NPS-PM-26-231

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Residual Audit and Accountability Risk in Navy Ordnance Reporting and Reconciliation Under Ordnance Information System 2.0

June 2026

LT Matthew R. Kenyon, USN
LCDR Christopher L. Runge, USN
LCDR Wave K. Ryder, USN

Thesis Advisors: Dr. Juanita M. Rendon, Lecturer
Dr. Ira A. Lewis, Professor

Department of Acquisition, Finance and Manpower

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943

ACQUISITION RESEARCH PROGRAM
DEPARTMENT OF ACQUISITION, FINANCE AND MANPOWER
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Department of Acquisition, Finance and Manpower 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 Acquisition, Finance and Manpower
Naval Postgraduate School

ABSTRACT

Navy ordnance reporting and reconciliation continues to generate recurring audit and accountability deficiencies under Ordnance Information System (OIS) 2.0 despite documented processes, established internal controls, and ongoing remediation efforts. This study examines residual audit and accountability risk by analyzing 161 ordnance-related deficiencies documented in the Navy's Deficiency Tracking Tool (DTT). Using a qualitative diagnostic research design, the study classified deficiencies through the Auditability Triangle and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control–Integrated Framework, then evaluated residual risk through an ISO 31000-informed qualitative risk assessment. Findings indicate that recurring deficiencies are not confined to OIS 2.0. Of the 161 reviewed deficiencies, 28 were directly associated with OIS, while 133 were associated with the broader enterprise environment. Across both environments, deficiencies were concentrated primarily in process and internal control conditions rather than personnel factors, with recurring weaknesses in control activities and information and communication. The study concludes that recurring ordnance-related deficiencies reflect structural process, control, information, and governance constraints within the current operating environment rather than isolated execution failures.

THIS PAGE INTENTIONALLY LEFT BLANK

ABOUT THE AUTHORS

LT Matt Kenyon is a Navy Supply Corps Officer. He was commissioned through Officer Candidate School (OCS) following completion of his undergraduate studies at Cazenovia College, where he earned a Bachelor of Science in Criminal Justice, Homeland Security, and Psychology. After graduating from the Naval Postgraduate School, he will report to NAVSUP Fleet Logistics Center Norfolk, Virginia, where he will serve in a contracting billet.

LCDR Wave Ryder is a Navy Supply Corps Officer who graduated from the United States Naval Academy in 2014 with a Bachelor of Science in Economics. He served aboard USS JEFFERSON CITY (SSN 759) in Pearl Harbor, where he earned his Submarine qualification, before transferring to Priority Material Office as the West Region Officer in Charge and Logistics Integration Action Officer. He later returned to sea aboard USS MAKIN ISLAND (LHD 8), serving as Stock Control Officer and Aviation Support Officer while earning his Surface Warfare Supply Corps Officer and Naval Aviation Supply Officer warfare qualifications. In 2023, he reported to NAVSUP FLC San Diego, serving in Code 430 as Fuels and Operations Officer supporting the Littoral Combat Ship class and later in Code 500 as Logistics Operations Officer. He is currently pursuing a Master's in Defense Contract Management at the Naval Postgraduate School and, upon graduation, will report to NAVSUP WSS Philadelphia.

LCDR Christopher Runge earned his commission through Navy Officer Candidate School in Newport, Rhode Island. His assignments include Supply Officer at PCU VERMONT (SSN 792), Supply Response Section Division Officer at Aviation Support Detachment Lemoore, California, and Aviation Support Officer aboard USS KEARSARGE (LHD 3). He then attended the Naval Postgraduate School. Upon graduation, he will report to Diego Garcia to serve as Director, Fleet Logistics Center Diego Garcia.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express our sincere appreciation to the individuals who supported this research through their time, expertise, and willingness to assist our team. We are especially grateful to Steven Flowers, Donald Moor, Amber Lehman, and Amanda Crockett. Their support helped our team better understand the ordnance reporting, reconciliation, OIS modernization, and auditability environment examined in this study. We also thank Dr. Juanita Rendon for taking us on as our advisor and for guiding the development of this capstone. We are grateful to Michelle Morneau of the Graduate Writing Center at the Naval Postgraduate School for her writing support and feedback. Finally, we thank our families for their patience and encouragement throughout this process.

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-PM-26-231

ACQUISITION RESEARCH PROGRAM
SPONSORED REPORT SERIES

Residual Audit and Accountability Risk in Navy Ordnance Reporting and Reconciliation Under Ordnance Information System 2.0

June 2026

LT Matthew R. Kenyon, USN
LCDR Christopher L. Runge, USN
LCDR Wave K. Ryder, USN

Thesis Advisors: Dr. Juanita M. Rendon, Lecturer
Dr. Ira A. Lewis, Professor

Department of Acquisition, Finance and Manpower

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943

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

A-123	Office of Management and Budget Circular A-123
A-94	Office of Management and Budget Circular A-94
COMNAVSUPSYSCOM	Commander, Naval Supply Systems Command
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DoD	Department of Defense
DoD OIG	Department of Defense Office of Inspector General
DON	Department of the Navy
DTT	Deficiency Tracking Tool
EY	Ernst & Young
FIAR	Financial Improvement and Audit Readiness
FY	fiscal year
GAGAS	Government Auditing Standards
GAO	Government Accountability Office
Green Book	GAO Standards for Internal Control in the Federal Government
IRB	Institutional Review Board
ISO	International Organization for Standardization
IT	information technology
MICP	Manager's Internal Control Program
NALC	NAVSUP Ammunition Logistics Center
NAVSUP	Naval Supply Systems Command
NFR	Notice of Finding and Recommendation
NMC	Navy Munitions Command
NOMP	Naval Ordnance Management Policy
OIS	Ordnance Information System
OIS-R	Ordnance Information System-Retail
OIS-W	Ordnance Information System-Wholesale
OM&S-O	Operating Materials and Supplies-Ordnance
OMB	Office of Management and Budget
OPNAV	Office of the Chief of Naval Operations

OPNAVINST	Office of the Chief of Naval Operations Instruction
PII	personally identifiable information
RMIC	Risk Management and Internal Control

I. INTRODUCTION

Accurate reporting and timely reconciliation are foundational to the Navy's conventional ordnance enterprise because they directly support operational readiness, explosive safety, and Department of Defense (DoD) financial audit requirements. Ordnance transactions occur across multiple organizations and operating environments, including the Naval Supply Systems Command (NAVSUP) Ammunition Logistics Center (NALC), Navy Munitions Commands, Type Commanders, and operational units. These organizations collectively perform reporting and reconciliation activities used to document ordnance receipts, issues, transfers, and inventory adjustments. When reporting is incomplete, delayed, or inconsistent, ordnance visibility degrades, discrepancies accumulate across systems and records, and the conditions necessary for audit support are undermined.

Beyond operational visibility, accurate ordnance reporting is essential to achieving auditability for Operating Materials and Supplies-Ordnance (OM&S-O). Independent audits require reliable, timely, and complete transaction records to support assertions related to existence, completeness, and valuation. Despite formally documented processes and sustained remediation efforts, audits continue to identify recurring discrepancies affecting ordnance reporting and reconciliation across the Navy under Ordnance Information System (OIS) 2.0. The persistence of these deficiencies suggests that auditability challenges remain embedded in current operating conditions, even where corrective actions have been formally initiated.

Prior research has examined the Navy ordnance enterprise primarily from organizational, governance, and system modernization perspectives (Potvin et al., 2021). However, that research has not systematically analyzed how recurring audit deficiencies persist under current operating conditions. As a result, remediation efforts risk addressing procedural symptoms without fully accounting for the operational and informational constraints that shape how controls function in practice.

This research uses two theoretical frameworks to analyze recurring audit and accountability deficiencies. First, the Auditability Triangle provides a basis for

distinguishing whether deficiencies are primarily associated with personnel, processes, or internal controls (Rendon & Rendon, 2015). Second, the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control–Integrated Framework, hereafter referred to as the COSO Framework, provides a basis for examining how internal controls are described, applied, and constrained in practice (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2013). Together, these frameworks support the analysis of auditability conditions within the current OIS 2.0 operating environment. A qualitative risk assessment informed by International Organization for Standardization (ISO) 31000 principles is then used to synthesize relative levels of residual audit and accountability risk (ISO, 2018). This study focuses on conditions that persist under existing system constraints and provides decision-relevant insight into the audit and operational risk posture the Navy continues to manage while remediation efforts remain ongoing.

A. BACKGROUND

A review of prior oversight and research demonstrates that recurring accountability problems in Navy ordnance reporting remain insufficiently explained under current system conditions. Navy ordnance reporting and reconciliation have been the subject of recurring audit findings despite the existence of formally documented processes and sustained remediation efforts, as documented in multiple Department of Defense Office of Inspector General reports (Department of Defense Office of Inspector General [DoD OIG], 2022, 2024a). Prior research on examining the organization and governance of the Navy ordnance enterprise likewise identified persistent challenges related to accountability, process alignment, and end-to-end visibility; however, that work did not examine how such challenges are manifested in recurring audit findings under current system conditions (Potvin et al., 2021). Independent oversight products from the Government Accountability Office (GAO) have similarly identified deficiencies in DoD-wide logistics data accuracy, inventory record reliability, and business-system compliance, though these findings are not specific to the Navy ordnance enterprise (GAO, 2024). Taken together, these oversight and research efforts establish that recurring accountability challenges are well documented, but they do not isolate how those

challenges continue to persist within the Navy's ordnance reporting environment under existing system constraints.

Deficiency information consolidated within the Deficiency Tracking Tool (DTT) indicates that these issues are documented within the operating environment of OIS 2.0, which relies on delayed system updates and manual reconciliation between retail and wholesale records. While OIS 3.0 is expected to improve data integration and timeliness, its implementation has been deferred, requiring the ordnance enterprise to continue operating under OIS 2.0 through the upcoming audit cycle. Consequently, audit and accountability risks must be managed within existing system constraints while remediation efforts continue.

The COSO Framework recognizes that internal controls as a process "[provides] reasonable assurance of achievement of an entity's objectives" (COSO, 2013, p. 1). The framework emphasizes that, even when internal control is effective, it reduces risk only to an acceptable level because inherent limitations remain, including human error, flawed judgment, management override, collusion, and external events outside organizational control (COSO, 2013). Within this framework, system and information constraints shape how controls are selected, implemented, and monitored, particularly where relevant, quality information or supporting technology controls are limited (COSO, 2013). In this context, system and information constraints are important conditions affecting control performance, especially regarding the effectiveness of technology-supported control activities. Accordingly, recurring audit effectiveness of technology-supported control activities and residual risk may remain even when controls are properly designed and implemented (COSO, 2013). Within this context, system and information constraints shape the conditions under which internal controls operate, influencing the persistence of certain audit findings without necessarily indicating control absence or noncompliance.

This research study examines the residual audit and accountability risk associated with ordnance reporting and reconciliation under OIS 2.0, as documented in the DTT deficiency population. Rather than evaluating future system performance or proposing governance reforms, this research focuses on practices and control weaknesses reflected in documented deficiencies under existing OIS 2.0 conditions. By analyzing documented

ordnance-related deficiencies consolidated in the DTT from multiple oversight sources, this study classifies recurring audit and accountability deficiencies using the Auditability Triangle, maps them to COSO internal control components, and evaluates their relative residual risk using the ISO 31000-informed qualitative risk framework described in Chapter III. This approach provides a structured assessment of the frequency, classification, and relative severity of recurring audit and accountability deficiencies documented under OIS 2.0.

B. IMPORTANCE OF THE RESEARCH

Persistent accountability and reporting deficiencies in Navy ordnance reporting indicate that residual audit and accountability risk continues to be managed within current processes and system conditions. Despite sustained remediation efforts and formally documented controls, independent oversight continues to identify recurring deficiencies, suggesting that some risks are embedded in operating conditions rather than attributable solely to control design or personnel compliance.

By systematically analyzing documented deficiencies using established internal controls, auditability, and qualitative risk management frameworks, this research clarifies where controls function as intended, where execution is constrained by information quality or system limitations, and where residual risk persists under current operating conditions. This distinction is critical for decision-makers because it enables more precise prioritization of remediation efforts and supports differentiation between risks that can be mitigated through improved execution and those that must be actively managed until system constraints change.

C. RELEVANCE TO THE DEPARTMENT OF THE NAVY AND DEPARTMENT OF DEFENSE

Persistent audit and accountability deficiencies in Navy ordnance reporting carry implications for audit readiness, financial reporting reliability, and ordnance governance across the Department of the Navy (DON) and the DoD. As the Navy continues to operate under OIS 2.0, senior leaders must assess and manage audit and accountability risk within existing system constraints while remediation efforts remain ongoing. By synthesizing documented deficiencies consolidated across multiple independent oversight sources, this study provides structured analytic insight to support risk awareness and

internal control decision-making consistent with federal audit and internal control standards (DoD OIG, 2022; DoD OIG, 2024b; GAO, 2025). In doing so, this research contributes to a clearer understanding of the operational risk posture the DON continues to manage under current system conditions.

D. RESEARCH PURPOSE

The purpose of this research is to conduct an internal control and qualitative risk analysis of Navy ordnance reporting and reconciliation under OIS 2.0 using documented deficiencies consolidated within the DTT. This study examines recurring deficiencies identified across multiple independent oversight sources, including Ernst & Young (EY) Notices of Finding and Recommendation (NFR), Navy and Marine Corps financial audits, roadmaps, Statements of Assurance, GAO reports, and DoD OIG reports.

Deficiencies are analyzed using the Auditability Triangle and the COSO Framework to identify which control components and execution conditions are most frequently implicated. A qualitative risk evaluation aligned with ISO 31000 is then applied to assess residual accountability and reporting risk within the current OIS 2.0 operating environment (International Organization for Standardization [ISO], 2018). This study develops practical, non-structural insights intended to inform risk management and internal control execution without assuming system replacement or organizational restructuring.

E. RESEARCH QUESTIONS

To guide the analysis, this study addresses five research questions examining how OIS-related deficiencies compare with the broader deficiency population and what those patterns indicate about recurring control deficiencies.

1. Of all the deficiencies documented in the DTT, how many of those deficiencies are directly related to OIS 2.0?
2. How do the identified deficiencies align with the Auditability Triangle drivers to distinguish whether breakdowns are primarily driven by personnel, processes, or internal controls?
3. How do the identified deficiencies align with the five components of the COSO Internal Control Framework, and which internal control components are most frequently implicated?
4. How do the deficiencies aligned to the Auditability Triangle drivers and mapped to the COSO internal control components manifest as qualitative

audit and accountability risks when viewed through the lens of ISO 31000?

