2015

Expanding the Navys Managers Internal Control Programs (MICP) capability to prepare for external financial audits

Pagnucco, Jonathan P.

Monterey, California: Naval Postgraduate School

http://hdl.handle.net/10945/45919

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EXPANDING THE NAVY'S MANAGERS' INTERNAL CONTROL PROGRAM'S (MICP) CAPABILITY TO PREPARE FOR EXTERNAL FINANCIAL AUDITS

by

Jonathan P. Pagnucco

June 2015

Thesis Advisor: Juanita M. Rendon
Co-Advisor: Philip J. Candreva

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*		2. REPORT DATE June 2015	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE EXPANDING THE NAVY'S MANAGERS' INTERNAL CONTROL PROGRAM'S (MICP) CAPABILITY TO PREPARE FOR EXTERNAL FINANCIAL AUDITS			5. FUNDING NUMBERS	
6. AUTHOR(S) Jonathan P. Pagnucco				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The Department of the Navy's Managers' Internal Control Program (MICP) is an important tool for ensuring the Department is well managed. In 2013, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) added 17 principles to the five existing internal control components. In 2014, the Government Accountability Office's (GAO) updated *the Standards for Internal Control in the Federal Government* and directed federal managers to adopt the update by fiscal year 2016. The Navy's internal control program does not yet comply.

After analyzing the content of the MICP against the COSO and GAO publications, this thesis developed templates to supplement the MICP in order to bring the Navy program into compliance and provide a tool for internal assessment that may aid commands as they prepare for external financial audits.

14. SUBJECT TERMS Effective Internal Controls, Auditability, Internal Audits, External Audits, GAO's Five Standards of Internal Control in the Federal Government, Financial Improvement and Audit Readiness (FIAR), DOD Inspector General , Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 17 Principles, Office of Financial Operations (FMO), Managers' Internal Control Program, Managers' Internal Control Manual.			15. NUMBER OF PAGES 169
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

EXPANDING THE NAVY'S MANAGERS' INTERNAL CONTROL PROGRAM'S (MICP) CAPABILITY TO PREPARE FOR EXTERNAL FINANCIAL AUDITS

Jonathan P. Pagnucco
Lieutenant, United States Navy
B.S., Youngstown State University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

**NAVAL POSTGRADUATE SCHOOL
June 2015**

Author: Jonathan P. Pagnucco

Approved by: Juanita M. Rendon
               Thesis Advisor

               Philip J. Candreva
               Co-Advisor

               William R. Gates
               Dean, Graduate School of Business & Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Department of the Navy's Managers' Internal Control Program (MICP) is an important tool for ensuring the Department is well managed. In 2013, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) added 17 principles to the five existing internal control components. In 2014, the Government Accountability Office's (GAO) updated the *Standards for Internal Control in the Federal Government* and directed federal managers to adopt the update by fiscal year 2016. The Navy's internal control program does not yet comply.

After analyzing the content of the MICP against the COSO and GAO publications, this thesis developed templates to supplement the MICP in order to bring the Navy program into compliance and provide a tool for internal assessment that may aid commands as they prepare for external financial audits.

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

ASN(FM&C)	Assistant Secretary of the Navy (Financial Management and Comptroller)
CNO	Chief of Naval Operations
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DOD	Department of Defense
DODIG	Department of Defense Inspector General
DON	Department of the Navy
ERP	enterprise resource planning
FFMIA	Federal Financial Management Improvement Act
FIAR	financial improvement and audit readiness
FIP	Financial Improvement Program
FMO	Office of Financial Operations
FMP	fraud mitigation program
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GMRA	Government Management Reform Act
IA-CM	Internal Auditing—Capability Model
ICOFR	Internal Controls Over Financial Reporting
IIA	Institute of Internal Auditors
IPA	independent audit firm
IR	item to be revisited
IT	information technology
MAU	Major Assessable Unit
MICM	Managers' Internal Control Manual
MICP	Managers' Internal Control Program
MW	material weakness
NAS	Naval Audit Service
NAVSEA	Naval Sea Systems Command
NDAA	National Defense Authorization Act

RC	reportable condition
SBA	Schedule of Budgetary Activity
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SFIS	Standard Financial Information Structure
SOA	Statement of Assurance

ACKNOWLEDGMENTS

I would like to recognize everyone who helped turn this thesis into a reality. First, I would like to thank God and my family for their steadfast love and support. Next, I would like to thank and express my most sincere gratitude to my advisors, Dr. Juanita Rendon and Dr. Philip Candreva, along with the Conrad Committee, Capt. Hank Sanford, USN (Ret), Dr. Kenneth Euske, and Dr. Robert Eger, for their expertise, mentorship, and patience throughout this process. Their contributions were invaluable to this thesis. Finally, I would like to thank my editor, Rich Black-Howell, for his comments and recommendations. Without all of you, this thesis simply would not have been possible, and I am extremely grateful for all of your efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The Department of Defense (DOD) continues to encounter many challenges that affect its ability to provide accurate, reliable, timely, and useful financial information that is readily available to key decision-makers such as senior leaders and Congress and supports operating, budgeting, and policy decisions (Blair, 2011). One of the most critical challenges within DOD is meeting the statutory mandate of having auditable financial statements by September 30, 2017.

Daniel R. Blair, Department of Defense (DOD) Deputy Inspector General for Auditing, stated: "Poor internal controls increase the risk of fraud, waste, and abuse" and "Until the Department resolves these pervasive weaknesses, it will be very difficult for DOD to reliably assert that it is ready for an audit by 2017" (Blair, 2011, p. 7). Therefore, effective internal controls have a direct impact on DOD's audit readiness and auditable financial statement mandates. While the audit readiness mandate applies to organizations DOD-wide, the focus of this research is on the Department of the Navy (DON) and internal controls.

DON's guidance on internal control is provided by the DON MICP and found within its Managers' Internal Control Manual (MICM). The MICP supports DON personnel in achieving effective internal control systems using the United States Government Accountability Office's (GAO) Standards of Internal Control for the Federal Government, also known as the Green Book. Both industry and the federal government have incorporated the May 2013 revision to The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control—Integrated Framework. The DON MICP, however, has not adopted the recent revision. The DON MICM meets all of GAO's minimum requirements with the exception of GAO's 17 new principles that were adopted from the COSO's updated Framework (Government Accountability Office's

[GAO], 2014). For federal agencies, external auditors use the Green Book to evaluate DON's internal control but will not be able to express an unmodified audit opinion if the MICP does not meet GAO's minimum internal control requirements for the federal government (GAO, 2014).

Internal controls are a key area to preparing for external financial audits. "Three key areas to financial management reform are improving the quality of the data, internal controls, and financial systems" (Blair, 2011, p. 4). An effective internal control system may help provide reasonable assurance that organizations will meet their objectives. Implementing an effective internal control system and conducting meaningful internal audits are important to an organization's attempt to improve accountability, achieve financial auditability, and maintain audit readiness. The Department of the Navy (DON) Managers' Internal Control Program (MICP) is an important program for ensuring the DON is well managed. Expanding DON internal control capabilities may improve commands' audit readiness efforts in support of DOD's goal of having auditable financial statements. DON may benefit not only from having more effective internal controls while preparing for external financial audits, but also from having auditable financial statements that provide reliable and useful information for key decision-makers. Furthermore, DON may benefit from a tool that commands can use to improve the effectiveness of their internal control programs.

As a first line of defense, internal controls help protect assets, help prevent errors, help deter fraud, waste, and abuse, and assist senior leaders in meeting their organizations' goals and missions through stewardship of taxpayer dollars (Blair, 2011, p. 6). Developing a tool to supplement the MICM with the 17 newly required principles may not only show external auditors that DON is in compliance with the Green Book, but also may provide a way to document DON self-assessments on the effectiveness of its internal control program. The MICP may use this tool to expand its capabilities in preparing commands for self-assessments and internal audits before undergoing external financial audits.

B.   PURPOSE OF RESEARCH

The purpose of this research is to examine expanding the DON MICP's internal control capability in preparation for external financial audits. The MICP supports DON personnel in achieving results using the GAO federal standards for internal control, but has not yet adopted GAO Green Book's recent revisions. The MICM is missing the 17 new principles that GAO requires all federal agencies to adopt beginning in FY 2016. This research explores developing a tool to supplement the MICM, which may help close the gap between the MICP's guidance and the updated internal control framework used by both industry and the federal government.

A tool can be developed and added into the MICM, which may help commands identify and correct internal control deficiencies before upcoming external financial audits. Developing a standardized tool that can be used across all DON commands to report upward to the Office of Financial Operations (FMO) may provide a unifying mechanism that helps improve DON's internal control system when tested by external auditors during financial audits. Ultimately, supplementing the MICM with a self-assessment tool may move DON a step closer to receiving an unmodified audit opinion in support of DOD's efforts toward achieving audit readiness and having auditable financial statements by 2017.

C.   RESEARCH QUESTION

This research study will answer the following question:

- How would updating the MICP's capabilities to current internal control guidance help commands achieve audit readiness?

D.   METHODOLOGY

This study will assess the relationship between the current state of the MICP and how the external environment outside DOD and DON has changed related to internal control guidance. This study will also conduct a content analysis to examine the relationship between the MICM, Green Book, and COSO's Internal Control–Integrated Framework (Framework): Internal Control

over Financial Reporting—Illustrative Tools for Assessing Effectiveness of a System of Internal Control (Illustrative Tools). Based on the analysis, a series of supplemental templates will be developed to help the DON MICP expand its internal control capability and add the missing 17 principles to its MICM. These templates may help bridge the gaps by aligning the MICM with the Green Book using COSO's Illustrative Tools.

DON may consider incorporating this tool in its MICM to help commands achieve audit readiness in support of meeting the overall goals of preparing for external financial audits and having auditable financial statements annually.

E.   BENEFITS

This research study provides recommendations on how DON can enhance the MICP to help commands prepare for external financial audits by improving DON's internal control programs. Having effective internal controls is an integral part of an organization's internal audit division's goal of preparing the organization for external audits. Adding COSO's 17 principles to the existing five internal control components may make DON's internal control system more effective by helping to mitigate material weaknesses in internal controls.

Effective internal controls may assist DON managers and DOD in confronting the issues associated with audit readiness. For example, effective internal control systems may help DON safeguard financial information, ensure adequate supporting documentation exists, provide reliable financial data, and assist management in communicating with auditors. Furthermore, effective internal control systems may also help DON mitigate against risks, such as fraud, waste, and abuse, which adversely impact DON's ability to achieve its objectives.

The MICP's guidance on internal control is outdated, and DON may benefit by updating the MICM to reflect the current federal internal control guidance and the industry's internal control framework. Commands may also benefit by being better equipped to inspect themselves before going through external audits. Expanding the MICP's capabilities may improve financial audit

readiness toward meeting Congress' mandate of producing auditable financial statements by FY 2017.

F.   ORGANIZATION OF STUDY

This research consists of six chapters, including this introduction. Chapter II undertakes a literature review to explain the role of internal controls in financial auditability. It reviews DOD's Financial Improvement and Audit Readiness (FIAR) plan and obstacles to auditability, details DON's internal control program, and shows DON's roadmap to auditability. Chapter II concludes with the current industry internal control framework set by COSO and GAO's incorporation of COSO's internal control components into the Standards on Internal Control for the Federal Government.

Chapter III, Content Analysis, examines the relationship between the MICM and the COSO internal control framework, along with the GAO internal control standards. Chapter IV, Findings, discusses the findings of the literature review and content analysis to answer the research question. Chapter V, Development of Templates and Recommendations Based on Analysis, details the development of four recommended templates, which are adopted from COSO, using GAO's application requirements and can supplement the MICM. Chapter VI, Summary, Conclusions, and Areas for Further Research, summarizes this research and offers recommendations for areas for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

This chapter will review internal control literature from various sources and explain internal control's role in financial auditability, an internal and external auditor's role in internal control, and internal control guidance in the federal government. Next, the literature review addresses the consequences of weak internal controls, explains internal control's role in Department of Defense (DOD) financial auditability, and provides a background on financial auditability in the Department of the Navy (DON). The DOD's Financial Improvement and Audit Readiness (FIAR) program, DON's roadmap to financial auditability, and obstacles to auditability are discussed. This chapter concludes with the current industry internal control framework set by The Committee of Sponsoring Organizations' (COSO) and Government Accountability Office's (GAO) incorporation of the COSO internal control components into the Standards of Internal Control for the Federal Government (Green Book).

The purpose of this literature review is to examine the current state of the DON Managers' Internal Control Program (MICP) and changes in the external environment outside the Department of Defense (DOD) in relation to internal control.

B. INTERNAL CONTROL AND AUDITABILITY

Effective internal control systems are significant in helping organizations improve performance and reach objectives. Internal auditors review corporate governance and prepare organizations for external financial audits. Private sector companies often use internal auditors to check the effectiveness of the company's internal control system before undergoing an external audit. External auditors test the effectiveness of an organization's internal control system during independent financial audits of that organization's financial statements. An internal control system must be free of any material weaknesses, or external

auditors cannot issue an unmodified opinion, known as a clean audit, on an organization's internal control over financial reporting. Public sector organizations have struggled over two decades to receive a clean audit opinion, in part due to internal control weaknesses.

