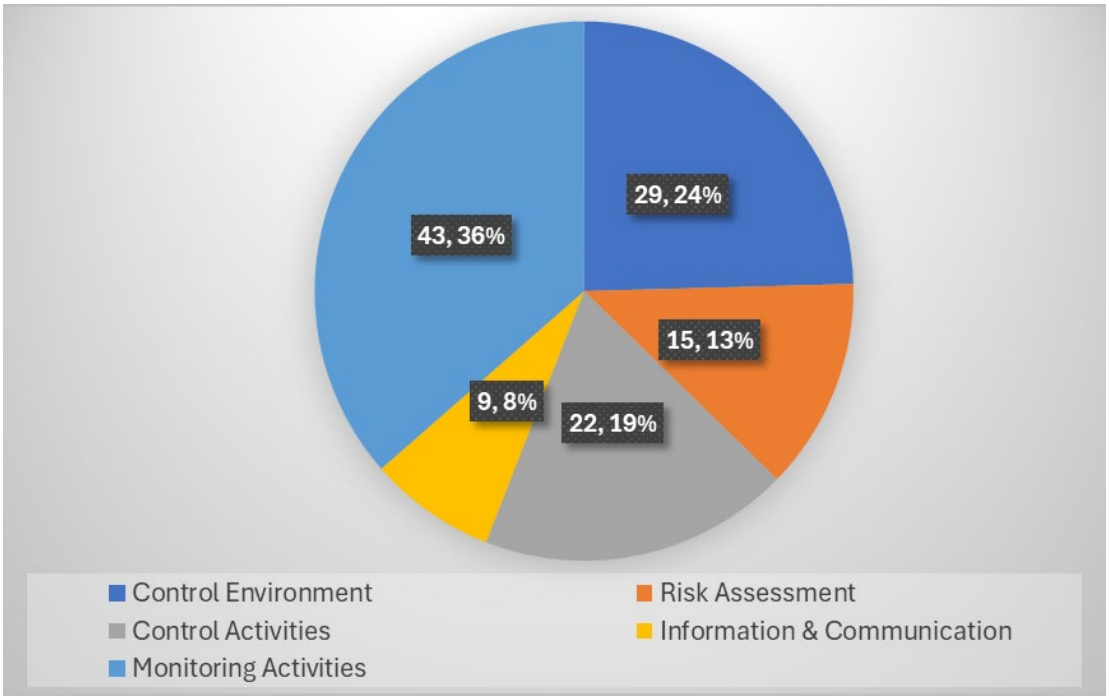

Figure 4. Secondary Internal Control Component Failures

B. ANALYSIS

The incidents recorded in the two databases are the same incidents; however, the incidents in each database are assigned to a different internal control component. The incidents recorded in the databases highlighted major issues with the recording process of fuel transfers called Transfer Movement Requests (TMRs), overall ethics of military members, and ineffective internal control systems.

1. Primary Fuel Fraud Database

The PFF Database highlighted major vulnerabilities with the control activities over the fuel management process in Afghanistan. The PFF database is a record of each specific event detailed in the court records of individuals found guilty of fuel theft in Afghanistan. The specific events are attributed to an internal control component failure primarily responsible for the failure according to the COSO Framework definitions of the components. As Table 1 shows of the total incidents recorded, 43% of those incidents' primary failures were attributed to deficiencies in the control activities. This significant percentage highlights major issues with the control activities over TMRs, tracking of fuel after it was moved off base, awarding of contracts, monitoring of trucks entering and leaving base, and fuel tracking of fuel usage.

Additionally, Table 1 highlights 24% of primary events being related to control environment component deficiencies. The issues with control environment include problems such as allowing fuel to be diverted, instructing subordinates to break the law, paying other military members to break the law, and taking steps to ensure illegal acts are hidden. These incidents call attention to problems with overall ethics, morals, and environment created by the organization and those in command.

Table 1 also shows failures in the risk assessment component, to which 21% of primary component failures were attributed. The incidents of risk assessment were actions taken by military personnel that were not foreseen; therefore, there was no risk planning for military members receiving bribes, stealing fuel, selling fuel illegally, or failing to safeguard U.S. government property.

As shown in Table 1, monitoring activities accounted for 11% of primary component failures, which calls attention to a lack of verifying that systems in place were operating appropriately. Failures of monitoring activities resulted in problems with fuel transfers being falsely certified as completed, false reasons being reported for increased fuel usage, failure to download all fuel from trucks, and creation of TMRs in excess of fuel requested.

Information and communication component failures are responsible for only 1% of primary component failures as shown in Table 1. The primary component failures attributable to information and communication were due to the collection of fuel documents by personnel that were participating in a fuel fraud scheme instead of allowing the submission of those documents to be submitted to supervisors.

The primary component failures highlighted significant issues with the management process and internal controls in place over Afghanistan fuel management practices. The next section addresses the secondary component failures and the incidents attributed to each internal control component.

2. Secondary Fuel Fraud Database

The SFF Database shows significant failures across the entire COSO Framework regarding secondary component failures. Table 1 highlights the highest amount of secondary component failures as monitoring activities at 36%. Incidents that could have been stopped or discovered with properly implemented monitoring activities include the creation and acceptance of false TMRs, unauthorized personnel entering and exiting bases, significant amounts of fuel being diverted, and false fuel documents being presented by unapproved personnel to leave base with fuel.

As shown in Table 1, control environment accounted for 24% of secondary component failures. Incidents that the control environment component should have mitigated include military members falsifying TMRs, military members diverting fuel to secondary locations, contracting procedures being bypassed by military personnel, members allowing unauthorized personnel to enter and exit base to steal fuel, and military people loading unapproved trucks with fuel.

Additionally, Table 1 shows 19% of secondary component failures were attributed to control activities. The incidents recognized as control activity failures included falsely certifying that fuel transfers had been completed, members selling fuel on the black market, failing to download the full amount of fuel from delivery trucks, members allowing fuel to be diverted off base, and members falsely recording the amount of fuel delivered.

Furthermore, risk assessment accounted for 13% of secondary component failures in the recorded incidents. These incidents included collecting bribes on behalf of other military personnel, bringing other military members into the fuel theft scheme, supervising the manipulation of TMRs, and instructing subordinates to falsify fuel records.

Table 1 also highlights that 9% of secondary internal control failures for the recorded incidents were attributed to the information and communication component. The incidents for which information and communication were the secondary component failure were reporting false reasons for the increase in recorded fuel usage, creating TMRs in excess of the requested amount, and paying another soldier to illegally escort a fuel driver on and off base and load fuel into drivers' trucks. The secondary internal component failures highlight further issues with the overall management process over fuel management in Afghanistan.

3. Internal Control Failures

The previous sections provided an analysis of the two databases created in this research and what the findings revealed from the databases. The following sections are an examination of the failures of each internal control component across the recorded fuel fraud incidents.

a. Control Environment

Based on the findings, control environment accounted for 57 (24%) of the total internal control component deficiencies as shown in Table 1. A properly operating control environment provides the overall structures an organization utilizes to implement effective internal controls (COSO, 2013). In Afghanistan, across the fuel fraud schemes

in this study, control environment failures highlight a deficiency in the organization's ethical framework, reflecting leadership's failure to establish a strong tone at the top. While the criminal actions in the database were not committed by those at the top, the root cause points to a lack of accountability and ethical guidance from leadership. Leaders who permitted or ignored these behaviors set a precedent that allowed fraud to increase, indirectly supporting rule breaking by failing to emphasize the importance of integrity and compliance with rules and regulations.