5. What are the overarching organizational factors contributing to recurring deficiencies?

F. OVERVIEW OF METHODOLOGY

This research evaluates residual audit and accountability risk in Navy ordnance reporting and reconciliation under the current OIS 2.0 operating environment. The period of analysis ranges from FY2005 to FY2025. The scope of this study is limited to secondary, pre-existing deficiency data extracted from the DTT, which consolidates documented deficiencies identified through federal audit and oversight activities. These sources include EY NFRs, Navy and Marine Corps financial audits, Statements of Assurance, audit roadmaps, and reports issued by the GAO and the DoD OIG. The documented deficiencies are treated as independent evidence of recurring discrepancies affecting the completeness, accuracy, timeliness, and supportability of Navy ordnance reporting and reconciliation processes. This study's primary emphasis is on OM&S-O reporting and closely related ordnance populations, thereby concentrating on the population most directly implicated in recurring audit findings. No personally identifiable information (PII) will be used in this research study.

This study employs a structured qualitative diagnostic approach to systematically interpret documented deficiencies as recurring indicators of control execution and auditability constraints. Each event is evaluated using three complementary analytical lenses: the COSO Framework, the Auditability Triangle, and qualitative risk assessment concepts consistent with ISO 31000. The analysis focuses on identifying recurring themes and patterns across deficiencies, determining which internal control components and auditability drivers are most frequently implicated, and assessing the relative level of residual audit and accountability risk associated with persistent discrepancies.

The scope of recommendations produced by this study is intentionally limited to practical, non-structural improvements that can be implemented within existing system constraints. This research does not evaluate future system performance, does not assess the effectiveness of OIS 3.0, and does not propose enterprise-level governance restructuring. Instead, it provides decision-relevant insight into the residual risk that remains under OIS 2.0 and identifies feasible actions to reduce repeat deficiencies

through improved internal control execution, monitoring, documentation discipline, and risk prioritization.

G. LIMITATIONS OF RESEARCH

This research study is subject to several limitations. First, this study relies on deficiency data consolidated within the DTT, which reflects the scope, timeframe, and linkage of prior audit and oversight activities. As a result, the dataset may not capture all operational challenges affecting ordnance reporting and accountability, particularly those that have not resulted in formally documented deficiencies. In addition, this study references limited system briefings and contextual information provided by points of contact at the NALC to clarify data provenance and operational context in which deficiencies occur. This information is used solely to inform the analytical context of this study and is not treated as independent research evidence or subject to formal analysis.

Second, the research relies on qualitative classification to map deficiencies to COSO internal control components, Auditability Triangle drivers, and ISO 31000 risk concepts. These classifications rely on professional judgement and the level of detail available in the documented deficiency descriptions. Although standardized coding criteria are applied to improve consistency, some degree of subjectivity is inherent in interpreting deficiency language and assigning analytical categories.

Third, residual audit and accountability risk is evaluated using qualitative assessments rather than quantitative financial modeling. The analysis is intended to support prioritization and managerial decision-making by identifying higher-risk themes and recurring control breakdowns. It does not calculate precise dollar impacts, statistical confidence intervals, or predictive estimates of misstatements.

Finally, this study is bound by the OIS 2.0 operating environment and does not assess the effectiveness of future modernization initiatives or system replacements. Recommendations are designed to be feasible under current system constraints and may not address broader structural or enterprise-wide reforms outside the scope of this research.

H. ORGANIZATION OF THE STUDY

This research is organized into five chapters:

Chapter I introduces this study by providing the background on Navy Ordnance reporting and reconciliation under the OIS 2.0 operating environment. It defines the research problem, research purpose, and research questions, and explains the importance of examining residual audit and accountability risk associated with recurring independent audit findings. In addition, this chapter discusses the methodology used in this research as well as the limitations of this research.

Chapter II presents the literature review and establishes the theoretical foundation for this study. It includes a review of internal control concepts and frameworks applicable to public-sector auditability, including the COSO Framework, auditability theory and the Auditability Triangle, and qualitative risk management concepts consistent with ISO 31000. This chapter also summarizes prior research and institutional context related to Navy ordnance accountability, audit remediation efforts, and the challenges of achieving sustained auditability in complex OM&S-O environment.

Chapter III describes the research methodology and analytical approach. It presents an explanation of the study design, data sources, and procedures used to extract documented conditions, causes, and effects from EY NFRs contained within the DTT, and converts them into a structured event-level database. This chapter details how events are coded and analyzed using the Auditability Triangle, mapped to COSO internal control components, and assessed through a qualitative residual risk evaluation aligned with ISO 31000 principles.

Chapter IV presents the results of the event-level analysis. It summarizes the overall DTT dataset, identifies the most frequent recurring auditability and internal control breakdown themes, and highlights patterns across the OIS and Enterprise Environments. This chapter provides descriptive findings showing where control execution breakdowns persist and where residual risk remains concentrated under current system constraints. It also presents recommendations based on the findings of this research, including measures to reduce recurring deficiencies, strengthen control execution, improve information reliability, and support more durable remediation outcomes.

Chapter V presents this study's summary and conclusions. This chapter also summarizes the key findings, addresses the research questions, and identifies areas for future research. Additionally, Chapter V synthesizes the overall significance of the findings and explains how the results contribute to understanding recurring ordnance-related audit and accountability risk across the ordnance accountability enterprise.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Understanding why recurring audit deficiencies persist under OIS 2.0 requires grounding the analysis in established theory and regulatory standards governing auditability, internal control, and risk management. This chapter reviews the theoretical and regulatory foundations that frame how audit findings may persist despite documented procedures, qualified personnel, and ongoing remediation efforts within the Ordnance Enterprise.

A. INTRODUCTION

The review begins by discussing OIS 2.0 and prior thesis work that identified challenges in ordnance reporting and accountability and establishing the basis for further examination of the ordnance reporting system (Potvin et al., 2021). It then examines auditability theory and its applicability to the Navy's OIS 2.0, with attention given to the interaction between personnel, processes, and internal controls. Building on this foundation, the chapter reviews literature on the COSO Framework (2013) to explain how auditability conditions identified through the Auditability Triangle can be further examined through an internal control lens. Finally, the chapter reviews risk management literature on ISO 31000 to frame the assessment of residual audit and accountability risk under existing system constraints. The following section discusses OIS 2.0.

B. ORDNANCE INFORMATION SYSTEM 2.0

The Navy requires a method for tracking ordnance, accounting for ordnance transactions and balances, and maintaining the records needed to support operational control and financial accountability. Supporting this requirement is OIS 2.0, which functions as the Navy's enterprise ordnance information program for transaction processing, accountability, and reporting (Moor, D., PowerPoint slides, September 9, 2024). Office of the Chief of Naval Operations Instruction (OPNAVINST) 8000.16G identifies Commander, Naval Supply Systems Command (COMNAVSUPSYSCOM) as the responsible entity for the program management for OIS, with COMNAVSUPSYSCOM field activities performing maintenance of the system in support of the Naval Ordnance Management Policy (NOMP) (Office of the Chief of

Naval Operations [OPNAV], 2021). This assignment of responsibility places OIS 2.0 within the Navy's formal logistics and accountability structure.

OIS 2.0 is divided into two main parts: OIS-Retail (OIS-R) and OIS-Wholesale (OIS-W). OIS-R supports routine transaction processing, including use by fleet units that may temporarily lose communications and later synchronize their transactions back to the main system. OIS-W serves as the aggregate system used for broader reporting and data consolidation (Moor, D., PowerPoint slides, September 9, 2024). OIS 2.0 also relies heavily on batch processing rather than real-time posting, with about 250 batch jobs running on scheduled intervals (Moor, D., PowerPoint slides, September 9, 2024). As a result, transactions moving between OIS-R and OIS-W may take roughly 10 to 55 hours to process depending on the direction of transfer and message type (Moor, D., PowerPoint slides, September 9, 2024). These characteristics show that OIS 2.0 relies on scheduled processing and delayed data exchange, which can affect the timeliness, traceability, and reconciliation reliability of ordnance reporting. Understanding these system-level constraints helps frame the conditions under which prior analyses examined ordnance reporting challenges and helps explain why persistent discrepancies have been interpreted in different ways. The following section addresses prior analyses of Navy ordnance reporting.

C. PRIOR ANALYSES OF NAVY ORDNANCE REPORTING

Prior analyses of Navy ordnance reporting have identified systemic challenges related to asset visibility, inventory accuracy, and organizational alignment, but did not evaluate how these challenges manifest in recurring audit findings under current system conditions (Potvin et al., 2021). Potvin et al. (2021) examine overaged in-transit ordnance and concluded that persistent discrepancies were primarily attributable to fragmented command relationships and the absence of a single end-to-end process owner. Their study relied on 12 months of overaged in-transit data and a detailed mapping of the existing ordnance organizational structure. Based on one period of transactional data, the authors recommend large-scale organizational realignment intended to consolidate authority and standardize practices across multiple echelons of the ordnance supply chain (Potvin et al., 2021).

Although Potvin et al. (2021) establish that ordnance accountability challenges are systemic rather than isolated, its emphasis on organizational restructuring reflects conclusions drawn from a limited dataset. Their research does not examine overaged, in-transit data through an explicit accountability or internal control framework. Consequently, their analysis does not assess how audit and accountability risk may persist under existing system and control constraints, even in the absence of structural reorganization. The following section discusses Auditability Theory.

D. AUDITABILITY THEORY

Power (2007) argues that auditability reflects an organization's ability to produce verifiable evidence of its control environment through structured documentation and information systems. Auditability, in this sense, precedes the audit itself and reflects the institution's use of documentation systems and control processes that make objective verification possible.

Building on this foundation, this study operationalizes auditability as emerging from the interaction of personnel competence, process capability, and the design and execution of internal controls, consistent with the Auditability Triangle framework advanced by Rendon and Rendon (2015). Therefore, in both public-sector and defense accounting environments, auditability extends beyond procedural compliance and reflects the organization's capacity to generate verifiable evidence that substantiates financial and operational statements.

Generally Accepted Government Auditing Standards (GAGAS) require auditors to base findings and conclusions on sufficient and appropriate evidence and to assess the reliability of system-generated data used in forming those conclusions (GAO, 2024). As a result, audit outcomes depend not only on whether policies exist or procedures are followed, but on whether underlying systems and control processes generate information that can be verified and relied upon, a requirement reflected in both federal auditing standards and the emphasis on internal controls and information quality in auditability theory (GAO, 2025; Rendon & Rendon, 2015). An organization may formally comply with internal documented requirements and still have ineffective internal controls if its

financial recordkeeping systems fail to generate information that enables objective verification, regardless of compliance with procedures.

The DoD's experience with financial statement audits illustrates this distinction between compliance and auditability. Although remediation initiatives have addressed many previously identified deficiencies, DoD financial statement audits have repeatedly concluded with a disclaimer of opinion because auditors determined that available audit evidence and system-generated data did not provide a verifiable evidentiary basis for an opinion (DoD OIG, 2022). The persistence of these outcomes has been associated with limitations in data reliability, system integration, and control execution rather than the absence of corrective action alone (DoD OIG, 2022). This pattern reflects a broader reality in complex organizations where procedural reform and documented compliance do not automatically translate into improved auditability when system constraints and data limitations degrade the quality of available evidence.

Within the Navy ordnance enterprise, accountability challenges have similarly persisted over time. Historical analyses identified long-standing deficiencies in ammunition accountability and inventory reporting, even as systems and procedures evolved (Horan, 1981). More recent research indicates that ordnance reporting discrepancies are systemic rather than isolated, reflecting enterprise-level conditions that span organizational boundaries and information systems (Potvin et al., 2021). That analysis emphasized governance fragmentation and organizational alignment as primary explanatory factors and accordingly advanced structural and ultimate authority remedies. This research study instead evaluates whether auditability constraints may also arise from the interaction of personnel, processes, internal controls, and system behavior, independent of formal command structure. This distinction supports examining auditability as a function of system and control interaction rather than if governance reform or procedural rigor alone would resolve recurring audit findings.

In complex public-sector environments, auditability is increasingly shaped by the effectiveness and integration of enterprise information systems rather than by the presence of documented procedures alone (DoD OIG, 2022). When enterprise systems introduce delays, data gaps, or reconciliation constraints, audit evidence may fail to meet

sufficiency thresholds even when controls are formally designed and executed (DoD OIG, 2022). These conditions reflect auditability challenges rooted in system architecture rather than discrete instances of noncompliance. The following section addresses the Auditability Triangle.

E. AUDITABILITY TRIANGLE

Rendon and Rendon (2015) frame auditability as an organizational condition shaped by the interaction of personnel competence, process integrity, and internal control execution, rather than as a simple function of procedural compliance. The framework identifies three interdependent elements: personnel, processes, and internal controls that collectively shape an organization's capacity to produce auditable evidence (see Figure 1). Their central argument is that auditability cannot be explained by workforce competence alone, as trained personnel operate within procedural and control environments that condition whether evidence can be generated, retained, and evaluated (Rendon & Rendon, 2015).

GAGAS require auditors to establish that the evidentiary basis for their conclusions is both substantively adequate and trustworthy, with the strength of that evidence influenced by the origin, method of generation, and integrity of the underlying data (GAO, 2024). When audit evidence is derived primarily from information systems, personnel performance alone does not determine auditability; rather, audit conclusions depend on whether system-generated evidence can support audit objectives. From an auditability perspective, this creates conditions in which personnel may execute required actions as intended while remaining unable to substantiate those actions if the available evidence does not meet audit standards.

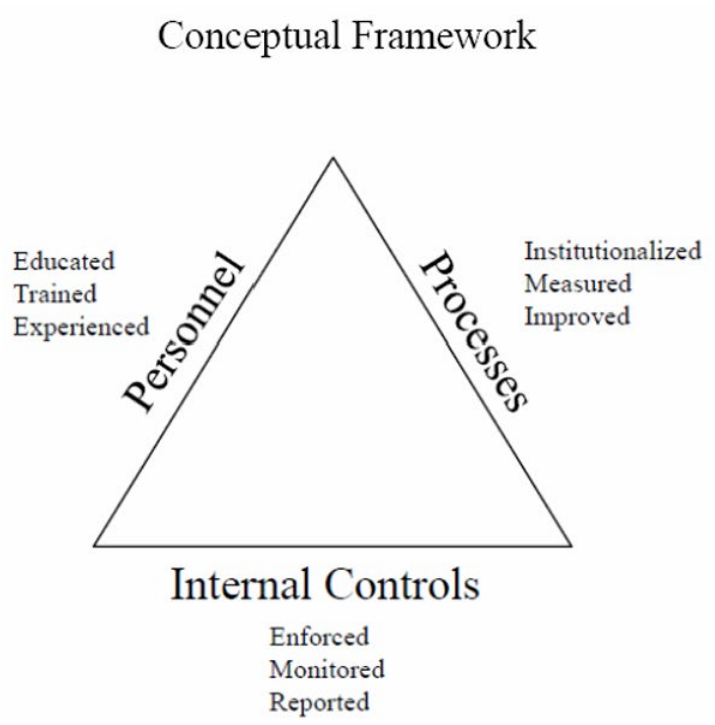

Figure 1. Auditability Triangle. Adapted from Rendon and Rendon (2015)

1. Processes as an Auditability Condition

Rendon and Rendon (2015) describe processes as the structured procedures through which transactions are initiated, recorded, and carried out, and through which internal controls are embedded and executed. These processes shape how activities are executed and how information flows across the organization, influencing whether transactions can be documented in a manner that supports accountability.