Having an effective internal control system is important to DOD and DON audit readiness efforts. DON leaders should be concerned about the effectiveness of their internal control because it only takes one material internal control deficiency to disqualify an organization from receiving an unmodified audit opinion by external auditors. More importantly, effective internal controls can help DON managers and DOD confront the issues associated with audit readiness, such as safeguarding financial information, ensuring adequate supporting documentation exists, providing reliable financial data, and assisting management in communicating with auditors. Therefore, effective internal controls have a direct impact on DON obtaining auditable financial statements.

1. Internal Auditors' Role in Internal Control

Internal auditors act as a safeguard to organizational management since they monitor the tone at the top and evaluate an organization's risks in major areas like company strategy, compliance, financial reputation, and operations. Internal auditors are usually an employee of the organization, but the internal audit function is sometimes contracted out. Furthermore, internal auditors add value by getting involved in and understanding all areas of the organization, such as its personnel, processes, and objectives. The internal auditing profession brings a composite of in-depth knowledge and best business practices in the areas of internal control and risk assessment (Richards, 2006). The internal auditing profession has broadened to keep up with rapid changes in economic, regulatory, and technological advancements (Haas, Abdolmohammadi, & Burnaby, 2006).

Organizations need internal auditors who solve problems, assure management adequate internal controls are in place, and improve corporate

governance through their consulting (Deloitte, 2004). Management can aid the internal auditing process by supporting the design and monitoring processes through collaborating and building trust with internal auditors. Organizations should keep internal auditors abreast of changes in expectations as the business evolves. Doing so helps expand internal auditing capabilities that help organizations remain relevant and add value amid change (PWC, 2014).

Internal auditors can create value by aligning their audit strategy to focus on the risks that matter to the organization. The more mature organizations are in risk management practices, the more likely they are to outperform their competition financially (EY, 2012). A mature internal audit activity should apply a critical thinking approach beyond financial, compliance, and operational objectives. Internal auditors should be invited to the organization's strategic committees, task forces, and initiatives (KPMG, 2014).

2. External Auditors' Role in Internal Control

Independent external auditors test a company's internal controls during financial statement audits before issuing an audit opinion. Audits on government organizations must be conducted in accordance with GAO's Generally Accepted Government Auditing Standards (GAGAS), referred to as the Yellow Book, which details the auditing standards that must be followed for government audits. Depending on the type of audit, audit reports usually address three things: financial statements, compliance with laws and regulations, and internal control. External auditors must report all significant internal control deficiencies and note all material weaknesses (GAS, 2011).

Typically, independent external auditors plan the internal control audit and then determine if any additional testing is necessary to support an opinion on financial statements. Auditors usually follow five stages when conducting internal control audits (Whittington & Pany, 2014, p. 278):

1. Plan an integrated audit that encompasses both the financial statement and internal control over financial reporting audits

2. Prioritize which controls will be tested, using a top-down approach

3. Evaluate design effectiveness

4. Evaluate operating effectiveness

5. Express an opinion on internal control effectiveness (Whittington & Pany, 2014, p. 278):

The appearance or discovery of weak controls will result in more costly and time-consuming audit testing. An effective internal control system has the characteristics listed in Table 1, which shows the relationship between each characteristic and its corresponding internal control component. External auditors evaluate various factors, such as the competence and responsibilities of personnel, proper procedures, safeguards, verification that documentation is being followed, and verification that independent checks on performance are being conducted (Porter, Simon, & Hatherly, 2014).

Characteristics	Corresponding Component
(i) Competent, reliable personnel who possess integrity	Control environment
(ii) Clearly defined areas of authority and responsibility	Control environment
(iii) Proper authorization procedures	Control environment and control activity
(iv) Adequate records	Information system
(v) Segregation of incompatible duties	Control activity
(vi) Independent checks on performance	Control activity
(vii) Physical safeguarding of assets and records	Control activity

Table 1. Characteristics of Effective Internal Control System
(after Porter et al., 2014)

In the case of DON financial audits, external auditors communicate with individuals from all levels. For example, external auditors conduct sample transactions of external parties with whom business transactions occurred. External auditors may gather supporting documentation from individuals to

evaluate the design, operating effectiveness, and compliance of internal control systems. External auditors review business operations from end to end. DON is preparing all stakeholders for external financial audits by communicating the impact and implication of external audits on each stakeholder. Commands are trained to prepare for the audits in several ways. They must validate the financial recording and reporting processes across all business segments for audit readiness, ensure effective internal control systems are in place, and use audit trail checklists to organize and highlight key areas on the supporting documentation (Cook, 2015).

3. Internal Control Guidance for the Federal Government

The Federal Managers' Financial Integrity Act of 1982 (FMFIA) requires federal agencies to establish and maintain an internal control system. The federal policy on internal control is provided by the Office of Management and Budget (OMB) Circular A-123, Management's Responsibility for Internal Control. The policy holds management responsible for establishing and maintaining those controls. Actions include the following:

1. Develop and implement appropriate, cost-effective internal control for results-oriented management

2. Assess the adequacy of internal control in federal programs and operations

3. Separately assess and document internal controls over financial reporting consistent with the process defined in Appendix A

4. Identify needed improvements

5. Take corresponding corrective action

6. Report annually on internal control through management assurance statements (Executive Office of the President Office of Management and Budget [OMB], 2004)

The OMB Circular No. A-123 lists three objectives of internal control: "to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations" (OMB, 2004, p.

11

5). OMB's philosophy behind internal control is that it should be a continuous process and not merely a stand-alone tool for managers. Excess controls can lead to inefficiencies, so a delicate balance needs to exist between controls and risk. Management must assess whether the benefits outweigh the cost in their decision making over an internal control system (OMB, 2004).

OMB later made additions to its internal control guidance to clarify audit requirements. The OMB Circular No. A-123 was updated with Appendix D, Compliance with the Federal Financial Management Improvement Act of 1996, through a memorandum to the heads of executive departments and establishments. While the Government Management Reform Act (GMRA) only requires agencies to publish annual audited financial reports, the Federal Financial Management Improvement Act (FFMIA) makes more stringent requirements. The FFMIA ensures that federal financial management systems provide reliable financial figures consistently, uniformly, and annually (OMB, n.d.). FFMIA allows oversight of federal financial management by the president, Congress, and general public (Gotbaum, 2001).

As mentioned earlier, the FMFIA requires the Comptroller General to issue standards for internal control in the federal government. The OMB Circular No. A-123 provides specific requirements for assessing and reporting on controls in the federal government (GAO, 2014). Based on these and other government requirements, the GAO established the Standards for Internal Control in the Federal Government, the Green Book, which provides an overall framework for establishing an effective internal control system for federal agencies.

4. Auditability Triangle

Without effective internal controls, an organization's capability to reach its objectives in a timely manner may be adversely affected since deficiencies may not be discovered (OMB, 2004). Organizations with weak internal controls may assume unnecessary risks that adversely impact their ability to achieve organizational objectives. Examples of these unnecessary risks include the risk

of material misstatements; the risk of omissions due to fraud, illegal acts, and corruption; and the risk of management override (COSO, 2013d). Effective internal controls are an important part of audit readiness and one of the three components of the auditability triangle (Rendon & Rendon, in press).

The auditability triangle is a conceptual framework based on the theory of auditability that encompasses three aspects of governance: competent personnel, capable processes, and effective internal controls. The focus of this research is on the internal control component of the auditability triangle shown in Figure 1, which involves using COSO's Internal Control—Integrated Framework (Framework) to enforce internal control policies. Effective internal controls help ensure compliance with legal and regulatory requirements through monitoring and reporting material internal control weaknesses. Organizations should stress auditability in their operations and internal control processes and ensure personnel understand how weaknesses in an internal control system may lead to fraud (Rendon & Rendon, in press).

Conceptual Framework

Educated
Trained
Experienced

Personnel

Processes

Institutionalized
Measured
Improved

Internal Controls

Enforced
Monitored
Reported
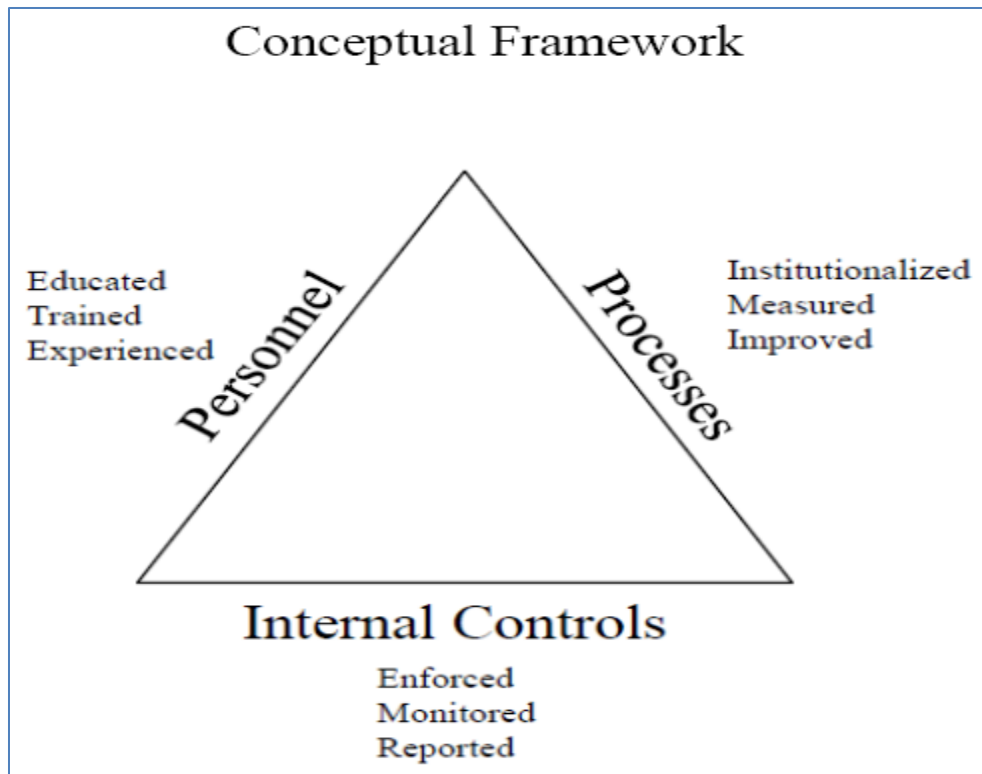
Figure 1.   Auditability Triangle (from Rendon & Rendon, in press)

5.   Internal Control's Role in DOD Financial Auditability

Implementing an effective internal control system and conducting meaningful internal audits are essential to DOD achieving financial auditability. Congress and the National Defense Authorization Act (NDAA) of 2010 mandate fully auditable financial statements by FY 2017. DOD is one of the last federal agencies out of 24 that has not successfully received an unmodified opinion. Effective internal control is significant to auditability because it is a requirement to obtaining an unmodified audit opinion.

Internal control is emphasized more as commands strive toward audit readiness as they transition from undergoing command inspections to financial audits. Previously, command inspections were focused upon the personnel's performance of a mission. Now, financial audits have shifted the focus to provide reasonable assurance on the reliability of internal control functions like

14

processes, controls, and documentation. Documentation and continuous improvement are essential to obtaining and sustaining clean audits (Cook, 2015).

All four processes are derived from internal control functions, including management controls, key supporting documentation, systems and data, and audit response that are depicted in Figure 2 (Cook, 2015). Effective internal control systems help organizations safeguard financial information, ensure adequate supporting documentation exists, provide reliable financial data, and assist management in communicating with auditors.

FY15 SBA Audit Focus: Improving DON's Business Processes and IT Systems

- Established a **segment approach, based on major business processes,** to audit readiness which enables DON to prepare key parts of its business prior to the SBA audit
- With Enterprise-wide support, DON has made significant progress in the following areas to enhance preparation for the SBA audit:

Management Controls		Key Supporting Documentation		Systems & Data		Audit Response
Safeguarding financial information	+	Evidencing financial transactions	+	Demonstrating integrity and completeness of information	+	Coordinating requests and helping auditors understand DON processes

Figure 2.   Preparing for Financial Audits (from Cook, 2015)

6.   Financial Auditability in DON

The Financial Improvement and Audit Readiness Branch is responsible for supporting DON in financial audit readiness through DON's FIAR program. Audit readiness in DON means being constantly prepared to demonstrate proper processes, both manual and automated, and documentation. The DON can achieve audit readiness through sustainable, traceable, and repeatable business processes (FMO, n.d.-c). The following section discusses the Office of Financial Operations' (FMO) role and responsibility in bringing DON down the path of financial auditability. A background of FMO's MIC program, MIC manual, and

MIC plan is provided before discussing the DON roadmap to auditability and the obstacles to auditability.

a.   FMO's Role

Authority over DON's financial statement reporting has been delegated to the FMO. FMO instituted an internal control program that falls under and reports to DOD's Managers' Internal Control Program (MICP). FMO also assists DON commands with auditing guidance and training.