(1) Primary Failures

The findings highlight that 28 (24%) of identified primary fuel control failures resulted in control environment deficiencies, shown in Figure 14. The following provides an analysis of the primary fuel control failures that were aligned to the control environment component.

When subordinates allowed Afghan contracted truck drivers to divert fuel, it was more than an individual act; it reflected a permissive control environment where accountability was careless and misappropriation was implicitly tolerated. The findings indicate that soldiers on those U.S. military bases knew fuel was being stolen and sold on the black market and chose to take money in exchange for keeping silent instead of reporting the theft. Without clear ethical guidance and a strong and consistent stance against resource reallocation from the top, subordinates likely interpreted this tolerance as a form of approval, weakening the effectiveness of internal controls.

The disregard for internal controls also highlights a lack of involvement by leadership and indicates that the tone at the top was insufficient to deter unethical actions. This lack of emphasis on ethical conduct may have increased the number of individuals willing to participate in fraudulent activities, leading to a pervasive culture of fraud. The culture is highlighted by actions recorded in the database, such as instructing subordinates to break the law and paying other military members to break the law. Individuals participating in the fraud had confidence in their actions going unnoticed, resulting in them not only continuing but including others in the fuel theft schemes as well.

The concealment of illegal acts after the fact by subordinates speaks to a possible breakdown in the military's commitment to transparency and accountability. Leaders' passive role in enforcing compliance allowed for not only illegal actions to take place but also enabled the effective concealment of those actions after the fact. Without proactive oversight, involved leadership, and clear ethical boundaries, the control environment culture enabled military members to engage in fuel fraud with little risk of exposure.

(2) Secondary Failures

The findings highlight that 29 (24%) of identified secondary fuel control failures resulted in control environment deficiencies, shown in Figure 15. The following provides an analysis of the secondary fuel control failures that were aligned to the control environment component.

The falsification of TMRs by military personnel was a clear breach of integrity that should have been detected by an organization with strong internal controls and a strong ethical culture. Falsifying TMRs reflects an indifference towards transparency and accuracy, suggesting that the control environment failed to reinforce the importance of accuracy and adherence to protocol in recordkeeping.

Leadership's failure to instill a strong ethical foundation undermined the credibility of control mechanisms and left subordinates without a clear framework of accountability. Another failure was the diversion of fuel to secondary locations by military members. This was more than willfully ignoring Afghan trucking contractors' illegal actions because U.S. military members were a direct part of diverting the fuel. U.S. military members' illegal actions in conjunction with Afghan contractors' illegal actions indicates a lack of control over resource allocation and accountability for mission-critical assets. Without a robust control environment that holds subordinates accountable, it becomes possible for personnel to reroute resources for unauthorized purposes. This diversion also underscores the need for leadership to clearly demonstrate a culture of positive ethics and to enforce repercussions for deviations from the standards.

The bypassing of contracting procedures by military personnel reflects inadequate oversight and a lax stance toward procedures resulting in inappropriate shortcuts. In an

environment with strong internal controls, bypassing contracting requirements would trigger immediate scrutiny, as it represents a serious violation of protocol designed to protect organizational integrity and mitigate fraud risk. By failing to consistently enforce contracting standards, leadership allowed subordinates to view these controls as flexible, fostering a culture where rules could be circumvented without consequence.

Allowing unauthorized personnel to access bases for the purpose of fuel theft highlights a lack of security oversight, demonstrating that the control environment was not sufficiently rigorous enough to enforce access controls and physical security protocols. This breach not only facilitated resource theft but also posed significant operational security risks. Such lapses suggest that leadership did not prioritize strict adherence to security protocols and set a tone where subordinates felt empowered to permit unauthorized access.

Finally, incidents of military personnel loading unapproved trucks with fuel reveal a breakdown in adherence to authorized procedures and accountability for mission resources. This failure indicates that the organization's control environment did not instill the necessary oversight mechanisms to ensure that only approved vehicles received resources. In an effective control environment, unauthorized loading activities would be detected and prevented through strong supervisory practices and regular audits.

b. Risk Assessment

Based on the findings, risk assessment accounted for 40 (17%) of the total internal control component deficiencies as shown in Table 1. Risk assessment requires organizations to execute a comprehensive evaluation to identify internal and external threats to the organization (COSO, 2013). The incidents involving military personnel receiving bribes, stealing fuel, selling fuel illegally, and failing to safeguard U.S. government property highlight a gap in the risk assessment process, which did not anticipate these internal threats. The secondary failures reveal additional layers of risk that were not planned for in the organization's risk assessment, specifically the willingness of military members to participate and join in fuel fraud schemes and the manipulation of fuel records within the chain of command.

(1) Primary Failures

The findings highlight that 25 (21%) of identified primary fuel control failures resulted in risk assessment deficiencies, shown in Figure 14. The following provides an analysis of the primary fuel control failures that were aligned to the risk assessment component.

The absence of risk planning for military members receiving bribes points to the organization's failure to recognize the influence of external pressures in a high-stakes environment like Afghanistan. Risk planning should have anticipated bribery as a possible risk, particularly given the incentives that can compromise personal integrity in conflict areas. Without this foresight, the organization lacked controls to deter or detect bribery, leaving personnel vulnerable to external influence without a plan for the threat.

The findings also indicate that the U.S. Army's risk assessment plan did not account for the possibility of internal fuel theft, missing an opportunity to implement safeguards around the asset. While external threats to fuel supplies may have been considered, the Army's risk assessment plan did not include the potential for personnel to misappropriate resources, particularly under conditions that could cause such behavior. This oversight left the organization without efficient deterrents or monitoring processes, likely causing fuel theft by military members to go undetected.

The organization's risk assessment failed to adequately plan for the potential for military personnel to sell fuel illegally. This incident not only was a failure of ethical standards but also compromised military operational readiness. An effective risk assessment would have planned for this possibility, prompting more measures to monitor and secure fuel distribution points. By not recognizing this risk, the organization left a vulnerability that allowed personnel to exploit fuel for personal gain, directly undermining operational objectives and facilitating fraud.

Lastly, the failure to plan for risks associated with safeguarding U.S. government property indicates an oversight in assessing both internal and external threats to U.S. government assets. Effective risk assessment should have strict plans in place for asset protection, ensuring that controls monitor personnel access and enforce accountability for resources. Due to the lack of this risk planning, personnel were left with insufficient

guidance or oversight regarding their responsibility to protect government property, increasing the likelihood of unauthorized use or negligence.

(2) Secondary Failures

The findings highlight that 15 (13%) of identified secondary control fuel failures resulted in risk assessment deficiencies, shown in Figure 15. The following provides an analysis of the secondary fuel control failures that were aligned to the risk assessment component.

Incidents of collecting bribes on behalf of other military personnel demonstrate a weakness in anticipating how ethical gaps might increase among personnel. The incidents of collecting bribes indicate not only a failure to plan for the risk of bribery but also an oversight in understanding how one individual's involvement could draw others into corrupt activities. Effective risk assessment should have considered the risk of collusion, pressure, and involvement within the ranks. The findings reveal that military members' willingness to accept bribes on behalf of fellow military members also highlights the lack of reporting options that might have been utilized by those being asked to aid in fuel fraud schemes.

Bringing other military members into the fuel theft scheme further underscores the lack of preventive measures to plan for internal schemes. The risk assessment process failed to prevent the spread of fraudulent behavior from one individual to another, leaving the organization vulnerable to systems of corruption that could more easily bypass controls. Preparing for this risk would have required a closer examination of the internal culture of military members and an understanding that unethical behavior can spread through influence or pressure.