GAGAS require auditors to base their conclusions on a defensible evidentiary record and place responsibility on management to produce information that allows internal control performance to be independently assessed (GAO, 2024). In system-mediated environments, process design characteristics, such as sequencing, system handoffs, and reconciliation logic, directly influence whether transactions can be traced and supported by auditable records (Moor, D., PowerPoint slides, September 9, 2024). Government Auditing Standards emphasize the importance of understanding internal control and the information systems that support program operations, including how data are generated, processed, and communicated within and across organizational boundaries

(GAO, 2024). Even where individual process steps are documented and executed, limitations in process integration may constrain auditors' ability to obtain evidence necessary to support management assertions.

2. Internal Controls as an Auditability Condition

Effective internal controls are essential to organizational accountability and auditability. Internal controls provide the mechanisms through which processes are governed, monitored, and corrected to support organizational objectives (COSO, 2013). Control standards emphasize the importance of producing relevant, reliable, and complete information to support accountability and oversight (GAO, 2025). Rather than defining internal controls in prescriptive terms, Rendon and Rendon (2015) situate them within a broader auditability system, emphasizing that Internal Controls must function in concert with personnel and processes to support the production of auditable evidence. This perspective underscores why internal controls must be examined not only as formal requirements, but also as practical tools that shape the reliability of procurement outcomes.

When internal controls depend on information systems that do not produce evidence meeting audit standards, auditability may be constrained regardless of personnel competency or procedural compliance. Rendon and Rendon (2015) emphasize that auditability is contingent on the coordinated performance of Personnel, Processes, and Internal Control structures; when these elements are misaligned, organizational effectiveness in achieving accountability and transparency is diminished, and the organization's capacity to produce information suitable for audit and verification is correspondingly reduced. Consistent with this perspective, DoD OIG audits of financial statements in fiscal years 2021 and 2023 report recurring deficiencies in internal control execution, particularly those related to system integration, data reliability, and reconciliation.

3. Implications for Ordnance Accountability Analysis

A structured conceptual framework is necessary to evaluate the sources of recurring audit findings. By anchoring this study in the Auditability Triangle, the analysis avoids presuming that recurring audit findings reflect inadequate training or procedural

noncompliance (Rendon & Rendon, 2015). Instead, the framework provides a structured basis for examining how personnel actions, process design, and internal control execution interact under system constraints to shape audit outcomes. This conceptual foundation supports subsequent analysis applying internal control frameworks and qualitative risk assessment methods to evaluate residual audit risk under OIS 2.0, particularly in environments where controls rely heavily on system-generated evidence. The following section discusses the generally accepted government audit standards (GAGAS).

F. GOVERNMENT AUDITING STANDARDS

A clear understanding of GAGAS is essential to evaluating audit evidence and audit conclusions. GAGAS, also known in practice as the Yellow Book, establish the professional standards for audits of federal programs, operations, and financial statements conducted by government auditors (GAO, 2024). GAGAS establish the requirements for obtaining sufficient, appropriate evidence, which auditors use to determine whether audit objectives have been met. Additionally, the GAO (2024) developed a visual representation of their Auditability Conditions which is articulated in Figure 2.

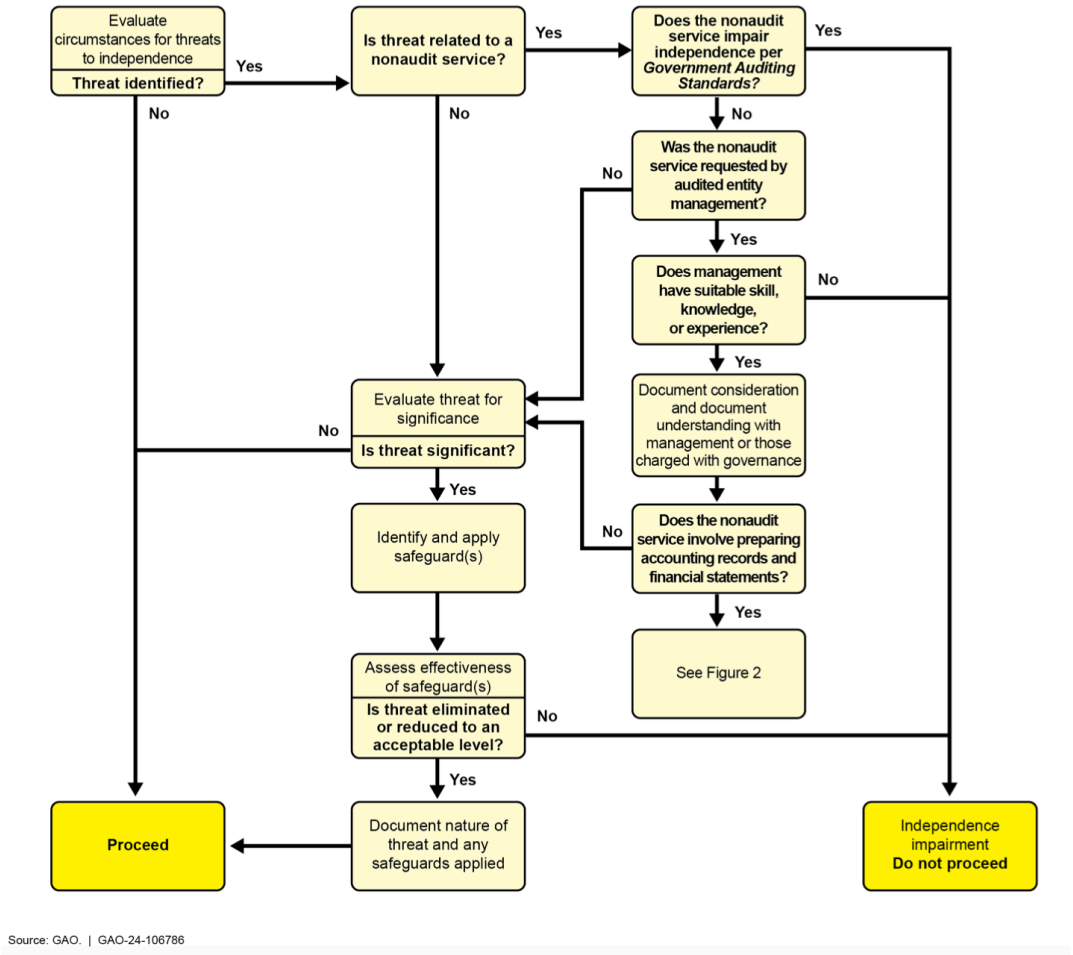

Figure 2. Auditability Conditions and Internal Control Execution. Source: GAO (2024).

Under GAGAS, auditors must base their conclusions on a defensible evidentiary foundation, with evidentiary adequacy encompassing both the quantity of supporting information and its credibility, the latter determined by the provenance of the data and their alignment with the audit objective (GAO, 2024). Auditors are required to exercise professional judgment in determining whether the evidence collected meets these criteria in relation to the audit objectives. The Yellow Book explains that the appropriateness of audit evidence depends on its relevance and reliability, and that reliability varies based on the source and nature of the evidence (GAO, 2024). When audits rely on data produced by information systems, auditors must evaluate whether that evidence is sufficiently reliable and relevant to support the audit objectives. The following section discusses the external oversight products and documented deficiencies.

G. EXTERNAL OVERSIGHT PRODUCTS AND DOCUMENTED DEFICIENCIES

By framing deficiencies as externally validated indicators of residual audit and accountability risk, this study avoids attributing causality or assigning responsibility and instead focuses on understanding how internal controls operate in practice under current system constraints. This approach is consistent with GAGAS, which emphasize that audit findings reflect the availability and reliability of audit evidence rather than management intent or remediation effort (GAO, 2024). Therefore, external oversight products provide a defensible, consistent foundation for examining why deficiencies persist and what level of audit and accountability risk the Navy continues to manage while operating within the OIS 2.0 Environment.

External oversight products provide the primary source of documented deficiencies affecting auditability and accountability within the Navy ordnance enterprise. These products include Notices of Finding and Recommendations issued by independent auditors, DoD OIG reports, GAO studies, Statements of Assurance, and related audit roadmap documentation. Collectively, they document conditions in which audit objectives could not be supported because control execution, process design, or supporting documentation did not produce sufficient evidence to meet audit requirements. Rather than evaluating management intent, these reports describe the evidentiary limitations that constrained audit conclusions.

GAGAS require audit findings to be grounded on a defensible evidentiary basis and structured around clearly articulated criteria, observed conditions, causal factors, and resulting effects (GAO, 2024). This structure allows oversight products to function as externally validated problem statements rather than subjective evaluations. Therefore, documented deficiencies represent assessed limitations in auditability at a defined point in time, regardless of whether remediation efforts are underway.

In DoD financial statement audits, the DoD OIG has repeatedly linked persistent findings to data reliability gaps, system integration constraints, and control execution limitations rather than to the absence of formal policies (DoD OIG, 2022). GAO reviews of defense logistics and financial reporting similarly identify recurring challenges involving transaction timeliness, documentation completeness, valuation support, and

cross-system reconciliation (GAO, 2024). Taken together, these oversight assessments suggest that accountability deficiencies frequently reflect structural characteristics of enterprise systems and information flows rather than isolated instances of noncompliance.

Within this study, documented deficiencies derived from external oversight products serve as the primary units of analysis. This research does not reassess auditor judgments or remediation plans. Instead, it treats deficiency statements as indicators of auditability conditions operating under the OIS 2.0 Environment. By analyzing these externally validated findings, this study focuses on how internal controls perform in practice under existing system constraints, thereby providing a defensible basis for evaluating residual audit and accountability risk. The following section discusses the internal control framework of the federal government.

H. INTERNAL CONTROL FRAMEWORKS IN THE FEDERAL GOVERNMENT

An internal control framework is necessary to assess whether controls function effectively in system-mediated environments. The COSO Framework provides the analytical lens for this study because it treats internal control as an objective-oriented system rather than a static checklist (COSO, 2013). In the federal context, this study adopts the broader view reflected in authoritative federal guidance, which characterizes internal control as an integrated, risk-based system embedded in governance, business processes, and organizational operations (GAO, 2025; OMB, 2016). The COSO Framework describes five components: control environment, risk assessment, control activities, information and communication, and monitoring activities, that operate together to support "the achievement of an organization's objectives" (COSO, 2013, p. 59). The *GAO Standards for Internal Control in the Federal Government* (Green Book) apply the same logic in the federal context, requiring that all five components of internal control be suitably designed, deployed into use, and functioning as intended, and that they work collectively as a coordinated whole in order to demonstrate their effectiveness as controls within an organized structure (GAO, 2025). This integrated perspective is particularly relevant in system-mediated environments, where information quality, business processes, and governance structures directly influence whether formally

established controls function as intended (GAO, 2025; OMB, 2016). The COSO Framework provides an appropriate basis for assessing how system design, information quality, and governance conditions influence the effectiveness of internal controls in practice.

1. Control Environment

The Control Environment serves as the foundation of the COSO Framework because it shapes the leadership, structure, and accountability conditions under which all other control elements operate (COSO, 2013). Empirical research applying the COSO Framework in public-sector organizations indicates that the control environment is the only one of the five components demonstrating a statistically significant relationship with overall organizational performance (Zahari et al., 2024). This finding reinforces COSO's core premise that effective internal controls begin with engaged leadership, clearly defined authorities, and enforced accountability mechanisms, rather than reliance on procedural compliance alone (COSO, 2013).

In federal organizations, the control environment provides the governance framework that enables accountability, stewardship, and the effective operation of internal controls. The COSO Framework describes the control environment as the basis of the internal control system, shaping organizational standards, structures, accountability relationships, and expectations for ethical stewardship of resources (COSO, 2013). Zahari et al. (2024) further note that this foundational role influences how the other components function within organizations. Within federal organizations, this includes clearly defined responsibilities, delegated authorities, and mechanisms for enforcing accountability across organizational boundaries. The Green Book similarly links internal control to stewardship of public resources and reliable reporting by requiring management to assign responsibility, delegate authority, and ensure that personnel are answerable for carrying out their assigned internal control duties (GAO, 2025). Therefore, internal control reflects not only technical procedures but also the clarity of governance and oversight embedded within the organization.

Deficiencies in the control environment can undermine internal control effectiveness by weakening the authority, accountability, and governance needed to

sustain corrective action. When management determines that a control objective cannot be reliably achieved due to a principle or component being absent, poorly designed, or not integrated with the broader control structure, the situation rises to the level of a major deficiency (McNally, 2013). Deficiencies in the control environment are not limited to overt leadership deficiencies. They may also arise from fragmented governance structures, unclear ownership of processes, or inconsistent enforcement of accountability. Prior research in the Navy ordnance enterprise indicates that such positional authority is structurally fragmented. In their research, Potvin et al. (2021) conclude that NALC "has no positional authority over the Navy Munitions Commands (NMCs) nor over the operational units," and that "afloat units do not fall under NALC governing authority" (p. 31), limiting enforcement capability. Even when policies are formally documented, internal control effectiveness depends on management's sustained responsibility to maintain and assess those controls (Zahari et al., 2024). Where authority is fragmented or oversight mechanisms are inconsistently applied, corrective actions may not be fully implemented or sustained over time.

In complex logistics and financial reporting environments, such fragmentation can dilute responsibility for resolving recurring deficiencies. The COSO Framework requires that all internal control principles, including those addressing integrity, oversight responsibility, organizational structure, and accountability, be "present and functioning" (p. 5), for the system to be effective (McNally, 2013). Therefore, recurring audit findings may reflect structural accountability gaps rather than isolated procedural failures. If responsibility for remediation is distributed among multiple organizations without clearly defined enforcement authority, the broader control system may struggle to correct persistent deficiencies despite documented policies and remediation plans. Accordingly, this study evaluates whether documented ordnance deficiencies reflect structural accountability and governance conditions consistent with control environment weaknesses.

2. Risk Assessment

Under the COSO Framework, risk is defined as the "possibility that an event will occur and adversely affect the achievement of objectives" (2013, p. 60). COSO further describes risk assessment as a "dynamic and iterative process for identifying and

assessing risks to the achievement of objectives" (2013, p. 59). Effective risk assessment ensures that control activities are designed and prioritized in proportion to the magnitude and likelihood of identified exposure. Empirical audit research reinforces that risk identification must meaningfully influence response. Carmona Ibáñez finds that when internal control threats are structured in accordance with the COSO Framework, auditors adjust their substantive procedures in proportion to assessed risk, concentrating additional work on areas judged to present higher risk (Carmona Ibáñez, 2008). Therefore, modern risk-based audit methodology links risk recognition directly to the design and scope of control and audit responses.