DON guidance for internal control standards are found within the Managers' Internal Control Manual (MICM), in which FMO explains how to meet the reporting requirements in relation to GAO's five internal control standards. The Secretary of the Navy's (SECNAV) MICP issued the manual because the FMO-lead program falls under the overarching DOD MICP. Neither DOD nor DON MICP have updated their guidance to be in alignment with the recently updated GAO Green Book that sets the internal control standards within the federal government.

b.   MIC Program

The Assistant Secretary of the Navy (Financial Management and Comptroller) (ASN(FM&C)) holds the overall responsibility for preparing an annual Statement of Assurance (SOA). This authority, however, has been delegated to the FMO and detailed in the MICM and MICP. FMO's MICP supports DON's personnel by developing and offering training to command coordinators so that they can practice sound internal control to achieve organizational results, safeguard the integrity of programs, and be good stewards of federal resources (FMO, n.d.-a).

All of the MICP's internal control accomplishments and deficiencies are compiled through two venues: DON's Major Assessable Units (MAUs) and Naval Audit Service (NAS). MAUs submit the internal control certification statements to ASN(FM&C) via FMO. Commands self-report control deficiencies upward

(SECNAV, 2008). MAUs maintain MICP documentation to fulfill four of FMFIA's processes which include (SECNAV, 2008):

1. Risk assessment

2. Internal control assessment

3. Corrective actions for material weaknesses and reportable conditions

4. MIC Plan

FMO meets with NAS personnel quarterly to review audit reports from three sources: GAO, Department of Defense Inspector General (DODIG), and Naval Audit Service (NAS). This review helps pinpoint material control deficiencies, determine materiality, and choose what to include in the Statement of Assurance (SOA) (SECNAV, 2008). NAS is DON's internal audit organization. NAS's mission is to give independent and objective audit services to help leadership assess risk, enhance efficiency and accountability, and make programs more effective (SECNAV, n.d.).

Beyond the MAU and NAS self-reporting of control deficiencies, the annual SOA includes a separate certification statement. The statement is on the Internal Controls Over Financial Reporting (ICOFR) and is required by Appendix A of the 2004 revised OMB Circular A-123. The addition to the ICOFR strengthens internal control over financial reporting (OMB, 2004; SECNAV, 2008). The ICOFR aids DON in fulfilling OMB's reissued A-123 that mandates each DOD branch report annually on the effectiveness of their internal controls to ensure the integrity of their financial reporting.

ICOFR's primary goal is for every DON component to develop a strategy on measuring their business and internal control processes that lay the foundation for sustaining auditable financial statements. Audit readiness is not "just a one-time achievement," but rather a "consistent state of financial integrity that must be continually sustained" (FMO, n.d.-b). The DON FMO's Financial Improvement Program (FIP) works toward fulfilling OMB Circular A-123 Appendix

A requirements and aims to achieve an unmodified audit opinion of DON financial statements (SECNAV, 2008).

c.   MIC Manual

The DON MIC Manual, hereafter referred to as MICM, Secretary of the Navy (SECNAV) Manual M-5200.35, Department of the Navy Managers' Internal Control Manual, implements internal control policy found in the SECNAV Instruction 5200.35F, Department of the Navy (DON) Managers' Internal Control (MIC) Program. The SECNAV Instruction 5200.35F was updated in 2014, but the MICM has not been updated since 2008. The MICM gives DON guidance on implementing effective internal controls (SECNAV, 2008). The MICM's procedures serve as a management baseline for reporting DON's Annual Statement of Assurance to the Secretary of Defense (SECDEF). The SOA provides explicit assurance regarding the effectiveness of internal controls (SECNAV, 2014). The MICM contains a MIC Plan that provides guidance to DON MIC coordinators for executing their command's internal control program.

d.   MIC Plan

The MIC Plan, an executive summary of a command's MIC program, lays out DON's approach to implementing an effective internal control program. The MIC Plan is the primary resource for command MIC coordinators to use. The MIC Plan's format is designed to help MIC coordinators understand their organization's internal control program, comply with reporting requirements, and relate to GAO's federal standards on internal control (SECNAV, 2008).

A sample MIC Plan template is provided for Commanders to tailor to their commands. The format was designed to fulfill the requirements based on the 1999 GAO Green Book, Standards for Internal Control in the Federal Government. The sample MIC Plan template helps commands develop their own internal control plan.

The MIC Plan is built on GAO's and COSO's five components of internal control. Both frameworks have recently embedded 17 principles into the five components to help the public and private sectors keep up with changes that have evolved over the last two decades (GAO, 2014). The new 17 principles have not yet been incorporated into the MICM or the MIC Plan, however.

e.   DON's Roadmap for Financial Auditability

FMO is responsible for preparing commands for financial audits, and a paradigm shift is needed to embrace the volume, intensity, and fast pace of a Schedule of Budgetary Activity (SBA) audit. DON is following DOD's FIAR plan in an effort to be fully audit ready by FY 2017. Recent OUSD(C) guidance added a requirement for all military departments to initiate audits of the SBA on October 1, 2014. DON is on a critical path to financial auditability, as shown in Figure 3, because it must report the results of full financial statement audits to Congress by 2019 (Cook, 2015). DON has encountered many obstacles in its efforts towards financial auditability.
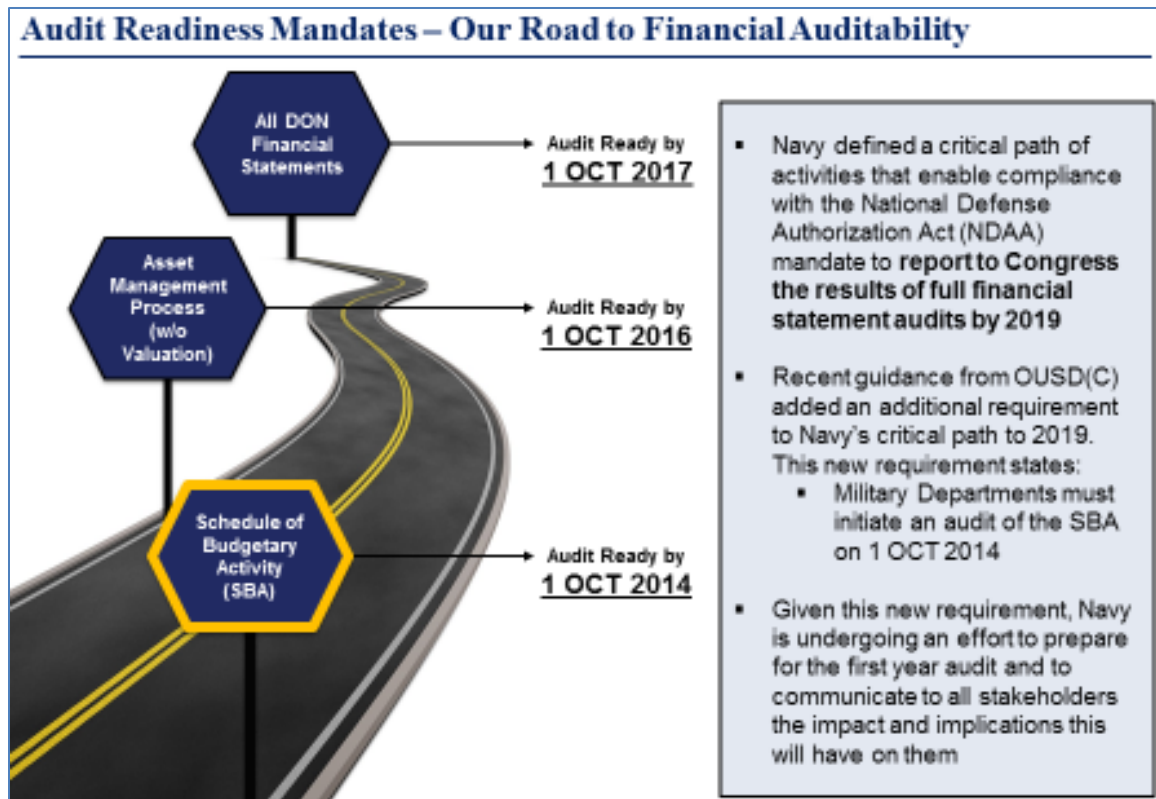
Figure 3.   DON's Road to Financial Auditability (after Cook, 2015)

7.   Obstacles to Auditability

An effective internal control system may help remove some major obstacles that are blocking the path to DOD's auditability efforts. DOD may not receive an unmodified opinion if its internal control systems cannot produce reliable financial information. DON is planning for financial audits with limited funding and may benefit from both academic and private sector frameworks to strengthen business processes through expanding its internal control capabilities.

The Under Secretary of Defense (USD) Comptroller identified three significant challenges to auditability in DOD: budgetary turmoil, planning for and supporting DOD-wide audits, and resolving issues in the business process (Hale, 2014). First, uncertainty in the defense budget caused turmoil in DOD because the ambiguity sidetracked financial managers' devotion to audit efforts (Hale, 2014). Second, planning for and supporting massive scale audits is challenging

in a tight fiscal environment. Also, finding firms with the experience to support DOD-wide audits is problematic because many capable independent audit firms are DOD consultants and are, therefore, ineligible to conduct such an audit. Third, independent auditors often find issues in business processes that are challenging to resolve due to DOD's size and complexity (Hale, 2014). Beyond DOD, DON has its own auditability challenges.

The Assistant Secretary of the Navy (Financial Management and Comptroller) identified three significant challenges to auditability in DON: information technology (IT) systems, the ability to consistently produce adequate documentation to substantiate transactions, and effective internal controls surrounding business processes along with the verification that they have been tested (Commons, 2012). DON is constructing the infrastructure necessary to contain, retrieve, and evaluate the electronic audit documentation that external audits require. This infrastructure will help overcome DON's three significant challenges to audit readiness. Further, this infrastructure acts as an audit management tool because it supports assertion preparations, financial audits, and sustainment activities (Commons, 2012). The next section will discuss the industry standard on internal control.

C.   INDUSTRY STANDARD ON INTERNAL CONTROL

The COSO's Internal Control—Integrated Framework (Framework) is the world's leading internal control framework (COSO, 2013a). The original Framework was developed in 1992 to establish an industry standard in the field of internal control and was updated in May 2013 to keep up with evolutions in global business and operating environments over the last couple of decades (COSO, 2013a). The 2013 Framework is similar to the original version because it retains the five components of internal control and the definition of internal control. The new Framework, however, embeds 17 new principles into the five components of internal control (COSO, 2013a).

Internal control is "a process, effected by an organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (COSO, 2013a, p. i). There is a direct relationship between three elements: the objectives of internal control, an organization's structure, and COSO's five integrated components, as illustrated in Figure 4 (COSO, 2013a).
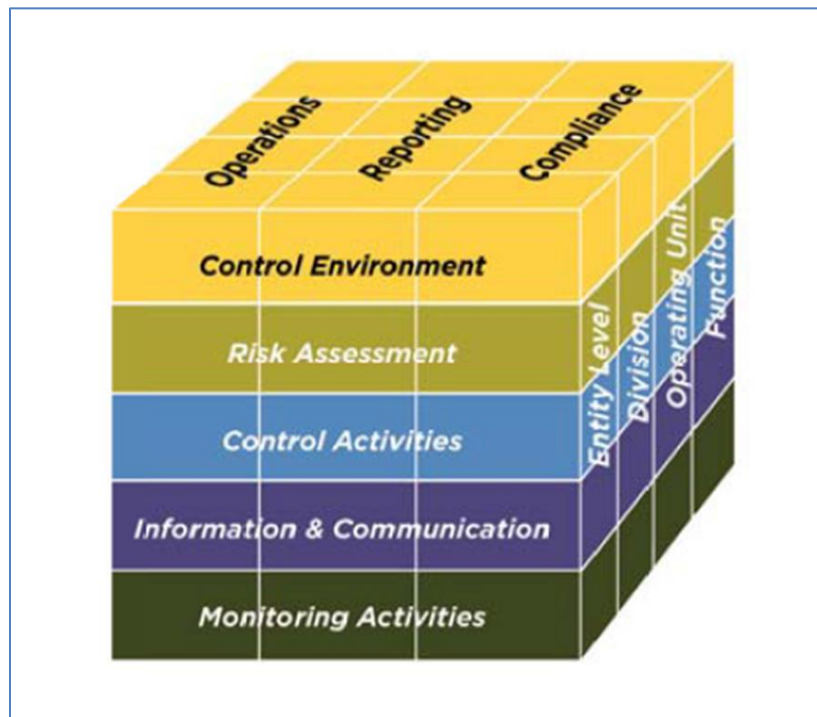
Figure 4. COSO's Components, Objectives, and Organizational
Structure of Internal Control (from Protiviti, 2014)

As shown in Figure 4, there are five integrated components to internal controls in organizations: (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring activities (COSO, 2013a). The framework organizes the 17 principles by each associated component. All principles apply to the operations, reporting, and compliance objectives and help organizations achieve effective internal controls. COSO

categorized the 17 new principles into the five components of internal control (COSO, 2013a). Figure 5 summarizes the 17 principles and categorizes them into the corresponding internal control component.

