NPS-AM-26-001

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

A Critical Analysis of Material Weakness in the U.S. Navy's Assurance Reports from 2013 to 2022

December 2025

LT Daniel O. Ofuka, USN

Thesis Advisors: Dr. Juanita M. Rendon, Lecturer
Dr. Amilcar A. Menichini, Associate Professor

Department of Defense Management

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943

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 study examines a decade of Department of the Navy (DON) Statement of Assurance (SOA) reports from Fiscal Year (FY) 2013–2022 to determine why recurring material weaknesses persist despite reform efforts. Using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Integrated Framework and auditability theory, 122 material weaknesses were mapped to internal control components and assessed for persistence over time. These material weaknesses were cataloged in a structured database and analyzed via quantitative trend analysis and qualitative cross-component evaluation. The findings revealed recurring material weaknesses in five areas: Property, Plant, and Equipment (PP&E) accountability; feeder-system reconciliation; contract oversight; Corrective Action Plan (CAP) validation; and Information Technology (IT) access controls. These stem from decentralized execution, personnel turnover, and manual controls, highlighting systemic barriers to auditability within the DON. The findings also indicated that 50% of persistent deficiencies occurred in control activities, underscoring gaps in the implementation of processes. This study concluded that sustained audit readiness demands enterprise-wide process standardization, workforce stability, expanded automation, and enhanced leadership accountability. These recommendations provide a roadmap for durable DON internal control improvements and the Department of Defense's (DoD) clean audit goal.

THIS PAGE INTENTIONALLY LEFT BLANK

ABOUT THE AUTHOR

LT Daniel Ofuka is a Surface Warfare Officer. He was commissioned through the Officer Candidate School in February 2021. After which, he served as the Main Propulsion Officer and the Operations Intelligence Officer on board the USS William P. Lawrence (DDG 110). After graduating from the Naval Postgraduate School, he will report to the Surface Mine Warfare Development Center (SMWDC) in San Diego as the Admin Officer.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I am deeply grateful to my thesis advisors, Professor Juanita Rendon and Professor Amilcar Menichini, for their exceptional guidance, patience, and commitment throughout this journey. Professor Rendon, thank you for your consistent responsiveness and for so generously sharing your expertise, which greatly enhanced the quality and depth of my research. It has been a privilege and an honor to work closely with you, learning not only from your academic insight but also from your thoughtful approach to mentorship. Your encouragement, constructive feedback, and steady guidance have left a lasting impact on both this project and my professional development.

To my wife, Ruth, and my children, Jasmine and Denzel, I extend my heartfelt appreciation for your unwavering patience and understanding during the countless hours I devoted to writing, revising, and researching. Thank you for continually motivating me to remain focused and reminding me of the purpose behind this work. Your love, support, and sacrifices have been essential to completing this endeavor, and I am immeasurably grateful for the inspiration you have provided throughout this process.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-AM-26-001

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

A Critical Analysis of Material Weakness in the U.S. Navy's Assurance Reports from 2013 to 2022

December 2025

LT Daniel O. Ofuka, USN

Thesis Advisors: Dr. Juanita M. Rendon, Lecturer
Dr. Amilcar A. Menichini, Associate Professor

Department of Defense Management

Naval Postgraduate School

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

AFR	Agency Financial Report
BSO	Budget Submitting Office
CAP	Corrective Action Plan
CFO	Chief Financial Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DoD	Department of Defense
DON	Department of the Navy
DCMO	Deputy Chief Management Officer
ERP	Enterprise Resource Planning
ERM	Enterprise Risk Management
EY	Ernst & Young
FFMIA	Federal Financial Management Improvement Act
FMFIA	Federal Managers' Financial Integrity Act
FIAR	Financial Improvement and Audit Remediation
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GMRA	Government Management Reform Act
IRB	Institutional Review Board
NAS	Naval Audit Service
NDAA	National Defense Authorization Act
OIG	Office of Inspector General
OMB	Office of Management and Budget
PP&E	Property, Plant, and Equipment
SAC	Senior Assessment Council
SAT	Senior Assessment Team
SOX	Sarbanes-Oxley Act
SOA	Statement of Assurance

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Auditability is essential for ensuring transparency, accountability, and proper management of public resources within the U.S. Department of the Navy (DON). Despite years of reform efforts, the Department of Defense (DoD), under which the DON falls, remains the only major federal agency that has never received a clean audit opinion (U.S. Government Accountability Office [GAO], 2023a). To understand how this situation came about, it is essential to review the legislative and policy milestones that have shaped federal financial management. The foundation for modern federal financial reporting was established by two landmark laws: the Chief Financial Officer's Act (CFO Act) of 1990 and the Government Management Reform Act (GMRA) of 1994. These laws created uniform financial reporting standards, strengthened internal controls, and increased agency accountability (Colgren, 2019). Together, they built a framework for ongoing improvements in governance and compliance practices.

Momentum toward full audit readiness grew with the fiscal year (FY) 2010 National Defense Authorization Act (NDAA, 2009), which required the DoD to validate the audit readiness of its financial statements by September 30, 2017. To oversee this effort, the department established the Financial Improvement and Audit Remediation (FIAR; formerly Financial Improvement and Audit Readiness) Governance Board and the independent DoD Audit Advisory Committee, which provide strategic guidance on internal controls, audit processes, and financial management (NDAA, 2009). Within this regulatory framework, the Statement of Assurance (SOA) report became a key mechanism for assessing compliance with the Federal Financial Management Improvement Act (FFMIA) of 1996. The SOA report determines whether systems meet federal accounting standards and if corrective action is required when deficiencies are identified (Office of the Under Secretary of Defense [Comptroller], 2024).

Despite remediation efforts, the DON's SOA reports consistently show recurring weaknesses in financial management and internal control systems. These challenges stem

primarily from outdated business systems, as noted by the GAO (2023b). While the DoD has taken steps to retire legacy systems and develop audit roadmaps, the GAO's (2023a) assessments highlight gaps in execution, particularly the absence of a comprehensive department-wide plan to achieve a clean audit opinion. These deficiencies continue to undermine oversight, internal controls, and financial integrity.

Given this historical and regulatory context, this study examines the recurring material weaknesses identified in the DON's SOA reports from FY2013–FY2022. This period is particularly significant because it captures the decade following primary legislative mandates, including FY 2010 NDAA audit readiness requirement and spans multiple reform initiatives and internal control improvement campaigns. By analyzing these SOA reports, this research seeks to understand the underlying drivers, such as possible systemic process inefficiencies, technological limitations, and gaps in organizational accountability, that may have allowed these weaknesses to endure across multiple reporting cycles.

This study's objective is twofold: first, to trace patterns in the types of material weaknesses reported year over year, highlighting where corrective measures have succeeded and where they have repeatedly failed, and second, to connect these findings to broader challenges in defense financial management, such as outdated business systems, inconsistent oversight mechanisms, and the cultural barriers to sustained reform identified by the GAO (2023b). This longitudinal analysis offers a clearer picture of why auditability challenges remain unresolved despite billions invested in remediation efforts and decades of regulatory pressure.

B. PURPOSE OF THE RESEARCH

The purpose of this study is to identify recurring material weaknesses and significant deficiencies reported in the DON's SOA reports by conducting a 10-year analysis of SOA reports from FY2013–FY2022. The identified recurring material weaknesses will be aligned to the five COSO internal control components and to the three elements of the Audibility Triangle. By highlighting these ongoing challenges and systemic shortcomings, this study seeks to identify recurring challenges, identify gaps in

accountability, and propose practical solutions to improve internal controls and compliance with financial and operational standards.

The recurring material weaknesses documented in the DON's SOA reports highlight ongoing challenges in achieving audit readiness, even after decades of legislative and policy reforms. Although federal mandates, such as the CFO Act, GMRA, and NDAA, have established comprehensive frameworks for financial reporting and internal controls, the persistence of these weaknesses suggests deeper systemic and operational issues that remain insufficiently addressed. Understanding these weaknesses requires cataloging their frequency and examining the underlying causes and conditions that allow them to recur despite repeated remediation efforts.

This research analyzes a decade of DON SOA reports to identify patterns and root causes behind recurring material weaknesses. It aims to show how gaps in governance, internal control execution, and system integration contribute to ongoing auditability challenges. The findings could inform strategies to enhance financial management, strengthen oversight, and support the DoD 's pursuit of its first clean audit opinion.

C. RESEARCH QUESTIONS

This research addresses the following questions:

1. **What were the key themes identified over the ten-year analysis of DON's SOAs regarding the recurring material weaknesses??**
2. **How did the identified material weaknesses align to the five COSO internal control components over the ten-year analysis (FY 2013 – FY 2022) of DON's SOAs reports?**
3. **How did the identified material weaknesses map to the Auditability Triangle elements over the ten-year analysis (FY 2013 – FY 2022) of DON's SOA reports?**
4. **How did the identified recurring material weaknesses found in the DON's SOA over a ten-year period (FY 2013 – FY2022) align to primary and secondary COSO internal control components?**

D. METHODOLOGY

This study uses documentary analysis and established theoretical frameworks to identify recurring internal control material weaknesses and deficiencies in the DON. By

leveraging the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Integrated Framework (hereafter, the COSO Framework) and auditability theory, this study offers a systematic approach to categorizing and analyzing these material weaknesses and deficiencies. The methodology outlined in the following sections details the data sources, analytical steps, and tools utilized to identify long-term trends and assess systemic control weaknesses in the DON's financial management and internal control environment.

The DON's SOA reports from FY2013–FY2022, obtained from the DON website, served as the primary source, with the DON's Agency Financial Reports (AFR), also available on the DON website, serving as a supplementary source. The researcher created an Excel database. Each SOA report was reviewed to extract material weaknesses and related significant deficiencies, which were cataloged to highlight recurring themes and systemic issues in the DON's internal control and financial management processes. Each identified material weakness was then aligned to a corresponding component of the COSO Framework: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. Each identified material weakness was also mapped to a corresponding element of the Auditability Triangle: People, Processes, and Internal Controls, This classification enabled a focused analysis and comparison of recurring material weaknesses over 10 years.

The COSO Framework and the auditability theory were the theoretical foundations for this research and were used to evaluate the underlying causes of audit challenges. This model was used to identify whether recurring material weaknesses originated from personnel, processes, internal controls, or a combination of these factors. To identify key trends, material weaknesses were classified and quantified across the study period. The data was then visualized using line and pie charts in Excel, enabling clear comparisons of internal control challenges over time.

Additionally, a cumulative analysis was conducted by combining data from FY 2013– FY 2022, enabling an assessment of long-term trends and persistent vulnerabilities in the DON's internal control systems. This comprehensive approach allowed for an informed evaluation of these recurring challenges. It supported the development of

actionable recommendations to strengthen controls, improve accountability, and enhance operational effectiveness. This study did not involve human subjects or the collection of personal data, so the Institutional Review Board (IRB) determined that an IRB protocol was not required.

While the methodology outlined previously provides a structured approach to analyzing internal control challenges within the DON, it is important to acknowledge limitations that may affect the interpretation and generalizability of the findings. Recognizing these constraints helps frame the scope of this research and clarifies the context in which the conclusions should be understood.

E. LIMITATIONS OF THE RESEARCH

1. Limited Scope to the DON

This research is exclusively focused on the DON's SOA reports; therefore, the findings may not directly apply to other branches of the Department of Defense or to other government entities operating in different contexts. If the findings are applied to other agencies, they would have to be approached with this consideration.

2. Reliance on Existing Data

This research relies on the quality and accuracy of the DON's past SOA reports; therefore, this research may contain limitations or inconsistencies in how material weaknesses and significant deficiencies were collected, analyzed, documented, and reported over the 10 year period. An analysis of individual FYs with respect to the methods used to categorize and collect material weaknesses may be required to obtain a more accurate representation of the findings.

3. External Factors

This study may not fully account for external factors. External factors may include shifts in political leadership, funding constraints, or unexpected global events (e.g., pandemics) that could have affected the implementation of the DON's internal controls. Events such as the recent COVID pandemic may have significantly affected SOA reports

during the period when the pandemic was at its peak and global working conditions were disrupted. The data collected during this period may also have been skewed.

4. Potential for Missing Unreported Issues

This research relies on public reports, so it may not reflect unreported issues or those considered less significant, even if they still affected the DON's operations. Although no unreported issues were identified in the reports, factors such as human error and turnover could have still led to unreported or missed information.

5. Implementation Challenges

This study proposes actionable recommendations based on the findings. However, there may be some limitations to the practical application due to resistance to change, budget constraints, or organizational inertia within the DON.

F. IMPORTANCE OF THE RESEARCH

This research addresses critical accountability and governance challenges within the DON. Through comprehensive data analysis, decision-makers can gain a deeper understanding of the underlying issues affecting financial reporting, internal controls, and auditability that have been identified but remain insufficiently addressed, thereby supporting more informed policy decisions. These findings could offer practical solutions to address critical material weaknesses and enhance mission readiness.

In contrast to studies that focus solely on achieving a clean audit through process improvements and increased compliance, this research explores material weaknesses that persist despite ongoing remediation efforts. It highlights the relationship between these recurring issues and the DON's audit readiness, offering recommendations for sustainable improvement and compliance with regulatory standards. To contextualize these insights, the study is organized into a logical sequence of chapters that progress from background analysis to data interpretation and final recommendations. The importance of this research is that it provides actionable insights into the DON's material weaknesses and deficiencies undermining audit readiness offering a foundation for sustainable internal control reform and evidence-based policy decisions.

G. BENEFITS OF RESEARCH

1. Improve Accountability and Internal Controls

This research provides valuable insights into recurring material weaknesses and deficiencies. The findings of this study may help the DON identify gaps in its internal control systems and enable it to take targeted corrective actions.

2. Enhance Data-Driven Decision-Making

This study analyzes 10 years of data to equip decision-makers with a comprehensive understanding of trends and challenges. This may enable them to make more informed policy decisions.

3. Propose Actionable Solutions

The findings propose specific, actionable solutions to enhance the DON's internal controls and overall operational integrity. This could positively impact short-term and long-term DON operations.

4. Enhance Policy Compliance

This study aligns DON operations with regulatory standards and Office of Management and Budget (OMB) directives. This may enhance compliance and accountability in the DON.

5. Contribute to Broader Research

These research findings could extend beyond the DON to other public sector organizations. This study may provide a framework for tackling similar material weaknesses and deficiencies in different government agencies.