Within the OIS 2.0 Environment, risk assessment occurs in a technically complex and data-intensive system. The NAVSUP Ammunition Logistics Center's A121 Metrics/ Data Mining/Reports/Financial Improvement and Audit Readiness (FIAR)/Strategy team (KHAOS) exists to structure and analyze ordnance data embedded across numerous Oracle tables (Ponti et al., 2023). Over the past two decades, the team has developed more than 100 supplemental analytic tools and hundreds of pivot tables to enhance data visibility, some serving as temporary solutions pending integration into OIS. Continued reliance on supplemental tools suggests that risk mitigation often depends on compensating analytical controls outside the core system architecture.

The FIAR function further illustrates institutionalized risk assessment. The FIAR team supports GAO, DoD OIG, and Chief Financial Officer reporting requirements and prepares quarterly inventory reports across multiple Budget Submitting Offices (Ponti et al., 2023; OUSD(C)/CFO, 2017). Additionally, annual stratification of approximately 7,655 ordnance National Item Identification Numbers (NIIN), representing roughly $48 billion in inventory, is conducted three times to validate retention levels and data accuracy (Ponti et al., 2023). These processes demonstrate formal recognition of financial reporting and inventory accountability risk under OIS 2.0.

However, risk assessment effectiveness ultimately depends on whether identified exposures translate into proportionate control responses. When system limitations, asynchronous updates, or reliance on manual reconciliations become normalized as routine operating conditions, risks may be acknowledged but insufficiently prioritized.

This is a dynamic consistent with Carmona Ibáñez (2008) in that finding that risk recognition must meaningfully influence the audit response. Where that alignment remains incomplete, residual audit risk may persist despite documented remediation efforts. This study evaluates whether documented ordnance deficiencies reflect misalignment between formally recognized risk and proportionate control response.

3. Control Activities

As the operational expression of risk response, control activities translate internal control principles into day-to-day practice. According to COSO (2013), control activities are "the actions established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out" (p. 87). These actions may include approvals, verifications, reconciliations, supervisory reviews, and system-based validations (COSO, 2013). The GAO Green Book similarly states that management is responsible for designing control activities that reduce risk to acceptable levels in relation to the entity's objectives (GAO, 2025). Control activities are not merely procedural steps. They are operational mechanisms that translate identified risk into tangible safeguards within routine organizational processes.

Research examining the COSO Framework in practice reinforces this distinction. Research applying COSO concepts in information technology (IT) makes a similar distinction between transaction-level controls and the broader control environment that supports them. In "Attending to COSO General Controls Before Disaster Strikes," Storkman (2005) explains that application controls are designed to support the "completeness, accuracy, and validity of transaction processing" (p. 2), while general controls address the dependability and protection of the information systems that support those applications. Storkman (2005) further notes that general controls include areas such as access security, infrastructure, software change, and maintenance processes. Read together, these points suggest that transaction controls may not operate reliably when the broader IT control structure is weak or inconsistently maintained. When general controls are weak or inconsistently applied, even well-designed transaction controls may not function as intended. In other words, the formal execution of control activities does not guarantee effective control if the underlying system environment is unstable or poorly governed.

This point is particularly relevant in audit-sensitive environments. Control activities may formally exist and be performed as required yet fail to achieve their intended objectives if the underlying data are incomplete, delayed, or inconsistent. COSO's integrated structure recognizes that control activities depend on reliable information flows and stable system configurations to operate effectively (COSO, 2013). Deficiencies in entity-level and system-level controls can cascade downward, undermining reconciliations, supervisory reviews, and automated validations even when personnel perform their assigned duties as prescribed (McNally, 2013). Together, these perspectives indicate that breakdowns in control activities may reflect not only failures in execution, but also deficiencies in the information and system conditions required for those controls to function as intended.

4. Information and Communication

The Information and Communication components of the COSO Framework enables the functioning of all other internal control components. Organizations must obtain, generate, and use information that is timely, complete, accurate, and accessible to support internal control responsibilities (COSO, 2013). Effective communication ensures that this information flows to individuals responsible for executing and overseeing controls.

Empirical research reinforces COSO's emphasis on the centrality of reliable information systems to internal control effectiveness. Bedard et al., (2005) demonstrate that auditors frequently identify deficiencies in management information quality as contributors to elevated control risk. Their findings show that deficiencies in information quality are associated with higher risk assessments and expanded audit procedures in the management information quality area (Bedard et al., 2005). They also observe that when systems produce low-quality information, the monitoring function of internal control becomes weakened and increases the likelihood that control failures will not be detected (Bedard et al., 2005). Consistent with COSO (2013) and the GAO Green Book (2025), the quality, accessibility, and integration of information systems fundamentally determine whether internal controls can operate as intended in practice. This relationship highlights why Information and Communication must be examined as a distinct component of internal control in the analysis that follows in this research study.

This component is particularly critical in financial reporting and auditability environments. When information is delayed, incomplete, or unreliable, internal controls may be performed mechanically but fail to achieve substantive assurance objectives. In organizations reliant on multiple interconnected systems, limitations in data synchronization or integration can materially constrain control execution. Therefore, persistent audit findings in such environments may reflect structural information quality limitations rather than procedural noncompliance. This study assesses whether recurring deficiencies reflect systemic information quality limitations consistent with the COSO information and communication component.

5. Monitoring Activities

Monitoring activities involve evaluating whether internal controls remain present and functioning as intended over time (COSO, 2013). COSO distinguishes between ongoing evaluations embedded in operations and separate evaluations, such as audits or inspections, as part of determining whether internal control mechanisms are operating effectively as intended. Effective monitoring also requires that deficiencies be identified and communicated in time for management to take corrective action and adapt controls as conditions and risks change (COSO, 2013; GAO, 2025). Viewed through this framework, audit remediation environments require more than tracking the closure of corrective actions. They require assessing whether controls continue to reduce residual risk over time. Repeat findings may suggest that controls are being monitored for procedural completion without being reassessed for sustained effectiveness under changing conditions (COSO, 2013; GAO, 2025). This perspective is particularly relevant in audit remediation environments, where recurring findings indicate that controls may be monitored procedurally but not evaluated for sustained effectiveness over time.

Effective monitoring depends on sustained management attention as to whether controls continue to function as intended over time. Moeller (2013) emphasizes that controls may not remain effective once they have been designed and implemented. Even strong control arrangements can weaken when personnel stop following established procedures or when routine oversight by management declines. Therefore, monitoring functions need to take the form of continuing reviews of control performance through recurring and stand-alone evaluations. Moeller's (2013) discussion suggests that, without

sustained oversight, control quality can erode, making management oversight and timely corrective action necessary to address control deficiencies before those weaknesses become recurring deficiencies.

This aligns with COSO's requirement that monitoring activities evaluate not only the existence of controls but their sustained performance over time. In audit remediation environments characterized by recurring findings, monitoring that emphasizes corrective action closure without evaluating residual or systemic risk may fail to produce sustained control improvement. Thus, monitoring effectiveness depends on feedback mechanisms capable of identifying structural constraints and adapting controls accordingly, consistent with both COSO (2013) and the GAO Green Book (2025). This study examines whether repeated ordnance deficiencies indicate monitoring processes that emphasize remediation tracking without a demonstrable reduction in residual audit risk. The following section discusses the standards for internal control in the federal government.

I. STANDARDS FOR INTERNAL CONTROL IN THE FEDERAL GOVERNMENT

The Standards for internal control in the Federal Government, or GAO Green Book, provides the authoritative framework for federal agencies (GAO, 2025). The Green Book is closely aligned with the COSO Framework and adapts principles to the federal operating environment, with particular emphasis on accountability for public resources and compliance with laws and regulations (GAO, 2025). As with COSO, the Green Book requires that internal controls be properly designed, implemented, and operated effectively to achieve agency objectives (GAO, 2025).

A key element of the Green Book (2025) is its emphasis on the role of information systems in supporting internal control execution. GAO explains that "quality information is appropriate, current, complete, accurate, accessible, verifiable, retained as appropriate, and provided on a timely basis" (2025, p. 84). This principle underscores the degree to which effective internal control relies on reliable system process execution. When systems do not provide reliable or current data, organizations may struggle to execute controls consistently, even when those controls are formally documented.

The Green Book (2025) also recognizes that internal controls can exist formally while failing to operate effectively in practice, often due to system inefficiencies, data inaccuracies, or procedural misalignments. According to GAO (2025), agencies must demonstrate not just that control procedures exist on paper but that they operate reliably in day-to-day practice within the organization's environment. This recognition is particularly relevant in complex financial and logistics systems where controls rely on data from multiple systems or require manual reconciliation. In such cases, internal controls may be compliant on paper but limited operationally due to system constraints (GAO, 2025). This distinction is important because it highlights the difference between formal control design and actual control performance in practice. The following section addresses the applications of internal controls in the DoD.

J. APPLICATIONS OF INTERNAL CONTROLS IN THE DEPARTMENT OF DEFENSE

Internal control requirements are implemented across the DoD through Office of Management and Budget (OMB) Circular A-123, which establishes management's responsibility for internal control and enterprise risk management. Circular A-123 emphasizes that internal control should be integrated with risk management and decision-making, instead of being treated as a stand-alone compliance or reporting exercise (OMB, 2016). Within the DoD, these requirements are carried out through DoD Instruction 5010.40, which governs the Risk Management and Internal Control (RMIC) program. DoD Instruction 5010.40 integrates internal control with enterprise risk management and establishes expectations for identifying control deficiencies, assessing risk, and reporting on internal control effectiveness (DoD, 2024). This guidance reflects the DoD's recognition that they must evaluate internal controls in relation to operational realities, including system limitations and enterprise complexity.

At the execution level, internal controls within the DoD have traditionally been associated with the Risk Management and Internal Control (RMIC) program, formerly known as the Manager's Internal Control Program (MICP), which places significant emphasis on documenting controls, conducting reviews, and reporting deficiencies. While these activities are necessary to meet federal internal control requirements, DoD guidance acknowledges an ongoing tension between procedural compliance and effective

operational execution, particularly in complex environments (DoD, 2024). In large-scale logistics and financial systems, controls may be properly documented and reported yet remain constrained by system latency, data fragmentation, or reliance on manual processes, limiting their effectiveness in practice (GAO, 2025). This distinction is important because it shows that compliance with documentation requirements does not necessarily translate into effective control performance in practice.

This tension is directly relevant to ordnance reporting and reconciliation under OIS 2.0. Internal control policy supports the view that control effectiveness depends not only on compliance with procedures, but also on whether information systems enable those controls to function consistently in practice. As a result, persistent audit findings may reflect limitations in control execution driven by system and information constraints rather than failures of policy or managerial oversight alone. The following section discusses the limits of audit and internal control frameworks under system constraints.

K. LIMITS OF AUDIT AND INTERNAL CONTROL FRAMEWORKS UNDER SYSTEM CONSTRAINTS

Audit and internal control frameworks like the COSO Framework, the GAO Green Book, and GAGAS establish expectations for control design, execution, and audit evidence in public-sector organizations. The COSO Framework states that an "organization should obtain, generate, and use relevant, quality information to support the functioning of internal control" (2013, p. 6). GAGAS further require auditors to obtain "sufficient, appropriate evidence" to provide "a reasonable basis" for findings and conclusions (GAO, 2024, p. 182). When these information conditions are not met, internal controls may exist formally yet operate with reduced effectiveness, thereby limiting the degree to which audit objectives can be achieved.

Auditability literature similarly recognizes that audit outcomes reflect the interaction of personnel, processes, and internal controls rather than isolated deficiencies within a single dimension (Rendon & Rendon, 2015). Rendon and Rendon (2015) describe auditability as a condition shaped by this interdependence, emphasizing that internal control effectiveness depends on how these elements function together within the organization, including the systems through which information is generated and communicated. GAGAS acknowledge that reliance on system-generated information

introduces audit risk when data are delayed, incomplete, or difficult to reconcile, which may prevent auditors from substantiating balances or transactions despite the presence of established controls (GAO, 2024). This relationship is important because it underscores that auditability depends not only on the existence of controls, but also on how effectively personnel, processes, and systems function together in practice.

Prior audit reporting further distinguishes between the identification of audit findings and the resolution of underlying audit and accountability risk. DoD audit publications document that certain findings recur across audit cycles even as corrective actions are implemented, particularly when remediation efforts are constrained by legacy systems, complex data interfaces, or manual reconciliation requirements (DoD OIG, 2022; GAO, 2024). In these circumstances, corrective actions may address specific conditions identified during an audit, while broader auditability challenges persist due to the operating environment in which controls are executed. The following section discusses qualitative risk assessment and ISO 31000.

L. QUALITATIVE RISK ASSESSMENT AND ISO 31000

ISO 31000 provides a useful framework for evaluating risk in environments shaped by uncertainty, incomplete information, and system constraints. The framework defines risk as "the effect of uncertainty on objectives" (ISO, 2018, p. 7) and treats risk management as a decision-support process that may be applied using qualitative, semi-quantitative, or quantitative methods depending on the purpose of the analysis, the available information, and the organizational context. In the context of Navy ordnance reporting, uncertainty may be observed in the form of delayed system updates, incomplete transaction data, fragmented information flows, or inconsistent system-generated audit evidence (Moor, D., PowerPoint slides, September 9, 2024). These conditions make ISO 31000 relevant as a framework for evaluating how documented deficiencies affect accountability and reporting objectives under existing OIS 2.0 conditions.

A qualitative risk approach is appropriate in this setting because this study is concerned less with estimating numerical probabilities than with assessing the persistence, significance, and organizational implications of recurring deficiencies. Aven

(2016) cautions that when background knowledge is limited or empirical data are insufficient, numerical probability assignments may imply a level of precision that the evidence does not support. Within this study, ISO 31000 (2018) complements the COSO Framework by shifting attention from the design and operation of specific controls to the residual risk that remains when control performance is weakened by recurring deficiency conditions. ISO 31000 (2018) directly supports the use of likelihood, impact, and the effectiveness of existing controls as core risk-assessment considerations. The additional contextual factors used in this study were tailored to the DTT deficiency environment and are described in Chapter III. Used in this way, ISO 31000 supports structured qualitative judgment about recurring audit and accountability exposure without overstating analytical certainty. The following section describes the qualitative content analysis as an analytical framework.

M. QUALITATIVE CONTENT ANALYSIS AS AN ANALYTICAL FRAMEWORK

Qualitative content analysis provides a structured approach for interpreting documentary evidence in a systematic and defensible way. According to Krippendorff (2019), content analysis employs explicit procedures for examining documents and other recorded material so that interpretation and inference are carried out in a consistent and reviewable manner. He presents the method as systematic in design but still dependent on contextual reading and analytic judgment. This makes qualitative content analysis useful for research based on institutional and organizational documents, where the goal is to interpret recorded evidence, compare recurring patterns across sources, and develop defensible conclusions from the documentary record.

A central contribution of Krippendorff's (2019) work is his treatment of content analysis as an inferential method. He argues that texts do not speak for themselves and that analysis must connect textual material to questions that extend beyond the text alone. With this approach, coding categories and analytical constructs help the researcher take recorded material and move them to claims that can be explained, examined, and, in principle, validated. Krippendorff (2019) stresses that content analysis depends on explicit design choices, including how texts are unitized, sampled, coded, and interpreted.