Internal Control Component	Principles
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that board exercises oversight responsibility 3. Establish structures, reporting lines, authorities and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally 15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

Figure 5.   COSO's 17 Principles within Each Internal Control Component
(from COSO, 2013)

23

1.   Control Environment

The first component of the Framework, control environment, is the set of standards, processes, and structures that lay the foundation for an internal control system throughout the organization. Management sets the tone at the top and sets the expectations over standards of conduct, integrity, and ethical values of the organization. COSO's new Framework adds five new principles to strengthen the control environment component because it has a pervasive impact on an organization's internal control system. The five principles in the control environment include (COSO, 2013b, p. 31):

1.   The organization demonstrates a commitment to integrity and ethical values.

2.   The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3.   Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4.   The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5.   The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

The control environment is the foundation for the rest of the five components because it sets the tone within the organization and increases employees' awareness of internal control. The control environment ranges from organizational traits like management philosophy, organizational structure, authority and roles of responsibility, and policies and procedures to individual attributes like integrity, ethics, and competency. The effectiveness of an organization's internal control relies upon leadership to set the tone at the top by communicating and enforcing the control environment (Whittington & Pany, 2011).

An effective control environment relies upon an organization's management to act with integrity and in accordance with its standards of conduct; otherwise, an organization is vulnerable to fraud. The cornerstone of an anti-fraud environment is a value system grounded on integrity (AICPA, 2002). An organization's standards of conduct should be communicated to all personnel in a way that is understandable and in a positive manner that evokes ownership of its content. The standards of conduct should be formally included in an employee manual so they can be easily referenced as needed (AICPA, 2002).

Internal auditors assess an organization's control environment. Support from senior management is essential to internal auditing effectiveness (Lenz & Hahn, 2015). Auditors are encouraged to focus carefully on two areas that have been found to be relatively weak in organizations: tone at the top and management override of controls (Hermanson, Smith, & Stephens, 2012). Tone at the top affects the organization's public perception and reputation. Organizations with poor tone at the top often have a "special" group that does not follow institutional governance since this group believes that they are above the rules. This group typically uses their internal leverage to avoid confrontation when personnel notice improper activities (Spoehr, 2012). Integrity starts at the top and is essential to establishing effective internal controls (Cosmin, 2011).

Testing the tone at the top is important since employees are more likely to embrace the same attitude that management displays because they realize that they will be held similarly accountable (Bresnahan, 2007). Documented punishments for employee violations of internal control compliance also are a good indicator that the organization is taking the tone at the top seriously (Tsay, 2010). Auditors may survey employees, customers, and vendors with questions about each of their perceptions on management's commitment to its standards of conduct. Auditors may also test employees' awareness and training on their standards of conduct (AICPA, 2005). Auditors assess management override by testing the tone at the top.

2. Risk Assessment

The second component of the Framework, risk assessment, addresses the various risks that organizations face from external and internal sources. Risk assessment identifies obstacles to achieving an organization's objectives. These objectives include operating, reporting, and compliance. Management considers the potential impact of external or internal changes that may deter the effectiveness of the organization's internal control system. COSO's new Framework adds the following four new principles to enhance the risk assessment component (COSO, 2013b, p. 59):

1. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

2. The organization identifies risks to the achievement of its objectives across the organization and analyzes risks as a basis for determining how the risks should be managed.

3. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

4. The organization identifies and assesses changes that could significantly impact the system of internal control.

The risk assessment component is about management processes for identifying, analyzing, and responding to risks. Common risks include external and internal sources that hinder an organization's ability to meet its operational, financial reporting, and compliance objectives. An auditor's risk assessment is predominately focused on evaluating the probability of material misstatements in the organization's financial statements, whereas leadership is concerned with a broader scope that ranges from managing the operation to law compliance risks (Whittington & Pany, 2011).

The risk assessment process centers on identifying and responding to business risks that impact financial reporting objectives (Porter, 2014). Organizations often seek external expertise in identifying and managing potential risks to the attainment of their objectives. Corporations frequently hire internal audit firms to assist in the risk assessment of their internal control system. Audit

firms can aid in forecasting the potential impact of change on their internal control system. The internal audit function supports risk management by providing assurance over organizational risk assessment processes (Pitt, 2014).

Risk assessment processes include risk identification, analysis, and response (Liebesman, 2012). The ultimate goal of risk assessment is to communicate timely and accurate risk information to decision-makers. Internal auditors provide organizations with an independent, objective view of risk (Trudell, 2014). Auditors should identify and document the risks within the process as well as controls necessary to manage those risks, such as fraud risks (Koutoupis, 2017). The risk assessment process helps organizations deter fraud. Organizations can assess fraud risks simultaneously with their risk assessment or conduct fraud assessment separately ("Managing the Business Risk," 2008).

Risk assessment may help organizations deter fraud and reduce losses if the component is properly implemented. The risk assessment process is important because material financial statement fraud may hurt an organization's efforts toward achieving strategic objectives and damage its reputation. Organizations must consider corruption and inadequate safeguarding of assets in the risk assessment process to mitigate fraud risk (Liebesman, 2012). There are three fundamental elements in preventing, deterring, and detecting fraud: (1) maintain a culture of high ethics, (2) evaluate fraud risks and implement mitigating measures, and (3) establish an adequate oversight process (AICPA, 2002).

Risk assessment can include the evaluation of the effectiveness of lean processing principles by internal auditors. Lean principles focus on continuous improvement by enhancing organizational processes, especially those related to how risk assessment is conducted and communicated. For instance, both management and internal auditors should continuously identify areas posing the most significant risk and look for ways to mitigate them. Internal auditors can help organizations keep up with best practices within the profession and annually review potentially valuable technological advancements (Allen, 2014).

Risk assessment should go beyond simply checking the box to satisfy requirements for another year (Bokhari, Simon, & Gathings, 2014). Risk assessments should produce valuable information to management. Risks having a major impact on financial reporting objectives should be pursued and prioritized (Tsay, 2010). Unfortunately, academic research indicates that the first two internal control components, control environment and risk assessment, are relatively weak across organizations (Hermanson et al., 2012). Management should continuously assess the effectiveness of the internal control system because a system may no longer be effective as the organization's internal and external environment changes. An organization's control activities need to adapt to significant environmental changes, and an internal control system must evolve to remain effective (COSO, 2013c).

3.   Control Activities

The third component of the Framework, control activities, involves the actions established through organizational policies and procedures to ensure that management's risk mitigation directives are executed (COSO, 2013b). Generally, organizations establish control activities to address specific risks associated with the risk assessment (COSO, 2013c). Control activities help prevent and detect internal control deficiencies across all organizational levels. Segregation of duties is typically factored in when selecting and developing control activities. Examples of control activities include segregating which personnel or automated systems should be authorizing, approving, verifying, reconciling, and performing business reviews. COSO's new Framework adds the following three new principles to enhance the control activities component (COSO, 2013b, p. 87):

1.   The organization selects and develops control activities that contribute to the mitigation of, or risks to, the achievement of objectives to acceptable levels.

2.   The organization selects and develops general control activities over technology to support the achievement of objectives.

3.   The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

Control activities within a good internal control system have the following characteristics: segregation of incompatible duties, independent checks on performance, and the safeguarding of assets and records (Porter, 2014). Control activities relevant to financial statement audits include performance reviews, information processing, physical controls, and segregation of duties (Whittington & Pany, 2011).

Segregation of duties is the foundation of an effective operational and internal control system (Mulcahy, 2008). It is a major part of control activities because it provides a system of checks and balances by using a two-person integrity approach. Careful allocation of duties enables employees to cross-check each other's work. The segregation of incompatible duties helps detect unintentional errors since even competent, reliable, and trustworthy employees make accidental mistakes. Independent, internal checks by other employees are necessary to ensure the reliability of financial data and to safeguard an organization's assets and records (Porter, 2014). Segregation of duties is the driving principle behind strong internal controls (Cosmin, 2011).

4.   Information and Communication

The fourth component of the Framework, information and communication, entails the information needed for an organization to execute its internal control responsibilities. Management relies on relevant, quality information to support the organization's internal control system. This information is internally disseminated as well as externally communicated. COSO's new Framework adds the following three new principles to improve the information and communication component (COSO, 2013b, p. 105):

1.   The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

29

2.   The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

3.   The organization communicates with external parties regarding matters affecting the functioning of internal control.

The information and communication component centers on proper recordkeeping and documentation so that accountability is maintained. It is essential to properly communicate the individual roles and responsibilities to employees so that they understand what they are expected to do in relation to financial reporting. Communication channels should remain open or else the accounting information system will not function correctly. The processors of information need to know how their activities affect others' work. The accounting information system is particularly important to financial statement audits. Leadership should regularly reiterate the negative implications of reporting deficiencies to employees (Whittington & Pany, 2011). Major deficiencies and material weaknesses should be communicated to leadership (Whittington & Pany, 2011).

Having adequate records is essential to the information component because it also safeguards an organization's assets and financial data. Properly documenting financial transactions and information is key to having adequate records (Porter, 2014). Information should be relevant, reliable, and timely. Direct information can be gathered through observing control procedures and re-creating them. Indirect information can be collected from either comparative industry metrics or the organization's key performance and risk indicators and operating statistics (Tsay, 2010). Management relies on the underlying reliability and adequacy of its records to confidently communicate relevant, quality information internally and externally. Accurate communications depend on reliable supporting evidence. Communications should be accurate, objective, clear, concise, constructive, complete, and timely (Pitt, 2014).

An organization's information technology capability has a major impact on the effectiveness of internal control and the efficiency of an audit (Chen, Smith, Cao, &

Xia, 2014). Strong information technology has a pervasive impact and may benefit the audit process by preventing costly audit delays due to material weaknesses in one of COSO's five internal control components. Research suggests information technology capability impacts whether each internal control component is present, functioning, and effective (Chen, Smith, Cao, & Xia, 2014).

Information and communication is a challenge for some organizations. Rendon and Rendon's (in press) research in government acquisition suggests that contracting officers may be overly-optimistic about their procurement internal control knowledge. This overconfidence may make organizations susceptible to fraud. Survey results indicated that the internal control component with the lowest score was information and communication. Furthermore, the research findings showed that contracting officers ranked this component as the most vulnerable to fraud. An organization may strengthen its internal control by ensuring that employees have a mechanism to report suspected fraud (Rendon & Rendon, in press).

5.   Monitoring Activities

The fifth component of the Framework, monitoring activities, is a part of the internal controls component of the auditability triangle as shown in Figure 1. Monitoring entails ongoing or separate evaluations to determine whether the components and principles of internal control are present and effectively functioning. Findings from the evaluations are compared against management's criteria and regulatory criteria to identify deficiencies. COSO's new Framework adds the following two new principles to enhance the monitoring activities component (COSO, 2013b, p. 87):

1.   The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

2.   The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

The monitoring activities component involves regularly assessing internal control performance. Routine activities should be regularly monitored; non-routine activities such as random internal audits, on the other hand, require separate evaluations. Internal auditing is a critical part of an organization's monitoring activities (Whittington & Pany, 2011).

An effective internal control system has all five of the COSO Framework's components operating together to provide reasonable assurance that the organization will meet its objectives. Without effective monitoring, each of the five components will lose its effectiveness and eventually stop operating properly. Organizations should also monitor internal control systems to assess the system's performance and quality over time (Ionescu, 2011).

Monitoring activities should be continuous, and constant improvements should be made to the internal control system as needed. Controls that are not delivering expected results should be reassessed and strengthened to fulfill their purpose. Additionally, a cost/benefit analysis should be conducted to ensure that the costs are not outweighing the benefits of the controls in place. Internal auditors are recommended to assist in the monitoring process because of the independent, objective, and professional opinions they provide (Cosmin, 2011). Ongoing internal control evaluations provide instant, continuous feedback to decision makers on the effectiveness of an internal control system (Tsay, 2010). Monitoring activities provide oversight on the organization's internal control system, which aids in preventing control deficiencies and deterring fraudulent activity. The risk of management's override of internal control should also be monitored (AICPA, 2005).

Monitoring internal controls has been an area that the federal government has not taken seriously. Grant Thornton, a global leading firm in independent auditing, assessed a federal agency's internal control over financial reporting and found that internal control monitoring was merely a paper exercise that federal agencies quickly conducted before the end of each fiscal year (Bresnahan, 2007). Instead, federal agencies should review their internal control testing

methods at the start of the fiscal year to identify weaknesses for management to closely monitor (Bresnahan, 2007). Once an internal control system is effective, management must monitor the system to sustain its effectiveness. The following section will discuss COSO's guidance on effective internal control.