Military members supervising the manipulation of TMRs highlights a breakdown in the reliability of the reporting and documentation processes. In a comprehensive risk assessment, the possibility of manipulation would be planned for in advance, resulting in specific controls that would be implemented to safeguard documentation processes and ensure that TMRs could not be easily manipulated. The lack of controls in this area allowed military personnel to oversee and support the falsification of records. Also, the

supervision of TMRs by fellow military members highlights the reoccurring issue of a risk assessment that did not consider the internal threat of soldiers' ethical breakdowns.

Lastly, instructing subordinates to falsify fuel records points to a failure in the organization's risk assessment. Not only did the risk assessment fail to identify the potential for record falsification, but it also failed to account for the influence of senior personnel over subordinates in continuing fraudulent activities. Effective risk assessment would include identifying risks associated with senior military influence and setting up precautions against the misuse of authority for illegal purposes.

c. Control Activities

Based on the findings, control activities accounted for 73 (73%) of the total internal control component deficiencies as shown in Table 1. Control activities include instituting policies and procedures that aid a company's leadership in successfully completing the entity's goals (COSO, 2013). An issue across these processes was the lack of segregation of duties, allowing individuals' unchecked control over multiple stages, which increased the risk of fraud. The gaps in both preventive and detective controls across these stages contributed to the widespread mismanagement and manipulation within fuel operations. Each failure underscores the need for stringent verification processes, segregation of duties, and regular audits to ensure the integrity of fuel control activities.

(1) Primary Failures

The findings show that 51 (43%) of identified primary fuel control failures resulted in control activity deficiencies, shown in Figure 14. The following provides an analysis of the primary fuel control failures that were aligned to the control activities component.

The failures and deficiencies in control activities over various stages of fuel processes in Afghanistan reveal vulnerabilities. The protocols for tracking fuel after it left the base likely lacked sufficient controls to maintain accountability and prevent diversion. Effective tracking measures, such as inventory reconciliation and GPS monitoring, were either insufficient or absent, leaving fuel susceptible to theft. Without these preventive

controls, fuel could be diverted without detection, and the absence of detective controls meant that fuel theft often went unnoticed until later, if it was noticed at all.

In the contract awarding process, limited vetting and a lack of review measures increased risks of bribery and unauthorized contract awards. A lack of control activities over which contractors received contracts and whether that contractor was realistically the best choice allowed military members to award contracts illegally. Military members circumvented the established contracting procedures allowing those participating in fuel fraud schemes to ensure the contractors had legitimate access to military bases and fuel. Thorough oversight from higher military personnel into contractor screening might have prevented contracting procedures from being bypassed in favor of specific trucking companies. Additionally, performance reviews and compliance checks were either ineffective or absent, making it difficult to identify and address fraudulent contractors once they were engaged in the fuel process.

The findings show that monitoring of vehicles entering and leaving the base also revealed control failures. The absence of preventive measures, such as vehicle checks, inspections, and escort requirements, weakened the effectiveness of control environment efforts. This absence left military bases vulnerable to unauthorized access, which aided in the number of fuel theft schemes. Controls, such as checkpoints, video surveillance, and entry–exit logs would have provided data to identify irregularities much quicker and possibly reduced the willingness of military members to participate in fuel fraud.

Lastly, tracking of fuel usage highlighted insufficient reconciliation and verification steps needed to cross-reference recorded and actual fuel consumption. Preventive controls, like fuel usage authorizations linked to specific operations or specific personnel, would have restricted access to authorized personnel only. Also, a lack of requiring dual verification for fuel records provided individuals the ability to manipulate records without being concerned that someone else would notice irregularities.

(2) Secondary Failures

The findings show that 22 (19%) of identified secondary fuel control failures resulted in control activity deficiencies, shown in Figure 15. The following provides an

analysis of the secondary fuel control failures that were aligned to the control activities component.

The issue of falsely certifying fuel transfers as complete highlights a lack of verification steps in the certification process. Effective control activities would require dual authorizations or independent verification by a separate military member or government contractor before certification, ensuring that reported transfers align with actual fuel deliveries. The weaknesses in control activities over fuel allowed military members to exploit weaknesses in the system resulting in losses of money, fuel, and reliability of the entirety of fuel records.

Another incident aligned to control activities was members selling fuel on the black market, which highlights a breakdown in controls over access and distribution. Strong preventive controls, like clear accountability for each stage of fuel handling and secure storage practices, would have restricted unauthorized access to fuel supplies. Additionally, detective measures, such as regular reviews of fuel distribution records and comparison of usage amounts, could have revealed unusual fuel consumption, indicating possible theft to oversight personnel.

Military members failing to download the full amount of fuel from delivery trucks points to inadequate supervision and reconciliation processes. Effective control activities would include checks by an independent observer or additional military member upon delivery and reconciliation of delivery amounts with purchase orders. Without preventive controls, such as accurate measurement tools at unloading points and detective controls, like after-the-fact reconciliation of expected versus received quantities, fuel would remain vulnerable to misappropriation.

The diversion of fuel off base further highlights the insufficient preventive measures in tracking and access controls over fuel. To prevent diversion, control activities should include documented protocols for vehicle movement, GPS tracking, and secure checkpoints. Additionally, detective controls, such as reviews of GPS records and comparison with authorized routes, would help identify any unauthorized diversions quickly.

Lastly, the false recording of delivered fuel quantities reflects a lack of integrity in recordkeeping and weak controls over record accuracy. Preventive measures should include the use of automated tracking systems to record actual delivery volumes, reducing reliance on manual input. Also, periodic audits and comparing fuel logs with inventory amounts could have identified inconsistencies in recorded versus actual amounts of fuel, which could have alerted military senior leadership to potential fraud.

d. Information and Communication

Based on the findings, information and communication accounted for 10 (4%) of the total internal control component deficiencies as shown in Table 1. Information and communication includes the information and sharing mechanisms, both internal and external, that a company must utilize to ensure success of the entity's goals (COSO, 2013). The small percentage of incidents that the information and communication component accounts for highlights the intentionality of the actions of the individuals involved in these schemes. Military members involved in the schemes were clearly aware of the procedures and took specific actions to go against operating procedures and break the law. Senior military leadership's failure to establish clear, protected lines of internal communication allowed individuals with fraudulent intentions to intercept and manipulate essential documentation. Without effective information and communication systems in place, the U.S. military inadvertently created opportunities for personnel involved in the fraud scheme to intercept fuel documents, conceal discrepancies, and perpetuate fuel fraud schemes.

(1) Primary Failures

The findings highlight that 1 (1%) of identified primary fuel control failures resulted in information and communication deficiencies, shown in Figure 14. The following provides an analysis of the primary fuel control failures that were aligned to the information and communication component.

The issue of fuel documents being collected by personnel involved in a fraud scheme rather than being submitted directly to supervisors highlights a failure in the information and communication component of internal controls. Effective internal

communication processes should ensure that critical documents, like fuel receipts and movement records, flow directly to designated oversight personnel, who can review them without interference. This process breakdown indicates that control responsibilities were either not clearly communicated across the organization or were intentionally circumvented, and staff members were either unaware of or disregarded the need to submit fuel documents to the proper individuals.

(2) Secondary Failures

The findings show that 9 (8%) of identified secondary fuel control failures resulted in information and communication deficiencies, shown in Figure 15. The following provides an analysis of the secondary fuel control failures that were aligned to the information and communication component.