These features distinguish the method from unsystematic coding by requiring procedures that are defined clearly enough to support consistency and replication.

Unitizing is central to that design because it determines what could count as textual material to be analyzed. Krippendorff (2019) describes units as methodological distinctions drawn within an observational field and emphasizes that unitizing should omit irrelevant matter while keeping together what cannot be divided without loss of meaning. He distinguishes among sampling units, recording units, and context units, each of which serves a different analytical purpose (Krippendorff, 2019). These choices affect what information enters the analysis, how observations are described, and how reliably patterns can be compared across texts. Poorly chosen units can obscure relationships or strip away necessary context, whereas well-defined units make the analysis more coherent and defensible.

Once units have been defined, the next methodological task is to classify them in ways that support this study's analytic objectives. Within this framework, categories operate as analytic constructs created to support specific inferences rather than as inherent properties of the text. Their purpose is to organize interpretation and enable comparison, not to exhaustively represent all possible meanings contained within the material. Schreier (2012) reinforces this applied orientation by showing that coding frames are developed to address specific research questions and to capture selected aspects of the material. In applied research settings, developing and documenting consistent classifications across cases is essential because coding categories function as analytic constructs designed to support specific inferences rather than as exhaustive interpretations of each text (Crawford & Ostrom, 1995). This study prioritizes systematic, rule-guided classification that supports analytic comparability across cases.

Taken together, these contributions show that qualitative content analysis offers a credible framework for the systematic examination of documentary evidence. Because the method emphasizes transparent procedures, traceable coding decisions, and defensible inference, it provides an appropriate foundation for the analytic design used in this study. A federalized application of internal control principles is necessary to assess control effectiveness in public-sector, system-dependent environments. Although COSO

provides a broadly applicable internal control integrated framework, its principles are adapted for federal use through the GAO Green Book, which emphasizes accountability for public resources and the role of information systems in control execution (GAO, 2025). Both frameworks recognize that internal controls may exist formally yet fail to operate effectively when information is not timely, complete, or reliable. This recognition is particularly relevant in environments where controls depend on cross-system data flows or delayed reconciliation processes. In such cases, internal control effectiveness is constrained not by policy design but by the system conditions under which controls must operate (COSO, 2013; GAO, 2025). Overall, COSO helps frame the central question of this thesis. The COSO Framework allows the analysis to focus on whether internal controls governing ordnance reporting can function consistently given the constraints of OIS 2.0. By utilizing the COSO Framework as an analytical lens, this study examines internal control effectiveness in its operational context, without assuming system modernization or organizational changes. The following section provides a summary of this chapter.

N. SUMMARY

This literature review examined OIS 2.0, prior analyses of Navy ordnance reporting, auditability theory, the Auditability Triangle, government auditing standards, internal control frameworks, qualitative risk assessment, and qualitative content analysis. Together, this literature establishes the conceptual and analytical foundation for examining recurring ordnance deficiencies as indicators of residual audit and accountability risk under existing system conditions. The following chapter addresses the methodology used in this research study.

III. METHODOLOGY

Before presenting the methodology, it is important to establish how the research approach aligns with the purpose of the study. Because this study examines the auditability and accountability within a complex Navy ordnance reporting environment, the methodology was designed to provide a structured means of evaluating system conditions, internal control effectiveness, and residual risk. Rather than relying on a single framework, this study used complementary analytical models to assess how governance, processes, personnel, and control limitations affect the reliability of ordnance reporting through OIS 2.0.

A. INTRODUCTION

This chapter explains the methodology used in this study. It defines the research design, identifies the NALC-provided DTT spreadsheet as the primary data source, and describes how deficiencies were coded using the Auditability Triangle drivers, COSO internal control components, and an ISO 31000-informed qualitative risk framework. It also explains the procedures used to classify residual risk and analyze recurring patterns within the deficiency population. The following section discusses the research design of this study.

B. RESEARCH DESIGN

This study employed a qualitative diagnostic research design to examine recurring ordnance-related audit deficiencies documented in the Navy deficiency environment. The design was qualitative because this study relied on textual documentary evidence, including deficiency narratives, root causes, and recommendations, rather than experimental or survey data. It was diagnostic because the purpose was to identify, classify, and interpret patterns of control deficiencies, process breakdown, and auditability risk within an existing operational environment rather than to test a causal hypothesis or predict future outcomes. Therefore, this study focused on understanding how documented deficiencies manifested under OIS 2.0 conditions and what those recurring patterns indicated about residual audit and accountability risk.

This design was appropriate because this study drew from a population of deficiencies provided by NALC through the DTT spreadsheet, each of which had already been identified through formal audit, oversight, or remediation processes. Rather than asking whether deficiencies existed, this research examines how those deficiencies could be systematically interpreted through the Auditability Triangle drivers, the COSO internal control components, and an ISO 31000-informed risk framework. In this sense, the design was intended to support structured diagnosis of persistent deficiencies within the documented ordnance reporting and reconciliation environment, not statistical generalization or predictive modeling. The method treated the deficiency record as the starting point for analysis and used rule-guided qualitative classification to identify recurring patterns across the population.

The unit of analysis was the individual deficiency event. Although the NALC-provided dataset contained deficiency records at the deficiency ID level, this study analyzed the specific documented condition within each record as the analytically relevant event and then applied the research coding structure to that event. This approach allowed each observation to be classified consistently across the three analytical lenses used in this study: dominant Auditability Triangle driver, primary COSO internal control component, and ISO 31000-informed residual risk factors. Treating the individual deficiency event as the unit of analysis preserved traceability to the source record while allowing structured comparison across the broader deficiency population. No PII was used in this research study. The Naval Postgraduate School Institutional Review Board (IRB) reviewed this research study's methodology and determined that this research did not require a full IRB protocol. The following section addresses the data source and case boundaries used in this study.

C. DATA SOURCE AND CASE BOUNDARIES

The primary data source for this study was the Navy's Deficiency Tracking Tool (DTT) spreadsheet provided by NALC. The DTT file served as the core analytical dataset because it contained the documented deficiency records used for classification and comparison in this study. These records included source fields such as deficiency identifiers, titles, condition statements, root causes, recommendations, audit source references, fiscal year, end-to-end process, process owner, supporting organizations, and

affected business segments. This research team used the POC-provided DTT file as the base dataset and then appended additional coding fields to support this study's analytical framework. Those added fields began after the recommendations column and were used to classify each coded observation by Auditability Triangle driver, COSO internal control component, functional domain, and ISO 31000-informed residual risk factors. The study period includes deficiencies ranging from fiscal year (FY) 2005–2025. As previously stated, no PII was used.

The DTT spreadsheet incorporated deficiencies originating from multiple oversight and audit sources relevant to Navy financial reporting, internal control, and ordnance accountability. These included independent financial statement audit NFRs, internal control findings, audit roadmap items, Statements of Assurance, and selected oversight products from organizations such as EY, GAO, DoD OIG, Naval Audit Service, and other Navy or Marine Corps review authorities reflected in the source dataset. Because this study relied on the deficiency records as documented in the DTT file, those underlying oversight products were treated as the originating basis for the deficiency population rather than as separate analytical datasets. NALC provided a total population of 168 deficiencies in the POC-provided dataset. Of those, seven deficiencies were excluded from analysis because many of the relevant fields were blank and did not provide sufficient documentary detail to support accurate coding under this study's analytical framework. Therefore, the final analyzed population consisted of 161 deficiencies. In this sense, the DTT spreadsheet functioned as the consolidated source record for this study's primary analysis.

Additional materials were used only for contextual and background support. These included POC-provided briefing materials describing the current capabilities and known shortcomings of OIS 2.0. These materials were not incorporated into the coded deficiency dataset and were not treated as standalone observations for analysis. Instead, they were used, where appropriate, to provide system context for understanding the operating environment in which documented deficiencies occurred. Therefore, their role was interpretive and contextual rather than evidentiary for frequency counts, coding totals, or comparative risk analysis. Materials related to future-state capabilities or system

modernization beyond the current OIS 2.0 Environment were outside the analytical scope of this study.

The scope of the dataset was limited to deficiencies relevant to this study's focus on Navy ordnance reporting, reconciliation, accountability, and audit support under OIS 2.0 conditions. Accordingly, this study treated the POC-provided DTT spreadsheet as the population from which relevant observations were selected and coded. This study did not attempt to create an exhaustive inventory of all historical Navy deficiencies outside that population, nor did it evaluate future system performance, proposed modernization outcomes, or projected improvements associated with successor systems. Data outside the DTT population, including generalized system descriptions or future-state capability materials, were used only when necessary to explain the current operating context and were not included in the formal analytical results. The following section describes the data interpretation and coding procedures used in this study.

D. DATA INTERPRETATION AND CODING PROCEDURES

To promote consistency in coding, all three research team members reviewed the dataset together during the classification process. Where a coding decision was straightforward, the team applied the established decision rules and proceeded with classification. When disagreement arose regarding the appropriate classification, the team reviewed all relevant documentary information associated with the deficiency and each member explained the reasoning supporting their proposed classification. Coding resumed only after the team reached agreement on the most appropriate assignment. This process was used to improve consistency across the dataset and reduce the risk of unsupported individual judgment.

1. Auditability Triangle Classification

Each coded observation was assigned one primary Auditability Triangle driver: personnel, process, or internal control. The classification of the drivers reflected the dominant causal mechanism most directly responsible for the auditability failure documented in the source record. Coding was based on the earliest point in the control chain at which the deficiency prevented reliable traceability, accountability, or audit support. An observation was classified as internal control when the documented

deficiencies centered on the failure, absence, or ineffectiveness of a control activity or monitoring mechanism. This included cases in which reconciliations, reviews, validations, or other control procedures did not operate effectively, did not produce sufficient evidence, or depended on unreliable or delayed inputs. An observation was classified as process when the deficiency stemmed from the structure of the workflow itself rather than the failure of discrete control. Process coding was used when transaction flow, sequencing, documentation design, or coordination across systems or echelons prevented reliable traceability or standardized execution. An observation was classified as personnel only when the documentary record indicated that individuals failed to execute established procedures despite the presence of otherwise functioning processes and controls. Therefore, personnel coding was reserved for clearly identifiable execution failures, such as failure to follow guidance, failure to retain required documentation, or failure to correctly complete required actions.

Where multiple elements were present, the observation was coded to the dominant Auditability Triangle driver rather than all potentially relevant factors. This rule was intended to preserve consistency across the deficiency population and avoid inflating overlap among categories. The following section addresses COSO Internal Control component mapping.

2. COSO Internal Control Component Mapping

Each coded observation was assigned one primary COSO internal control component to identify the principal internal control domain most directly implicated by the documented deficiency. The "five components of internal control: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities" were used in the coding of each deficiency (COSO, 2013, p. 3). Primary COSO assignment was based on the component that best captured the main internal control limitation reflected in the source record.

Control Environment was assigned when the primary limitation stemmed from broader structural, governance, or accountability conditions rather than a discrete process or control failure. These cases involve unclear responsibilities, insufficient accountability structures, or organizational conditions that weakened effective control performance.

Risk Assessment was assigned when the documented issue reflected inadequate identification, evaluation, or mitigation of known risks. This included situations in which management had not formally assessed known system limitations, process vulnerabilities, or control risks relevant to financial reporting and auditability. Each coded observation was assigned to both a primary and a secondary COSO internal control component. The primary COSO assignment identified the main internal control domain as the most directly implicated by the documented deficiency. The secondary COSO assignment captured an additional internal control domain relevant to the same observation where the documentary record reflected overlap or interdependence across components. This approach allowed the dataset to preserve more of the internal control context present in the source material while maintaining one principal component for structured comparison.

Control Activities were assigned when the principal deficiencies involved the failure, absence, or ineffective operation of specific control procedures. This included deficiencies in reconciliations, reviews, validations, approvals, or other control steps intended to ensure accurate and supportable transaction processing or reporting.

Information and Communication was assigned when the documented auditability failure stemmed primarily from deficiencies in the availability, completeness, timeliness, accessibility, or synchronization of information needed to support control execution or audit evidence. These included cases involving delayed system updates, incomplete data, inaccessible supporting evidence, or unsynchronized records across systems or reporting layers.

Monitoring Activities was assigned when the deficiency reflected failure to identify, track, verify, or correct known problems over time. This included cases in which deficiencies persisted across audit cycles, corrective actions were not effectively followed through, or oversight mechanisms failed to detect continuing deficiencies. The following sections discuss ISO 31000-Informed Qualitative Risk Evaluation.

3. ISO 31000–Informed Qualitative Risk Evaluation

Each coded observation was evaluated using a qualitative risk framework informed by ISO 31000. The purpose of this stage was to assess the relative severity and

persistence of each documented deficiency under current operating conditions rather than to estimate quantitative loss or produce predictive risk modeling. Consistent with this study's focus on residual audit and accountability risk, the evaluation considered both the immediate significance of each deficiency, but also the broader conditions affecting recurrence, detectability, mitigation, and sustained control performance.

As shown in Table 1, the qualitative risk evaluation was structured around three analytical dimensions informed by ISO 31000 (2018): likelihood, impact, and control effectiveness. ISO 31000 (2018) frames risk analysis as an examination of consequences, likelihood, and existing controls, with that analysis supporting subsequent risk evaluation and treatment decisions. Within this study, likelihood represented the qualitative expectation that a deficiency would recur under prevailing system or process conditions, including evidence that the issue had appeared as a repeat finding across audit cycles. This interpretation is consistent with ISO 31000's (2018) treatment of likelihood as expressible through frequency, probability, or expected occurrence. Impact captured the relative severity of the deficiency with respect to audit assertions, financial reporting reliability, and accountability outcomes. ISO 31000 (2018) conceptualizes this dimension as consequence and recognizes that consequences may be articulated using qualitative or quantitative descriptors. Control effectiveness assessed the extent to which existing controls substantively mitigated the identified risk in operational practice rather than merely in design. This factor reflects ISO 31000's guidance on evaluating whether existing controls are "appropriately designed, functioning, reliable, effective, and adequate for current objectives and conditions" (2018, p. 45).

In addition to these three ISO 31000-informed dimensions, the coding framework included five contextual factors developed from recurring conditions observed in the DTT deficiency population: system constraints, governance and oversight, process integration across echelons, data environment and information quality, and operational tempo or workload conditions. These contextual factors were not treated as ISO 31000-derived categories. Rather, they were used to further operationalize the study's assessment of residual audit and accountability risk under OIS 2.0 conditions. They captured organizational and operating conditions affecting the sustainability of risk mitigation, including whether system architecture constrained control performance,

whether governance mechanisms supported remediation, whether processes remained synchronized across commands and reporting layers, information systems provided timely and traceable evidence, and whether workload or execution pressure materially affected control operation.