6.   COSO on Effective Internal Control

An effective internal control system aids organizations in mitigating the risks of not accomplishing its goals. Two conditions must exist for an internal control system to be considered effective. First, each internal control component and relevant principle must be present and functioning properly. Second, all five internal control components must be operating together in an integrated fashion. If these two conditions are not met, at least one major deficiency exists in the internal control system (COSO, 2013a). An effective internal control system provides reasonable assurance that the organization:

1.   Achieves effective and efficient operations when external events are considered unlikely to have a significant impact on the achievement of objectives or where the organization can reasonably predict the nature and timing of external events and mitigate the impact to an acceptable level

2.   Understands the extent to which operations are managed effectively and efficiently when external events may have a significant impact on the achievement of objectives or where the organization can reasonably predict the nature and timing of external events and mitigate the impact to an acceptable level

3.   Prepares reports in conformity with applicable rules, regulations, and standards or with the entity's specified reporting objectives

4.   Complies with applicable laws, rules, regulations, and external standards (COSO, 2013a, p. 8).

COSO's framework does not eliminate the necessity for management's judgment. Management must exercise discretion during the design and implementation and during the assessment of the effectiveness of the organization's internal control system. Management must also be aware of local laws, regulations, and standards. Awareness of these rules is necessary to make

sound decisions about internal control (COSO, 2013a). The framework cannot prevent poor judgment or external events outside of the organization's control that derail the organization from its goals. Human bias, management override, and collusion can ruin an effective internal control system (COSO, 2013a). The following section will detail the federal government's adoption of COSO's Framework.

D.   FEDERAL GOVERNMENT STANDARD ON INTERNAL CONTROL

For the federal government, GAO requires all agencies to comply with the Green Book beginning FY 2016 (GAO, 2014). The Green Book defines the federal government's standards for internal control, and FMFIA mandates that organizations establish internal controls according to these standards. The Green Book explains why the standards are essential to an organization's internal control system (GAO, 2014). An internal control system is defined as "a continuous built-in component of operations, affected by people, that provides reasonable assurance, not absolute assurance, that an organization's objectives will be achieved" (GAO, 2014, p. 6). Internal control is not a one-time event but, rather, a series of continuous actions throughout an organization's operations, and management should use it to guide its operations to help managers achieve the organization's objectives versus being its own separate system (GAO, 2014).

The GAO adapted COSO's terminology to fit within the federal government. COSO's five components now have 17 principles that help establish an effective internal control system. These principles support the effective design, implementation, and operation of the five internal control components. The GAO also kept all five of COSO's components with the exception of not changing the name of the fifth internal control component. COSO's new Framework changed Monitoring to Monitoring Activities, yet GAO did not make that change. A brief synopsis of the Green Book's tailored 17 principles incorporated into the five components of internal controls is depicted in Figure 6:

Control Environment

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

10. Management should design control activities to achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies.

Information and Communication

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

Monitoring

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

17. Management should remediate identified internal control deficiencies on a timely basis.

Source: GAO. | GAO-14-704G

Figure 6. "Green Book's Implementation of COSO's 17 Principles within
the Five Components of Internal Control"
(from GAO, 2014, p. 9)

Except in rare instances, all five components and all 17 principles are relevant in creating an effective internal control system (GAO, 2014). The Green Book, however, does not dictate how management must precisely design, implement, and operate its organization's internal control system (GAO, 2014). The standards are not meant to interfere with legislation, rulemaking, or discretionary policy-making. Management is responsible for tailoring policies and procedures to the organization when implementing the Green Book (GAO, 2014). Therefore, individual judgment is required in order to respond to differing factors. Internal control systems are like fingerprints: no two organizations have identical ones. The uniqueness exists due to differences in factors like an organization's size, mission, strategy, regulations, risk tolerance, and information technology (GAO, 2014).

The Green Book applies to an organization's objectives of operations, reporting, and compliance. An organization's objectives are directly related to the five components of internal control and the levels of organizational structure. The five components are required to achieve organizational objectives. Organizational structure encapsulates the operational units, processes, and structures that management utilizes to accomplish its objectives. This interrelationship is shown in Figure 7.
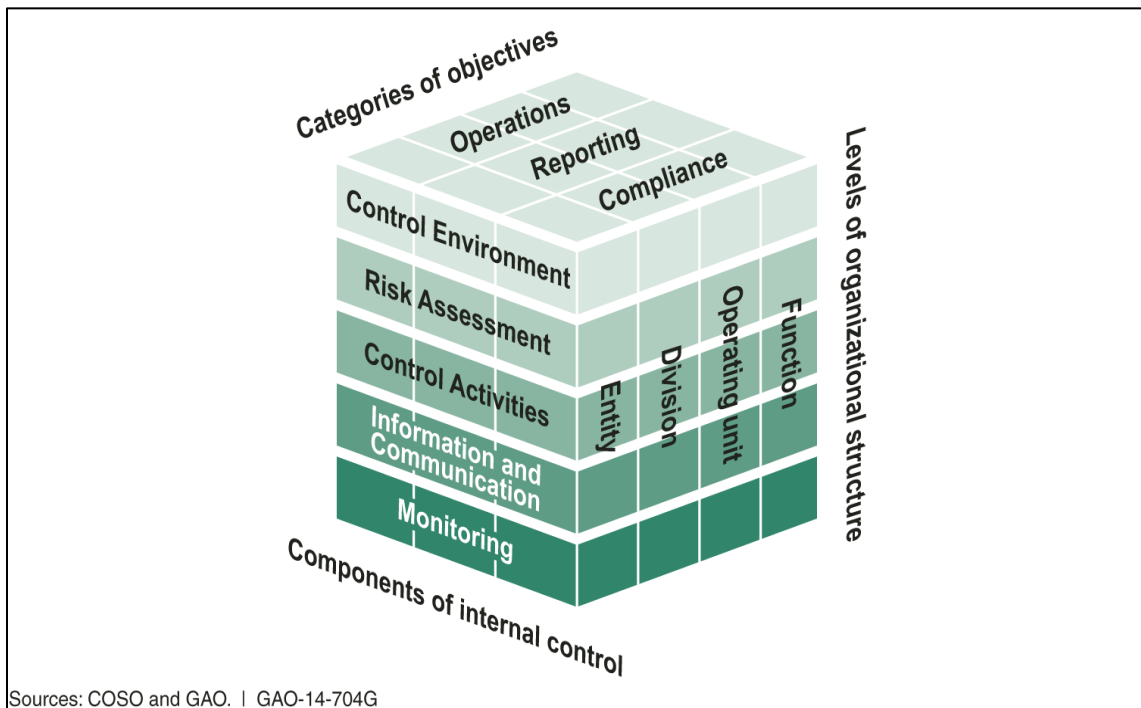
Figure 7.   "The Components, Objectives, and Organizational Structure of Internal Control" (from GAO, 2014, p. 10)

1.   Key Role Players in an Internal Control System

The three general roles of an internal control system are an oversight body, management, and personnel. External auditors and the DODIG are not a part of the federal government internal control system; therefore, responsibility falls on DOD management to assess and implement auditor recommendations.

The Green Book clarifies the responsibilities of an oversight body, management, and personnel as follows (GAO, 2014, pp. 11–12):

1. Oversight body – provides oversight and strategic direction regarding the accountability of the organization. The oversight body is responsible for reviewing management's design, implementation, and operation of each component and principle within an organization's internal control system.

2. Management – Management is directly responsible for an effective design, implementation, and operation of an organization's internal control system.

3. Personnel – Personnel assist management in the design, implementation, and operation of an internal control system and report issues impacting the organization's objectives in the areas of operations, reporting, and compliance.

a. *Overview of the Green Book's Five Internal Control Standards*

A detailed overview of each of the five standards of internal control is provided at the beginning of each related section in the Green Book. The control environment lays the structural foundation, which impacts the overall quality of internal control, how objectives are defined, and how control activities are arranged. Management must set a positive tone at the top to foster a thriving control environment (GAO, 2014).

After the control environment is addressed, management makes a risk assessment on any threatening obstacles to the organization achieving its objectives and develops adequate risk responses. Management assesses organizational risks stemming from internal and external sources (GAO, 2014). Afterwards, management considers control activities, which are specific actions management establishes to achieve objectives to mitigate internal control system risks (GAO, 2014). Quality information and effective internal and external communication are essential to achieving organizational objectives. Communication should be relevant and reliable (GAO, 2014).

Internal control is an evolving process that must be adaptable as new risks emerge. Consequently, monitoring is crucial to keeping up with changes in

organizational objectives, resources, and risks as well as shifts within the outside environment and laws. Monitoring the quality of performance is important in promptly resolving material internal control deficiencies through corrective actions, which complement control activities and, thereby, help organizations achieve objectives (GAO, 2014). The following section will discuss GAO's guidance on effective internal control.

2. Green Book Guidance on Evaluating the Effectiveness of Internal Control in the Federal Government

The Green Book offers management evaluation factors to test the effectiveness of an internal control system. An effective internal control system provides reasonable assurance that an organization will achieve its objectives by possessing all five internal control components. Each component must be effectively designed and implemented, and it must operate with the other components in an integrated fashion. An internal control system is not considered effective if either any single principle or component is not effective or all the components are not operating in harmony with each other (GAO, 2014).

Each executive branch agency head must annually evaluate their internal control systems to determine whether they comply with FMFIA requirements. The annual report must identify any material weaknesses in the agency's internal control systems and include their corrective action plans. The OMB Circular No. A-123 contains OMB's guidance for evaluating this process (OMB, 2004). Heads of agencies evaluate three overall aspects of their internal control systems: 1) design and implementation, 2) operating effectiveness, and 3) effect of deficiencies on the system (GAO, 2014).

3. Design and Implementation

Management evaluates the design and implementation of its organization's internal control system. Management evaluates a control's design individually and in conjunction with other controls to determine if they are capable of achieving organizational objectives and mitigating related risks. Design

deficiencies occur when a control is missing or not properly designed. Implementing a control is futile if it is not effectively designed. Implementation deficiencies also occur when a properly designed control is not properly implemented (GAO, 2014).

4. Operating Effectiveness

Management evaluates the implementation to determine if the control is being appropriately used in operations. While evaluating operating effectiveness, management will determine if controls were consistently applied at relevant times by the right personnel in the right way. Effective design and implementation is a precursor for a control to be effectively operating. Operational deficiencies occur when a properly designed control is not operating as designed or when performed by personnel without adequate authority or competence (GAO, 2014).

5. Impact of Deficiencies on the Internal Control System

Management will evaluate material internal control system deficiencies identified through management's continuous monitoring. Internal control deficiencies occur when the design, implementation, or operation does not allow management to accomplish control objectives and address correlated risks (GAO, 2014). Management will make a judgment and a determination on the effectiveness for each principle based upon the results after evaluating the three aspects of their internal control systems in relation to each of the five components of internal control (GAO, 2014). Weak internal controls can cause multiple deficiencies in an internal control system and result in a material deficiency.

E. SUMMARY

This chapter reviewed internal control literature from various sources and explained internal control's role in financial auditability, an internal and external auditor's role in internal control, and the internal control guidance in the federal government. In addition, the Auditability Triangle was discussed. Next, the

literature review provided a background on financial auditability in DOD and DON, which included a discussion of the DOD's FIAR program as well as DON's roadmap to financial auditability. Furthermore, obstacles to auditability were discussed. This chapter concluded with the current industry internal control framework set by COSO and GAO's incorporation of the COSO internal control components into the Green Book. The next chapter will discuss the content analysis.

III.   CONTENT ANALYSIS

A.   INTRODUCTION

This chapter analyzes the content of the COSO Framework's Illustrative Tools for Assessing Effectiveness of a System of Internal Control (Illustrative Tools), the Department of the Navy (DON) Managers' Internal Control Manual, hereafter referred to as the MICM, and the United States Government Accountability Office's (GAO) Standards of Internal Control for the Federal Government (Green Book). The purpose of this content analysis is to examine the relationship between the current state of the MICP and how the external environment outside DON has changed related to internal control guidance.

B.   COSO FRAMEWORK—ILLUSTRATIVE TOOLS FOR ASSESSING EFFECTIVENESS OF A SYSTEM OF INTERNAL CONTROL (ILLUSTRATIVE TOOLS)

COSO issued a companion document to its May 2013 updated Internal Control–Integrated Framework (Framework): Internal Control over Financial Reporting—Illustrative Tools for Assessing Effectiveness of a System of Internal Control (Illustrative Tools). The Illustrative Tools contains templates for evaluating and documenting the effectiveness of internal control (Prawitt & Tysiac, 2013). Organizations can tailor the templates found in the Illustrative Tools to self-assess their particular organizations and document the findings. The templates allow organizations to summarize their internal control self-assessments (COSO, 2013c).

Within the Illustrative Tools, COSO provides four different categories of templates for organizations to use: 1) Overall Assessment, 2) Component Evaluation, 3) Principles Evaluation, and 4) Deficiencies. The templates are interrelated; and COSO offers the following assessment process to be used to facilitate key information to management: 1) Principle Evaluation, 2) Component Evaluation, and 3) Overall Assessment. During the principle evaluation (Figure 8), organizations consider the controls to affect each principle. Internal control

deficiencies are identified, an initial severity is determined, and the information is listed on the Deficiencies template (Figure 9). Information is considered for relevance and rolled up onto the Component Evaluation template (Figure 10). At this stage, the severity of internal control deficiencies is re-evaluated to check whether controls affect other principles since other principles may compensate for the deficiency. Finally, information is rolled up to the organization's management to the overall assessment of the effectiveness of internal control (Figure 11). Management assesses whether the components are operating together in an integrated fashion by evaluating whether major internal control deficiencies exists based on the aggregated information (COSO, 2013c).