The ability to report false reasons for increased fuel usage indicates a lack of accurate and transparent communication channels within the organization. If information on fuel usage trends and authorizations had been routinely collected, shared, and reviewed at multiple levels, discrepancies between reported reasons and actual operational needs could have been detected. The findings indicate an ineffective internal communication system that did not ensure that supervisors or higher miliary members regularly reviewed the authenticity and necessity of reported fuel increases.

The creation of TMRs in excess of requested amounts reveals inadequate information oversight and weak communication protocols within the U.S. military's control processes. The absence of clear communication channels to ensure TMR requests align with actual fuel requirements allowed for over-inflated requests to pass through unchecked, which likely compromised the integrity of fuel supply chain management and enabled fuel fraud incidents. Stronger internal communication also might have aided military members in reporting irregularities in fuel reports.

Lastly, the incidents of paying another soldier to illegally escort a fuel truck driver on and off base and load fuel into trucks highlights a breakdown in both internal and external communication mechanisms. Internally, there was a lack of clear messaging about the importance of following authorized access protocols and the reporting of

suspicious behavior. Internal communication might have resulted in gate guards reporting suspicious or illegal escorting of trucks to higher military members at bases. Also, an external communication channel could have provided an outlet for military members to report such misconduct without fear of reprisal.

e. Monitoring Activities

Based on the findings, monitoring activities accounted for 56 (24%) of the total internal control component deficiencies as shown in Table 1. Monitoring activities are the evaluations, both constant and isolated, that ensure the internal control system in place is operating as necessary for the success of the organization (COSO, 2013). The lack of properly implemented monitoring activities in the Afghanistan's fuel management process led to incidents that could have been prevented or promptly detected. Many of these incidents involved manipulation of fuel records and false reporting of fuel usage. These incidents could have been detected through routine checks of fuel management systems and uncovered problems with the monitoring activities before fuel fraud became widespread.

(1) Primary Failures

The findings show that 13 (11%) of identified primary fuel control failures resulted in monitoring activities deficiencies, shown in Figure 14. The following provides an analysis of the primary fuel control failures that were aligned to the monitoring activities component.

The issue of fuel transfers being falsely certified as completed highlights a breakdown in the monitoring activities of fuel systems. Effective monitoring would involve regular checks into the certification process, such as automated recording of fuel transfer data, providing real-time alerts if discrepancies arose. Without these incorporated evaluations, false certifications were able to proceed unchecked, allowing military members to take advantage of the system and continue fuel fraud. Also ensuring fuel transfers that were listed as completed were checked against the reported receiving command could have aided in monitoring that fuel being recorded as delivered was received by the listed entity.

Reporting false reasons for increased fuel usage further illustrates a lack of effective monitoring, as there were little or no evaluations to assess the accuracy of usage reports. Ongoing evaluations that flagged and scrutinized increases in usage would provide data to evaluate reported reasons against actual operational needs. In the absence of such measures, military personnel were able to report false reasons, and the lack of monitoring activities resulted in the inaccurate reasons being accepted as fact. Reviews of the reported increases could inform senior leadership and allow for corrective action or further investigation. Without these reviews, fraudulent reporting on fuel consumption could continue undetected.

The failure to download the full amount of fuel from trucks highlights a lack of monitoring activities during fuel receipt and distribution. The lack of oversight by an independent observer or secondary military member at delivery points would provide continuous data and help ensure fuel amounts were recorded accurately. Without these checks, monitoring relied on manual reports, which were vulnerable to manipulation, and separate evaluations alone could not provide adequate and timely insight to catch shortages immediately.

Lastly, the creation of TMRs in excess of the fuel requested highlights the need for better oversight in fuel requests and receipts areas. Ongoing evaluations that reviewed the alignment between TMRs and actual fuel needs would ensure that TMR being issued reflected accurate requirements. Effective monitoring activities, including both ongoing evaluations for immediate control and separate evaluations for general oversight, could help detect discrepancies. The absence of both continuous and periodic evaluations allowed these deficiencies to remain unaddressed, weakening the reliability of the fuel management process.

(2) Secondary Failures

The findings show that 43 (36%) of identified secondary fuel control failures resulted in monitoring activities deficiencies, shown in Figure 15. The following provides an analysis of the secondary fuel control failures that were aligned to the monitoring activities component.

One issue was the creation and acceptance of false TMRs. The creation and submission of a TMR, which was never requested, highlights an issue with the authorization needed to create and execute a TMR. Further monitoring of which military members were submitting TMRs and verifying the listed receiving command requested fuel could have alerted to some of the false TMRs. Evaluations within the TMR approval process, such as routine cross-checks with actual fuel requirements and authorizations, would provide validation of each request. Periodic audits of TMR creation patterns could further detect discrepancies over time, helping to uncover fraudulent or excessive requests.

Unauthorized personnel entering and exiting bases also highlights a failure in monitoring activities. Effective monitoring activities should include access controls and monitoring of who military members are vouching for on and off base. These ongoing evaluations would provide immediate alerts if unauthorized personnel attempted entry. Separate monitoring activities could periodically assess security records for gaps or anomalies.

Fuel being diverted reflects inadequate oversight during fuel transportation and offloading. Military members were able to divert fuel undetected, which highlights issues with tracking of amounts and location of fuel. Monitoring activities such as tracking fuel trucks' movements and fuel inventory verification would ensure that fuel is accounted for at every stage. Unannounced audits and spot checks on delivery records would further verify the accuracy of reports. Both types of evaluations could help identify any fuel that had been diverted, providing senior military leadership with timely information on where fuel losses occurred.

Lastly, the acceptance of false fuel documents by unapproved personnel to remove fuel from the base underscores the need for monitoring of fuel procedures. Military members participating in fuel schemes intentionally circumvented the established fuel procedures. Monitoring of which members signed fuel documents and whether those personnel were approved to be the signing authority could have highlighted issues with the fuel process. Periodic review of fuel documentation records could aid in alerting senior military leadership of personnel who were not following

procedures and alert to possible fuel fraud. Table 2 provides a summary of the internal control failures identified in this research study.

Internal Control Component (With Total # of Control Failures)	Key Internal Control Failures
Control Activities (73)	•Circumvention of contracting procedures •Insufficient reconciliation of fuel in tanks with records •Lack of protocols for tracking fuel after it left the base
Control Environment (57)	•Allowed fuel to be diverted •Tone at the top was insufficient to deter unethical actions •Concealment of illegal acts after the fact
Monitoring Activities (56)	•Falsely certified fuel tranfers as complete •Failure to download the full amount of fuel from trucks •Lack of oversight of fuel requests and receipts
Risk Assessment (40)	•Did not account for the possibility of internal fuel theft •Failed to plan for the potential for military personnel to sell fuel illegally •Absence of risk planning for military members
Information and Communication (10)	•Reported false reasons for increase in fuel "usage" •Created TMRs in excess of the fuel requested •Bypassed fuel reporting procedures

Table 2. Summary of Key Internal Control Failures

This section provided an analysis of the PFF Database and SFF Database. The following section discusses the implications of the results of this research study based on the findings and analysis.

C. IMPLICATIONS OF RESULTS

The implications of these results indicate a defective internal control system across all internal control components. Each component deficiency—control

environment, risk assessment, control activities, information and communication, and monitoring activities—highlights systemic weaknesses in leadership, oversight, and accountability. These deficiencies enabled widespread fuel fraud and fuel mismanagement, which compromised the resource of fuel and undermined the U.S. military's operational effectiveness, specifically the U.S. Army's fuel operations.