As shown in Table 1, all eight factors were coded using ordinal qualitative descriptors appropriate to the risk construct being assessed and then converted to a standardized three-point scale, where 1 indicated lower concern, 2 indicated moderate concern, and 3 indicated higher concern. The factor values were averaged to generate a composite priority score for each deficiency in the DTT. Although the underlying factor ratings are ordinal, their use in this study functioned as a structured classification device rather than as a claim of interval measurement. The composite score was used to support consistent placement of each case into an overall qualitative risk category. Because the scoring model ranged from 1.00 to 3.00, the total possible range was 2.00 points. Dividing that range into three equal-width bands produced a transparent and reproducible classification rule consistent with ISO 31000's emphasis on qualitative risk evaluation and with Aven's (2016) caution against unwarranted numerical precision. Accordingly, composite scores from 1.00 and 1.66 corresponded to low residual risk, scores from 1.67 to 2.33 corresponded to moderate residual risk, and those ranging from 2.34 to 3.00 corresponded to high residual risk.

Table 1. Risk Factors and Coded Values

Risk Factors	Risk Severity Assigned Value		
	Low Concern (1.0)	**Moderate Concern (2.0)**	**High Concern (3.0)**
Likelihood	Low	Moderate	High
Impact	Low	Moderate	High
Control Effectiveness	Effective	Partially	Ineffective
System Constraints	Low	Moderate	High
Governance	Strong	Mixed	Weak
Process Integration Across Echelons	Integrated	Partial	Fragmented
Data Environment and Information Quality	Reliable	Degraded	Poor
Operational Tempo and Workload Conditions	Normal	Elevated	Stressed

Qualitative judgment remained central to this process because each factor required interpretation of the documentary record rather than mechanical extraction from a single data field. To support consistency, each factor was assigned using predefined decision rules tied to this study's analytical context. For example, likelihood was rated high when recurrence appeared probable under existing system or process conditions, impact was rated high when the deficiency affected financial statement balances or enterprise accountability, and control effectiveness was rated ineffective when controls did not materially reduce the identified risk. Similar rule-guided logic was used for the contextual factors, including governance strength, degree of process integration, condition of the information environment, and the extent to which operational tempo affected execution. This approach allowed this study to preserve qualitative interpretation while applying the risk framework consistently across the analyzed deficiency population. The following section explains the analysis procedures.

E. ANALYSIS PROCEDURES

Following completion of coding and residual risk classification, the dataset was analyzed using descriptive and comparative procedures designed to identify recurring

patterns across the deficiency population. The analysis relied on frequency counts, percentages, cross-tabulations, and pivot-table summaries to examine how deficiencies were distributed across this study's principal analytic frameworks. These procedures were used to compare patterns within the OIS environment and the broader Enterprise Environment, and to evaluate how deficiencies were concentrated across Auditability Triangle drivers, COSO internal control components, and ISO 31000-informed risk conditions.

Descriptive frequency analysis was used first to summarize the overall deficiency population and to show the distribution of coded observations across key categorical fields. This included counts and percentages by both OIS and Enterprise Environments, Auditability Triangle driver, and primary COSO component. These summaries established the baseline distribution of the analyzed population and provided the foundation for the comparative analyses that followed.

Cross-tabulation and pivot-table analysis were then used to compare coded patterns across analytic categories and environments. These procedures supported side-by-side examination of OIS and enterprise deficiencies, including comparison of Auditability Triangle driver distributions, primary and secondary COSO component patterns, and the frequency of contextual organizational factors associated with recurring deficiencies. Where appropriate, pivot-table aggregation was used to summarize the coded data into interpretable category counts and percentages suitable for figure development and narrative comparison.

To examine how risk concentrated across internal control structures, a risk concentration matrix was constructed by combining Auditability Triangle driver classifications with COSO internal control components and calculating the average composite priority score for each observed combination. These matrix values were used to generate this study's heat map figures and to identify where higher relative concentrations of prioritized risk occurred across the analyzed deficiency population. The resulting matrices were used comparatively across the OIS and Enterprise Environments to show whether similar concentrations were observed across both populations or whether they were more heavily associated with one environment.

Thematic grouping was also used to examine patterns that extended beyond single categorical variables. In particular, the analysis considered persistence across fiscal years, recurring deficiencies spanning multiple audit cycles, and the concentration of contextual organizational drivers such as governance, process integration, data environment quality, system constraints, operational tempo, and control effectiveness. For this purpose, the dataset was filtered to isolate recurring deficiencies persisting across two or more fiscal years, and pivot-table frequency analysis was then used to identify the dominant contextual conditions associated with that recurring subset.

Finally, the coded and aggregated results were brought together through cross-framework synthesis. This step did not create a new coding layer but instead interpreted how the findings from the Auditability Triangle, COSO Framework, and ISO 31000-informed analyses reinforced or qualified one another. The purpose of this synthesis was to identify whether recurring ordnance auditability deficiencies reflected isolated issues within one framework or a broader convergent pattern across process, control, information, and organizational risk conditions. This integrative step supported the later development of findings-based recommendations by linking classification patterns to the structural conditions most closely associated with recurring auditability deficiencies. The following section discusses validity, reliability, and study controls.

F. VALIDITY, RELIABILITY, AND STUDY CONTROLS

Several methodological controls were used to promote consistency, traceability, and procedural discipline throughout the analysis. First, coding was guided by predefined decision rules for each analytical framework. These rules established how observations were classified under the Auditability Triangle driver classifications, how primary and secondary COSO components were assigned, and how ISO 31000-informed risk factors were evaluated. The use of predefined rules reduced ad hoc interpretation and helped ensure that similar documentary conditions were treated consistently across the dataset.

Second, the coding process incorporated team-based review and calibration. All three members of the research team reviewed the data together during the classification process to promote consistency in application of the coding rules. When disagreement arose regarding a particular coding decision, the team reviewed the relevant documentary

information associated with the observation, and each member explained the reasoning supporting the proposed classification. Coding resumed only after the team reached agreement on the most appropriate assignment. This process was intended to strengthen consistency across the dataset and reduce the risk of unsupported individual judgment.

Third, this study preserved traceability between each coded observation and its underlying documentary source. The POC-provided DTT spreadsheet functioned as the base analytical file, and the research team appended this study's coding fields directly to that file after the recommendations column. This structure preserved the original deficiency identifiers, titles, condition narratives, root causes, recommendations, audit source references, and other source metadata while allowing each coded observation to remain linked to its originating deficiency record.

This study also incorporated procedural limits intended to preserve analytical discipline. Primary classifications were used for descriptive counts and comparative summaries to prevent double counting across categories. Secondary classifications were retained in the dataset to preserve additional internal control context and were used to construct a supplementary table examining secondary internal control patterns across the analyzed deficiency population. Similarly, contextual briefing materials regarding OIS 2.0 capabilities and known system shortcomings were used only to inform background understanding of the operating environment and were not treated as standalone analytical observations.

Several limits of interpretation also remain. This study relied on documented deficiencies as recorded in the POC-provided DTT file and depended on the completeness and quality of those underlying records. Seven deficiencies from the POC-provided population were excluded because the relevant documentary fields were largely blank and did not provide sufficient information for reliable coding, leaving a final analyzed population of 161 deficiencies. This study also remained limited to the current OIS 2.0 Environment and did not evaluate future-state performance, modernization outcomes, or projected effects associated with successor systems. Accordingly, the findings should be interpreted as a structured analysis of documented deficiencies within the defined population and study period (FY 2005–FY 2025) rather than as a predictive

assessment of future system performance. The following section provides a summary of the chapter.

G. SUMMARY

This chapter explained the methodology used to analyze recurring ordnance-related deficiencies within the POC-provided DTT dataset. It defined this study's qualitative diagnostic design, identified the DTT spreadsheet as the primary source dataset, and explained how the research team extended that dataset with additional coding fields aligned to the Auditability Triangle, COSO Framework, and an ISO 31000-informed qualitative risk structure. This chapter also described the procedures used to classify coded observations, generate composite priority scores and residual risk categories, and analyze the resulting dataset through descriptive summaries, cross-tabulations, risk concentration matrices, and thematic comparison. The final sections explained the controls used to promote coding consistency, traceability, and analytical discipline. The next chapter presents the analysis and findings produced through those procedures. These findings provide the evidentiary basis for the governance and control improvement discussion presented in the findings chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS, FINDINGS, AND RECOMMENDATIONS BASED ON THE FINDINGS

This chapter presents the findings from the coded analysis of 161 ordnance-related deficiencies documented in the DTT. Using the methodology established in Chapter III, this study determined how many deficiencies were directly related to OIS 2.0 and compared those OIS-related deficiencies with the broader Enterprise Environment deficiency population. The analysis applied the Auditability Triangle, the COSO Framework, and ISO 31000-informed qualitative risk concepts to identify recurring patterns within the DTT.

A. INTRODUCTION

This chapter proceeds through the major analytical sections of the study. It begins by describing the reviewed deficiency population and then presents the principal findings across the Auditability Triangle drivers, COSO internal control components, functional domains, ISO 31000-informed residual risk analysis, duration of recurring deficiencies, and organizational drivers of recurring deficiencies. It then examines the implications of those findings and develops recommendations based on the patterns identified in the data. This chapter concludes with a summary of the principal results and their significance within the current OIS 2.0 Environment. The next section provides an overview of the DTT NFR dataset used for the analysis.

B. OVERVIEW OF THE DEFICIENCY TRACKING TOOL DATASET

The reviewed deficiency population consisted of 161 deficiencies documented in the DTT provided to the research team by NALC. Of these, 28 deficiencies (17.39%) were identified as directly related to OIS 2.0 and were classified as the OIS environment. The remaining 133 deficiencies (82.61%) were classified as the Enterprise Environment because they fell outside the set of deficiencies directly attributable to OIS 2.0. This distinction is analytically important because it situates OIS-related deficiencies within the larger population of ordnance audit deficiencies, many of which are recurring. It also allows comparison of common areas of weakness across both deficiency populations. Table 2 summarizes the deficiency population by environment. The following section explains the patterns in the auditability analysis.

Table 2. Deficiency Population by Association

Deficiencies by Environment	Count	Percent
Enterprise Environment	133	82.61%
OIS Environment	28	17.39%
Grand Total	**161**	**100.00%**

C. AUDITABILITY ANALYSIS AND FINDINGS

This section presents the distribution of OIS environment and Enterprise Environment deficiencies across the Auditability Triangle driver classifications. Each deficiency was assigned one primary Auditability Triangle driver classification based on the dominant causal mechanism reflected in the documented deficiency.

Table 3 presents the frequency distribution of Auditability Triangle drivers for the 28 OIS environment deficiencies identified in the dataset. The analysis and findings indicate that process was the most frequently coded driver of the Auditability Triangle, accounting for 53.57% of the sample. Internal control deficiencies represented 39.29%, while personnel-related deficiencies accounted for only 7.14%.

Table 3. Auditability Triangle Results for OIS Environment

Auditability Triangle Driver	Count	Percentage
Process	15	53.57%
Internal Control	11	39.29%
Personnel	2	7.14%
Grand Total	**28**	**100.00%**

Table 4 presents the distribution of Auditability Triangle drivers for the Enterprise Environment population, consisting of 133 deficiencies that were not directly attributable to the OIS 2.0 Environment. As with the OIS environment population, process was the dominant driver, accounting for 63.91% of the observations. Internal control deficiencies represented 35.34%, while personnel-related deficiencies accounted for less than one percent of the population. The next section discusses the COSO Internal Control Component analysis and findings.

Table 4. Auditability Triangle Results for Enterprise Environment

Auditability Triangle Driver	Count	Percentage
Process	85	63.91%
Internal Control	47	35.34%
Personnel	1	0.75%
Grand Total	**133**	**100.00%**

D. COSO INTERNAL CONTROL COMPONENT ANALYSIS AND FINDINGS

As shown in Table 5, coding of the 28 primary OIS 2.0 deficiencies by primary COSO component indicated a substantial concentration in control activities, which accounted for 16 of the 28 deficiencies (57.14%). Information and communication was the second most frequent category, accounting for eight deficiencies (28.57%). Monitoring activities accounted for three deficiencies (10.71%), while control environment accounted for one deficiency (3.57%). Risk assessment did not account for any deficiencies as a primary COSO category in the analyzed subset. These results suggest that the OIS deficiency population was concentrated most heavily in the execution of controls and the information needed to support those controls.

Table 5. Primary COSO Drivers by OIS Environment

Primary COSO for OIS Environment	Count	Percent
Control Activities	16	57.14%
Information and Communication	8	28.57%
Monitoring Activities	3	10.71%
Control Environment	1	3.57%
Risk Assessment	0	0.00%
Grand Total	**28**	**100.00%**

Table 6 presents coding of the 133 Enterprise Environment deficiencies by primary COSO component and shows a substantial concentration in control activities, which accounted for 55 of the 133 deficiencies (41.35%). Information and communication was the second most frequent category, accounting for 33 deficiencies (24.81%). Monitoring activities accounted for 20 deficiencies (15.04%), followed by risk assessment with 17 deficiencies (12.78%) and control environment with eight

deficiencies (6.02%). Unlike the OIS environment, deficiencies in the Enterprise Environment were distributed across all five COSO components. Control activities and information and communication remain the most frequently represented categories within both the analyzed environment populations.

Table 6. Primary COSO Drivers by Enterprise Environment

Primary COSO for Enterprise Environment	Count	Percent
Control Activities	55	41.35%
Information and Communication	33	24.81%
Monitoring Activities	20	15.04%
Risk Assessment	17	12.78%
Control Environment	8	6.02%
Grand Total	**133**	**100.00%**

The secondary COSO coding reinforces this pattern. As shown in Table 7, control activities and information and communication were tied as the most frequently identified secondary categories in the OIS environment, with 10 deficiencies each (35.71%). Monitoring activities followed with seven deficiencies (25%), while risk assessment accounted for only one deficiency (3.57%).

Table 7. Secondary COSO Drivers by OIS Environment

Secondary COSO for OIS Environment	Count	Percent
Control Activities	10	35.71%
Information and Communication	10	35.71%
Monitoring Activities	7	25.00%
Risk Assessment	1	3.57%
Control Environment	0	0.00%
Grand Total	**28**	**100.00%**

Table 8 presents secondary COSO findings for Enterprise Environment. Control activities were the most frequently identified secondary category, accounting for 49 out of the 133 deficiencies (36.84%). Monitoring activities and information and communication each accounted for 35 deficiencies (26.32%), followed by risk assessment with nine deficiencies (6.77%), and control environment with five deficiencies (3.76%). This distribution provides additional support for the determination that the primary OIS deficiencies were rooted not only in control execution problems, but

also in the supporting information environment and the limited ability to assess control effectiveness over time. Compared to the Enterprise Environment, the OIS environment remained more concentrated in control activities, and information and communication, while the Enterprise Environment showed relatively greater representation in monitoring activities and risk assessment. The following section explains the functional domain observations.