Figure 8 is an example of one of the 17 Principles Evaluation templates, which also summarizes management's determination of whether all components and relevant principles exist and are functioning properly. There is one Principle Evaluation template per principle within each of the five internal control components. Each of these templates lists multiple points of focus associated with each principle to provide further explanation. Internal control deficiencies occur when controls needed to affect relevant principles are missing. Management's judgment is necessary in determining if an internal control deficiency exists (COSO, 2013c). These templates can be used at the organizational and sub-organizational level.

3. Principle Evaluation			
Principle Evaluation – Control Environment			
Principle 1: Demonstrates Commitment to Integrity and Ethical Values –The organization demonstrates a commitment to integrity and ethical values.			
Points of Focus			
• Sets the Tone at the Top – The board of directors and management at all levels of the entity demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.			
• Establishes Standards of Conduct – The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the organization and by outsourced service providers and business partners.			
• Evaluates Adherence to Standards of Conduct – Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.			
• Addresses Deviations in a Timely Manner – Deviations of the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.			
• (Other entity specific points of focus, if any)			
Summary of Controls to Effect Principle 1			
Deficiencies Applicable to Principle 1			

Identification No.	Internal control deficiency description	**Evaluate internal control deficiency severity:** (Consider whether controls to effect other principles within and across components compensate for the internal control deficiency.)		List internal control deficiencies related to another principle that may impact this internal control deficiency
		Preliminary Severity – Is internal control deficiency a major deficiency? (Y/N)	Comments/ Compensating Controls	
Evaluate deficiencies within the principle:* Evaluate if any internal control deficiencies or combination of internal control deficiencies, when considered within the principle, represent a major deficiency.** <Update Summary of Deficiencies Template as required>		<Explanation>		
Evaluate the principle using judgment.**		Y/N	Explanation/Conclusion	
Is the principle present?				
Is the principle functioning?				
* Note: Record deficiencies in Summary of Deficiencies Template.				
** If it is determined that there is a major deficiency, management must conclude that the principle is not present and functioning and the system of internal control is not effective.				

Figure 8.   Principles Evaluation Template (from COSO, 2013c, tab Principle)

As shown in Figure 9, the Deficiencies template allows management to log every identified internal control deficiency onto one document and to monitor progress in resolving deficiencies. The Deficiencies template enables management to aggregate all of the identified internal control deficiencies when evaluating the components and principles (COSO, 2013c, tab Introduction).

As shown in Figure 10, COSO offers five Component Evaluation templates, one for each internal control component. This allows management to summarize their determination of whether all components and relevant principles exist and are functioning properly. Identified deficiencies are listed by associated principles and the deficiency's severity is assessed. Management's judgment is necessary in the assessment of the potential impact of each deficiency on the internal control components (COSO, 2013c).

Each of the five Component Evaluation templates collect information from the Principle Evaluation templates that are associated with each component. Likewise, the information from each of the five Component Evaluation templates is rolled up onto the Overall Assessment template in Figure 11.

4. Summary of Deficiencies									
Summary of Deficiencies									
ID #	Source of the internal control deficiency		Internal Control Deficiency Description	Severity Considerations	Is internal control deficiency a major deficiency? (Y/N)	Owner	Remediation Plan and Date	Impact on Present/ Functioning	List any internal control deficiencies in other principles that may have contributed to this internal control deficiency
	Component	Principle							

This template is an example of a summary of deficiencies. Management may tailor this template to include additional columns to capture other relevant information, as needed.

Figure 9.   Deficiencies Template (from COSO, 2013c, tab Deficiencies)

2. Component Evaluation			
Component Evaluation – Control Environment			
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
1. **Demonstrate Commitment to Integrity and Ethical Values**—The oversight body and management should demonstrate a commitment to integrity and ethical values.			
Identification No.	Internal control deficiency description	**Evaluate internal control deficiency severity**: (Consider whether controls to effect other principles within and across components compensate for the internal control deficiency.)	List internal control deficiencies related to another principle that may impact this internal control deficiency
		Is internal control deficiency a major deficiency? (Y/N) / Comments/Compensating Controls	
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion

Figure 10.   Component Evaluation Template (from COSO, 2013c, tab Components)

1. Overall Assessment of a System of Internal Control			
Overall Assessment of a System of Internal Control			
Entity or part of organization structure subject to the assessment (entity, division, operating unit, function)			
Objective(s) being considered for the scope of internal control being assessed	Considerations regarding management's acceptable level of risk		
Operations			
Reporting			
Compliance			
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
Control Environment			
Risk Assessment			
Control Activities			
Information and Communication			
Monitoring Activities			
Are all components operating together in an integrated manner? Evaluate if a combination of internal control deficiencies, when aggregated across components, represent a major deficiency* <Update Summary of Deficiencies Template as needed>			
Is the overall system of internal control effective? <Y/N>*			
Basis for conclusion			
* If it is determined that there is a major deficiency, management must conclude that the system of internal control is not effective.			

Figure 11.   Overall Internal Control System Assessment Template (from COSO, 2013c, tab Introduction)

C. RELATIONSHIP BETWEEN THE MICM, GREEN BOOK, AND COSO ILLUSTRATIVE TOOLS

COSO's Illustrative Tools and Green Book contain the current internal control framework used by industry and the federal government that is not contained in the MICM. Each publication is written for different audiences. The Illustrative Tools is designed to assist private sector, public sector, and non-profit organizations in making their internal control system more effective. The Green Book uses COSO's internal control framework to set the federal government standard on internal control. The MICM applies the Green Book's internal control framework to DON to help commands maintain an effective internal control system. Since the MICM was written in 2008, it applies the previous internal control framework. The MICM may be modified since the internal control framework external to DON has evolved or be supplemented with templates that account for these changes.

A summary table in Table 2 compares the MICM, Green Book, and COSO Illustrative Tools internal control structures. Each internal control structure has five components. The MICM does not have 17 Principles or the associated Points of Focus. The documentation requirements are different between the three publications. The MICM has four documentation requirements, which meets the six minimum requirements within the Green Book, except for accounting for the missing 17 principles. The COSO does not have minimum documentation requirements since every industry and organization is different, but rather offers Illustrative Tools for organizations to tailor the COSO's sample templates to their organizations.

48

Item:	MICM	Green Book	COSO
Five Components	Yes	Yes	Yes
17 Principles	No	Yes, tailored to federal government	Yes
Characteristics of Principles	No	Yes, "Attributes"	Yes, "Points of Focus"
Documentation Required	Yes, 4	Yes, 6	Yes, but no minimum

Table 2.   Key Differences Between the MICM, Green Book, and
COSO Illustrative Tools Internal Control Structures

The MICM, Green Book, and COSO's Illustrative Tools do not prescribe a specific format for organizations to conduct internal control self-assessments, but rather offer a sample format that can be tailored to each organization. By not prescribing a stringent format, management has flexibility in judging how to properly document internal controls. The MICM and COSO Illustrative Tools provide internal control assessment examples, whereas the Green Book only lists GAO's minimum required internal control documentation required for federal agencies, as listed in Figure 12.

1. "If management determines that a principle is not relevant, management supports that determination with documentation that includes the rationale of how, in the absence of that principle, the associated component could be designed, implemented, and operated effectively.

2. Management develops and maintains documentation of its internal control system.

3. Management documents in policies the internal control responsibilities of the organization.

4. Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues.

5. Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis.

6. Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis" (GAO, 2014, p. 20).

Figure 12.   Green Book's Six Minimum Documentation Requirements

The MICM needs to add the 17 principles to meet all of the Green Book documentation requirements. The remaining Green Book documentation requirements are already being met by the MICP since the MICM addresses them within the MICM documentation requirements.

The MICM has four documentation requirements for commands: 1) Risk Assessment, 2) Internal Control Assessment, 3) Corrective Actions for material weaknesses and reportable conditions, and 4) MIC Plan. The first three MICM documentation requirements address risk assessment, internal control assessment, and corrective action plans, and are closely aligned with the Green Book and the COSO Illustrative Tools. The fourth requirement, the MIC Plan, is not in compliance with the Green Book or aligned with the Illustrative Tools since it only addresses the five internal control components and not the 17 new principles.

1. MICM Documentation Requirement #1: Risk Assessment

The first documentation requirement of the MICM, Risk Assessment, assesses risk through three types (Inherent, Control, or Combined) as well as three levels (Low (L), Moderate (M), or High (M)), as shown on the matrix in Figure 13. This matrix clarifies the criteria that commands use to assess the risk type and level.

Risk	Low	Moderate	High
Inherent	Hazard or misstatement does not have severe consequences and is unlikely to occur.	Hazard or misstatement has severe consequences or is likely to occur.	Hazard or misstatement has severe consequences and is likely to occur.
Control	Controls will prevent or detect any hazard or aggregate misstatements that could occur in the assertion in excess of design materiality.	Controls will more likely than not prevent or detect any hazard or aggregate misstatements that could occur in the assertion in excess of design materiality.	Controls will unlikely prevent or detect any hazard or aggregate misstatements that could occur in the assertion in excess of design materiality.
Combined	Any hazard or aggregate misstatements in the assertion do not exceed design materiality.	More likely than not, any hazard or aggregate misstatements in the assertion do not exceed design materiality.	More unlikely than likely, any hazard or aggregate misstatements in the assertion do not exceed design materiality.

Figure 13.   Risk Type and Level (after SECNAV, 2008)

After the risk type and level have been determined, commands list the internal control in place to mitigate the risk onto a risk assessment table, shown in Figure 14. The Green Book and Illustrative Tools do not offer risk assessment tables. The Illustrative Tools offers a template for each of the four principles associated with the risk assessment internal control component, and the Green Book tailors each principle to the federal government. The four principles emphasize defining objectives, and identifying, analyzing, and responding to risk relating to the objectives, fraud, and the internal control system.

Risk Assessment					
Command:	ASN(FM&C) FMO				
Preparer:	John Doe				
Process:	Time and Attendance				
(1) **Control Number**	**(2)** **Risk / Hazard**	**(3)** **Inherent Risk**	**(4)** **Control Risk**	**(5)** **Combined Risk**	**(6)** **Internal Control Currently in Place**
1	Employee inaccurately records hours worked	Moderate	Low	Moderate	Supervisor reviews employee's timesheet and approves hours worked
2	Timekeeper could inaccurately input data into the T&A system	Low	Low	Low	Employee reviews time account with timekeeper and signs/dates to verify that the information is accurate

Figure 14.   Risk Assessment Table (after SECNAV, 2008)

In its adoption of the COSO Framework, the GAO modified COSO's terminology throughout the Green Book. A key example that affects the recommended templates is the term "Attributes" instead of the COSO Framework's "Points of Focus," which are important characteristics describing the principles in more detail. These Attributes are provided to aid management in designing, implementing, and operating internal controls to align with the principles (GAO, 2014). The Attributes for each principle are shown on the recommended templates in Appendix B.

2.   MICM Documentation Requirement #2: Control Assessment

The second documentation requirement of the MICM, Control Assessment, assesses internal controls through having commands test each control carried over from the risk assessment table, as shown in the control assessment table in Figure 15 (SECNAV, 2008). Based on this testing, a determination on the effectiveness of each internal control is made and a new control risk level is assigned.

Control Assessment							
Command: ASN(FM&C) FMO							
Preparer: Jane Doe							
Process: Time and Attendance							
Control Number	Internal Control Currently in Place	Control Test Objective	Description of Design Test	Control Design Effective?	Description of Test	Control Operation Effective?	New Control Risk Level
1	Supervisor reviews employee's timesheet and approves hours worked	To ensure supervisors are accurately reviewing timesheets	Review existence of approved timesheets	Yes	Compare employee's time with approved timesheet	Yes	Low
2	Employee reviews time account with timekeeper and validates information is correct	To ensure employee review effectively reduces inaccuracies on recorded timesheets	Review existence of verification forms	Yes	Compare approved timesheets with timesheets recorded in the T&A system	Yes	Low

Figure 15.   Control Assessment Table (after SECNAV, 2008)

This control assessment example from the MICM in Figure 15 does not specify which one of the five internal control standards or 17 principles are being addressed. The Green Book and COSO Illustrative Tools do not provide control assessment tables.

3.   MICM Documentation Requirement #3: Corrective Action Plans

The third documentation requirement of the MICM, Corrective Action Plans, is a part of the fifth internal control component, Monitoring, and involves classifying internal control deficiencies into three categories: material weakness (MW), reportable condition (RC), and item to be revisited (IR). The MICM defines each term as follows:

> A material weakness is a reportable condition or combination of reportable conditions, which is significant enough to report to the next higher level. The determination is a management judgment as to whether a weakness is material.

> A reportable condition is a control deficiency, or combination of control deficiencies, that adversely affects the ability to meet mission objectives but are not deemed by the Head of the Component as serious enough to report as material weaknesses.