H. ORGANIZATION OF THE STUDY

This study is comprised of five chapters. Chapter I introduces the background of financial management and internal control requirements within the DON, emphasizing the significance of the SOA reports and AFRs. It outlines the legislative mandates and policy directives that established the DON's current accountability and audit readiness practices. Chapter II provides a review of the theoretical foundations and relevant literature, including

scholarly research and federal guidance on internal control frameworks, auditability, and recurring material weaknesses in the DON. Chapter III presents a description of the methodology, detailing the collection and analysis of data from the DON's SOA reports and outlining how material weaknesses and significant deficiencies were categorized and aligned with the COSO Framework and the Auditability Triangle. Chapter IV presents the research findings, identifying patterns in recurring material weaknesses and examining their implications, followed by recommendations to address systemic issues revealed through the analysis. Chapter V concludes the study by summarizing key findings, addressing the research questions, and identifying opportunities for future research to strengthen financial management and audit readiness.

I. SUMMARY

This chapter established the historical and regulatory context underlying the DON's audit challenges by highlighting key legislative acts that shaped federal financial oversight and stating the relevance of the SOA reports in revealing recurring material weaknesses and their implications for audit readiness. It defined the purpose of the research, presented four guiding research questions, and detailed the methodology anchored in the COSO Framework and auditability theory while acknowledging limitations related to data scope, reporting inconsistencies, and external influences. This chapter also underscored the critical role of financial accountability amid evolving defense challenges and articulated the importance and benefits of this research. It concluded by previewing the study's structure and transitioning into the literature review, which situates this analysis within the wider discourse on federal financial management, internal control evaluation, and audit readiness.

II. LITERATURE REVIEW

A. INTRODUCTION

This chapter establishes the theoretical and regulatory foundation for analyzing the DON's internal control environment and recurring material weaknesses. It begins by reviewing the evolution of federal financial management legislation and policy guidance that define accountability standards across federal agencies. The discussion then explores key frameworks for assessing audit readiness and internal control effectiveness. Drawing on both government and academic literature, the chapter highlights how these models contribute to understanding the causes of persistent material weaknesses and the mechanisms for remediation. Collectively, these elements provide the conceptual structure for interpreting trends in the DON's SOA reports, which form the empirical basis of this study.

Achieving financial accountability in the DON depends on a comprehensive approach that integrates internal controls, transparent reporting, and consistent oversight. Legislative mandates such as the Federal Managers' Financial Integrity Act (FMFIA) of 1982 and the CFO Act of 1990 significantly advanced federal financial management, strengthened internal control assessments, and improved public accountability (OMB, 2000). These reforms, reinforced by guidance such as OMB Circular A-123 and the *Standards for Internal Control in the Federal Government* (hereinafter, the "Green Book"), institutionalized agency-wide evaluations of internal controls and the disclosure of material weaknesses (Comptroller General of the United States, 2013).

Prior literature further underscores the importance of comprehensive internal controls, rigorous audit standards, and effective risk management in improving audit readiness and ensuring reliable financial reporting (COSO, 2013; GAO, 2023a; McGivern, 2024). Theories of auditability, including the Auditability Triangle, provide frameworks for evaluating and enhancing organizational preparedness by examining personnel, processes, and internal control structures (Rendon & Rendon, 2015). When combined with

government and industry standards, these conceptual models inform strategies for addressing material weaknesses and strengthening financial integrity.

To frame the scope of this research, the following section presents an examination of the key documents and theoretical frameworks that shape the DON's financial oversight environment and underpin the analysis of recurring material weaknesses presented in this study.

B. THEORETICAL FOUNDATIONS

Examining the DON's persistent internal control material weaknesses requires a grounding in established theoretical frameworks. Central among these is the COSO Framework, widely recognized for its comprehensive structure that guides the design and evaluation of internal controls (see Figure 1). The COSO Framework is regarded as foundational because it defines how organizational governance interacts with internal controls and risk management, thus directly influencing financial accountability and compliance (Mohammed et al., 2021; Rae et al., 2017).

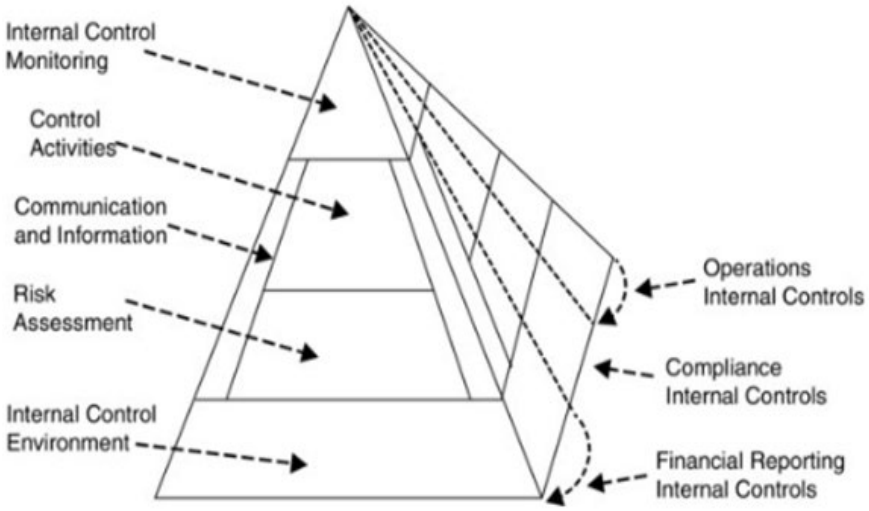

Figure 1. Internal Control Pyramid. Source: Moeller (2013).

Furthermore, the auditability theory, especially as outlined in the Auditability Triangle by Rendon and Rendon (2015), emphasizes the importance of aligning skilled personnel, standardized processes, and strong internal controls. Empirical evidence

suggests that adequate information flows, clear communication, and rigorous monitoring significantly enhance an organization's auditability and compliance readiness (Rae et al., 2017). Therefore, these theoretical models offer essential analytical perspectives for diagnosing systemic issues within the DON's internal control systems. The following section discusses the COSO Framework.

1. COSO Internal Control Integrated Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed the *Internal Control Integrated Framework* in 1992 to establish a comprehensive model for designing, implementing, and evaluating internal control systems across both public and private organizations (COSO, 2013). The framework was updated in 2013 to reflect evolving business risks, technological advancements, and governance expectations, making it the global benchmark for assessing internal control effectiveness (COSO, 2013). Based on the COSO Framework, internal control represents the collective actions and routines of leaders and employees that support confidence in achieving organizational goals related to day-to-day operations, the reliability of reporting, and adherence to applicable rules and requirements.

While COSO provides the overarching structure for assessing internal controls, the Green Book, adapts COSO's principles specifically for federal agencies, aligning them with accountability requirements under the Federal Managers' Financial Integrity Act (FMFIA). The Green Book serves as the federal government's authoritative source for internal control standards and will be discussed in detail in a subsequent section of this chapter.

The five components of the COSO Framework are highlighted in the next section. In addition to these five components, the COSO also lists 17 principles that provide depth to them (see Table 1).

a. Control Environment

Adequate internal controls are essential for reducing operational and financial risks within federal agencies, and their foundation lies in a strong control environment. Research consistently emphasizes the vital role of a strong control environment as the foundation for

adequate internal controls (GAO, 2023a). Specifically, leadership integrity, clear ethical standards, and an organizational culture that actively encourages compliance significantly increase the chances of successful internal control implementation and improved organizational performance (Zahari et al., 2024). Zahari et al. (2024) demonstrated through empirical analysis that, among the COSO components, the control environment, which reflects management's commitment and ethical tone, has the most significant positive impact on public organization performance. This component sets the organizational tone, shaping ethical conduct, establishing governance expectations, and reflecting leadership's commitment to integrity (COSO, 2013). Zahari et al. (2024) demonstrated that leadership integrity, ethical clarity, and a compliance-oriented culture significantly enhance internal control effectiveness and public sector performance. Their analysis confirmed that management's ethical tone has the strongest positive effect on performance among all COSO elements.

Similarly, Ramos (2008) emphasized that fostering integrity and accountability at the leadership level is crucial to establishing sustainable internal controls, particularly within large organizations such as the DoD. These findings reinforce that internal control success begins with leadership behavior and institutional culture, rather than relying solely on procedural mechanisms.

While cultural and ethical foundations are integral to a successful control environment, the regulatory environment also influences the strength and sustainability of the control environment. Schantl and Wagenhofer (2020) found that internal control systems perform best when enforcement strategies are balanced moderately; they concluded that strict penalties tied to actual manipulation cases lead to better compliance and financial integrity. Conversely, overly harsh penalties or aggressive enforcement can provoke defensive behaviors that weaken compliance (Schantl & Wagenhofer, 2020). Regulatory frameworks such as the Sarbanes-Oxley Act and the Securities and Exchange Commission guidelines aim to establish this balance in enforcement strategies (Ramos, 2008).

b. Risk Assessment

Risk assessment is a critical component of the internal control system, requiring organizations to identify, evaluate, and respond to risks both internally and externally that could compromise the achievement of operational, reporting, or compliance objectives (COSO, 2013). This includes setting clear goals, determining specific risks to those goals, evaluating potential fraud risks, and accounting for changes that may affect the effectiveness of internal controls over time (Mohammed et al., 2021). Fraud risk assessment plays a crucial role in understanding how incentive structures, pressures, or opportunities may lead to misconduct, particularly in large and complex environments such as the DON (Rendon & Rendon, 2015). Inadequate risk identification, such as underestimating the threat of outdated information technology (IT) systems or weak financial reconciliation processes, has repeatedly resulted in material weaknesses in the DON's SOA reports and audit findings from FY2013–FY2022. Risk assessment must be dynamic, forward-looking, and tied closely to institutional objectives and changing operating conditions.

Furthermore, risk assessment is interdependent with the broader control environment and must be informed by the organization's tone at the top. A leadership culture that values integrity, oversight, responsibility, and accountability directly strengthen the risk assessment process by fostering transparency in identifying and reporting emerging threats (COSO, 2013; Mohammed et al., 2021). Without a clearly established authority structure and a commitment to ethical performance, risk assessments may become reactive or superficial. When paired with other components such as control activities that address identified risks, communication systems that ensure risk data flows internally and externally, and monitoring functions that validate responses, risk assessment becomes part of a continuous, iterative internal control process (Rae et al., 2017). Risk assessment serves as a central diagnostic function within the COSO Framework, influencing and being influenced by leadership, control actions, and feedback mechanisms (Rae et al., 2017).

c. Control Activities

Within an internal control system, control activities function as the formal actions and guidance used to respond to known risks and to support reliable execution of leadership directives at every organizational level. (COSO, 2013). These include segregation of duties, proper authorizations, reconciliations, and documentation, all of which help reduce the risk of fraud, error, and operational inefficiency. Control activities also contribute to achieving organizational goals by reinforcing consistency and reliability in daily operations. Empirical research suggests that control activities are not isolated but are interlinked with other COSO components, particularly risk assessment and monitoring, which collectively support the quality of internal oversight and governance (Mohammed et al., 2021; Rae et al., 2017).

Beyond traditional practices, control activities encompass the development of supervisory mechanisms, the implementation of general IT controls, and the creation of actionable, standardized institutional policies (Rae et al., 2017). Rae et al. (2017) used structural equation modeling support to show that control activities are both influenced by and contribute to other COSO components, particularly through their reciprocal associations with risk assessment and information and communication processes, suggesting that internal controls are not linear but rather iterative and context dependent. These findings underscore the importance of organizations like the DON to viewing control activities as part of an integrated, dynamic system that supports monitoring and fosters effective corporate governance.

d. Information and Communication:

The information and communication component of internal control ensures that relevant, timely, and accurate information flows throughout the organization to support decision-making, risk management, and accountability (COSO, 2013). Effective internal controls rely on clear communication of responsibilities, expectations, and feedback, both vertically and horizontally.

Within this component, organizations must gather and disseminate information internally to personnel at all levels, ensuring they have the necessary knowledge to carry

out their internal control responsibilities. Externally, communication with oversight bodies, regulatory agencies, and stakeholders is essential for maintaining transparency and compliance (COSO, 2013). As Mohammed et al. (2021) explained, the use of relationship-based and relevant information enhances the integration of control functions and supports alignment across the other COSO components, including risk assessment and control activities.

According to Rae et al. (2017), aspects of information and communication, such as information accuracy, openness, and feedback flow, are directly associated with improved risk assessment and indirectly strengthen the control environment. Their structural equation modeling revealed that communication quality facilitates reciprocal relationships among internal control elements, thereby reinforcing the COSO Framework's dynamic, iterative nature (Rae et al., 2017). Within the DON and other federal organizations, robust internal communication ensures that audit findings, performance evaluations, and control updates are effectively transmitted and acted upon, reducing the risk of recurring material weaknesses (GAO, 2023b). Ultimately, the effectiveness of the entire internal control system depends on the integrity and responsiveness of its information and communication pathways.

e. Monitoring Activities

The monitoring activities component involves continuous and periodic evaluations to determine whether internal controls are appropriately designed, implemented, and operating effectively over time (COSO, 2013). These assessments, which fall under an organization's accounting system, are critical for detecting control failures, identifying deficiencies, and ensuring timely corrective action. Monitoring may be conducted through formal mechanisms such as internal audits, program evaluations, and supervisory reviews, as well as informal procedures embedded in day-to-day operations (COSO, 2013). The goal is not only to identify control weaknesses but also to foster a culture of accountability and continuous improvement throughout the organization.

Monitoring serves as the feedback loop of the COSO Framework, ensuring that control activities remain relevant and responsive to organizational risks. According to

Mohammed et al. (2021), monitoring activities are enhanced when supported by practical information and communication systems, enabling timely identification and reporting of deficiencies. Additionally, Rae et al. (2017) found that strong reciprocal associations exist between monitoring, risk assessment, and control activities, emphasizing that monitoring does not operate in isolation but is deeply interconnected with other internal control components (Rae et al., 2017). For example, poor risk identification or weak communication flow can undermine the ability of monitoring systems to detect emerging issues. In the DON, continuous monitoring through tools such as the SOA reports have been instrumental in tracking persistent material weaknesses and guiding reform initiatives (DON, 2015b). Ultimately, effective monitoring ensures that internal controls evolve with the organization's objectives, risks, and operating environment.

Table 1. COSO Internal Control Principles. Source: Moeller (2013)

Control Environment
1. Commitment to integrity and ethical values.
2. Independent board of directors' oversight.
3. Structures, reporting lines, authorities, and responsibilities.
4. Attract, develop, and retain competent people.
5. People held accountable for internal control.
Risk Assessment
6. Clear objectives specified.
7. Risks identified to achievement of objectives.
8. Potential for fraud considered.
9. Significant changes identified and assessed.
Control Activities
10. Control activates selected and developed. 11. General IT controls selected and developed.
12. Controls developed through policies and procedures.
Information and Communication
13. Quality information obtained, generated, and used.
14. Internal control information internally communicated.
15. Internal information externally communicated.
Control Activities
16. Ongoing and/or separate evaluations conducted.
17. Internal control deficiencies evaluated and communicated.