1. Compromised Operational Integrity and Resource Security

The control environment failures, specifically the lack of an ethical framework and weak tone at the top, provided an environment that perpetrated illegal incidents. This failure of leadership accountability created an environment where subordinates felt able to engage in fraud, compromise fuel supplies, and allow unauthorized access to restricted areas. As a result, operational security was significantly compromised and fuel, an essential resource, was misallocated, stolen, and sold on the black market. This undermined the availability of fuel, a critical operational asset, potentially jeopardizing mission readiness and safety.

2. Increased Risk of Conspiracies and Fuel Fraud Schemes

The ineffective risk assessment component failed to anticipate internal threats, such as bribery, collusion, and resource misappropriation by military personnel. Without recognizing these risks, the organization lacked preventative measures to deter or identify conspiracies among military personnel, allowing fraud networks to grow and involving multiple members in fuel fraud schemes. This not only amplified the scale of fraud but also made it more challenging to detect, as individuals could manipulate records, falsify documents, and hide illegal actions within the network of participating military members.

3. Decrease of Accountability and Transparency

Failures in control activities, specifically in tracking, verification, and segregation of duties, further decreased accountability. The absence of effective preventive and detective controls meant that fraud went undetected across fuel management system areas, such as the creation of TMRs and fuel transfers. By failing to enforce regular reconciliations, separate verifications, and dual authorizations, the organization allowed military personnel to take advantage of the system and commit fuel fraud. The

implications of these deficiencies increase the lack of accountability and highlight broader internal control weaknesses that could cause similar mismanagement in other areas.

4. Breakdown in Communication and Reporting Mechanisms

The weaknesses in the information and communication component highlights a breakdown in both internal and external reporting mechanisms, contributing to fraudulent actions being hidden. Military personnel involved in fuel fraud schemes intercepted documents and bypassed proper communication channels, indicating that established fuel reporting systems were either unclear or intentionally circumvented. Without clear and consistent communication procedures, senior military leadership could not receive accurate and timely information on fuel systems. The lack of communication allowed fuel fraud to continue unchecked and decreased the organization's transparency and reliability.

5. Failure to Detect and Address Fraud in a Timely Manner

The monitoring activities component's deficiencies highlight a lack of continuous oversight, fuel amount verification, and routine audits, all of which allowed fraudulent actions to increase. By failing to implement ongoing evaluations or perform periodic audits with adequate scope and frequency, the organization missed opportunities to detect fraudulent activities early. This failure resulted in delayed response times to fuel fraud, allowing fuel fraud schemes to continue undetected for extended periods of time. The continuation of the fuel fraud schemes caused increased financial loss and physical fuel loss and undermined efforts at damage control.

6. Strategic and Reputational Damage

The cumulative impact of these control failures likely undermines the U.S. military's credibility, both internally and externally. The inability to control and protect fuel, enforce ethical behavior, and monitor military personnel actions can decrease trust both within the military and among private American citizens and allied and partner nations. The strategic impact of these failings could reduce the U.S. military's effectiveness in future operations, affect funding, and require corrective measures.

Overall, these findings underscore the need for a thorough overhaul of internal controls, a strengthened ethical culture, and a more proactive approach to managing risk and accountability in conflict areas. These changes are essential to restoring operational integrity, securing resources, and reestablishing the credibility of the U.S. military necessary for mission success and confidence from other nations.

D. RECOMMENDATIONS BASED ON THE FINDINGS AND ANALYSIS

Addressing the implications requires a wide range of recommendations based on the findings and analysis. First, a stronger control environment must be established by reinforcing an ethical culture led by senior management, prioritizing transparency and accountability. Enhancing risk assessments is needed to consider internal threats and potential collusion, combined with improving control activities to incorporate stronger checks and balances, can mitigate vulnerabilities in the fuel management process. Additionally, improved information and communication channels must be introduced to prevent document interference and ensure accurate reporting of fuel amounts. Lastly, strong monitoring activities with routine evaluations and tracking will help detect irregularities quicker, allowing the organization to respond effectively to potential fuel fraud. The following sections discuss the five recommendations based on the findings and analysis.

1. Establish a Strong Ethical Framework and Tone at the Top

Leadership should prioritize establishing a strong ethical culture by openly communicating the importance of integrity, accountability, and compliance throughout the organization. This includes visibly exhibiting these values consistently and creating policies that support ethical behavior and discourage misconduct. Additionally, training programs focused on ethics, accountability, and anti-fraud measures should be developed for all military personnel, emphasizing the role each military member plays in maintaining control of all resources. Introducing a zero-tolerance policy for fraudulent or unethical actions, with clear and consistent consequences, will further deter misconduct by military members. By regularly reinforcing this policy, the U.S. military can build a control environment that discourages fraud and enhances ethical standards.

2. Enhance Risk Assessment to Address Internal Threats and Collusion

Expanding the risk assessment component to address internal threats, such as bribery, collusion, and fuel fraud by personnel, is essential to be better prepared to address these risks. A more thorough risk assessment will better prepare the organization to anticipate and mitigate weaknesses. This component should include means and practices for regularly reassessing risks, thereby allowing for adjustments to be made as new threats emerge.

3. Strengthen Control Activities with Verification and Oversight

Stronger verification and oversight are needed to strengthen control activities, especially in areas like fuel management. Automated tracking systems, such as GPS tracking for fuel shipments and automated fuel volume monitoring, will help reduce errors and prevent opportunities for fraud. Applying dual authorization and independent verification for fuel processes, such as TMR creation, fuel transfers, and contractor approvals, adds necessary checks and ensures that multiple military personnel review each transaction. Additionally, random checks on TMR documents and contract awards will help detect unauthorized or excessive requests and discourage fraudulent fuel activities.

4. Improve Information and Communication Processes

Developing a secure document submission process and ensuring the procedures for fuel documents are adhered to will prevent manipulation of fuel documents like fuel receipts and records. Additionally, establishing clear internal communication procedures that outline documentation and reporting procedures will ensure that personnel understand how and to whom they should provide fuel documents. This should include regular reminders and training on the importance of accurate information. Providing access to an external reporting mechanism will further encourage military personnel to report suspicious activity without fear of reprisal, enhancing transparency and decreasing the risk of potentially compromised internal reporting options.

5. Implement Stronger Monitoring Activities and Continuous Evaluations

Accurate monitoring tools such as stronger access control, badge scans, and increased surveillance at entry and exit points are necessary to prevent unauthorized personnel from accessing military bases with and without the help of military personnel and tampering with or stealing resources. Conducting periodic and unannounced audits of fuel usage, delivery, and inventory levels will help detect discrepancies early. Regular reconciliations between expected and actual fuel levels, as well as tracking all deviations from normal usage patterns, will help identify fraudulent activities before they can increase. Placing independent oversight personnel in charge of monitoring trends in fuel usage, TMR creation, and contractor activity will improve monitoring efforts. By highlighting irregular patterns for investigation, the U.S. military can implement an active stance in detecting and addressing potential fuel fraud.

E. SUMMARY

This chapter provided an analysis of the research findings, highlighting implications of the results. The analysis utilized two databases developed during the research for this study, PFF Database and SFF Database. Broader implications of the findings were addressed, offering insights into vulnerabilities and areas for improvement in the fuel control system. Based on the findings and analysis, the chapter provided targeted recommendations to address fuel control weaknesses. The following chapter discusses the summary, conclusions, and areas for further research based on the findings and analysis to address fuel control weaknesses.