> An item to be revisited is an internal control brought to management's attention with insufficient information to determine whether the control deficiency is material or not. These issues will be revisited throughout the following fiscal year to determine the materiality of the control deficiency. (SECNAV, 2008, p. 16)

All Chief of Naval Operations (CNO) echelon 2 commands upwardly report internal control deficiencies using these three categories on MIC Certification Statements. Recent examples include the U.S. Navy Bureau of Medicine and Surgery's (BUMED) MW in attenuating hazardous noise in acquisition and weapon system design, the U.S. Navy Bureau of Naval Personnel's (BUPER) RC in post-deployment health reassessments, and Naval Reserve Force's (NAVRESFOR) IR in selected reservist sexual assault victim support (CNO, 2014). The MICM's Corrective Action Plan process addresses the fifth internal control component, monitoring.

4. MICM Documentation Requirement #4: MIC Plan

The fourth documentation requirement of the MICM, MIC Plan, is shown in Appendix A and addresses all five internal control components but is missing the 17 principles. The MIC Plan is less than three pages and vague in comparison to the updated internal control framework in the Green Book and the COSO Illustrative Tools.

D. SUMMARY

This chapter compared the content of the COSO Illustrative Tools, MICM, and Green Book. The next chapter will discuss findings based on the literature view and content analysis.

IV. FINDINGS

A. INTRODUCTION

This chapter will discuss the findings of the literature review and content analysis to answer the research question. Gaps between the internal control frameworks are analyzed to identify internal control gaps in the DON Managers' Internal Control Program manual.

B. FINDINGS BASED ON THE ANALYSIS

This section addresses the following research question:

- How would updating the MICP's capabilities to current internal control guidance help commands achieve audit readiness?

The Department of the Navy (DON) has outdated instructions governing the internal control process. The external environment has changed because the Green Book has now adopted COSO's updated internal control framework. The MICM is deficient in that its four documentation requirements fail to address the 17 principles, which is necessary to fully align with the Green Book's application requirements. Expanding the MICP's internal control capability to embrace the 17 principles may better assist commands in preparing for external financial audits in key areas, such as continuously monitoring, improving, and resolving business processes, controls, and documentation issues. The MICP may benefit by adopting a current internal control framework from the private sector into its program, manual, and guidance.

The COSO Internal Control—Integrated Framework has additional illustrative tools, approaches, and examples that are not found in the Green Book and may be useful for the MICP. Specifically, the MICP may benefit by supplementing its MICM with templates derived from COSO's Illustrative Tools. COSO recommends that organizations adjust these templates to meet their particular organization's needs. The MICP may meet the GAO's FY16 compliance requirement by supplementing its MICM with templates from COSO's

Illustrative Tools that are adapted and tailored in this research study to match GAO's application requirements of the 17 principles.

This author developed the templates in Appendix B for federal government use. The templates are derived from COSO's Illustrative Tools and were modified to align with the terminology within the Green Book and documentation requirements within the MICM. The rationale and counter-arguments for updating the MICM are explained below.

1.   Updating MIC Manual

Updating the MICM with the recommended templates may provide the DON MICP with short-term and long-term benefits. Short-term benefits may include compliance with the Green Book and improved communication with external auditors. Long-term benefits may include more effective internal controls and increased audit readiness.

In the short-term, compliance with the Green Book is an important reason since the Green Book requires all federal agencies to address the 17 principles in addition to the five internal control standards beginning FY 2016. Therefore, the MICP may want to either revise or supplement its MICM to meet this upcoming requirement. A failure to account for the 17 principles would cause a major deficiency in DON's internal control system since the MICM would not even meet the federal requirements listed in the Green Book.

However, failure to implement the 17 principles may cause many other major deficiencies. Such a gap may cause many internal control problems. External auditors will assess DON internal control systems during financial audits, and not meeting any one requirement listed in the Green Book would disqualify DON from receiving a clean audit opinion due to a major deficiency in the DON internal control system.

Besides helping the MICM comply with the Green Book, the recommended templates may assist commands in communicating with external

auditors. The templates are designed to help commands present their internal controls in a way that external auditors understand since the format is similar to and based off of the COSO Framework used in the private sector. Using internal control self-assessment forms that have recognizable terminology congruent with the MICM, Green Book, and COSO Framework may help all stakeholders.

The templates may assist commands in documenting their internal controls in a manner that external auditors can quickly trace internal control deficiencies to the 17 new principles. The templates also allow commands to retain current MICM processes by continuing to use the MICM's four documentation requirements: 1) Risk Assessment Tables, 2) Internal Control Assessment, 3) Corrective Action Plans, and 4) MIC Plan.

The MICM's risk assessment table can accomplish the four principles associated with the risk assessment component without making any modifications. The MICM, however, may benefit from having a template that lists each principle to ensure that each is addressed and not overlooked. Furthermore, having a template that also lists each Attribute associated with each principle may help ensure that thorough self-assessments of internal controls are in place.

The MICM's internal control assessment example does not specify which one of the five internal control standards or 17 principles are being addressed. This ambiguity may make it difficult for external auditors to understand how documented deficiencies relate to the Green Book's requirements and the COSO Framework. The MICM's control assessment table may either be modified to map each item to the corresponding internal control component or principle, or the information currently documented can instead be placed onto the recommended templates in Appendix B. This mapping process is described in Chapter V, Development of Templates.

The information currently documented within Corrective Action Plans may already comply with the two principles associated with the monitoring

component, but commands would need to document how their monitoring activities in fact fulfill the two monitoring principles. To accomplish this, the MICM's Corrective Action Plans may either be modified to map current monitoring activities to each internal control principle or the information from commands' current Corrective Action Plan documentation can be placed onto the recommended templates in Appendix B.

Modifying the MICM documentation requirements, specifically the MIC Plan, to align with the evolution of internal control frameworks external to DON may make command internal control systems more effective by improving the monitoring of internal control deficiencies. Furthermore, commands may benefit from the Green Book's Attributes associated with each principle being added to the MIC Plan because it may help DON internal control systems become more effective. The recommended templates in Appendix B incorporate the Green Book's Principles and Attributes using the Illustrative Tools and may be used to address each internal control in more detail and cover new areas previously overlooked.

Beyond the short-term potential benefits, DON may benefit in the long-term from adding the 17 principles, which are intended to help make an organization's internal control systems more effective. Similar to how the private sector benefits from the COSO Framework, DON may likewise use it to conduct risk assessments in various areas, such as cybersecurity, supply-chain, vendor, and change management. The MICP may be more effective in mitigating risks, deterring fraud, and meeting long-term objectives.

In addition, commands may be empowered to make stronger self-assessments when preparing for external audits by having a more detailed MICM that uses a cutting-edge internal control framework found within industry. Distributing an updated MICM to commands may bring a fresh look at internal control. The recommended templates may be a valuable tool to help management in identifying and correcting material internal control weaknesses before officially undergoing an external audit.

From a broader perspective, DOD has been unable to obtain a clean audit opinion for decades, and internal control deficiencies are one contributing factor. Expanding the MICP's capabilities to current internal control guidance may help commands achieve audit readiness. Audit readiness is dependent upon effective internal control systems operating without any material weaknesses. The templates may ultimately help DON establish and sustain effective internal control systems and maintain audit readiness at all times as DOD pursues its first clean audit on its financial statements.

2. Counter-Arguments to Supplementing MICM with the Recommended Templates

There are counter-arguments to supplementing the MICM with the recommended templates despite many reasons and evidence supporting the rationale for updating the MICM. Exploring whether the benefits are worth the costs is important before committing to revising or supplementing the MICM. Having effective internal control systems is only one function of preparing for external financial audits, and other competing priorities may be a better investment.

Existing and new policies are not always practiced by employees. Unfortunately, even if new policies are practiced by employees, some may resort to implementing policies using a checklist approach that treats the recommended templates as another "check in the box." Even worse, DON might not obtain a clean audit opinion on their financial statements even if updating the MICM helped commands prepare for external financial audits due to other obstacles.

Even if supplementing the MICM with the recommended templates is the best way to comply with the Green Book and make the DON internal control systems most effective, FMO may have more important priorities to which to allocate their resources. Other competing priorities may be more important or urgent than investing more time, money, manpower, and other resources in updating a manual, creating new training guidance, and implementing a new

process across DON before Congress's FY 2017 deadline to achieve financial auditability.

Despite the possible benefits of expanding the DON MICP's capabilities, supplementing the MICM with templates may be cumbersome to commands and FMO. Commands may view the templates as additional paperwork to fill out, and this requires training and more man hours. Not to mention, FMO may not feasibly be able to expand the DON MICP's capabilities through adding supplemental templates to the MICM before the beginning of FY 2016, the GAO's required deadline to account for the 17 principles.

Furthermore, DON may have other competing priorities for commands to focus on, which are presenting more challenging and urgent obstacles to financial auditability. For instance, enterprise resource planning (ERP) information technology financial data compliance and synchronization challenges may be a larger concern to DON. DON may decide to focus efforts elsewhere, even though a single major internal control deficiency can prevent an external auditor from issuing a clean audit opinion on DON's financial statements. However, despite the counter-arguments, the potential benefits of the supplemental templates may be worth the effort.

C. SUMMARY

This chapter answered the research question, and discussed the rationale for supplementing the MICM with templates to help expand MICP's capabilities to provide current internal control guidance and to help commands achieve audit readiness. However, despite these counter-arguments, this research indicates that the short-term and long-term benefits may be worth DON's efforts to supplement the MICM with the recommended templates since it may help in expanding the MICP's capabilities to prepare commands for financial audits. The next chapter will discuss the development of templates and offer recommendations on bridging the gap between the MICM, the Green Book, and the COSO Illustrative Tools.

V. DEVELOPMENT OF TEMPLATES AND RECOMMENDATIONS BASED ON ANALYSIS

A. INTRODUCTION

Based on the findings from the literature review and content analysis, templates are developed in this chapter to help the Department of Navy (DON) Managers' Internal Control Program (MICP) expand its internal control capability and add the missing 17 principles to its MICP Manual, hereafter referred to as the MICM. The recommended templates presented in this chapter are designed to supplement the MICM and may help bridge the gap by aligning the MICM with the Standards of Internal Control for the Federal Government (Green Book) using The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Illustrative Tools. Recommendations are made based on the analysis. DON may consider supplementing the MICM with the recommended templates to help commands achieve audit readiness.

Organizations, such as Office of Financial Operations (FMO), individual commands and their subordinate commands can use the templates in a self-assessment process by consolidating information from the principle evaluation and component evaluation into the overall assessment template. Instead of allocating significant resources to overhaul current MICM guidance, the recommended templates are intended to supplement the MICM's current processes, but not eliminate them. Current MICM procedures may be used to minimize the time and cost of implementing a new process.

The summarized results of all four MICM documentation requirements can be placed onto the recommended templates using the Green Book's application requirements and current MICM's terminology, but based on COSO's Illustrative Tools. Tailoring COSO's language to DON application requirements and terminology may make the templates more relevant to users. For instance, FMO may consolidate templates from individual commands, which may also consolidate templates from their subordinate commands.

Terminology from the MICM has been applied to the recommended templates since MIC coordinators are familiar with the MICM's documentation requirements. The main difference between the MICM's requirements and filling out the recommended templates is that there is an added step to the process to comply with the Green Book: mapping the deficiency to the corresponding component and principle. This extra step may help commands generate "outside the box" solutions to internal control systems since it requires critical thought about what other principles may be affected by single internal control deficiencies.

The mapping process may be a paradigm shift for MIC Coordinators and help them consider how other principles can compensate for the deficiency instead of merely listing an identified deficiency. Presently, MIC Coordinators merely identify deficiencies in the context of the five components without consideration of the Green Book's 17 Principles and associated Attributes. Perhaps, a more thorough review may result in solutions and risk mitigation strategies for material internal control deficiencies and closer tracking by management. After the mapping process, all of the information is summarized on the recommended templates, assigned a tracking identification number, and may be referenced by DON senior leaders or external auditors.

Mapping the deficiencies to principles after the outside agencies discover weaknesses may be useful for monitoring corrective action plans. More value may be realized by commands when MIC Coordinators can use the template during self-assessments to identify internal control weaknesses before outside agencies like DODIG or external auditors discover them. Regardless of when internal control deficiencies are discovered, having all the information captured into one template may be beneficial for every stakeholder.

The recommended templates may encourage management to be proactive in evaluating internal control activities. The recommended templates may help DON senior leaders and external auditors better map internal control deficiencies to the 17 principles and five internal control components, which may

make the MICP more effective, meet the Green Book's application requirements, and make DON more ready for external financial audits. A sample scenario of how commands may apply each recommended template is provided with each of the four recommended templates along with a recommended tracking number system is provided in the following section.

B.   DEVELOPMENT OF TEMPLATES

There are four recommended internal control self-assessment templates to supplement the MICM and expand the DON MICP's internal control capabilities. The recommend templates are presented in order of COSO's recommended assessment process: 1) Principle Evaluation, 2) Deficiency Summary, 3) Component Evaluation, and 4) Overall Internal Control System Assessment. All the recommended templates utilize a tracking number system and are designed to help commanders communicate internal control deficiencies to external auditors.

The assessment process begins by evaluating each principle at the lowest level that tracks individual internal control deficiencies, such as at the command or subordinate levels. This information would be reported upward onto principle, deficiency summary, and component evaluation templates. Management's judgment at the Major Assessable Units (MAU) and Senior Assessment Team levels is needed to assess the information before reporting it upward onto the overall assessment template for FMO to make the overall assessment, which external auditors would examine during an external financial audit.