Together, the five COSO components form a holistic system that, when effectively implemented, supports operational integrity and audit readiness. Within the DON, however, recurring deficiencies in areas such as property accountability, contractor oversight, and financial reporting indicate breakdowns in one or more COSO components. By mapping these control failures to the COSO Framework components, this study seeks to provide a structured assessment of where internal control vulnerabilities persist and why corrective actions have often proven insufficient over time. The following section discusses the Auditability theory and the Auditability Triangle .

2. Auditability Theory and the Auditability Triangle

While the COSO Framework defines what an effective internal control system should look like, auditability theory examines whether an organization's operations and systems are capable of being audited (Rendon & Rendon, 2015). Developed in the context of organizational transparency and oversight, auditability theory focuses on the degree to which processes, records, and workforce responsibilities are clearly documented, consistently followed, and open to independent verification (Rendon & Rendon, 2015).

Auditability theory provides a conceptual foundation for evaluating whether an organization's operations and systems are structured to allow them to be independently verified and assessed. Rather than focusing solely on the presence of controls, this theory examines the degree to which organizational processes are transparent, workforce responsibilities are clearly defined, and records are both accurate and accessible. According to Rendon and Rendon (2015), auditability is achieved when skilled personnel, standardized processes, and effective internal controls operate in concert to ensure that financial and operational data can withstand external scrutiny.

This approach shifts the focus from compliance checklists to structural readiness, requiring that information flows are complete and traceable across all levels of the organization. Empirical research supports this perspective, demonstrating that adequate documentation, communication, and oversight mechanisms are crucial in mitigating material weaknesses and enhancing audit preparedness (Rae et al., 2017). Within the DON, the persistence of recurring control deficiencies in property management, contractor oversight, and financial reporting highlights the importance of applying this theoretical lens to identify root causes rather than treating symptoms through isolated corrective actions.

The Auditability Triangle (see Fig. 2), which visualizes this theory, frames personnel, processes, and internal controls as mutually reinforcing components of audit readiness (Rendon & Rendon, 2015). Although the auditability theory provides additional insight into this study, the focus of this research is on the internal control component of the Auditability Triangle. The following are the three components of the Auditability Triangle.

a. Personnel

First, the personnel component of the Auditability Triangle underscores the importance of having a competent, well-trained, and ethically grounded workforce to execute procurement and financial responsibilities effectively (Rendon & Rendon, 2015). This is critically essential in a government establishment such as the DON, where there is typically high turnover and personnel must keep pace with evolving technology and multiple database management systems. Implementing a robust internal control process requires key personnel, such as program managers, contracting officers, finance managers, and technical experts, to be fully qualified and familiar with the nuances involved in daily operations. As noted by Rendon and Rendon (2015), personnel competence includes not only technical knowledge but also the formal education, practical experience, and specialized training required to navigate complex procurement regulations and systems.

Empirical data on fraud risk and internal control weaknesses further reinforce the criticality of personnel competence. According to the Association of Certified Fraud Examiners (ACFE, 2012), a lack of internal controls was the most frequently cited weakness exploited by employees (34%) and managers (29%) involved in occupational fraud. Among owner/executive-level perpetrators, 23% of the cases involved a poor tone at the top, an issue deeply tied to leadership accountability and ethical culture (ACFE, 2012, p. 43). Notably, the override of existing internal controls was a common issue across all levels, cited in 23% of employee and manager cases, and 20% of owner/executive cases (ACFE, 2012, p. 43). These findings highlight how deficiencies in personnel competence and ethical conduct can directly translate into systemic vulnerabilities, particularly when individuals are either untrained, unsupervised, or capable of bypassing control mechanisms. This underscores the need to invest in both technical and ethical training for all personnel levels, from frontline employees to senior executives (ACFE, 2012).

For the DoD, personnel requirements are established and standardized through the Defense Acquisition Workforce Improvement Act (DAWIA), which provides structured career development pathways and mandates certification based on functional roles (Rendon & Snider, 2008). This framework ensures that acquisition professionals meet minimum competency thresholds appropriate to their responsibilities, thereby reducing operational

risk and improving contract performance. DAWIA's institutionalization of certification and continuous learning reinforces the DoD 's commitment to building and maintaining a capable acquisition workforce aligned with organizational objectives and governing directives.

Furthermore, personnel competence directly supports organizational auditability by reducing the likelihood of process failures and reinforcing consistent, transparent execution across the procurement life cycle. Rendon and Rendon (2015) argue that a knowledgeable workforce enhances the reliability of internal controls, enables better documentation and oversight, and facilitates audit readiness. When personnel lack the required qualifications or fail to adhere to ethical standards, the organization becomes more vulnerable to material weaknesses, compliance violations, and operational inefficiencies. Thus, ensuring that personnel meet clearly defined competency standards is not merely a human resources function but rather is a strategic imperative for effective governance, auditability, and mission success.

b. Processes

Second, the process component of the Auditability Triangle addresses the maturity and institutionalization of best practices throughout the operational life cycle, including planning, solicitation, contract administration, and closeout (Rendon & Snider, 2008). These phases must be guided by documented procedures, standardized templates, and consistent review mechanisms to ensure transparency, accountability, and alignment with the mission. Without structured processes, procurement activities are vulnerable to inconsistencies, cost overruns, and even fraud (Rendon &Rendon, 2015). Federal agencies such as the DON, where procurement dollars are closely scrutinized, require mature processes that are traceable, reduce discretion, and serve as a bulwark against operational inefficiencies and ethical lapses.

The importance of having mature and standardized processes cannot be overstated. Raymond (2008) and Hong and Kwon (2012), *as cited in* Rendon and Rendon (2015), argue that process maturity is fundamental to public trust and effective oversight. As the Department of the Navy (DON) evolves to incorporate lessons learned and industry best

practices, it becomes better equipped to interpret risk signals, apply internal policies consistently, and respond to anomalies with agility. This iterative development fosters institutional learning, enhances interdepartmental coordination, and reduces the risk of audit findings resulting from process ambiguity or inconsistency.

Importantly, mature processes are not only essential for execution but also critical to the fraud detection and prevention infrastructure**.** According to the ACFE (2012), despite the rise of advanced detection technologies, most occupational fraud continues to be uncovered through basic organizational processes, specifically through internally governed mechanisms that enable observation, reporting, and accountability (ACFE, 2012). In the ACFE's 2012 *Report to the Nations on Occupational Fraud and Abuse*, 42% of occupational fraud cases were initially detected through tips, a number nearly three times that of any other detection method (p. 22). While the emphasis here is not on the tips themselves, the processes that make tips effective, such as structured intake, impartial evaluation, protected whistleblower channels, and routine escalation protocols, must be formalized, well-understood, and immune to manipulation. Without mature organizational processes to channel and act on signals of misconduct, even the most accurate information can be rendered ineffective. Thus, process maturity is not merely a technical or bureaucratic concern; it is the operating system through which an organization enforces integrity, transparency, and audit readiness.

c. Internal Controls

Third, the internal controls component of the Auditability Triangle encompasses the mechanisms and policies that ensure compliance with statutory requirements, safeguard organizational assets, and detect systemic deficiencies (Rendon & Rendon, 2015). Within this model, internal controls are not isolated compliance tools but a central element of auditability. When designed and executed effectively, internal controls help organizations minimize financial misstatements, detect anomalies, and promote transparency across procurement, accounting, and operational domains. However, internal controls alone are not sufficient to guarantee fraud prevention. According to the ACFE (2012), even organizations with formal anti-fraud frameworks remain vulnerable. In its 2012 *Report to*

the Nations on Occupational Fraud and Abuse, the ACFE found that 29% of occupational fraud cases stemmed from a lack of internal controls, and 20% were caused by overrides of existing controls, together accounting for nearly half of the incidents analyzed (p. 34). These findings highlight that the mere presence of control mechanisms does not equate to effectiveness; cultural reinforcement, leadership accountability, and routine evaluation must also be present.

Moreover, fraud does not arise in a vacuum; it often thrives in environments where oversight mechanisms are inconsistently enforced or culturally deprioritized. The ACFE (2012) report emphasizes that while many organizations implement controls to prevent, detect, or mitigate fraud, the success of these measures depends on their effective execution, adaptability, and integration into daily operations**.** Controls must not be static or performative; they should evolve with emerging threats and align with broader organizational strategy. The ACFE (2012) further encouraged benchmarking internal control environments against those of peer institutions to identify vulnerabilities and adopt industry best practices (p. 34). Within the DON, where complex procurement and logistics systems interface with national security priorities, embedding internal controls into the organizational culture is not simply best practice; it is essential to readiness, accountability, and operational integrity.

3. DON, SOAs, and Auditability Triangle

While the Auditability Triangle identifies personnel**,** processes**,** and internal controls as foundational to audit readiness, these components must be operationalized through formal reporting and disclosure mechanisms. For the DON, the SOA report serves as a critical bridge between theoretical models, such as the Auditability Triangle, and the DON's practical efforts to evaluate and disclose internal control effectiveness. By synthesizing input from across commands, assessing control weaknesses, and documenting material deficiencies, the SOA reports transform the abstract requirements of auditability into concrete, measurable declarations of accountability. The following section presents an exploration of the structure, statutory grounding, and evaluative significance of the SOA reports, situating it as a cornerstone of the DON's internal control and audit readiness infrastructure.

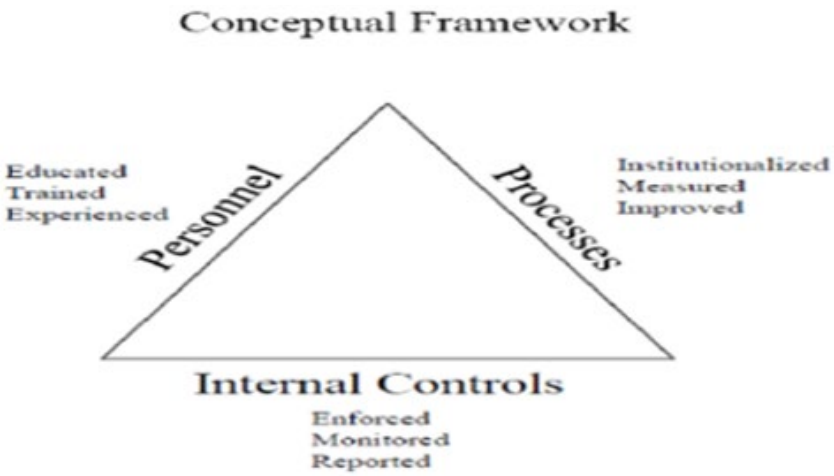

Figure 2. Auditability Triangle. Source: Rendon & Rendon (2015).

C. GOVERNMENT FINANCIAL REPORTS

1. Statement of Assurance Reports

The SOA report is the DON's core document for demonstrating accountability in internal controls and compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b). It provides a detailed evaluation of internal control conditions and discloses areas of weakness as mandated by federal law and OMB guidance (OMB, 2000, 2016). It is prepared annually in accordance with the FMFIA and OMB Circular A-123, providing a clear management assertion regarding the reliability of internal controls over financial reporting and operations (Colgren, 2019). The DON leadership utilizes the SOA report to identify, document, and certify material weaknesses that affect financial management, operational effectiveness, or legal compliance (GAO, 2023b).

As the authoritative source on the status of internal control within the DON, the SOA report provides stakeholders such as Congress, the DoD, and the public with data based on a direct assessment of the DON's internal control environment compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b). It highlights areas needing corrective action and guides targeted remediation efforts. These efforts reinforce fiscal governance and build institutional confidence in the DON's progress toward audit readiness.

Subsequent legislation further shaped SOA reporting. The CFO Act of 1990 expanded financial management responsibilities, introduced new accountability standards, and required audited financial statements, positioning the SOA report as a critical link between internal controls and financial statement reliability (Colgren, 2019). The FFMIA reinforced these standards by mandating that federal agencies implement financial systems that meet federal requirements, thereby enhancing the quality and transparency of SOA report disclosures (GAO, 2023a). Collectively, these statutes elevated the SOA report from a basic attestation to a comprehensive evaluation of financial management and internal controls, establishing it as a key document for oversight and ongoing improvement in federal financial management.

2. Agency Financial Reports

While the SOA report is the primary source for reporting internal controls and material weaknesses, the AFR provides a comprehensive financial overview for each fiscal year compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b). In accordance with OMB Circular A-136, the AFR presents the DON's fiscal condition, operational performance, and compliance with applicable regulations (OMB, 2023). It includes detailed financial information and management analysis of the DON's fiscal operations and budgetary activity.

The identification of material weaknesses in the AFR is based on disclosures made in the annual SOA report compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b). These AFR references reflect management's assertions and findings from the SOA reports (Colgren, 2019). As a result, the weaknesses highlighted in the AFR mirror those identified in the SOA reports, reinforcing the SOA report's central role in the DON's internal control and audit readiness framework (Rendon & Rendon, 2015).

The DON's SOA reports and AFR support oversight, remediation, and accountability throughout the organization. The SOA report is a key resource for auditors and oversight bodies such as the DoD Office of Inspector General (OIG) and the GAO. It

documents material weaknesses in internal controls, including issues such as segregation of duties, IT controls, and property accountability. These disclosures prompt the development of Corrective Action Plans (CAP) and ongoing monitoring, with management and oversight bodies utilizing the SOA reports to track remediation efforts. Progress is reflected in subsequent SOA reports, which are further detailed in the AFR. The AFR provides context on the DON's fiscal health, risk exposure, and the effectiveness of corrective measures. Addressing material weaknesses enhances report credibility, strengthens controls, and advances audit readiness.

While government financial reports such as the SOA report and AFR serve as the formal means for identifying and disclosing material weaknesses, they represent only one component of the DON's broader financial accountability framework. At the core of this framework is the internal control environment, which comprises the processes, standards, and oversight practices that govern the generation, validation, and management of financial data across the DON. The following section presents an exploration of the regulatory foundations and conceptual models that shape internal control expectations within the DON. These mechanisms are essential for preventing deficiencies, supporting audit readiness, and maintaining financial integrity.

D. INTERNAL CONTROLS GUIDANCE IN THE FEDERAL GOVERNMENT

The DON strengthens audit readiness and financial accountability by following government-wide standards that define effective internal control systems. Key federal entities such as the GAO and the OMB have established structured guidance to help agencies implement and evaluate internal controls with consistency, transparency, and accountability. The DON applies these frameworks to align its financial management practices with statutory requirements and best industrial practices. By actively integrating principles from the GAO's (2025) Standards for Internal Control in the Federal Government, OMB Circular A-123, and industry-proven models like the COSO Framework, the DON seeks to improve oversight, mitigate risk, and move closer to achieving an unmodified (clean) audit opinion. The following subsections provide an

examination of how these two principal sources of guidance help inform and shape the DON's internal control policies and operational practices.