V. SUMMARY, CONCLUSIONS, AND AREAS FOR FURTHER RESEARCH

This chapter provides a summary of this study's findings by giving an overview of the research conducted and the results collected. Conclusions are provided based on the research questions of this study. Lastly, potential areas for further research are provided to increase the understanding of fraud in conflict areas.

A. SUMMARY

The United States invested trillions of dollars in Afghanistan's reconstruction and development between 2001 and 2021. The funds were provided in an attempt to stabilize the nation and promote democracy in the area. However, widespread corruption and financial mismanagement plagued these efforts, resulting in numerous fraud cases, including the conviction of U.S. military members for their roles in fuel fraud schemes. Systemic failures in internal controls and oversight mechanisms were at the center of these issues, highlighting the need for improved financial management practices in conflict areas.

Auditability theory, specifically the auditability triangle, was utilized in this research study which encompasses the elements of "effective internal controls, competence personnel, and effective processes" (Rendon & Rendon, 2015, pg. 715). The auditability triangle component of effective internal controls was the focus of this research study. This study applied the COSO Framework to cases of fuel fraud in United States led Afghanistan reconstruction efforts, which aided in identifying deficiencies in the internal control systems over fuel operations in Afghanistan.

The purpose of this study was to analyze the fuel fraud cases within the Afghanistan reconstruction efforts through the lens of the COSO Internal Control Integrated Framework. This research found fuel fraud cases in which U.S. military members were participants, categorized each fuel fraud incident in those cases, identified the control failure within each fuel fraud incident, and aligned each control failure to a primary and secondary internal control component deficiency. The findings were compiled into two databases, the PFF Database and the SFF Database, which provided a

means for analyzing the way in which internal control failures contributed to systematic vulnerabilities over fuel in Afghanistan.

This research study uncovered deficiencies in the internal controls governing fuel management within the Afghanistan reconstruction efforts. The findings revealed weaknesses in oversight mechanisms, accountability, and fraud prevention measures, which allowed fuel fraud to increase. These weaknesses highlight broader issues with managing fuel within conflict zones, particularly in ensuring adherence with established internal control systems. Based on these findings, recommendations were provided to strengthen oversight, improve fraud detection and prevention mechanisms, and enhance the application of the COSO Framework in conflict areas.

B. CONCLUSIONS

The research study addressed three research questions, the answers to which are provided below.

1. Which internal controls were most frequently bypassed or compromised in cases of fuel theft and/or fraud in Afghanistan?

The most frequently bypassed internal control was aligned to control activities, specifically in the processes related to tracking, verifying, and securing fuel transfers. Military personnel exploited weaknesses in processes, such as the creation and approval of TMRs. TMRs, which authorized the movement of fuel, were often falsified, overstated, or approved without adequate oversight. This allowed individuals to divert large quantities of fuel for illegal purposes, often with little risk of detection. Weaknesses in verification processes, such as the absence of dual authorization or independent reviews, increased fuel fraud opportunities. For example, personnel were able to manipulate records of fuel deliveries and consumption without secondary checks to reconcile the reported and actual amounts. The lack of automated systems or accurate tracking tools also left the fuel transfer process susceptible to manual manipulation and intentional falsification.

Failures in monitoring activities further enabled the bypassing of controls. Insufficient oversight mechanisms meant that falsified records, excessive TMRs, and unauthorized diversions of fuel went unnoticed for extended periods. Routine audits, spot

checks, and reconciliations were either ineffective or inconsistently performed, allowing fraudulent schemes to continue. For example, unauthorized personnel often gained access to bases or fuel storage areas with the help of complicit military members, yet these security violations were rarely detected due to weak access controls and a lack of monitoring at entry points. These gaps in oversight not only enabled the theft of fuel but also provided a cover for continued fuel fraud activities.

The control environment also played a critical role in enabling the bypassing of internal controls. Leadership's failure to establish a strong ethical framework and enforce accountability created a culture in which fraudulent behavior was tolerated or overlooked. In some cases, military personnel instructed subordinates to falsify records or paid others to participate in fuel fraud schemes. This lack of ethical leadership and oversight might have tempted individuals to bypass controls, knowing there would likely be no consequences. Together, the issues with control activities, monitoring, and the control environment created an environment where fuel fraud could be executed and persistent.

2. Which COSO internal control components had the most fuel control failures?

The COSO internal control component with the highest number of fuel control failures was control activities, accounting for 73 incidents (73%) (Table 1) of total component failures. These failures were present in key operational processes, such as verifying fuel deliveries, monitoring fuel transfers, and issuing TMRs. Weaknesses in control activities included the absence of dual authorization for critical actions, insufficient reconciliation of fuel inventory, and poor contract oversight. The lack of automated systems to track fuel shipments and detect discrepancies also contributed to the high number of failures. This left gaps in accountability and allowed military personnel to exploit routine weaknesses to steal fuel and falsify records.

The second most frequently failing components were monitoring activities and the control environment. Monitoring activities accounted for 56 incidents (24%) (Table 1) of total component failures. Control activities accounted for 57 incidents (24%) (Table 1) of total component failures. Monitoring activities' deficiencies included a lack of continuous oversight mechanisms and insufficient periodic evaluations. This meant that fraudulent activities, such as the falsification of TMRs or unauthorized fuel diversions,

were not identified promptly, allowing schemes to persist over extended periods. The control environment also showed significant weaknesses, as leadership failed to create a culture of accountability and strong ethics. A permissive tone at the top meant that ethical misconduct, such as taking bribes or instructing subordinates to falsify records, was not deterred.

Additionally, risk assessment accounted for 40 incidents (17%) (Table 1) of total component failures, reflecting an underestimation of the internal risks posed by military personnel, such as collusion, bribery, and resource misappropriation. Finally, information and communication failures, while less frequent, accounted for 10 incidents (4%) (Table 1) of total component failures; this still contributed to the problem by enabling the concealment of fraudulent actions through the interception or manipulation of fuel documents.

The distribution of failures across the COSO Framework highlights the connection between internal control deficiencies within the five internal control components. While control activities were the most directly impacted, their effectiveness depended on the other components. For example, monitoring activities and risk assessment should have identified problems with control activities, such as unusual fuel patterns or discrepancies in fuel deliveries. Similarly, a strong control environment could have mitigated the fuel control frequency of failures in control activities by promoting ethical behavior and holding personnel accountable. The weaknesses of the information and communication component increased these failures by allowing fraudulent personnel to manipulate data and disrupt the flow of accurate information.

3. What were the primary methods used in fuel theft and/or fraud activities?

The primary methods used in fuel theft and fraud activities highlight a consistent exploitation of weaknesses in fuel management, distribution processes, and oversight mechanisms. One prevalent method involved military personnel deliberately allowing fuel to be diverted from its intended destinations, intentionally allowing unauthorized parties to access and misuse the fuel. Another common method to commit fuel fraud was military members fabricating false TMRs to account for stolen fuel, which allowed them to conceal their illegal activities. Another frequent practice was the direct diversion of

fuel by military personnel, who bypassed established procedures to redirect fuel to unauthorized locations and individuals.

Another common method used in the cases this research study reviewed was military personnel facilitating theft by assisting Afghan truck drivers to enter military bases and steal fuel, exploiting the lack of access controls and monitoring of individuals entering and exiting military bases. In addition to allowing unauthorized truck drivers on base, stolen fuel was also used to fill those unapproved vehicles. Additionally, falsified fuel documentation was provided to Afghan truck drivers, allowing them to exit the base with stolen fuel under the excuse of legitimate operations. This tactic not only facilitated fuel theft but also created an appearance of compliance with operating procedures that delayed detection efforts.