Table 8. Secondary COSO Drivers by Enterprise Environment

Secondary COSO for Enterprise Environment	Count	Percent
Control Activities	49	36.84%
Monitoring Activities	35	26.32%
Information and Communication	35	26.32%
Risk Assessment	9	6.77%
Control Environment	5	3.76%
Grand Total	**133**	**100.00%**

E. FUNCTIONAL DOMAIN OBSERVATIONS

In addition to the Auditability Triangle, COSO, and ISO 31000-informed risk analysis, this study also considered the functional domain classifications already contained in the NALC-provided DTT dataset. These classifications categorized deficiencies as financial, operational, or IT, providing a supplemental view of how the documented deficiencies were associated within the source dataset.

Table 9 presents how the 161 deficiencies were distributed across the three functional domains: financial, operational, and IT. Most deficiencies affect system and information reliability, with 89 deficiencies categorized within the IT domain. Financial reporting impacts were also significant, with 70 deficiencies affecting the reliability of reported balances or supporting audit evidence. By contrast, only two deficiencies were categorized as primarily operational in nature.

Table 9. Distribution of Deficiencies by Functional Domain

Functional Domain	OIS Environment	Enterprise Environment	Total	Percent
IT	19	70	89	55.3%
Financial	8	62	70	43.5%
Operational	1	1	2	1.2%
Grand Total	**28**	**133**	**161**	**100.00%**

Table 10 presents the distribution of deficiencies by Auditability Triangle driver and functional domain. Process-driven deficiencies were the largest category across both the financial and IT domains, with 47 financial deficiencies and 51 IT deficiencies. This indicates that recurring deficiencies were concentrated primarily in how activities were structured, executed, and coordinated rather than in isolated personnel failures. Internal control deficiencies were also prominent, particularly in the IT domain, where 36 deficiencies were identified.

Table 10. Distribution of Deficiencies by Auditability Driver and Functional Domain

Auditability Driver	**Functional Domain**			**Total**
	Financial	**IT**	**Operational**	
Process	47 (47%)	51 (51%)	2 (2%)	100
Internal Control	22 (38%)	36 (62%)	0 (0%)	58
Personnel	1 (33%)	2 (67%)	0 (0%)	3
Grand Total	**70**	**89**	**2**	**161**

Table 11 presents the distribution of deficiencies by COSO internal control component and functional domain. Control Activities accounted for the largest total number of deficiencies, with 71 deficiencies overall, including 29 financial deficiencies, 41 IT deficiencies, and one operational deficiency. Information and Communication was the second largest category, with 41 total deficiencies, split between 21 financial and 20 IT deficiencies. Monitoring Activities were more heavily concentrated in the IT domain, with 18 of 23 deficiencies categorized as IT-related. Risk Assessment and Control Environment were observed less frequently overall, with 17 and nine total deficiencies, respectively. The next section discusses residual audit and accountability risk assessment.

Table 11. Distribution of Deficiencies by COSO Internal Control Component and Functional Domain

COSO Internal Control Component	**Functional Domain**			**Total**
	Financial	**IT**	**Operational**	
Control Activities	29 (41%)	41 (58%)	1 (1%)	71
Information and Communication	21 (51%)	20 (49%)	0 (0%)	41
Risk Assessment	10 (59%)	6 (35%)	1 (6%)	17
Control Environment	5 (56%)	4 (44%)	0 (0%)	9
Monitoring Activities	5 (22%)	18 (78%)	0 (0%)	23
Total	**70**	**89**	**2**	**161**

F. RESIDUAL AUDIT AND ACCOUNTABILITY RISK ASSESSMENT

To examine how deficiencies manifest as auditability risks across internal control structures, risk concentration tables were constructed by combining Auditability Triangle driver classification with COSO internal control components. The values shown in Table 12 and Table 13 represent average composite priority scores for deficiencies within each Auditability Triangle and COSO pairing. As displayed in Chapter III, Table 1, each composite priority score was calculated by scoring eight qualitative risk factors on a three-point ordinal scale and averaging the assigned values. The scoring rubric included three ISO 31000-informed factors: likelihood, impact, and control effectiveness. It also included five contextual factors developed from recurring conditions observed in the DTT deficiency population: system constraints, governance, process integration across echelons, data environment and information quality, and operational tempo and workload conditions. Composite scores were interpreted using three residual-risk categories: low residual risk for scores from 1.00 to 1.66, moderate residual risk for scores from 1.67 to 2.33, and high residual risk for scores from 2.34 to 3.00.

Table 12 displays the average composite priority scores for deficiencies in the OIS environment by Auditability Triangle driver classification and COSO internal control component. The highest scores were observed in the process row under control environment and monitoring activities, each with an average score of (2.63). Process-related deficiencies also exhibited elevated risk concentrations within control activities, and information and communication, with both component pairings averaging (2.48).

Internal control-related deficiencies in the OIS environment produced similar but slightly lower average scores within control activities (2.44) and monitoring activities (2.25). In contrast, personnel-related deficiencies were observed infrequently and produced the lowest observed average score within the OIS environment, with a score of 1.94 within the control activities domain. The distribution shown in Table 12 indicates that the highest risk concentrations within the OIS environment occur primarily in combinations involving process-related deficiencies and key internal control domains associated with governance, oversight, and information reliability.

Table 12. ISO 31000 Risk Concentration Table: OIS Environment

Auditability Triangle	COSO Internal Control Components				
	Control Activities	Control Environment	Information and Communication	Monitoring Activities	Risk Assessment
Process	2.48	2.63	2.48	2.63	-
Internal Controls	2.44	-	-	2.25	-
Personnel	1.94	-	-	-	-

Table 13 presents the same risk concentration analysis for deficiencies categorized within the Enterprise Environment, which includes deficiencies originating outside the OIS operational system but affecting the broader ordnance accountability framework. As with the OIS environment, process-related deficiencies produced the highest average composite priority scores across several COSO control domains. The highest scores were observed in the process row under control environment and information and communication, with average scores of (2.52) and (2.51), respectively. Process-related deficiencies also were observed across the remaining COSO components, including control activities and monitoring activities, each averaging (2.38), and risk assessment at a moderate rating of 2.24.

Table 13. ISO 31000 Risk Concentration Table: Enterprise Environment

Auditability Triangle	COSO Internal Control Components				
	Control Activities	Control Environment	Information and Communication	Monitoring Activities	Risk Assessment
Process	2.38	2.52	2.51	2.38	2.24
Internal Controls	2.34	2.00	2.39	2.28	2.25
Personnel	2.38	-	-	-	-

As shown in Table 13, internal control deficiencies within the Enterprise Environment produced moderately elevated scores across multiple COSO components, including information and communication (2.39), monitoring activities (2.28), control activities (2.34), and risk assessment (2.25). Personnel-related deficiencies were infrequently observed within the enterprise dataset and were observed only within the control activities domain.

Overall, the Enterprise Environment demonstrates a broad distribution of elevated risk scores across multiple COSO components, with particularly high concentrations in areas associated with governance structures and the reliability of information flows supporting internal control execution.

Table 14 summarizes how long each deficiency persisted across the study period. The table does not show the number of deficiencies identified in each fiscal year. Instead, it groups deficiencies by their persistence period, or the number of fiscal years in which each deficiency was observed. For example, 67 deficiencies appeared across only one fiscal year, while 16 deficiencies appeared across two fiscal years. Deficiencies appearing in two or more fiscal years were treated as multi-year deficiencies.

Of the 161 identified deficiencies, 67 (41.61%) were limited to one fiscal year. The remaining 94 deficiencies (100% – 41.61% = 58.39%) were observed across two or more fiscal year periods. This indicates that more than half of the identified deficiencies persisted beyond one audit cycle. This multi-year pattern suggests that many deficiencies were not isolated, one-time issues, but recurring problems that may reflect broader challenges in remediation, process ownership, documentation, system limitations, or organizational coordination. The longest-running example in the population dataset was deficiency D008497, related to OM&S-R. This deficiency spanned a 20-year period, from FY05 through FY24. Although D008497 occurred outside the OIS environment and is not treated as a standalone case study in this study, its persistence provides useful context for understanding how auditability challenges can remain unresolved across multiple audit cycles when underlying process, system, and accountability issues are not fully corrected.

Table 14. Duration of Audit Deficiencies Across Fiscal Year Periods

Duration of Deficiency	Number of Deficiencies	Percentage
1-year span	67	41.61%
2-year span	16	9.94%
3-year span	6	3.73%
4-year span	23	14.29%
5-year span	17	10.56%
6-year span	14	8.70%

7-year span	4	2.48%
8-year span	9	5.59%
9-year span	3	1.86%
11-year span	1	0.62%
20-year span	1	0.62%
	161	**100.00%**

Table 15 identifies organizational factors associated with recurring deficiencies. To construct the table, the dataset was filtered to include deficiencies persisting across two or more fiscal years, resulting in a subset of 94 deficiencies. Contextual variables representing control effectiveness, system constraints, process integration, data environment quality, operational tempo, and governance were then aggregated using pivot-table frequency analysis. The results indicate that recurring deficiencies were most frequently associated with ineffective controls (75 of 94 deficiencies), weak governance (63 of 94 deficiencies), and low system constraints (56 of 94 deficiencies). Similarly, most recurring deficiencies occurred in environments characterized by fragmented or partially integrated processes (80 of 94 deficiencies combined). In contrast, recurring deficiencies were rarely associated with high system support, fully integrated processes, or effective controls. Collectively, these results suggest that recurring deficiencies are more strongly associated with organizational and process conditions than with operational tempo, which was coded as normal in most cases. The following section discusses the implications and findings of this study.

Table 15. Organizational Factors of Recurring Deficiencies

Control Effectiveness	Count	System Constraints	Count	Process Integration	Count	Data Environment Quality	Count	Operational Tempo	Count	Governance	Count
Ineffective	75	Low	56	Fragmented	42	Poor	16	Stressed	3	Weak	63
Partially	19	Moderate	30	Partial	38	Degraded	52	Elevated	11	Mixed	31
Effective	0	High	8	Integrated	14	Reliable	26	Normal	80	Strong	0
Grand Total	94		94		94		94		94		94

G. IMPLICATIONS OF ANALYSIS AND FINDINGS

The analysis and findings in this research study indicate that recurring ordnance-related audit deficiencies are not confined to the OIS 2.0 operating environment but are evident across the broader Enterprise Environment in similar patterns. This finding

suggests that the underlying auditability problem is broader than any single computer system and instead reflects structural process, control, information, and governance conditions within the larger ordnance accountability enterprise.

Deficiencies were not driven primarily by personnel-related factors. Instead, the findings indicate that the most persistent deficiencies were embedded in how ordnance-related activities were structured, controlled, supported by information, and monitored across organizational boundaries. This finding suggests that the recurring auditability problem was less a matter of individual competence or personnel execution than a reflection of the broader process and internal control conditions within which personnel operated.

Persistence of deficiencies across multiple fiscal years suggests that existing remediation efforts have not consistently produced durable reductions in residual risk. When deficiencies continue to recur across audit cycles, particularly in environments characterized by weak governance, degraded information, fragmented process integration, and ineffective controls, the issue is no longer simply whether a corrective action was documented or closed. Rather, the more significant issue is whether the broader process, control, and information conditions required for sustained improvement were ever fully restored. Viewed through this lens, recurring deficiencies indicate that auditability weakness is tied not only to individual findings, but also to repeat conditions that prevent remediation efforts from achieving lasting process improvement. The following section discusses the recommendations based on the findings of this research study.

H. RECOMMENDATIONS BASED ON FINDINGS

1. Strengthen Control Activities

First, Navy leaders should prioritize the standardization and strengthening of key control activities within OIS-related processes and across the Enterprise Environment supporting ordnance accountability. As shown in Table 11, Control Activities accounted for the largest total number of deficiencies, with 71 deficiencies across financial, IT, and operational domains. The findings indicate that many deficiencies were not isolated execution failures, but reflected recurring weaknesses in transaction processing,

reconciliation, review, and documentation. Therefore, corrective action should focus on clear control of ownership, standardized procedures, and repeatable reconciliation practices that reduce dependence on local workarounds and manually intensive processes. Strengthening these control activities would improve consistency across commands and reduce the likelihood that similar deficiency patterns will continue to recur in future audit cycles.

2. Strengthen Information and Communication Mechanisms

Second, leadership should continue strengthening information and communication mechanisms that support ordnance control execution under the current operating environment. As shown in Table 11, Information and Communication accounted for 41 deficiencies, split between financial reporting and IT-related domains. The findings in this study indicate that auditability problems were often connected not only to whether controls existed, but also to whether reliable, timely, and complete information was available to execute and verify those controls. Although OIS 3.0 is expected to improve reporting timeliness, reconciliation, and overall data visibility, the current findings suggest that information reliability and shared access to authoritative data remain important conditions for effective control execution across organizational boundaries. This finding includes the need to ensure that personnel at each echelon are working from timely, traceable, and consistent information needed to record, validate, and review transactions. In that sense, the issue is not simply system modernization alone, but also how information is communicated, shared, and used to support accountability across the broader ordnance enterprise.

3. Cross-Echelon Coordination Gaps

Third, the findings in this study suggest that fragmented governance and limited cross-echelon integration are important conditions associated with the recurrence of ordnance-related deficiencies across the Enterprise Environment. As shown in Table 15, all 94 multi-year deficiencies were associated with weak or mixed governance, and 80 were associated with fragmented or partial process integration. Many deficiencies were not confined to a single office, process, or system, but instead reflected weak coordination and uneven oversight across the operational, logistical, and financial relationships that support ordnance accountability. This finding indicates that corrective

action should be evaluated not only for whether it resolves an individual finding, but also for whether it addresses the broader governance and process conditions under which similar deficiencies have persisted across audit cycles. Without better cross-echelon integration and remediation oversight, corrective actions are likely to address local issues without resolving the broader conditions behind recurrence.

4. OIS 3.0 Implementation

Fourth, OIS 3.0 implementation should be informed by the recurring deficiency patterns identified in this study. Although this research does not evaluate OIS 3.0 performance, it does provide a baseline for the kinds of control, information, and integration deficiencies that modernization efforts should address. In that sense, OIS 3.0 should be viewed not only as a technical upgrade, but also as an opportunity to reduce recurring auditability deficiencies identified under the current operating environment.

5. Strengthen Monitoring of Remediation Effectiveness Over Time

Finally, the Navy should strengthen monitoring of remediation effectiveness over time. The recurrence of deficiencies across multiple fiscal years as shown in Table 14 suggests that corrective action may too often be measured by the administrative closure of individual findings rather than by whether the underlying process, control, and information deficiencies were corrected. Therefore, monitoring should assess not only whether a deficiency was closed, but whether corrective actions remained effective across reporting periods, organizations, and process handoffs. A more rigorous follow-through process would help distinguish administrative closure from genuine improvement in auditability. This finding is especially important given the persistence of recurring deficiencies across audit cycles, which indicates that remediation durability should be treated as a core measure of success. The following section is the summary of this chapter.