1. Standards for Internal Control in the Federal Government (Green Book)

The Standards for Internal Control in the Federal government (The Green Book), GAO (2025), serves as the federal government's authoritative guidance for internal control standards across federal agencies (Comptroller General of the United States, 2013). In 2014, the GAO formally adopted the updated COSO Framework as the foundational structure for the Green Book. By incorporating the COSO Framework, the Green Book aligns the federal internal control system with industry's best practices, emphasizing a comprehensive and risk-based approach to designing, implementing, and maintaining internal controls across all levels of government operations (Office of the Commandant, 2022). This alignment allows agencies like the DoD and the DON to benchmark against a widely accepted control framework that supports accountability and transparency.

The 2025 revision of the Green Book replaces the 2014 version and introduces key updates to strengthen agencies' ability to manage emerging risks (GAO, 2025). It emphasizes enhanced risk assessment and documentation practices, particularly in areas such as fraud, improper payments, information security, and major programmatic changes like emergency assistance efforts (GAO, 2025). Managers are now required to consider these specific risk areas when identifying, analyzing, and responding to risks as part of their internal control responsibilities.

Additionally, the 2025 revision mandates the documentation of risk assessment outcomes and introduces a formalized change assessment process to ensure internal control systems can quickly adapt to significant shifts in operations (GAO, 2025). Two new appendices offer practical resources such as examples of control activities, data sources, and references that agencies can use to design and operate effective internal controls (GAO, 2025). These updates reflect the GAO's (2025) effort to align federal standards with evolving oversight needs and modern risk management practices.

2. Office of Management and Budget Circular A-123

OMB Circular A-123 standardizes management responsibilities for internal controls across federal agencies. Originating from the FMFIA, it establishes policies for creating, assessing, and reporting on internal control systems (OMB, 2016). OMB Circular A-123 was updated to include Appendix D, aligning agency practices with FFMIA. Appendix D emphasizes uniformity in financial reporting and integrating Enterprise Risk Management (ERM) into federal internal control protocols (OMB, 2000). Circular A-123 also highlights the integration of ERM with internal control practices (OMB, 2016). The following section discusses continuous improvement challenges.

E. CONTINUOUS IMPROVEMENT CHALLENGES: GAO GUIDANCE AND INDUSTRY BEST PRACTICES

While the DON receives frequent recommendations from the GAO regarding enhancements to internal controls, implementing these recommendations has not always kept pace with the urgency or scope of the identified issues. GAO (2025) guidance often focuses on developing new procedures, upgrading financial management systems, and thoroughly verifying financial records (GAO, 2025). However, the DoD and the DON have historically faced challenges in promptly executing these corrective actions (GAO, 2023b).

This lack of timely follow-through risks falling short of standards mandated by governing guidance such as the FMFIA, OMB Circular A-123, and the Green Book. When corrective actions remain incomplete or delayed, the organization could inadvertently undermine its ability to meet internal control expectations and increase the likelihood that previously identified material weaknesses and significant deficiencies may persist or escalate. In some cases, unresolved issues could reemerge as recurring material weaknesses, thereby stifling audit readiness.

The DON also aims to incorporate established industry frameworks, such as the COSO Framework. It routinely adapts its processes to respond to emerging risks and evolving standards. The DON's goal is to produce audit-ready financial statements and increase organizational resilience by aligning itself with external oversight and recognized best practices. Despite these efforts, progress remains minimal, highlighting the need for

stronger accountability and sustained commitment to implementing GAO (2023b) and industry recommendations for continuous improvement in financial accountability and internal controls.

While the internal control frameworks established by the GAO (2025), OMB, and COSO provide the structural foundation for financial accountability, their effectiveness ultimately depends on how well they are implemented within the DON. As the DON works to strengthen its internal control environment, it is crucial to examine how these frameworks function in practice to support auditability and audit readiness. The following section provides an exploration of how the DON applies internal controls in pursuit of audit readiness, focusing on integrated audits, the roles of internal and external auditors, and enterprise-wide efforts such as the FIAR program. Together, these elements illustrate the DON's ongoing efforts and challenges in meeting federal audit standards and achieving full financial transparency.

F. AUDITABILITY IN THE DON

Implementing internal control best practices is critical for the DON's and DoD 's audit readiness. These control best practices will enable DON personnel to address the issues contributing to material weaknesses proactively. Strong controls also safeguard critical financial data, ensure comprehensive supporting documentation, enhance the reliability of financial reporting, and improve interactions with auditors. These practices are essential to the DON's goal of achieving its audit objectives and complying with the required standards.

1. Management Assertions in Financial Statement Audits

Management assertions represent the five implicit claims management makes when presenting financial statements, they include: existence or occurrence, completeness, rights and obligations, valuation or allocation, and presentation and disclosure (AICPA, 2017). A material weakness exists when a deficiency in internal control creates a reasonable possibility that one or more of these assertions will be materially misstated (GAO, 2018)). In federal financial reporting, OMB Circular A-123, the Generally Accepted Government Auditing Standards (GAGAS) (hereinafter, the "Yellow Book"), and the Green Book

explicitly require agencies to design and evaluate controls that provide reasonable assurance over these assertions (GAO, 2018; GAO, 2025; OMB, 2016).

The COSO Internal Control Integrated Framework serves as the primary mechanism for supporting management assertions, with Control Activities and Information and Communication components most directly linked to existence, completeness, and valuation. Rendon and Rendon (2015) argue that auditability in defense financial management ultimately hinges on the ability to substantiate these assertions with sufficient evidential matter. When processes are decentralized, systems are legacy, or personnel turnover is high, (common DoD characteristics) the risk of assertion failure rises significantly. An assertion-based lens is therefore essential for understanding why certain material weaknesses persist despite repeated remediation efforts.

2. Integrated Financial and Internal Control Audits in the DON

Under the CFO Act and OMB guidance, the DON must produce annual audited financial statements; auditors are required to perform these audits in accordance with the Generally Accepted Government Auditing Standards (GAGAS), obtain an understanding of internal controls relevant to the audit, test those controls as needed, and report any significant deficiencies or material weaknesses (OMB, 2023). These audits are conducted both internally by DON staff and externally by independent auditors. This combined approach enhances the accuracy of the DON's financial position and ensures that internal controls function as intended. Integrated audits, which include both an audit on the financial statements and an audit of the internal controls over financial reporting, identify opportunities to improve financial processes and uncover areas where compliance may be lacking, paving the way for targeted enhancements.

These audits provide a detailed assessment of the DON's financial condition and operational performance, revealing areas of strength and highlighting where corrective action is needed. This dual focus ensures that financial reporting and control mechanisms meet federal standards. Based on their assessments, auditors issue either an unmodified opinion (indicating the statements are accurate and compliant with standards), a modified opinion (indicating significant issues in reporting or operations), an adverse opinion

(indicating significant and pervasive non-compliance to the Generally Accepted Accounting Principles), or a disclaimer of opinion (given when there is a significant and pervasive scope limitation and the auditor cannot obtain sufficient appropriate audit evidence). The DON and DoD have consistently received a disclaimer of opinion, indicating systemic challenges that require attention and focused effort in critical areas such as financial reporting and internal controls. These audit findings are a crucial resource for the DON's leadership, supporting informed decision-making and promoting financial transparency and accountability.

3. Internal and External Auditors in the DON

The DON relies on internal and external auditors to ensure the integrity, reliability, and accuracy of its financial reporting and internal controls. Internally, the Naval Audit Service (NAS), established in 1966, is the DON's internal audit body responsible for reviewing financial management activities and evaluating internal control frameworks across commands. The NAS plays a crucial role in identifying risks, verifying the effectiveness of internal control implementation, and enhancing operational efficiency.

The DON contracts with Ernst & Young (EY) to conduct external independent audits of its financial operations. Operating under the oversight of the DoD's OIG, EY assesses the DON's financial statements and control systems for compliance with federal audit requirements. This partnership is part of a broader initiative to support audit readiness across the defense enterprise. EY operates under the DoD's OIG oversight, ensuring independent governance and objectivity throughout the audit process. Initial goals set for FY 2017 proved unattainable due to ongoing material weaknesses, prompting a revised audit readiness timeline. Current plans aim for audit readiness by FY 2028 (Federal News Network, 2021).

4. Generally Accepted Government Auditing Standards

Generally Accepted Government Auditing Standards (Yellow Book), guides government audits, outlining the ethical and procedural expectations of public sector auditors (Comptroller General of the United States, 2024). These standards ensure that federal audits are conducted with professionalism, independence, and credibility. The GAO

established GAGAS in 1972 to reinforce accountability and transparency across all levels of government (McGivern, 2024). The standards are frequently updated to reflect advances in auditing practices, new technologies, and evolving best practices. GAGAS also incorporates the Generally Accepted Auditing Standards, which are commonly used in the private sector.

5. The DoD's Financial Improvement and Audit Remediation Program

The DoD established the Financial Improvement and Audit Remediation program (FIAR) to address longstanding financial management weaknesses and advance the department's audit readiness objectives (Office of the Under Secretary of Defense [Comptroller]/Chief Financial Officer, 2017). The FIAR program, formerly known as Financial Improvement and Audit Readiness, was renamed in 2018 as the Financial Improvement and Audit Remediation in accordance with the NDAA. The Program was developed in response to legislative mandates and accountability standards, such as the CFO Act and the FFMIA. By establishing structured guidelines and milestones, the FIAR program aims to enhance the accuracy and integrity of financial data, modernize outdated systems, refine business processes, and strengthen internal controls throughout the department (Office of the Under Secretary of Defense [Comptroller]/Chief Financial Officer, 2017).

At its core, the FIAR program aims to ensure that DoD financial information is timely, accurate, and capable of withstanding independent audit scrutiny (McGivern, 2024). This ongoing initiative requires close collaboration among all DoD components, including military departments and defense agencies. Activities under the FIAR Program include documenting processes, identifying and correcting material weaknesses, implementing corrective actions, and continuously evaluating progress toward audit readiness. Through this sustained, department-wide effort, the DoD demonstrates its commitment to prudent management of taxpayer resources and its responsibility to deliver trustworthy financial information to decision-makers, Congress, and the public. The following section discusses emerging insights from contemporary scholarship.

G. EMERGING INSIGHTS FROM CONTEMPORARY SCHOLARSHIP

Recent research provides insights into persistent internal control weaknesses within the DON. Notably, McGivern (2024) conducted a comprehensive evaluation of the DON's AFRs from FY2018–FY2022, focusing on internal control material weaknesses identified by external auditors and aligning her findings with the COSO Framework. McGivern (2024) revealed vulnerabilities of recurring contract management and information systems.

McGivern (2024) examined auditor recommendations related to contract management, demonstrating how contractor oversight deficiencies significantly contribute to internal control failures. McGivern systematically categorized and quantified internal control deficiencies using qualitative and quantitative methods, providing actionable recommendations for strengthening the DON's internal control program and contract management. Insights gained from McGivern's study fill critical gaps in understanding the underlying issues that continue to surface in the form of recurring material weaknesses as reported annually in the DON's SOA reports. This report may be a valuable resource for policymakers and practitioners seeking to enhance audit readiness within the DON (McGivern, 2024).

H. SUMMARY

This chapter reviewed how financial accountability in the DON has been shaped by foundational legislation, internal control frameworks, and theoretical models. The COSO Framework was presented as a key structure for evaluating internal controls through its five interrelated components, while auditability theory and the Auditability Triangle were identified as foundational tools to examine whether the DON's systems were capable of withstanding independent audit scrutiny. This chapter also emphasized how the SOA reports and AFRs serve as the DON's principal tools for identifying and disclosing material weaknesses. It also highlighted how these reports are used to assess compliance with the FMFIA, the CFO Act, and OMB Circular A-123, and how the reports have guided remediation efforts across financial management systems.

In addition, this chapter provided an examination of how federal standards such as the Green Book and Yellow Book provided structured guidance for internal control

evaluation and ERM. Major highlights from the 2025 revision of the Green Book, such as its emphasis on fraud risk, information security, and adaptive control systems, were discussed. Integrated financial audits, conducted under GAGAS were identified as essential tools for evaluating both financial statements and internal controls, with internal and external auditors contributing to oversight. The chapter concluded with a review of recent scholarship, including McGivern's (2024) analysis of recurring material weaknesses in contract management and IT systems. These studies offer a clear understanding of persistent deficiencies and reinforce the importance of implementing robust internal controls, addressing audit recommendations, and institutionalizing continuous improvement practices to advance audit readiness in the DON. The following chapter will discuss the methodology used in this research study.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. INTRODUCTION

This chapter describes the methodology used to examine the DON's recurring material weaknesses and deficiencies as disclosed in the SOA reports from FY2013–FY2022. It outlines the data design, data sources, and analytical procedures used to classify these material weaknesses and deficiencies within the COSO Framework and auditability theory principles. The chapter begins with an overview of the integrated, risk-based methodology that guided the research and explains how documentary analysis was employed to identify systemic internal control challenges. The subsequent section on data sources details the primary and secondary documents used, emphasizing their reliability and relevance to the study's objectives. The data compilation and categorization section explains how material weaknesses were organized into a structured database, aligned to the five COSO components, and mapped to the three Auditability Triangle components, to enable comparative and longitudinal analysis. The Analytical procedures section describes the quantitative methods and visualization tools used to identify recurring trends. This chapter concludes with a summary that reinforces the idea that this structured, data-driven methodology provides a foundation for evaluating the persistence and patterns of internal control deficiencies within the DON.

B. INTEGRATED APPROACH

This research utilizes documentary analysis grounded in established frameworks to evaluate the DON's internal control challenges. Leveraging methodological guidance provided by Ramos (2008), the study categorizes reported material weaknesses extracted from SOA reports and AFRs according to the components outlined in the COSO Framework. Ramos (2008) emphasizes that utilizing the COSO Framework offers a practical structural foundation, allowing organizations to systematically address internal control weaknesses by clearly identifying which component, control environment, risk assessment, control activities, information and communication, or monitoring activities, may have failed or require remediation. By aligning these categories with empirical data,

the research clarifies the specific areas within the DON's internal control systems that consistently exhibit material weaknesses.