C. AREAS FOR FURTHER RESEARCH

The following are areas for which further research could increase the understanding of fraud in conflict areas:

1. Comparison Across Branches of the U.S. Military

Further research could examine fuel theft and fraud incidents across other branches of the U.S. military to identify similarities and differences in internal control deficiencies. Additionally, such research could explore whether the root causes of these deficiencies are linked to branch-specific operational procedures, resource controls, or overarching policy and oversight challenges throughout the Department of Defense. This could help determine whether the issues identified in this study are specific to the Army or represent general problems across all branches of the U.S. military.

2. Resource Fraud in Other Military Operations

Another area for further research could extend the scope of analysis beyond fuel to other mission-critical resources, such as medical supplies, food, or construction materials. Analyzing these resources would allow researchers to identify whether the vulnerabilities observed in fuel-related cases are prevalent throughout multiple areas of military logistics and resource management. This expanded focus could also provide

insights into whether internal control deficiencies vary by resource type or operational context.

3. Evaluation of Anti-Fraud Training Programs

Further research could evaluate the effectiveness of existing anti-fraud training programs within the military by examining their impact on improving awareness, understanding, and compliance with internal controls among military members. This research could include an analysis of training content, delivery methods, and frequency to determine whether these programs adequately address the root causes of fraud and theft. Additionally, this research could study how well these training programs prepare military members to identify and report fraudulent activities.

4. Analyzing Military Fraud Through the Fraud Diamond

Further research could focus on using the Fraud Diamond framework to explore the psychological and social factors that lead military personnel to engage in fraudulent activities. The study could examine how the elements of pressure or incentive, opportunity, rationalization, and capability contribute to fraudulent behavior in conflict zones. By applying the Fraud Diamond model, the research could provide a deeper understanding of the factors that bring about fraud within the military.

LIST OF REFERENCES

Accounting Insights. (2024, May 5). *Leveraging the fraud diamond to combat corporate fraud.* https://accountinginsights.org/leveraging-the-fraud-diamond-to-combat-corporate-fraud/#:~:text=The%20Fraud%20Diamond%20framework%2C%20by%20expanding%20on%20the,four%20key%20elements%3A%20opportunity%2C%20rationalization%2C%20pressure%2C%20and%20capability

American Institute of Certified Public Accountants. (2005). *Management override of internal controls: The Achilles' heel of fraud prevention.* AICPA.

Bureau of International Narcotics and Law Enforcement Affairs. (n.d.). *FY 2013 program and budget guide: Program overview*. Department of State. Retrieved August 22, 2024, from https://2009-2017.state.gov/j/inl/rls/rpt/pbg/fy2013/206612.htm

Candreva, P. J. (2006). Controlling internal controls. *Public Administration Review*, *66*(3), 463–465. https://doi.org/10.1111/j.1540-6210.2006.00602.x

Crawford, N. C., & Lutz, C. (2021, April 15). *Human and budgetary costs to date of the U.S. war in Afghanistan* [PowerPoint slides]. Watson Institute for International & Public Affairs. https://www.coso.org/_files/ugd/3059fc_ff11af647d0e433dac3eccfac3f8606a.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control – integrated framework: Executive summary.* https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2023). *Fraud risk management guide: Executive summary* (2nd ed.). https://www.coso.org/_files/ugd/3059fc_ff11af647d0e433dac3eccfac3f8606a.pdf

Department of Defense. (2009, January). Commanders' Emergency Response Program (CERP). In *Financial management regulation* (DoD 7000.14-R; pp. 27–1–27-15). https://comptroller.defense.gov/Portals/45/documents/fmr/archive/12arch/12_27_Jan09.pdf

Department of Defense Inspector General. (2017). *Combined Security Transition Command–Afghanistan improved controls over U.S.-funded Ministry of Defense fuel contracts, but further improvements are needed* (DODIG-2017-041). Department of Defense. https://media.defense.gov/2017/Dec/18/2001857911/-1/-1/1/DODIG-2017-041-REDACTED.PDF

Department of State. (n.d.-a). *Economic support fund*. https://2009-2017.state.gov/documents/organization/101425.pdf#:~:text=The%20Administration%E2%80%99s%20strategic%20priorities

Department of State. (n.d.-b). *Worldwide security protection*. https://2009-2017.state.gov/documents/organization/123557.pdf

Defense Security Cooperation Agency. (n.d.). *Afghanistan Security Forces Fund (ASFF).* Retrieved June 20, 2024, from https://www.dsca.mil/afghanistan-security-forces-fund-asff#:~:text=Purpose%3A,renovation%20and%20construction%2C%20and%20funding

Dickins, D., & Fay, R. G. (2017). COSO 2013: Aligning internal controls and principles. *Issues in Accounting Education*, *32*(3), 117–127. https://doi.org/10.2308/iace-51585

Division of Financial Services. (n.d.). *About the COSO framework.* Cornell University. Retrieved July 29, 2024, from https://finance.cornell.edu/controller/internalcontrols/cosoframework

Egel, D., Ries, P. C., Connable, B., Helmus, C. T., Robinson, E., Baruffi, I. … Stewart, R. (2016). *Investing in the fight: Assessing the use of the Commander's Emergency Response Program in Afghanistan* (Report No. RR1508-OSB). RAND. https://www.rand.org/pubs/research_reports/RR1508.html

Embroker. (2023, September 21). *What is the fraud triangle? (Three components explained).* https://www.embroker.com/blog/fraud-triangle/#:~:text=In%20the%201970s%2C%20criminologist%20Donald,motivation%2C%20opportunity%2C%20and%20rationalization

Executive Office of the President. (2016). *OMB circular no. A-123, management's responsibility for enterprise risk management and internal control* (M-16-17). Office of Management and Budget. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf

Executive Services Directorate. (2008). *Report on progress toward security and stability in Afghanistan*. Washington Headquarters Services. https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/10-F-0018_Report_on_Progress_Toward_Security_and_Stability_in_Aghanistan.pdf

Fourie, H., & Ackerman, C. (2013). The impact of COSO control components on internal control effectiveness: An internal audit perspective. *Journal of Economic and Financial Sciences*, *6*(2), 495–518. https://doi.org/10.4102/jef.v6i2.272

Government Accountability Office. (2009a). *Afghanistan: Key issues for congressional oversight* (GAO-09-473SP). https://www.gao.gov/assets/gao-09-473sp.pdf

Government Accountability Office. (2009b). *Afghanistan security: Lack of systematic tracking raises significant accountability concerns about weapons provided to Afghan National Security Forces* (GAO-09-267). https://www.gao.gov/assets/gao-09-267.pdf

Government Accountability Office. (2009c). *Military operations: Actions needed to improve oversight and interagency coordination for the Commander's Emergency Response Program in Afghanistan* (GAO-09-615). https://www.gao.gov/assets/gao-09-615.pdf

Government Accountability Office. (2012). *Defense management: Steps taken to better manage fuel demand but additional information sharing mechanisms are needed.* (GAO-12-619). https://www.gao.gov/assets/gao-12-619.pdf

Government Accountability Office. (2014). *Standards for internal control in the federal government* (GAO-14-704G). https://www.gao.gov/products/gao-14-704g