I. SUMMARY

This chapter proceeds through the major analytical sections of this study. It began by describing the reviewed deficiency population and then presented the principal findings across the Auditability triangle drivers, COSO internal control components, functional domains, ISO 31000-informed risk analysis, duration of recurring deficiencies,

and organizational drivers of recurring deficiencies. The chapter then examined the implications of those findings and developed recommendations based on the patterns identified in the data. It concluded with a summary of the principal results and their significance within the current OIS 2.0 Environment. The following chapter provides a summary and conclusions and addresses the research questions. It also provides areas for further research.

V. SUMMARY, CONCLUSIONS, AND AREAS FOR FURTHER RESEARCH

This chapter summarizes this study's findings, presents the principal conclusions, and identifies limited areas for further study. It interprets the results in relation to the research questions and the broader problem of recurring audit and accountability deficiencies in Navy ordnance reporting and reconciliation under current system constraints.

A. SUMMARY

This study analyzed 161 documented deficiencies in the Navy's DTT to assess recurring audit and accountability risk under OIS 2.0. Using the Auditability Triangle, the COSO Framework, and an ISO 31000-informed Qualitative Risk Assessment, this study found that recurring deficiencies were concentrated primarily in process and internal control conditions, especially those associated with control execution, information reliability, and process integration. Of the reviewed population, 28 deficiencies were directly related to OIS, while 133 occurred in the broader Enterprise Environment. The following section discusses the conclusions based on the findings.

B. CONCLUSIONS

The findings of this study indicate that recurring ordnance-related audit deficiencies under OIS 2.0 are driven primarily by structural conditions affecting process execution, internal control implementation, and the reliability of information supporting those controls.

First, most reviewed deficiencies were associated with the Enterprise Environment rather than the OIS environment. This finding indicates that OIS system modernization alone is unlikely to resolve many of the recurring audit conditions identified in this study. Therefore, responsibility for improving ordnance auditability extends beyond system management to the broader set of processes, governance structures, controls, and reporting relationships that shape how accountability information is generated and verified across the enterprise.

Second, recurring deficiencies reflect structural process and internal control conditions rather than isolated personnel shortcomings. The Auditability Triangle analysis indicated that most deficiencies were associated with process design and internal control execution rather than with workforce capability or training limitations. Taken together, these findings suggest that recurring deficiencies arise primarily from fragmented processes, constrained information flows, and control conditions that limit reliable execution across organizational boundaries.

Third, the findings suggest that internal control effectiveness is closely tied to the quality and reliability of the information environment supporting ordnance accountability. Deficiencies were concentrated in COSO components associated with control activities and information and communication, indicating that internal control breakdowns were closely linked to the data, documentation, and communication conditions needed to support ordnance accountability. Under OIS 2.0 conditions, auditability frequently depends on manual reconciliation processes and compensating procedures designed to address system limitations. In practice, this finding suggests that controls may exist and be executed as intended yet still fail to produce reliable audit evidence when the underlying information environment is incomplete, delayed, or fragmented.

Fourth, residual audit and accountability risk remain persistent under current operating conditions. The persistence of deficiencies across multiple fiscal years indicates that existing remediation efforts have not fully mitigated the underlying conditions generating recurring deficiencies. These patterns suggest that recurring deficiencies have not been resolved at the level of process execution, information reliability, governance, or remediation follow-through. As a result, recurring deficiencies continue to reflect not only unresolved individual findings, but also broader conditions that allow similar deficiencies to persist across audit cycles.

Finally, system modernization through OIS 3.0 may reduce some of the technical limitations associated with OIS 2.0, particularly those related to information integration and reconciliation (Moor, D., PowerPoint slides, September 9, 2024). However, the findings of this study suggest that lasting improvement in ordnance auditability will also

depend on stronger enterprise processes, governance structures, and control execution practices. Without corresponding improvement in these areas, system modernization alone is unlikely to eliminate the structural conditions that allow recurring deficiencies to persist. The following section addresses the research questions of this study.

C. RESEARCH QUESTIONS

This study addresses the five research questions examining how OIS-related deficiencies compare with the broader deficiency population and what those patterns indicate about recurring control deficiencies.

1. Of all the deficiencies documented in the DTT, how many of those deficiencies are directly related to OIS 2.0?

Of the 161 deficiencies reviewed (as shown in Table 2), 28 deficiencies were directly related to OIS 2.0, while 133 were associated with the broader Enterprise Environment. This finding indicates that OIS is a meaningful source of recurring deficiency, but it does not account for most of the ordnance auditability problem. Instead, the results suggest that the broader auditability challenge extends beyond a single system and is embedded across the wider ordnance accountability enterprise.

2. How do the identified deficiencies align with the Auditability Triangle drivers to distinguish whether breakdowns are primarily driven by personnel, processes, or internal controls?

In both the OIS and Enterprise Environments the deficiencies aligned primarily with process and internal control conditions rather than personnel-related conditions. As shown in Table 3 and Table 4, process accounted for 15 of 28 OIS environment deficiencies (53.57%) and 85 of 133 Enterprise Environment deficiencies (63.91%). Internal control accounted for 11 OIS environment deficiencies (39.29%) and 47 Enterprise Environment deficiencies (35.34%), while personnel accounted for only two OIS environment deficiencies (7.14%) and one Enterprise Environment deficiency (0.75%). Although the overall pattern was consistent across both environments, the Enterprise Environment showed a somewhat stronger concentration in process-related deficiencies. These results indicate that recurring auditability deficiencies were driven mainly by structural and control-related factors rather than by isolated personnel shortcomings.

3. How do the identified deficiencies align with the five components of the COSO Internal Control Framework, and which internal control components are most frequently implicated?

The deficiencies aligned most strongly with control activities, and information and communication across both the OIS and Enterprise Environments. As shown in Table 5 and Table 6, control activities accounted for 16 of 28 OIS environment deficiencies (57.14%) and 55 of 133 Enterprise Environment deficiencies (41.35%), while information and communication accounted for eight OIS environment deficiencies (28.57%) and 33 Enterprise Environment deficiencies (24.81%). This finding suggests that recurring deficiencies were concentrated in execution of controls and in the quality, availability, and communication of information needed to support those controls. As a result, these deficiencies affected the ability of the ordnance accountability enterprise to achieve reliable reporting, effective internal control, and sufficient audit support objectives.

4. How do the deficiencies aligned to the Auditability Triangle drivers and mapped to COSO internal control components manifest as qualitative audit and accountability risks when viewed through the lens of ISO 31000?

When viewed through the ISO 31000-informed risk framework, the deficiencies manifested as recurring qualitative audit and accountability risks. As shown in Table 12 and Table 13, those risks were concentrated primarily in process-related deficiencies mapped to COSO components associated with Control Environment, Information and Communication, and Monitoring Activities. In both the OIS and Enterprise Environments, these combinations produced some of the highest average composite priority scores, indicating that recurring audit and accountability risks were most pronounced where process deficiencies intersected with weak governance, limited oversight, and unreliable information conditions. This finding suggests that the identified deficiencies reflect continuing audit and accountability risk embedded in broader control and organizational conditions rather than isolated technical exceptions.

5. What are the overarching organizational factors contributing to recurring deficiencies?

The findings, as displayed in Table 15, indicate that recurring deficiencies were associated with weak or mixed governance, incomplete process integration, degraded

data environments, and ineffective or partially effective controls. Among the 94 deficiencies persisting across two or more fiscal years, 75 were associated with ineffective controls, 63 with weak governance, 42 with fragmented process integration, and 68 with degraded or poor data environment quality, including 52 coded as degraded and 16 coded as poor. These conditions suggest that recurring deficiencies were sustained by broader organizational factors rather than by temporary workload pressures or isolated local failures. The following section provides areas for further research.

Table 16. Summary of Findings Related to Research Questions

	Research Questions	Findings
Q1	Of all the deficiencies documented in the DTT, how many of those deficiencies are directly related to OIS 2.0?	28 of 161 deficiencies were directly related to OIS 2.0; the remaining 133 were associated with the broader Enterprise Environment.
Q2	How do the identified deficiencies align with the Auditability Triangle drivers to distinguish whether breakdowns are primarily driven by personnel, processes, or internal controls?	Deficiencies aligned mainly with process and internal control conditions, indicating that recurring breakdowns were structural and control-related rather than personnel-driven.
Q3	How do the identified deficiencies align with the five components of the COSO Internal Control Framework, and which internal control components are most frequently implicated?	COSO alignment showed the greatest concentration in control activities and information and communication across both the OIS and Enterprise Environments.
Q4	How do the deficiencies aligned to the Auditability Triangle drivers and mapped to the COSO internal control components manifest as qualitative audit and accountability risks when viewed through the lens of ISO 31000?	The ISO 31000-informed analysis showed elevated residual risk where process deficiencies intersected with weak governance, limited oversight, and unreliable information conditions.
Q5	What are the overarching organizational factors contributing to recurring deficiencies?	Recurring deficiencies were associated with weak or mixed governance, incomplete process integration, degraded data environments, and ineffective or partially effective controls.

D. AREAS FOR FURTHER RESEARCH

Further study should remain focused on the areas most directly connected to the findings of this research study. First, a post-implementation assessment of OIS 3.0 should examine whether system modernization materially reduces the recurring deficiency patterns identified under OIS 2.0, particularly those associated with control execution, information reliability, and process fragmentation. This study provides a baseline assessment of auditability conditions under the pre-OIS 3.0 Environment, making follow-on analysis especially useful for evaluating whether modernization improves auditability outcomes.

Second, a future study should examine remediation durability across multiple audit cycles. Although this study identified recurring themes in the deficiency population, it did not assess whether corrective actions produced sustained improvement over time. Tracking deficiencies across successive audit cycles could help determine whether certain categories are consistently remediated, repeatedly reopened, or replaced by functionally similar findings.

Third, future research study should directly compare the Navy ordnance accountability environment with those of the Army and Air Force to assess whether differences in governance structures, organizational authority, process integration, and system architecture materially affect auditability outcomes. This comparison would help determine whether the recurring patterns identified in this study are specific to the Navy ordnance enterprise or are more broadly shared across the military services. It would also provide a useful basis for evaluating whether different service approaches are associated with stronger auditability performance.

LIST OF REFERENCES

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bedard, J. C., Graham, L., & Jackson, C. (2005). Information systems risk and audit planning. *International Journal of Auditing*, *9*(2), 147–163. https://doi.org/10.1111/j.1099-1123.2005.00267.x

Carmona Ibáñez, P. (2008). Internal control risk influence when planning an audit: An empirical study of the COSO conceptual framework. *Revista de Contabilidad – Spanish Accounting Review, 10*(2), 11–32. https://revistas.um.es/rcsar/article/view/388861/268261

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control – Integrated framework.*

Crawford, S. E. S., & Ostrom, E. (1995). A grammar of institutions. *American Political Science Review*, *89*(3), 582–600. https://doi.org/10.2307/2082975

Department of Defense Office of Inspector General. (2022, May 18). *Understanding the results of the audit of the FY 2021 DoD financial statements*. https://www.dodig.mil/Portals/48/Documents/Reports/Understanding%20the%20Results%20of%20the%20FY%202021%20Audit_Final.pdf?ver=J5FksKFlPPWNBakBwWO88w%3D%3D

Department of Defense Office of Inspector General. (2024a, August 8). *Understanding the results of the audit of the FY 2023 DoD financial statements* (Report No. DODIG-2024-114*).* https://www.dodig.mil/Reports/Audits-and-Evaluations/Article/3868927/understanding-the-results-of-the-audit-of-the-fy-2023-dod-financial-statements/

Department of Defense Office of Inspector General. (2024b, December 20). *Fiscal year 2024 agency financial report*. https://media.defense.gov/2025/Jan/03/2003623632/-1/-1/1/DODIG%202024%20ANNUAL%20FINANCIAL%20REPORT.PDF

Government Accountability Office. (2016). *Defense logistics: Enhanced policy and procedures needed to improve management of sensitive conventional ammunition* (GAO-16-202). https://www.gao.gov/assets/gao-16-202.pdf

Government Accountability Office. (2024). *Government auditing standards: 2024 revision* (GAO-24-106786). https://www.gao.gov/assets/d24106786.pdf

Government Accountability Office. (2025). *Standards for internal control in the federal government* (GAO-25-107721). https://www.gao.gov/assets/gao-25-107721.pdf

Horan, D. J. (1981). *Navy must improve its accountability for conventional ammunition: Report to the Secretary of Defense* (PLRD-81-54). General Accounting Office. https://www.gao.gov/products/plrd-81-54

International Organization for Standardization. (2018). *Risk management—Guidelines* (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

Krippendorff, K. (2019). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications. https://doi.org/10.4135/9781071878781

McNally, J. S. (2013, June). The 2013 COSO framework and SOX compliance. One approach to an effective transition. *Strategic Finance.* https://www.sechistorical.org/collection/papers/2010/2013_0601_COSOMcNally.pdf

Moeller, R. R. (2013). *Executive's guide to COSO internal controls: Understanding and implementing the new framework* (1st ed.). John Wiley & Sons. https://doi.org/10.1002/9781118691656

Office of the Chief of Naval Operations. (2021, May 15). *The naval ordnance management policy (NOMP) manual* (OPNAV M-8000.16). Department of the Navy. https://www.secnav.navy.mil/doni/SECNAV%20Manuals1/8000.16.pdf

Office of Management and Budget. (2016, July 15). *OMB Circular No. A-123, Management's responsibility for enterprise risk management and internal control* (M-16-17) [Memorandum]. https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-17.pdf

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. (2017). *Financial improvement and audit readiness (FIAR) guidance.* https://comptroller.war.gov/Portals/45/documents/fiar/FIAR_Guidance.pdf

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. (2024, December 11). *DoD enterprise risk management and internal control program* (DoD Instruction 5010.40). Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/501040p.pdf

Ponti, F., Bolig, J., Michael, B., Abreu, K., & Gray, T. (2023, Winter/Spring). Navy's ordnance information system. *Navy Supply Corps Newsletter*, 17. https://mynavsup-public.nag.navy.mil/public/sites/navy_supply_journal/documents/Past%20Issues%20Page%20Files/2023_SCNews-Winter-Spring-web.pdf

Potvin, J. L., Shane, P. C., & Mercier, S. P. (2021). *Review and realignment of the Navy's in-service, conventional ordnance logistics supply chain (NAVSUP Ammunition Logistics Center)* [MBA thesis, Naval Postgraduate School]. NPS Archive: Calhoun. https://hdl.handle.net/10945/68792

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press. https://doi.org/10.1093/oso/9780199253944.001.0001

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

Schreier, M. (2012). *Qualitative content analysis in practice.* SAGE Publications. https://doi.org/10.4135/9781529682571

Storkman, W. D. (2005, September/October). Attending to COSO general controls before disaster strikes. *Newsletter of the AICPA*, *14*(5), 1–4. ProQuest.

Zahari, A. I., Said, J., Muhamad, N., & Ramly, S. M. (2024). Internal control on public organisation performance: A Smart PLS analysis using COSO framework. *Global Business and Management Research, 16*(4S), 340–356. https://www.gbmrjournal.com/pdf/v16n4s/V16N4s-22.pdf

Acquisition Research Program
Department of Acquisition, Finance and Manpower
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net