In alignment with best practices and standards outlined by the COSO Framework and reinforced by Ramos (2008), this study utilized a risk-based, top-down analytical method. This approach prioritizes identifying and analyzing entity-level risks and weaknesses before exploring more detailed activity-level controls, thus optimizing the focus of internal control evaluations (Ramos, 2008). This top-down methodology has been consistently recommended because it efficiently directs management and audit attention to the most critical, organization-wide vulnerabilities that have broader implications for the agency's overall control environment and financial integrity (Mohammed et al., 2021). Consequently, the analysis in this study first focused on understanding and evaluating risks and material weaknesses identified at the entity level, such as leadership oversight issues, ethical tone deficiencies, and significant system-wide control gaps, as these fundamentally shape the effectiveness of all subordinate activity-level controls.

After establishing a clear understanding of entity-level internal control challenges, the research proceeded with a systematic evaluation of activity-level material weaknesses and control deficiencies documented in SOA reports, enabling a detailed, comprehensive view of the DON's internal control landscape. By mapping these activity-level deficiencies back to the higher-level COSO components, this study facilitated targeted identification of systemic material weaknesses that transcended individual transactions or isolated operational issues. Ramos (2008) highlighted the effectiveness of this integrated approach because it helps organizations pinpoint root causes of internal control failures, rather than merely addressing surface-level symptoms. Overall, this rigorous methodological approach provided a structured and holistic evaluation, yielding actionable insights into the persistent and systemic nature of internal control weaknesses within the DON (Mohammed et al., 2021; Ramos, 2008; Zahari et al., 2024). The following section discusses the data sources utilized in this research study.

C. DATA SOURCES

The primary data source for this research consists of the DON SOA reports from FY2013–FY2022, which are publicly available on the DON's website. These reports provide annual disclosures of material weaknesses and significant deficiencies, accompanied by descriptions and contextual details related to the DON's operational challenges. AFRs for the same period were consulted as a secondary source to supplement and enhance the understanding of these material weaknesses. The AFRs offer additional context and insights that help clarify the circumstances and impact of the reported material weaknesses. This study did not involve human subjects or the collection of personal data, so the IRB determined that an IRB protocol was not required. The following section explains the data compilation and categorization used in this research study.

D. DATA COMPILATION AND CATEGORIZATION

A spreadsheet was created by the researcher to compile, organize, and structure the identified material weaknesses from FY2013–FY2022. These entries were subsequently categorized according to the five components of the COSO (2013) Internal framework to enable a comparative analysis and determine which areas exhibited the highest recurrence of material weaknesses. Each identified material weakness was then aligned to a corresponding component of the COSO Framework: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities. Each identified material weakness was also mapped to a corresponding element of the Auditability Triangle: People, Processes, and Internal Controls, Additionally, material weaknesses were classified by functional area, such as financial reporting, plant, property, and equipment, among others, to support a multidimensional evaluation across both control categories and operational functions. The following section discusses the analytical procedures utilized in this research study.

E. ANALYTICAL PROCEDURES

Quantitative analysis was conducted to classify and interpret the collected data. Material weaknesses were categorized by FY and sorted according to their COSO Framework component. Following this categorization, multi-series bar charts were created

to display the frequency and distribution of material weaknesses and significant deficiencies across various internal control elements. Pie charts were utilized to categorize the distribution of deficiencies across the COSO Framework components, facilitating the visualization of which aspects of internal control posed the most significant challenges.

Cumulative datasets were constructed to track trends and recurring patterns over the 10 years, providing a longitudinal perspective. This methodology enabled year-to-year comparisons, helped identify ongoing vulnerabilities, and facilitated the assessment of the most persistent systemic weaknesses. Visual tools such as bar and pie charts were used to highlight these patterns across FYs. The following section provides a summary of this chapter.

F. SUMMARY

This chapter provided an introduction to the methods used to analyze the DON SOA report data from FY2013–FY2022. The publicly available data source was obtained and used to demonstrate alignment of material weaknesses with the COSO Framework components and the Auditability Triangle elements, and to aggregate quantitative findings to uncover trends and ongoing issues. A structured database created by the researcher enabled thorough data compilation, categorization, and longitudinal analysis, which allowed for a comprehensive assessment of the DON's internal control environment. The analytical procedures upheld strict data privacy standards and research ethics. This methodology ensured that personally identifiable information (PII) was not collected, nor were human subjects interviewed as part of the study. Following this rigorous process, the analysis aimed to provide practical, data-driven recommendations for strengthening internal controls and improving the DON's overall financial management and audit readiness.

IV. DATA ANALYSIS, FINDINGS, AND RECOMMENDATIONS BASED ON FINDNGS

A. INTRODUCTION

The purpose of this chapter is to present and analyze data collected from the DON's SOA reports spanning FY2013 through FY2022. This analysis aims to identify the frequency and persistence of recurring material weaknesses within the DON's internal control environment. By analyzing these material weaknesses, recurring patterns and areas where internal control may need to be strengthened can be identified. Subsequently, these material weaknesses are mapped against the COSO Internal Control Integrated Framework components and the Auditability Triangle elements to offer an evidence-based understanding of where systemic vulnerabilities remain and how they can affect audit readiness.

The methodology for generating these findings involved a comprehensive review and classification of material weaknesses. Each identified material weakness was categorized into the five COSO components: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities (COSO, 2013). This categorization enabled pattern recognition across fiscal years. The data were further analyzed through the lens of the Auditability Triangle, placing the findings within the broader context of organizational auditability.

This chapter follows a logical progression beginning with the evolution of the DON's internal control reporting environment during the study period. It then presents an examination of the quantitative trends and distributions of material weaknesses identified across FYs. This is followed by an analysis of recurring themes. The analysis then shifts to evaluating longitudinal trends and broader patterns that illustrate how these material weaknesses have evolved within the study period. This chapter concludes by highlighting how the application of the COSO Internal Control Integrated Framework and the Auditability Triangle impact the findings, demonstrating how personnel, processes, and internal controls interact to influence audit readiness. It ends with a concise summary of the key findings and their implications for future improvement. The following section

examines how the DON's internal control reporting environment evolved during the study period.

B. OVERVIEW OF DON INTERNAL CONTROL REPORTING EVOLUTION (2013–2022)

From FY2013–FY2022, the DON's internal control reporting evolved from compliance-based assessments to an integrated, risk-informed approach. This evolution unfolded through three significant shifts: the FY2016 alignment with OMB Circular A-123, introducing ERM; the FY2018 adoption of full-scope audits structured around COSO principles; and the FY2020–FY2022 focus on data consolidation, systems modernization, and audit roadmaps. Together, these changes reflected a maturing control environment linking risk management, audit readiness, and performance accountability.

1. Integration of Enterprise Risk Management (FY2016)

Over the 10-year study period (FY2013–FY2022), several distinct shifts in emphasis and methodology of reporting were evident in the DON's internal control reporting practices. The first significant shift occurred in FY2016, when the SOA reporting process was realigned with the revised OMB Circular A-123. This revision mandated the integration of ERM into the federal government internal control framework. Consequently, commands were required to conduct risk identification, assessment, and mitigation in conjunction with their internal control evaluations, rather than as a separate compliance activity (OMB, 2016).

2. Alignment with Full-Scope Audits and COSO (FY2018)

The second significant shift coincided with the DON's entry into full-scope financial statement audits beginning in FY2018. During this phase, the AFR began reflecting discussions and remediation actions organized around major business processes, closely mirroring the COSO Internal Control Integrated Framework. The SOA reports for FY2020 through FY2022 show an increased alignment between management assurance statements and external auditor findings, including detailed discussions of CAPs and their impact on downgraded material weaknesses (DON, 2018b; DON, 2019b; DON, 2020b; DON, 2021b; DON, 2022b).

3. Focus on Data Consolidation and Audit Roadmaps (FY2020–FY2022)

The third significant shift, spanning from FY2020–FY2022, centered on data consolidation and the implementation of an audit roadmap. This period marked the introduction of structured milestones and performance indicators to track progress in resolving material weaknesses. The AFRs during these years emphasized the DON's transition toward a unified financial management environment, improved system interoperability, and the decommissioning of legacy platforms (DON, 2020a; DON, 2021a; DON, 2022a). Concurrently, the GAO reported that the DoD and its components, including the DON, were utilizing audit roadmaps to align remediation actions, monitor risk exposure, and track closure of long-standing material weaknesses (GAO, 2023a).

Overall, these developments reflect a steady evolution from compliance-focused internal control reporting to a more integrated, risk-informed, and performance-driven approach. By aligning SOA assertions with ERM practices and COSO principles, and by executing the audit roadmap, the DON demonstrated a maturing internal control environment that increasingly linked oversight, accountability, and audit readiness. The following section provides an overall analysis of the identified recurring material weaknesses.

C. OVERALL ANALYSIS OF RECURRING MATERIAL WEAKNESSES

1. Aggregate Findings

The DON reported 122 instances of material weaknesses in its SOA reports from FY 2013–FY2022, representing both newly identified and recurring material weaknesses across internal control assessments compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b). These encompassed roughly 41 distinct material weakness types, such as variations in property accountability and IT controls, with the annual count of open material weaknesses ranging from eight in FY2013 to a peak of 24 in FY2017, before declining to six by FY2022 compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b). This bell-shaped trajectory demonstrates measurable progress in remediation and audit readiness

under the FIAR initiative, achieving a roughly 75% reduction from the FY2017 peak; however, the persistence of core issues indicates that many material weaknesses remained only partially resolved, contributing to ongoing disclaimer of opinions on financial statements (GAO, 2020; DON, 2022b).

From FY2013–FY2016, the DON's internal control environment was characterized by limited standardization and reliance on outdated financial systems, which constrained comprehensive detection and reporting of material weaknesses (DON, 2014b; DON, 2015b; DON, 2016b). Between FY2017 and FY2019, the DON intensified FIAR-driven processes re-baselining and initiated full-scope financial statement audits starting in FY2018, uncovering widespread weaknesses in property accountability, IT general controls, and financial reporting reliability (DON, 2017b). From FY2020–FY2022, the adoption of the Integrated Risk Management framework and enterprise performance management initiatives, such as expanded Navy Enterprise Resource Planning (ERP) systems, enhanced alignment between risk assessment, internal controls, and mission outcomes, and supported further material weakness closures amid external challenges like the COVID-19 pandemic (DON, 2021b). Despite these advancements, ongoing deficiencies in property valuation, access controls, and contract oversight underscored persistent cultural and systemic barriers to full auditability (DON, 2022b). Table 2 provides a summary of the annual material weaknesses reported in DON SOAs for FY2013–FY2022.

Table 2. Material Weaknesses Reported in DON SOA by Fiscal Year (FY2013–FY2022)

Fiscal Year	Open Material Weaknesses	Key Themes Identified
FY2013	8	Limited scoping; early property and reporting gaps
FY2014	9	Fragmented systems; initial FIAR focus
FY2015	10	Decentralized oversight; IT controls emerging
FY2016	12	Pre-audit readiness; documentation inconsistencies
FY2017	24	Re-baselining spike; expanded testing reveals PP&E, IT, reporting issues
FY2018	20	First full audits; remediation begins
FY2019	15	Progress in CAPs; persistent contract and access controls
FY2020	10	IRM integration; COVID impacts noted
FY2021	8	ERP enhancements; risk alignment improves
FY2022	6	Residual property, reporting, IT gaps
Total Instances	**122**	

2. Trend Analysis of Material Weaknesses in the Department of the Navy (FY2013–FY2022)

Quantitative analysis of reported material weaknesses over the decade reveals a pronounced bell-shaped distribution (see Fig. 3), indicative of the DON's evolving audit maturity and structural reform of its internal control framework. In the initial audit-readiness phase (FY2013–FY2016), the number of identified material weaknesses remained consistently low (ranging from 8 to 14 annually), not as evidence of effective control but as a function of constrained detection capacity. Limitations, including siloed ERP systems, inconsistent documentation, and decentralized risk oversight, severely restricted management's ability to identify and evaluate latent deficiencies (DON, 2017b).

The inflection point in FY2017, marked by a near-doubling of reported material weaknesses to 24, coincides precisely with the DON's enterprise-wide re-baselining of financial and operational processes under the FIAR initiative. This escalation signified a diagnostic breakthrough driven by enhanced transparency. The revised OMB Circular A-123 (2016) mandated integration of ERM and expanded end-to-end process testing, compelling broader deficiency disclosure (DON, 2017). Concurrently, the FY2017 SOA report formalized a governance architecture wherein the Senior Management Council (SMC) and Senior Assessment Team (SAT) convened quarterly to evaluate risk profiles, monitor CAP execution, and adjudicate deficiency classification, escalation, or closure (DON, 2017b).

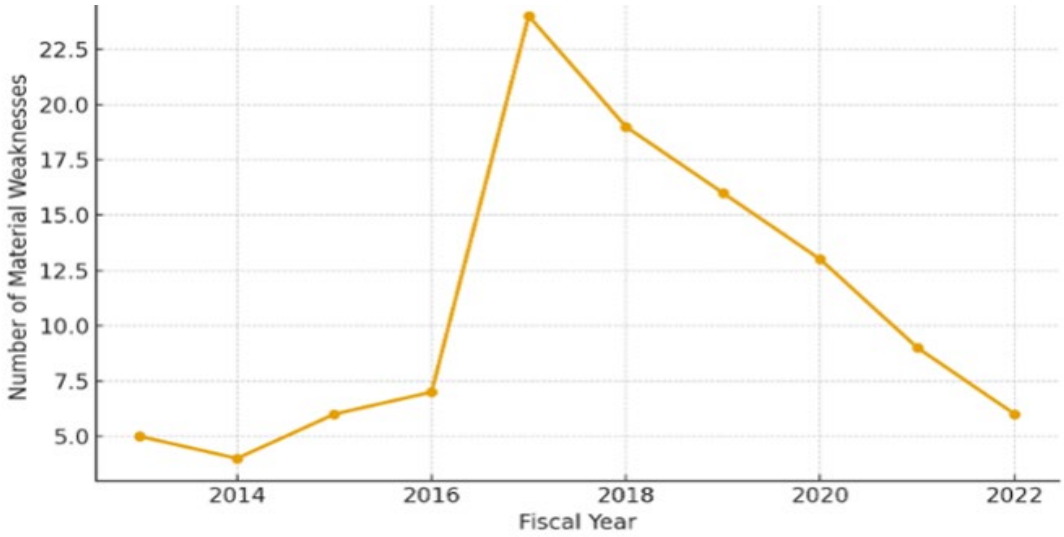

Figure 3. Trend in Material Weaknesses (FY2013–FY2022)

From FY2018 onward, a sustained downward trajectory in open material weaknesses reflects the institutionalization of remediation governance and control maturation. AFRs from FY2018–FY2022 consistently document the progressive alignment of internal controls with the COSO Integrated Internal Control Framework, the implementation of real-time CAP monitoring dashboards, and the embedding of remediation tracking within the annual assurance cycle (DON, 2018b; DON, 2019b; DON, 2020b; DON, 2021b; DON, 2022b). Leadership accountability exercised through the SMC, SAT, and audit committee was strengthened by structured performance indicators, and the strategic consolidation of legacy systems resulted in clear improvements in data integrity and in the traceability of audit evidence (DON, 2019b; DON, 2020b; DON, 2021b; DON, 2022b).