Government Accountability Office. (2021). *Afghanistan reconstruction: GAO work since 2002 shows systemic internal control weaknesses that increased the risk of waste, fraud, and abuse* (GAO-21-32R). https://www.gao.gov/assets/gao-21-32r.pdf

Government Accountability Office. (2024). *Standards for internal control in the federal government: 2024 exposure draft* (GAO-24-106889). https://www.gao.gov/products/gao-14-704g

Harte, J. (2015, May 5). *U.S. military personnel have been convicted of $50 million worth of crimes in Iraq and Afghanistan.* The Center for Public Integrity. https://publicintegrity.org/national-security/u-s-military-personnel-have-been-convicted-of-50-million-worth-of-crimes-in-iraq-and-afghanistan/

Hermanson, D. R., & Wolfe, D. T. (2024, June). The fraud diamond: A 20-year retrospective. *The CPA Journal*. https://www.cpajournal.com/2024/06/10/the-fraud-diamond/

InterAction. (n.d.). *Economic support fund*. Retrieved July 12, 2024, from https://www.interaction.org/choose-to-invest-fy-2022/development-assistance-economic-support-fund/economic-support-fund/

Machado, M. R., & Gartner, I. R. (2018). The Cressey hypothesis (1953) and an investigation into the occurrence of corporate fraud: An empirical analysis conducted in Brazilian banking institutions. *Revista contabilidade & finanças* [Accounting & finance review], *29*(76), 60–81. https://doi.org/10.1590/1808-057x201803270

Martins, M. (2005). The Commander's Emergency Response Program. *Joint Force Quarterly*, *37*, 46–52. https://apps.dtic.mil/sti/tr/pdf/ADA523853.pdf

Moeller, R. R. (2013). *Executive's guide to COSO internal controls: Understanding and implementing the new framework*. Wiley.

Office of Inspector General. (n.d.). *OIG oversight: USAID overview.* U.S. Agency for International Development. https://oig.usaid.gov/USAID

Office of Inspector General. (2023). *Inspection of the Bureau of International Narcotics and Law Enforcement Affairs*. Department of State. https://www.stateoig.gov/uploads/report/report_pdf_file/isp-i-23-08.pdf

Office of Public Affairs. (2014, December 8). *Defense contractor pleads guilty to major fraud in provision of supplies to U.S. troops in Afghanistan*. Department of Justice. https://www.justice.gov/opa/pr/defense-contractor-pleads-guilty-major-fraud-provision-supplies-us-troops-afghanistan

Office of the Secretary of Defense. (2017). *Justification for FY 2018 Overseas Contingency Operations (OCO) Afghanistan Security Forces Fund (ASFF).* Department of Defense. https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2018/FY18_ASFF_J-Book.pdf

Office of Special Projects. (2015). *Department of Defense spending on Afghanistan reconstruction: Contracts comprised $21 billion of $66 billion in total appropriations, 2002 – May 2014*. Special Inspector General for Afghanistan Reconstruction. https://www.sigar.mil/pdf/special%20projects/sigar-15-40-sp.pdf

Power, M. (1996). Making things auditable. *Accounting, Organizations and Society*, *21*(2/3), 289–315.

Rendon, R. G., & Rendon, J. M. (2015). Auditability in public procurement: An analysis of internal controls and fraud vulnerability. *International Journal of Procurement Management*, *8*(6), 710–730. https://hdl.handle.net/10945/62055

Special Inspector General for Afghanistan Reconstruction. (n.d.). *About SIGAR.* Retrieved May 3, 2024, from https://www.sigar.mil/about/#:~:text=Approximately%20%24147.71%20billion%20has%20been,narcotics%20and%20anti%2Dcorruption%20efforts

Special Inspector General for Afghanistan Reconstruction. (2009). *SIGAR enabling legislation (as amended).* https://www.sigar.mil/pdf/legislation/pl-110-181handout.pdf

Special Inspector General for Afghanistan Reconstruction. (2011). *Commander's Emergency Response Program in Laghman Province provided some benefits, but oversight weaknesses and sustainment concerns led to questionable and potential waste*. https://www.sigar.mil/pdf/audits/2011-01-27audit-11-07.pdf

Special Inspector General for Afghanistan Reconstruction. (2012a, January 30). *Quarterly report to the United States Congress.* https://www.sigar.mil/pdf/quarterlyreports/2012-01-30qr.pdf

Special Inspector General for Afghanistan Reconstruction. (2012b, October 30). *Quarterly report to the United States Congress.* https://www.sigar.mil/pdf/quarterlyreports/2012-10-30qr.pdf

Special Inspector General for Afghanistan Reconstruction. (2013). *Quarterly report to the United States Congress.* https://www.sigar.mil/pdf/quarterlyreports/2013-01-30qr.pdf

Special Inspector General for Afghanistan Reconstruction. (2014). *Quarterly report to the United States Congress*. https://www.sigar.mil/pdf/quarterlyreports/2014-10-30qr.pdf

Special Inspector General for Afghanistan Reconstruction. (2018). *Management and oversight of fuel in Afghanistan: DoD is taking steps to improve accountability, but additional actions are needed* (SIGAR 18–41-IP). https://www.sigar.mil/pdf/inspections/SIGAR-18-41-IP.pdf

Special Inspector General for Afghanistan Reconstruction. (2020). *Department of Defense: Implemented less than 40 percent of SIGAR'S audit and inspections recommendations and does not have a system for tracking them* (SIGAR 20–35). https://www.sigar.mil/pdf/evaluations/SIGAR-20-35-IP.pdf

Special Inspector General for Afghanistan Reconstruction. (2021a). *Fuel for the Afghan National Defense and Security Forces: Additional steps required for DoD to transition responsibilities to the Afghan government* (SIGAR 21–43). https://www.sigar.mil/pdf/evaluations/SIGAR-21-43-IP.pdf

Special Inspector General for Afghanistan Reconstruction. (2021b). *SIGAR financial audits: $494 million questioned because of insufficient supporting documentation or noncompliance with laws and regulations* (SIGAR 21–33). https://www.sigar.mil/pdf/evaluations/SIGAR-21-33-IP.pdf

Special Inspector General for Afghanistan Reconstruction. (2021c). *What we need to learn: Lessons from twenty years of Afghanistan reconstruction.* https://www.sigar.mil/pdf/lessonslearned/SIGAR-21-46-LL.pdf

Special Inspector General for Afghanistan Reconstruction. (2024). *Annual U.S. appropriations made available for Afghanistan reconstruction pre- and post-withdrawal – FY 2002 to June 30, 2024* [Data set]. https://www.sigar.mil/pdf/quarterlyreports/2024-07-30qr-f13.pdf

Weigand, H., Johannesson, P., Andersson, B., Bergholtz, M., & Bukhsh, F. (2013). Conceptualizing auditability. *Proceedings of the CAiSE'13 Forum, 998*, 49–56. https://ceur-ws.org/Vol-998/Paper07.pdf

Whitlock, C., Shapiro, L., & Emamdjomeh, A. (2019, December 9). The Afghanistan papers: A secret history of the war. *The Washington Post*. https://www.washingtonpost.com/graphics/2019/investigations/afghanistan-papers/documents-database/

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal,* 38–42.

Yellowbook-CPE. (2021, March 25). *COSO and the GAO Green Book are the same thing.* https://yellowbook-cpe.com/coso-and-the-gao-green-book-are-the-same-thing.html

Zeidan, A. (n.d.). *Withdrawal of United States troops from Afghanistan.* Britannica. Retrieved November 7, 2024, from https://www.britannica.com/topic/Taliban

Acquisition Research Program
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net