By FY2022, the DON had achieved an approximately 75% reduction in open material weaknesses relative to the FY2017 peak, underscoring substantive progress in audit readiness and control integration. However, residual deficiencies predominantly in property valuation and accountability, financial statement reliability, and information system access controls reveal persistent structural impediments that transcend technical remediation (DON, 2022b). Sustained advancement toward a fully auditable environment necessitates continued investment in governance rigor, risk-informed prioritization, and leadership commitment to cultural transformation.

3. Distribution of Identified Material Weaknesses by COSO Component

The classification of each material weakness was derived directly from the SOA report's internal control reporting narrative, management's assertions, and the contextual details surrounding each control function. Each material weakness was aligned to one of the five internal control components based on the COSO Internal Control Intergrated Framework. For instance, material weaknesses involving policy enforcement and ethical leadership were aligned to the Control Environment, while recurring issues in documentation, reconciliations, or property accountability were aligned to Control Activities. Similarly, information system reliability and data-sharing inefficiencies were aligned to Information and Communication, and shortcomings in tracking or validating corrective actions were aligned to Monitoring Activities. This analytical process ensured that each material weakness was assessed within a consistent conceptual framework, allowing the identification of dominant patterns, systemic control gaps, and interdependencies between the COSO Internal Control Integrated Framework components.

A total of 122 material weaknesses were identified and classified across the five COSO Internal Control Integrated Framework components, with Control Activities accounting for 50.0%, Monitoring Activities for 19.2%, Information and Communication for 14.8%, Control Environment for 9.6%, and Risk Assessment for 6.4% (see Fig. 4). These decade-average proportions, derived from systematic aggregation of deficiency listings in the DON's annual SOA reports, reveal a persistent dominance of execution-level and oversight failures. At the same time, foundational components, particularly Risk Assessment, remained relatively minor but consequential enablers of systemic risks (see Table 3). To complement these quantitative trends, the following section examines the characteristics of recurring material weaknesses which are aligned to the five COSO Internal Control components, providing deeper insight into the underlying conditions that sustained them over the decade.

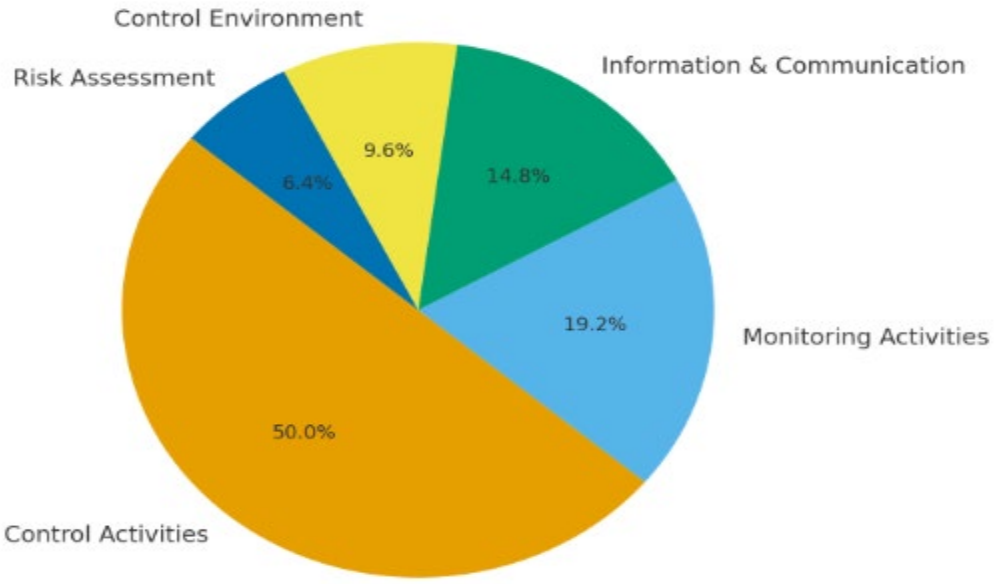

Figure 4. Proportion of SOA Material Weaknesses by COSO Component

D. ANALYSIS OF RECURRING MATERIAL WEAKNESSES ALIGNED TO COSO INTERNAL CONTROL COMPONENTS

1. Control Activities

Control Activities constituted 50% of recurring material weaknesses throughout the study period, reflecting systemic execution failures. recurring deficiencies centered on PP&E accountability, contract management, and account reconciliation processes, issues first documented in FY2013 and unresolved through FY2022 (DON, 2022b). The FY2019 AFR designated PP&E valuation and completeness as "key audit impediments," attributing failures to disconnected feeder systems and inadequate general ledger integration (DON, 2019a). While subsequent reports noted advancements through system modernization, such as enhancements to the Defense Property Accountability System and improved inventory protocols (DON, 2021a), data integration gaps and documentation deficiencies continued to compromise the reliability of audit evidence and control assurance (DON, 2022b).

2. Monitoring Activities

The material weaknesses in Monitoring Activities were predominantly linked to inadequate CAP tracking and inconsistent validation of remediations, accounting for 19.2%

of recurring material weaknesses. The FY2017 SOA report identified "delayed or incomplete validation of corrective actions" as a significant control failure (DON, 2017b), a deficiency that persisted into FY2021 (DON, 2021b). Recent AFRs highlight progress through the deployment of automated CAP dashboards and centralized monitoring frameworks (DON, 2020a; DON, 2022a).

However, uneven adoption across major commands and the Monitoring Activities' material weaknesses were predominantly linked to inadequate CAP tracking and inconsistent validation of remediations. The FY2017 SOA identified "delayed or incomplete validation of corrective actions" as a significant control failure (DON, 2017b), a deficiency that persisted into FY2021 (DON, 2021b). Recent AFRs highlight progress through the deployment of automated CAP dashboards and centralized monitoring frameworks (DON, 2020a; DON, 2022a). However, uneven adoption across major commands and the lack of standardized closure validation criteria continue to limit management's ability to confirm complete remediation and sustained control effectiveness (DON, 2022a).

3. Information and Communication

Deficiencies within the Information and Communication component constituted 14.8% of recurring material weaknesses. This reflected systemic problems with the accuracy, timeliness, and transparency of financial data. AFRs from FY2018–FY2021 repeatedly cited breakdowns in information flow between Budget Submitting Offices (BSOs), internal auditors, and the Office of the Comptroller. Inconsistent documentation practices and limited access to real-time financial information hindered both operational oversight and audit responsiveness (DON, 2018b; DON, 2020b). While data governance initiatives have since improved accessibility, the need for standardized communication protocols and centralized reporting platforms remains critical to sustaining reliable internal control operations (DON, 2022b).

4. Control Environment

Findings in the Control Environment category accounted for 9.6% of recurring material weaknesses which underscore ongoing governance and leadership challenges

across the DON. Over the decade, material weaknesses consistently pointed to gaps in tone at the top, accountability chains, and management oversight. The FY2017 SOA stressed the need for stronger "leadership integrity and accountability," signaling a recognition that audit readiness required cultural as well as procedural reform (DON, 2017b). By FY2021, the AFR also noted improvements in aligning leadership incentives and performance metrics with audit outcomes (DON, 2021a). Nonetheless, non-integrated oversight structures and inconsistent communication across echelons continued to weaken the DON's (2022) internal control culture and impede the sustainability of corrective efforts.

5. Risk Assessment

Findings in the Risk Assessment component accounted for 6.4% of recurring material weaknesses and frequently stemmed from incomplete documentation of risk evaluation processes and limited use of risk data in management decisions. Between FY2015 and FY2018, both the GAO and internal auditors observed the absence of an integrated, enterprise-level framework for identifying risks associated with legacy systems and financial reporting (DON, 2018b). By FY2022, the DON (2022) had begun implementing structured risk registers consistent with ERM principles. These tools provided greater visibility into mission and financial risks, though the translation of risk identification into actionable CAPs remained inconsistent across commands (DON, 2021b).

While these findings highlight the characteristics and root causes of individual material weaknesses, a broader assessment is needed to determine how these issues unfolded across the decade. The following presents an examination of the longitudinal trends of recurring material weaknesses, identifying issues that shaped the DON's internal control environment.

Table 3. Proportion of SOA Material Weaknesses by COSO Component

COSO Component	Percentage	Peak Year (Count)	FY2022 Status
Control Activities	50.00%	FY2017 (14)	3 open
Monitoring Activities	19.20%	FY2017 (6)	1 open
Information & Communication	14.80%	FY2018 (5)	1 open
Control Environment	9.60%	FY2017 (3)	1 open
Risk Assessment	6.40%	FY2018 (2)	0 open
Total	100.00%		6 open

E. LONGITUDINAL ANALYSIS OF RECURRING MATERIAL WEAKNESSES

Despite a 75% reduction in open material weaknesses from 24 in FY2017 to 6 in FY2022, a core subset of deficiencies exhibited high recurrence, appearing in at least 7 of the 10 FYs under review (DON, 2017b; DON, 2022b). These chronic control failures were predominantly concentrated in Control Activities and Monitoring Activities (See Table 3), with issues such as PP&E accountability, feeder system reconciliation gaps, and delays in CAP validation persisting despite repeated remediation efforts (DON, 2019b; DON, 2021b). Such recurrence underscores structural vulnerabilities that standard CAP processes have failed to resolve fully, due to the failures being rooted in legacy system issues, decentralized operational execution across major commands, and cultural inertia that resist standardized governance and accountability (DON, 2022b; GAO, 2020).

Table 4 highlights the five identified recurring material weakness areas, each persisting for seven or more years. PP& E existence, completeness, and valuation was the most persistent issue, reported for 10 years from FY2013–FY2022, driven by failures in Control Activities with secondary breakdowns in Information and Communication**.** Feeder system to general ledger reconciliation gaps followed closely at 9 years**,** also beginning in FY2013, and share the same primary and secondary COSO component alignment, showing chronic execution and data reliability problems. Contract payment and oversight

deficiencies appeared for 8 years starting in FY2014, tied primarily to Control Activities and secondarily to the Control Environment**,** highlighting oversight and accountability weaknesses. CAP validation delays and incomplete closure evidence lasted 8 years beginning in FY2017 and reflect shortcomings in Monitoring Activities with secondary links to the Control Environment and Information and Communication**;** this is the only weakness closed by FY2022. IT general access control issues lasted 7 years from FY2015–FY2022, rooted in Control Activities with the secondary drivers being the Control Environment and Information and Communication. Together these patterns show that persistent deficiencies cluster around weak control execution, inconsistent monitoring, and unreliable information flow.

This longitudinal analysis demonstrates that these recurring material weaknesses are not isolated control failures but entrenched structural issues. To further diagnose the source of these ongoing issues, the following section reframes these weaknesses through the Auditability Triangle, highlighting how personnel, processes, and internal controls collectively shape audit readiness.

Table 4. Most Recurring Material Weaknesses (Appearing in ≥7 Years)

Material Weakness Area Description	Primary COSO Component	Secondary COSO Component(s)	Years Reported	First Cited	Last Cited	Status in FY2022
PP&E existence, completeness, and valuation	Control Activities	Information & Communication	10	FY2013	FY2022	Open
Feeder system to general ledger reconciliation gaps	Control Activities	Information & Communication	9	FY2013	FY2022	Open
Contract payment and oversight deficiencies	Control Activities	Control Environment	8	FY2014	FY2022	Open
CAP validation delays & incomplete closure evidence	Monitoring Activities	Control Environment and Information & Communication	8	FY2017	FY2021	Closed (FY2022)
IT general access controls (segregation of duties)	Control Activities	Control Environment and Information & Communication	7	FY2015	FY2022	Open

F. CROSS-ANALYSIS WITH AUDITABILITY TRIANGLE

To deepen the COSO-based analysis, the identified material weaknesses were reframed through the Auditability Triangle framework, which posits audit readiness as the interdependent equilibrium of personnel, processes, and internal controls (Rendon & Rendon, 2015). This lens enables a diagnostic mapping of the five most recurring material weakness areas to reveal whether chronic failures originate primarily in human capacity, procedural design, or internal control enforcement. As shown in Table 5, Process deficiencies dominate, followed by Internal Controls, confirming that execution-level fragmentation is the primary driver of auditability gaps.

The ongoing issues of material weaknesses in the existence, completeness, and valuation of PP&E across all 10 years of the study (see Table 5) reflect deficiencies in processes, internal controls, and personnel. Similarly, as shown in Table 5, CAP validation delays (8 years) stem from process immaturity (lack of uniform closure criteria), control design flaws (reliance on manual validation), and personnel turnover (loss of institutional knowledge). This intersectionality underscores that recurring weaknesses are not siloed but emerge from systemic misalignments across the triangle, necessitating integrated rather than component-specific remediation.

This cross-analysis highlights the significance of the Process element of the Auditability Triangle as a contributor and primary driver to recurring weaknesses, aligning with the COSO finding that Control Activities accounted for nearly half of all identified material weaknesses between FY2013 and FY2022 (see Table 3). The Personnel element, while less frequently cited directly, was a root cause of many process and control breakdowns, particularly when turnover, insufficient training, or a lack of accountability undermined continuity of operations.

Finally, the Internal Controls element reflected weaknesses in design and enforcement, often due to overreliance on manual validation and insufficient monitoring automation. The intersection of these three factors demonstrates that audit readiness is not simply a matter of policy compliance, but of cultivating an integrated control culture in which skilled personnel execute standardized processes supported by robust, adaptive

control mechanisms (Rendon & Rendon, 2015). Insights from the Auditability Triangle reveal the underlying interactions that sustained ongoing deficiencies across the internal control environment. Building on these insights, the following section provides a discussion of these findings for the DON's internal control environment and its long-term audit readiness.

Table 5. Mapping of Recurring Material Weakness to Elements of the Auditability Triangle

Recurring Material Weakness Areas	Years	Personnel Issues	Process Issues	Internal Control Issues	Primary Driver
PP&E existence, completeness, and valuation	10	Training	Protocols	Reconciliations	Processes
Feeder system to general ledger reconciliation gaps	9	Turnover	Standards	Integration	Processes
Contract payment & oversight deficiencies	8	Knowledge &Training	Workflows	Segregation	Processes
CAP validation delays & incomplete evidence	8	Knowledge	Criteria	Automation	Processes
IT general access controls (segregation of duties)	7	Access mgmt	Policies	Enforcement	Internal Controls

G. DISCUSSION OF FINDINGS

1. Interpreting Trends through the COSO Internal Control Integrated Framework

Control Activities dominate 50.0% of the material weaknesses (see Table 3) driven by three ongoing material weakness areas: PP&E existence/completeness/valuation (10 years), feeder-to-ledger reconciliation gaps (9 years), and contract payment/oversight deficiencies (8 years), of which were still open in open in FY2022 (DON, 2022b). Monitoring Activities (19.2%) reflect CAP validation delays/incomplete evidence (8 years), which were closed only in FY2022 via automated dashboards (DON, 2020b). Information and Communication (14.8%) expose a disjointed data flow across BSOs, while Control Environment (9.6%) improved post-FY2019 through SMC/SAT metrics (DON, 2020b; DON, 2021b) but still suffers from turnover-driven accountability gaps**.** Risk

Assessment (6.4%) achieved 100% closure by FY2022 via ERM registers, validating uniform governance efficacy (DON, 2021b).

Further interpretation of these patterns reveals that the dominance of Control Activities material weaknesses reflects a structural dependency on manual, judgment-based processes that remain vulnerable to inconsistent execution and incomplete documentation (DoD OIG, 2022; GAO, 2024). Decentralized financial operations across BSOs and Echelon commands (GAO, 2023a) intensify this condition. Meanwhile, the slow remediation trajectory for Monitoring Activities and Information and Communication indicates that oversight mechanisms are maturing unevenly, with automated tools emerging only late in the study period (DON, 2020b; DON, 2022b). The relative improvement in Risk Assessment, compared to the ongoing deficiencies in Control Activities and data governance, suggests that targeted, governance-driven reforms are most successful when supported by enterprise-level policy standardization and leadership enforcement (GAO, 2024; OMB, 2016).

Collectively, these trends illustrate that auditability challenges are rooted not simply in isolated process failures but in long-standing misalignments between control design, system integration, and workforce continuity (GAO, 2024; Rendon & Rendon, 2015). The following subsection builds on this analysis by examining how these COSO component-aligned trends intersect with the Auditability Triangle to reveal the factors that continue to shape the DON's internal control reliability and audit readiness.

2. Auditability Findings

The Auditability Triangle (Chapter IV, Table 5) positions Processes as the primary recurrence driver (100% of chronic weaknesses), with Internal Controls (80%) and Personnel (60%) acting as amplifiers rather than isolated root causes (Rendon & Rendon, 2015). PP&E valuation repeatedly fails due to non-standardized inventory protocols (Processes), rotational knowledge loss and limited continuity (Personnel), and persistent dependence on manual reconciliation techniques (Internal Controls) (DON, 2022b; DoD OIG, 2022). Similarly, CAP validation closure occurred only after automation mitigated long-standing visibility deficits (Information & Communication) and leadership oversight

increased through more precise accountability mechanisms within the Control Environment (DON, 2020b; DON, 2022b). This convergence of process deficiencies, control insufficiencies, and workforce instability reinforces the conclusion that recurring material weaknesses are systemic and require integrated remediation strategies rather than siloed CAP execution (DoD IG, 2022; Rendon & Rendon, 2015).

The Auditability Triangle analysis further demonstrates that the DON's audit challenges are both technical and structural. Where processes lack standardization, internal controls become compensatory rather than preventative, driving continued reliance on manual workarounds that mask rather than correct deficiencies (DoD OIG, 2022). Likewise, high personnel turnover undermines institutional knowledge and increases the risk of inconsistent execution, especially in valuation, reconciliation, and evidence-retention tasks central to auditability (GAO, 2023b).

These patterns signal that future improvements must incorporate synchronized reforms across governance, technology, and workforce management to prevent weaknesses from re-emerging in new forms. Together, these auditability implications establish the foundation for the implications of the findings discussed in the next section.

H. IMPLICATIONS OF FINDINGS

The decade-long review of DON SOA reports (FY2013–FY2022) reveals five chronic material weaknesses were centered on PP&E management, system reconciliation, contract oversight, CAP validation, and IT access controls. These themes align closely with GAO and DoD OIG (2022) findings, which consistently cite legacy system disconnection, reliance on manual reconciliation, and decentralized process execution as root causes of audit disclaimers. The persistence of these issues, despite a 75% reduction in open weaknesses, indicates that standard CAP remediation is insufficient against structurally embedded failures.

Personnel turnover and rotational assignments exacerbate breakdowns in processes and controls, particularly in PP&E valuation and CAP validation, where institutional knowledge is regularly lost. Process variability across BSOs and echelon commands contributes to non-standardized documentation and inconsistent reconciliation practices. At

the same time, internal control design remains vulnerable due to overreliance on manual validation and inadequate automation. Achieving audit readiness demands a unified strategy that integrates stable and controlled personnel replacement plans, enterprise-standardized processes, and real-time monitoring systems to break the cycle of recurrence. The implications discussed in this section reveal the systemic conditions that enabled recurring material weaknesses to persist across the decade.

The persistence of these recurring material weaknesses reflects not merely technical deficiencies but also structural interdependencies within the DON's internal control environment, where foundational gaps in data architecture and command-level discipline perpetuate downstream execution and monitoring failures. For instance, the inability to fully integrate feeder systems with the general ledger has sustained PP&E valuation weaknesses across the entire decade. As shown in Table 4, the primary COSO component was aligned to Control Activities and the secondary COSO component was aligned to Information and Communication. At the same time, inconsistent CAP closure validation continues to undermine confidence in remediation effectiveness despite the introduction of automated dashboards (DON, 2020b). Table 4 provides a summary of these recurring material weakness areas aligned to primary COSO component and to a secondary COSO component . The following section provides recommendations based on findings.

I. RECOMMENDATIONS BASED ON FINDINGS

The findings of this study show that recurring material weaknesses in the DON stem from interdependent failures in process standardization, personnel continuity, and internal control enforcement. Decentralized execution, legacy system constraints, and frequent workforce rotations interact to erode the consistency and reliability of core financial processes. In response to these patterns, this section presents a set of multi-tiered recommendations based on the findings that directly target the conditions that have allowed these material weaknesses to persist.

The following recommendations align with the requirements of the FMFIA, OMB Circular A-123, and the 2025 Green Book to ensure that proposed actions strengthen compliance while advancing internal control maturity. If implemented, they could promote

sustained enterprise governance, accelerated technological modernization, and a culture that reinforces accountability at all levels. By acting on these areas simultaneously, the DON could shift from relying on reactive corrections to making durable improvements.

1. Strengthen Command Accountability and Risk Management

The findings of this research showed that 50% of material weakness areas identified during the study period (FY 2013–FY2022) were aligned to Control Activities. Auditability must be institutionalized as a command responsibility rather than a headquarters initiative. Each major command and BSO should be required to submit annual audit certification statements tied to CAP outcomes, and reviewed by the SMC and SAT Council. Integrating ERM with these certification processes will ensure that remediation priorities are aligned with the 2025 GAO Green Book. This dual approach could strengthen both accountability and proactive risk governance across all echelons of command.

2. Standardize and Automate Financial Processes

The findings of this research showed that the Processes element of the Auditability Triangle was the primary driver for the recurring material weakness areas identified during the study period (FY 2013–FY2022). The DON should adopt standardized templates and procedures for PP&E inventory, contract oversight, and reconciliation to ensure uniformity and comparability across commands. Automation must replace manual CAP validation by linking risk registers to corrective action databases, thereby ensuring timely documentation and audit verification. Embedding Lean Six Sigma or other continuous-improvement methods into periodic process reviews could drive efficiency and prevent recurrence of control failures.

3. Develop and Retain a Competent, Ethical Workforce

The findings of this research showed that Personnel issues included training, turnover, knowledge, and access management. Sustained audit readiness depends on a stable and skilled workforce grounded in ethical responsibility. Implementing biennial auditability certification for financial and acquisition personnel will maintain proficiency in internal control principles and audit procedures. A 90-day overlap during rotations should be standardized to preserve institutional knowledge. At the same time, leadership

accountability for internal controls must be reinforced through audit-readiness metrics and tone-at-the-top training.

4. Enhance Oversight through Technology and Continuous Monitoring

The findings of this research study showed that 19.2% of the identified material weakness areas were aligned to monitoring activities. To maintain visibility of corrective actions, the Navy should designate cross-command audit liaisons and deploy predictive dashboards that track CAP aging, identify high-risk areas, and forecast recurrence. Quarterly audit performance reviews presented to the SMC and SAT will embed transparency into the oversight cycle and link remediation progress to leadership evaluations. These measures ensure that monitoring activities become a continuous, data-driven feedback system that reinforces control discipline and accountability throughout the enterprise. The following section highlights the policy implications of these findings.

J. POLICY IMPLICATIONS OF FINDINGS

This research study identified five recurring material weakness areas that persist and dominate auditability challenges. Control Activities (50%) remain the largest category, driven by chronic PP&E, reconciliation, and contract oversight failures. Monitoring Activities (19.2%) reflect persistent CAP validation gaps, while Information and Communication (14.8%) highlights data flow issues. Control Environment (9.6%) and Risk Assessment (6.4%) show improvement, with the latter fully resolved by FY2022 (see Table 3). While the 75% reduction in open weaknesses from FY2017–FY2022 signals institutional progress, the survival of four of five recurring weaknesses into FY2022 underscores that technical modernization alone cannot eliminate systemic failures. Sustained audit readiness requires cross-functional integration of personnel stability, process standardization, and automated controls.

By applying the COSO Internal Control Integrated Framework and auditability theory in practice, the DON can emerge as a leading model for the DoD and other federal agencies confronting similar audit challenges. Initiatives such as ERP convergence, CAP automation, and risk-informed dashboards (DON, 2022b) could strengthen accountability from command-level execution to departmental reporting, while audit-readiness practices

aligned with the 2025 GAO Green Book position the Navy to contribute meaningfully to the DoD's objective of achieving a clean audit opinion by FY2027(DON, 2022b).

These policy shifts could move the Navy from reactive remediation toward a preventive control culture grounded in proactive risk governance and continuous monitoring. Because these implications point to ongoing systemic challenges, the following section outlines a summary of this chapter while areas where additional research can expand the evidence base and guide the next generation of auditability reforms are addressed in Chapter V.

K. SUMMARY

In this chapter the analytical framework for using the COSO Internal Control Integrated Framework and the Auditability Triangle for the decade-long SOA analysis (FY 2013–FY2022) was established, followed by an overview of the DON's internal control reporting evolution, which showed how internal control reporting matured through ERM integration, alignment with full-scope audits, and increased reliance on data consolidation and audit roadmaps. The quantitative analysis identified 122 material weaknesses during the study period, peaking in FY2017 and declining by FY2022, with Control Activities consistently representing the largest share of deficiencies. The qualitative analysis further demonstrated that weaknesses across leadership oversight, risk documentation, PP&E management, information flow, and CAP validation reflected systemic, rather than isolated, control failures.

The longitudinal analysis highlighted material weaknesses across five core areas, revealing entrenched issues stemming from legacy systems, decentralized execution, and inconsistent monitoring. The cross analysis with the Auditability Triangle confirmed that process immaturity, manual controls, and personnel turnover collectively sustained auditability gaps. From these analyses, the implications of findings showed that, despite measurable progress, the DON must strengthen process standardization, workforce continuity, and automated controls to achieve lasting audit readiness. These integrated insights set the foundation for the recommendations based on the findings. The following chapter discusses the summary, conclusions and areas of further study.

V. SUMMARY, CONCLUSIONS, AND AREAS FOR FURTHER RESEARCH

A. INTRODUCTION

This chapter consolidates the major findings of this research and interprets their significance within the broader context of the Department of the Navy's auditability challenges. It synthesizes the results of the decade-long analysis, highlights the research implications, and articulates areas where further study is warranted. In addition, this chapter presents overarching conclusions that integrate the study's empirical evidence with the conceptual frameworks used throughout the thesis. The following section provides a summary of this research.

B. SUMMARY OF RESEARCH

A quantitative aggregation of 122 material weakness instances from DON SOA reports (FY2013–FY2022) confirms a 75% reduction in open weaknesses from FY2017 – FY2022 (DON, 2017b; DON, 2022b) yet identifies five recurring material weakness reported during the study period. An analysis that maps these recurring material weaknesses to the COSO Internal Control Integrated Framework and the Auditability Triangle shows that these ongoing failures reveal audit-readiness impediments due to decentralized process implementation, personnel transience, and incomplete control automation, despite legislative mandates and FIAR-driven reforms. compliance (DON, 2013b; DON 2014b; DON 2015b; DON 2016b; DON 2017b; DON 2018b; DON 2019b; DON 2020b; DON 2021b; DON 2022b; GAO, 2024; Rendon & Rendon, 2015).

Building on these findings, this chapter interprets the implications of the DON's decade-long control environment through a systems lens, emphasizing how structural decentralization, uneven process execution, and legacy system dependence have shaped the persistence of material weaknesses. The findings demonstrate that audit outcomes are not isolated control failures but manifestations of broader organizational dynamics (GAO, 2024). These recurring material weaknesses could collectively constrain the DON's capacity to institutionalize corrective actions and achieve durable auditability. Table 6

provides a summary of key qualitative observations based on the COSO Internal Control Integrated Framework, followed by a conclusion addressing the research questions and areas of further research.

Table 6. Summary of Key Internal Control Issues Based on the COSO Internal Control Integrated Framework

	COSO Areas	Summary of Key Internal Control Issues
1	What factors have impacted recurring material weaknesses from 2013-2022?	Legacy financial systems, fragmented accountability, and inconsistent CAP validation sustained recurring weaknesses.
2	Which aspects of the control environment contributed to recurrence?	Leadership turnover, variable audit tone, and limited accountability weakened control consistency.
3	What control activities can be enhanced or implemented?	Standardize PP&E inventory, reconciliation, contract, and IT access control workflows; accelerate full Navy ERP convergence to integrate feeder systems; these account for over 80% of recurring weakness instances.
4	What is the impact of current risk assessment and communication methods?	Decentralized information systems limit visibility and delay management responses to control failures.
5	What monitoring methods can improve the Navy's internal control system?	Deploy AI-driven dashboards, cross-command audit liaisons, and risk-linked CAP databases with automated closure validation and enterprise-level validation triggers to improve closure accuracy and accountability.

C. CONCLUSION

Analysis of a decade of SOA (2013-2022) reports reveals five material weakness areas that persisted for 7 or more FYs, demonstrating that these deficiencies are structurally embedded within the DON's internal control environment. The endurance of these material weaknesses is linked to legacy business systems, decentralized execution of financial processes, and high personnel turnover that disrupt institutional knowledge cycles (DoD OIG, 2022; GAO, 2024). Challenges in Property, Plant, and Equipment (PP&E) valuation, feeder-system reconciliations, and contract oversight originate from non-integrated information systems and command-level variability in procedural implementation (DON, 2022b; GAO, 2023a). CAP validation was achieved only after automation began compensating for long-standing limitations in visibility and documentation reliability (DON, 2020b; DON, 2022b), illustrating the need for technological modernization to close critical control gaps. Similarly, failures in IT access controls stem from inconsistent policy

enforcement and recurring personnel rotations (DoD OIG, 2022), demonstrating how personnel instability could disrupt the effectiveness of the internal control environment.

Patterns in risk assessment, communication and monitoring activities further illuminate the systemic nature of these problems. Decentralized information systems have constrained the department's ability to act on risk information in a timely and reliable manner (GAO, 2024), inhibiting enterprise visibility and the formation of an integrated risk posture. Information and communication failures reveal that disjointed data pathways limit situational awareness at both the command and enterprise levels. Furthermore, durable remediation will require a shift toward modernized monitoring systems that integrate risk indicators with CAP status (DON, 2022b). Collectively, the findings confirm that achieving a sustainable audit-readiness posture requires coordinated reforms that integrate technology modernization, process standardization, and workforce continuity. These findings establish the basis for answering the research questions as outlined in the next section.

D. ADDRESSING RESEARCH QUESTIONS

1. What were the key themes identified over the ten-year analysis of DON's SOA reports regarding the recurring material weaknesses?

As reflected in Table 2, the key themes that were identified during the FY 2013-FY2022 period of analysis included property reporting gaps, IT gaps, fragmented systems, and documentation inconsistencies. In addition, there were issues with CAPs and decentralized oversight. Furthermore, this research study identified five material weakness areas to include: PP&E management, system reconciliation, contract oversight, CAP validation, and IT access controls.

2. How did the identified material weaknesses align to the five COSO internal control components over the ten-year analysis (FY 2013 – FY 2022) of DON's SOA reports?

As reflected in Table 3, 50% of the recurring material weaknesses were aligned to the Control Activities internal control component, 19.2% of the recurring material weaknesses were aligned to the Monitoring Activities internal control component. Furthermore, 14.8% of the recurring material weaknesses were aligned to the Information and Communication internal control component, 9.6 % of the recurring material weaknesses were aligned to the Control Environment internal control component, and 6.4% of the recurring material weaknesses were aligned to the Risk Assessment internal control component.

3. How did the identified material weaknesses map to the Auditability Triangle elements over the ten-year analysis (FY 2013 – FY 2022) of DON's SOA reports?

As reflected in Table 5, for the Personnel element of the Auditability Triangle, the key issues identified from the material weakness areas included training, turnover, knowledge gaps, and access management. For the Processes element of the Auditability Triangle, the key issues identified from the material weakness areas included protocols, standards, workflows, criteria, and policies. For the Internal Controls element of the Auditability Triangle, the key issues identified from the material weakness areas included reconciliations, integration, segregation, automation, and enforcement. Furthermore, the primary drivers for the material weaknesses were in the processes and internal controls elements of the Auditability Triangle.

4. How did the identified recurring material weaknesses found in the DON's SOA reports over a ten-year period (FY 2013 – FY2022) align to primary and secondary COSO internal control components?

As reflected in Table 4, the PP&E Existence, Completeness, and Valuation material weakness area aligned primarily to Control Activities and secondarily to Information and Communications. The Feeder system to General Ledger Reconciliation Gaps material weakness area primarily aligned to the Control Activities and secondarily to Information and Communication. The Contract Payment and Oversight Deficiencies material weakness area aligned primarily to Control Activities and secondarily to Control Environment. The CAP Validation Delays and Incomplete Closure Evidence material weakness area aligned primarily to Monitoring Activities and secondarily to Control Environment and Information and Communication. The IT General Access

E. AREAS FOR FUTURE RESEARCH

The longitudinal review of a decade of DON SOA reports in this study provides valuable insights into recurring material weaknesses, but it also reveals several areas that warrant deeper inquiry. While these documents offer valuable insight into the DON's auditability challenges, additional research is needed to more fully illuminate the structural, behavioral, and technological forces that shape audit readiness. Future inquiry should explore how organizational culture, leadership continuity, system modernization, and data integration influence the persistence or remediation of material weaknesses across commands and echelons. Such research would enrich academic understanding of federal government internal controls and support more targeted policy interventions to achieve durable audit outcomes.

1. Cross-Service Comparative Analysis.

Future studies should apply the same COSO–auditability mapping framework to other military branches, such as the Army and the Air Force, to evaluate institutional material weaknesses that affect audit readiness. A comparative approach would illuminate which governance structures, internal control mechanisms, or cultural factors enable certain services to handle material weaknesses more effectively than others, guiding enterprise-wide improvement.

2. Classified and Operationally Sensitive Data.

Expanding this analysis to include classified or operationally sensitive internal control data could reveal vulnerabilities not visible in public reports, particularly in logistics, acquisition, and IT networks. Examining these areas would provide a more comprehensive understanding of how security restrictions and classified systems affect auditability, risk reporting, and the integration of internal controls in mission-critical operations.

3. Post-FY2022 Trend Evaluation.

Continued monitoring through FY2027 would assess the impact of ERP convergence and the implementation of the Green Book (2025) on the recurrence of material weaknesses. Such longitudinal tracking would help determine whether recent reforms have achieved sustained control maturity as the DoD and DON transition to modernized systems and risk-based oversight.

F. SUMMARY

This chapter provided a summary of this research. In addition, conclusions were discussed, the research questions were addressed, and areas for further research were provided. The decade-long analysis of the DON's internal control environment demonstrates a complex landscape of progress and persistent vulnerability. While the reduction in open material weaknesses since FY2017 reflects meaningful advancement in transparency, oversight, and corrective action execution, the endurance of long-standing deficiencies reveals deeper systemic challenges. The integration of the COSO Internal

Control Integrated Framework and the Auditability Triangle within this study confirms that recurring weaknesses arise from interlocking failures in process consistency, workforce continuity, and the reliable application of internal controls. These factors are embedded in legacy system architectures and decentralized financial operations, creating conditions in which institutional knowledge dissipates across rotations and commands. The persistence of these deficiencies underscores that audit outcomes serve as indicators of organizational health, revealing not isolated errors but systemic misalignments between governance, technology, and human capital.

Sustainable audit readiness will require the Navy to move beyond compliance-driven remediation and adopt a holistic reform posture grounded in enterprise governance, standardized processes, and a culture of accountability. The multi-tiered recommendations based on findings presented in Chapter IV offer a coherent pathway for strengthening the Navy's internal control architecture by modernizing systems, improving personnel proficiency, enhancing monitoring through automation, and embedding risk-informed decision-making across all echelons. If fully implemented, these measures could establish a durable foundation for achieving and maintaining a clean audit opinion, an outcome that reinforces public trust, supports effective stewardship of national defense resources, and ensures that financial management practices align with the same rigor and discipline that defines the Navy's operational mission.

LIST OF REFERENCES

Association of Certified Fraud Examiners. (2012). *Report to the Nations on occupational fraud and abuse: 2012 global fraud study*. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Colgren, S. (2019). Understanding federal financial management reform: The evolution of accountability and transparency. *Journal of Government Financial Management, 68*(2), 20–27.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework: Executive summary.* https://www.sechistorical.org/collection/papers/2010/2013_0501_COSOInternal.pdf

Comptroller General of the United States. (2013). *Standards for internal control in the federal government* (GAO-14-704G). U.S. Government Accountability Office. Retrieved from https://www.gao.gov/assets/gao-14-704g.pdf

Comptroller General of the United States (2024, February). *Government auditing standards 2024 revision.* (GAO-24-106786). https://www.gao.gov/assets/d24106786.pdf

Department of Defense Office of Inspector General. (2022, November 15). *Audit of the FY 2022 Department of Defense financial statements* (DoDIG-2023-021). https://media.defense.gov/2022/Nov/15/2003122870/-1/-1/1/DoDIG-2023-021.PDF

Department of the Navy. (2013a). *Department of the Navy fiscal year 2013 annual financial report: Protecting freedom under extraordinary circumstances.* https://www.secnav.navy.mil/fmc/FR/FY13Navy_AFRprint.pdf

Department of the Navy. (2014a). *Department of the Navy fiscal year 2014 annual financial report: The nation's total force—At the right place, at the right time, all the time.* https://www.secnav.navy.mil/fmc/FR/FY14Navy_AFRprint.pdf

Department of the Navy. (2015a). *Department of the Navy fiscal year 2015 annual financial report: Around the globe, around the clock.* https://www.secnav.navy.mil/fmc/FR/FY15Navy_AFR.pdf

Department of the Navy. (2016a). *Department of the Navy fiscal year 2016 annual financial report: America's away team.* https://www.secnav.navy.mil/fmc/FR/FY16Navy_AFR.pdf

Department of the Navy. (2017a). *Department of the Navy fiscal year 2017 annual financial report: Accountability to America—Processes, people, capabilities.* https://www.secnav.navy.mil/fmc/FR/FY17Navy_AFR.pdf

Department of the Navy. (2018a). *United States Navy general fund fiscal year 2018 annual financial report: Accountability to America—Processes, people, capabilities.* https://www.secnav.navy.mil/fmc/FR/FY18Navy_AFR.pdf

Department of the Navy. (2019a). *Department of the Navy fiscal year 2019 agency financial report: Accountability to America—People, processes, capabilities.* https://www.secnav.navy.mil/fmc/FR/FY19Navy_AFR.pdf

Department of the Navy. (2020a). *Department of the Navy fiscal year 2020 agency financial report: Accountability to America—People, processes, capabilities.* https://www.secnav.navy.mil/fmc/FR/FY20Navy_AFR.pdf

Department of the Navy. (2021a). *Department of the Navy fiscal year 2021 agency financial report: One Navy–Marine Corps team.* https://www.secnav.navy.mil/fmc/FR/FY21Navy_AFR.pdf

Department of the Navy. (2022a). *Department of the Navy fiscal year 2022 agency financial report: One Navy–Marine Corps team.* https://www.secnav.navy.mil/fmc/FR/FY22Navy_AFR.pdf

Department of the Navy. (2013b). *Department of the Navy fiscal year 2013 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2014b). *Department of the Navy fiscal year 2014 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2015b). *Department of the Navy fiscal year 2015 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2016b). *Department of the Navy fiscal year 2016 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2017b). *Department of the Navy fiscal year 2017 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2018b). *Department of the Navy fiscal year 2018 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2019b). *Department of the Navy fiscal year 2019 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2020b). *Department of the Navy fiscal year 2020 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2021b). *Department of the Navy fiscal year 2021 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Department of the Navy. (2022b). *Department of the Navy fiscal year 2022 statement of assurance.* https://www.secnav.navy.mil/fmc/fmo/Pages/Financial-Reports.aspx

Federal News Network. (2021). Department of Defense financial management delays audit readiness target to 2028. Retrieved from https://federalnewsnetwork.com/defense-main/2021/05/dod-targets-2028-for-first-clean-financial-statement-audit/

Government Accountability Office. (2020, October 13). *DoD financial management: Continued efforts needed to correct material weaknesses identified in financial statement audits* (GAO-21-157). https://www.gao.gov/products/gao-21-157

Government Accountability Office. (2023a). *DoD Financial Management: Additional Actions Needed to Achieve a Clean Audit Opinion on DoD's Financial Statements (GAO-23-105784).* https://www.gao.gov/assets/gao-23-105784.pdf

Government Accountability Office. (2023b, July 13). *DoD financial management*: *Efforts to address auditability and systems challenges need to continue (GAO-23-106941)*. https://www.gao.gov/assets/gao-23-106941.pdf

Government Accountability Office. (2024, September 24). *Financial management: DoD has identified benefits of financial statement audits and could expand its monitoring* (GAO-24-106890). https://www.gao.gov/products/gao-24-106890

Government Accountability Office. (2025). *Standards for internal control in the federal government* (GAO-25-107721). U.S. Government Accountability Office. Retrieved October 26, 2025, from https://www.gao.gov/products/gao-25-107721

Grigoryan, K. (2023). Auditability theory: Frameworks for organizational transparency and accountability. *Journal of Public Sector Auditing, 15*(1), 45–61.

McGivern, C. (2024). Internal control weaknesses in Navy agency financial reports (2018–2022): A COSO-based analysis [Unpublished master's thesis]. Naval Postgraduate School.

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

Mohammed, H. K., Ahmed, I. A., & Ji, X. D. (2021). Internal control frameworks and its relation with governance and risk management: An analytical study. *Journal of Governance and Regulation, 10*(2), 8–17.

National Defense Authorization Act for Fiscal Year 2010, Public Law No. 111–84, §1003. Retrieved from https://www.congress.gov/111/plaws/publ84/PLAW-111publ84.pdf

Office of Management and Budget. (2000). Circular No. A-123: Management's responsibility for internal control. Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A123/a123_rev.pdf

Office of Management and Budget. (2016). OMB Circular No. A-123: Management's responsibility for enterprise risk management and internal control. Executive Office of the President. https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A123/a123_rev.pdf

Office of Management and Budget. (2023). *Bulletin No. 24-01: Audit requirements for federal financial statements.* Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2023/10/Bulletin-24-01-Audit-Requirements-for-Federal-Financial-Statements.pdf

Office of the Commandant. (2022). Internal controls and risk management guidance. U.S. Department of Defense.

Office of the Under Secretary of Defense (Comptroller). (2024, June). Department of Defense financial management regulation, volume 1: " General financial management information, systems, and requirements" (DoD 7000.14-R).https://comptroller.defense.gov/Portals/45/documents/fmr/Volume_01.pdf

Office of the Under Secretary of Defense (Comptroller)/(Chief Financial Officer. (2017). Financial improvement and audit readiness (FIAR) guidance. U.S. Department of Defense.

Rae, K., Sands, J., & Subramaniam, N. (2017). Associations among the five components within COSO Internal Control Integrated Framework as the underpinning of quality corporate governance. *Australasian Accounting, Business and Finance Journal, 11*(1), 28–54.

Ramos, M. J. (2008). *How to comply with Sarbanes-Oxley Section 404: Assessing the effectiveness of internal control* (3rd ed.). Wiley.

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://doi.org/10.1504/IJPM.2015.072388

Rendon, R. G., & Snider, K. F. (Eds.). (2008). *Management of defense acquisition projects*. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/4.479502

Schantl, S. F., & Wagenhofer, A. (2020). Optimal internal control regulation: Standards, penalties, and leniency in enforcement. *Journal of Accounting and Economics, 40(3)*,101–2316.

Zahari, A. S. M., Said, J., & Arshad, R. (2024). Internal control on public organisation performance: A SmartPLS analysis using COSO framework. *Public Administration and Policy, 27*(1), 1–17.

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

www.acquisitionresearch.net