1.   Recommended Template #1 of 4: Principle Evaluation

The Principle Evaluation template, in Figure 16 (divided into upper and lower halves), incorporates the Green Book's application requirements. This recommended template can be used at the command level or at their subordinate command.

Principle 11: Design Activities for the Information System

—Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

Attributes

- Design of the Entity's Information System—Management designs the entity's information system to respond to the entity's objectives and risks.
- Design of Appropriate Types of Control Activities—Management designs appropriate types of control activities in the entity's information system for coverage of information processing objectives for operational processes. For information systems, there are two main types of control activities: general and application control activities.
- Design of Information Technology Infrastructure—Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Information technology requires an infrastructure in which to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be shared by different units within the entity or outsourced either to service organizations or to location-independent technology services. Management evaluates the objectives of the entity and related risks in designing control activities for the information technology infrastructure.
- Design of Security Management—Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.
- Design of Information Technology Acquisition, Development, and Maintenance—Management designs control activities over the acquisition, development, and maintenance of information technology. Management may use a systems development life cycle (SDLC) framework in designing control activities. An SDLC provides a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the acquisition, development, and maintenance of technology. Through an SDLC, management designs control activities over changes to technology. This may involve requiring authorization of change requests; reviewing the changes, approvals, and testing results; and designing protocols to determine whether changes are made properly. Depending on the size and complexity of the entity, development of information technology and changes to the information technology may be included in one SDLC or two separate methodologies. Management evaluates the objectives and risks of the new technology in designing control activities over its SDLC.

Figure 16.   Principle Evaluation Template

Summary of Controls to Effect Principle 11

Deficiencies Applicable to Principle 11				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensa ting Controls	
C3.P11.A3.N.0.5-0001	ERP general ledger system did not produce accurate or reliable financial information	Y	N: P7-A1, A3; P13-A2	P7-A3: Risk mitigation response-Acceptance; P13-A2: Implement SFIS requirements for the Navy ERP System

Evaluate deficiencies within Principle 11:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 11, represents a major deficiency** <Update Deficiency Summary Template >	ID # C3.P11.A1.N.0.5-0001 represents a major deficiency.	
Evaluate Principle 11 using judgment.**	Y/N	Explanation/Conclusion
Is Principle 11 present?	Y	ERP has a general ledger system in place
Is Principle 11 functioning?	N	DODIG found that this system did not produce accurate or reliable financial information

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Figure 16.   Principle Evaluation Template (Lower Half)

As an illustration of how the templates are used, and how they interrelate, consider the case of the DOD IG report on ERP systems (DODIG, 2012). Principle 11, for example, relates to information technology systems and the third attribute specifically addresses the design of IT infrastructures. Based on the IG's findings, there is a significant weakness in the general ledger in NAVSEA's ERP. This would be documented on the Principle Evaluation Template as shown in Figure 16.

DODIG's finding can be placed into the description block in Figure 16, followed by a "Y" for Yes in the severity block. In the compensating and related principles blocks, NAVSEA could account for the first and third attributes in Principle 7, which covers the identification of risks and response to risks, by placing a "N" for No, "P7" for Principle 7 and "A1, A3" for first and third attributes associated with Principle 7. The third attribute involves four risk mitigation responses: acceptance, avoidance, reduction, and sharing of risks. NAVSEA could explain which risk response to the general ledger system was selected when entering the contract to procure the ERP system. In this scenario, perhaps this recommended template may have been more beneficial as a monitoring tool before the ERP contract was awarded.

Besides the potential benefit as a monitoring tool, the templates may help DON better document internal control deficiencies. Commands, such as NAVSEA, can document previously known internal control deficiencies onto centralized templates for DON senior leaders and external auditors to view in an organized fashion that is aligned with federal internal control standards. In using this approach, external auditors may be able to better understand the information on the recommended templates since they may have previously audited private sector organizations that used the COSO's Illustrative Tools. The information from this recommended template can be captured on the Deficiency Summary template and also be rolled up into the Component Evaluation template. This process is explained in the following two sections.

2. Recommended Template #2 of 4: Deficiency Summary

The Deficiency Summary template, in Figure 17, may help MIC coordinators document internal control deficiencies in a manner more congruent with the Green Book's application requirements and external auditors' expectations. The template incorporates information currently collected with commands to meet the Green Book's application requirements and adds a step to the process as individual deficiencies are mapped to their associated internal control component and principle. This mapping may help management in monitoring internal control deficiencies and external auditors in understanding DON internal control systems.

Commands may report the information onto the Deficiency Summary template using the MICM terminology that they already use. For example, commands already assess the risk type and level using risk assessment tables in the MICM, report on the type of deficiency, and document corrective action plans.

The results from the MICM's risk assessment table can be summarized onto this recommended template. For instance, the risk type would be labeled as Inherent, Control, or Combined, while the risk level would be categorized as Low (L), Moderate (M), or High (M). Likewise, the next cell, Material Deficiency, is meant to provide a summary answer, either "Y" or "N" for yes or no, on whether the internal control deficiency is material. Also, inputting a "MW, RC, or IR" for either material weakness (MW), reportable condition (RC), or item to be revisited (IR) may be a preferred approach to summarize the findings into the cell.

Deficiency Summary

Summary of Deficiencies

ID #	Source of each internal control deficiency		Internal Control Deficiency Description	Risk Type and Level (Inherent, Control, or Combined; Low (L), Moderate (M), or High (H)	Deficiency type: Material Weakness (MW), Reportable Condition (RC) or Item-to-be-Revisited (IR); Is it a major deficiency? (Y/N)	Point of Contact	Corrective Action Plan & Date	Impact on Present/ Functioning	List other applicable internal control deficiencies from other principles that may have impacted this internal control deficiency
	Component	Principle							
C3.P11.A3.N.0.5-0001	C3- Control Activities	P11-A3	ERP general ledger system did not produce accurate or reliable financial information	Combined; H	MW; Y	MIC Coordinator POC info	See Corrective Action Plan; 9/30/15	Y/N	P7-A3: Risk mitigation response-Acceptance; P13-A2: Implement SFIS requirements for the Navy ERP System

This is an example Deficiency Summary template. Management may tailor to include additional columns to document other relevant information.

Figure 17.   Deficiency Summary (after COSO Illustrative Tools, 2013)

The existing process of classifying major internal control deficiencies as Material Weakness (MW), Reportable Condition (RC), or Item-to-be-Revisited (IR) on corrective action plans may remain the same when using the recommended templates. Information from Certification Statements can be transferred over onto the templates. This recommended template allows all this information from the four MICM documentation requirements to be captured on one template. MIC Coordinators can list the description of each section internal control deficiency on the template along with the risk type and level, type of deficiency, and point of contact sections.

An example of how a command, such as NAVSEA, can use the Deficiency Summary template, in Figure 17, is explained by mapping the previously internal control deficiency example from the Principle Evaluation template in Figure 16 to other principles during the roll up process. The DODIG recommended that the Navy ERP program implement Standard Financial Information Structure (SFIS) requirements (DODIG, 2012). This corrective action is associated with the second attribute of Principle 13, which addresses using relevant data from reliable sources based on identified information requirements (GAO, 2014).

The Deficiency Summary template shows how these internal control deficiencies are mapped to multiple principles so that management can monitor them until corrective action is taken. In the NAVSEA example, as shown in Figure 17, "C3-Control Activities," would be placed into the Component cell and "P17; A3" would be placed into the Principle cell. The deficiency would be described in the next cell.

Beyond the administrative nature of the first four cells within the Deficiency Summary template, the next four cells may help FMO and commands transition consolidating the current MICM reporting requirements into the recommended supplemental templates. The fifth cell in Figure 17, Risk Type and Level, allows commands to use the MICM's risk assessment methodology that they are familiar with, as shown in Figure 14.

The next cell, Point of Contact, shows FMO which commands are responsible. Using the previous example ID # above to input the data into Figure 17, "5" would be placed into the cell to represent the NAVSEA POC responsible for monitoring and correcting the deficiency that could be listed on local command templates.

The Corrective Action cell may also provide FMO and external auditors with a summary view of each deficiency action item found on supporting documentation. This cell can capture a brief description of each action located on the enclosures to the MIC Certification Statements that commands currently use to fulfill the MICM requirements. The MICM currently requires corrective action plans for all material weaknesses and reportable conditions (SECNAV, 2008).

The final two cells require management to judge the impact of the deficiency on the current principle(s) and whether the control is present and functioning properly. Management may add other cells to list other relevant information. The cells, in Figure 17, list the minimum recommended information requirements for the Summary of Deficiencies template. The information from this template can be rolled up onto the recommended template, Principle Evaluation, in the following section.

3.   Recommended Template #3 of 4: Component Evaluation

Information from the 17 Principle Evaluation templates are rolled up to their five corresponding components on the Component Evaluation template, in Figure 18 (divided into upper and lower halves). The Component Evaluation template gives management a broader view of the internal control program.

Component Evaluation — Control Activities				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
10.	**Design Control Activities—Management should design control activities to achieve objectives and respond to risks.**			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
11.	**Design Activities for the Information System—Management should design the entity's information system and related control activities to achieve objectives and respond to risks.**			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
C3.P11.A3.N.0.5-0001	ERP general ledger system did not produce accurate or reliable financial information	Y	N: P7-A1, A3; P13-A2	P7-A3: Risk mitigation response- Acceptance P13-A2: Implement SFIS requirements for the Navy ERP System

Figure 18.   Sample Recommended Component Evaluation Template

Component Evaluation — Control Activities		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
12.	**Implement Control Activities –** Management should implement control activities through policies.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

	Explanation/Conclusion	
Evaluate deficiencies across the Control Activities component:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across the Control Activities component, represents a major deficiency**	ID # C3.P11.A3.N.0.5-0001 represents a major deficiency	
Evaluate the Control Activities component using judgment based on the principles and listed deficiencies**	Yes/No	
Is the Control Activities component present?	Y	ERP has a general ledger system in place
Is the Control Activities component functioning?	N	DODIG found that this system did not produce accurate or reliable financial information

* Note: Record deficiencies in Deficiency Summary Template.
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Figure 18.　　Sample Recommended Component Evaluation Template (Lower Half)

This recommended template may be beneficial to commands and management in assessing the five internal control components. Commands roll up the information from the Principle and Deficiency Summary templates to view each deficiency across components. This template may be valuable in assessing whether other controls across components may reduce the risk of each identified deficiency to an acceptable level. An important part of the component evaluation process is considering if any other internal control deficiencies are associated with the remaining principles to see if they impact the identified deficiency.

This template rolls up information from the preceding templates and allows commands to evaluate deficiencies across components. In the NAVSEA scenario, three principles spanning three different components were mentioned, including principle 7 within the Risk Assessment component, principle 11 within the Control Activities component, and principle 13 within the Information and Communication component. NAVSEA may use principles 7 and 13 to compensate or at least make efforts toward minimizing the internal control deficiency associated with principle 11, in Figure 18, through adjusting its risk mitigation and implementation approaches to the ERP general ledger system and documenting it into the applicable cells in Figure 18.

As NAVSEA evaluates the other two principles within the Control Activities component as well as the remaining components, other deficiencies may be identified and the severity can be assessed. As each deficiency is identified, this template can be used to consider compensating controls across each component. This process may assist commands in mitigating the risk deficiencies, such as the ERP general ledger system deficiency, but may not always help in mitigating a risk to an acceptable level. Therefore, commands may not always be able to downgrade a deficiency type from a material deficiency to a reportable condition or item to be revisited.

In many scenarios, such as this NAVSEA example, this template may be more useful in communicating to external auditors that internal control

deficiencies have been identified and explaining that corrective action plans are in place. However, the templates may not be useful in resolving every material deficiency like this NAVSEA example. Correcting internal control deficiencies is important, and the final recommended template may be most beneficial to FMO for monitoring commands' corrective actions that cannot be resolved by the recommended templates.

4.   Recommended Template #4 of 4: Overall Internal Control System Assessment

The Overall Internal Control System Assessment recommended template, in Figure 19, also incorporates the Green Book's application requirements, such as GAO's three objectives of internal control: operations, reporting, and compliance. This template provides a summary view of material internal control deficiencies. This view may help management better evaluate if all components are operating together in an integrated fashion and whether collective deficiencies aggregated across all five components represent a material deficiency.

Having an overall view is important because the existence of even just one material deficiency in the entire internal control system requires management to conclude that the overall internal control system is not effective. The information from the NAVSEA scenario is rolled up from the first three templates to the final template in Figure 19 and illustrates how one material deficiency makes the entire internal control system ineffective.

Overall Internal Control System Assessment				
Name of Organization:		DON		
Type of Objective:		Risk Assessment Considerations		
Operations				
Reporting	External financial	A high, combined risk was identified in the Control Activities component and determined to be a major deficiency that resulted in a material weakness.		
Compliance				
Internal Control Component # (1-5):		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
1. Control Environment				
2. Risk Assessment				
3. Control Activities		Y	N	ERP has a general ledger system in place, but DODIG found that this system did not produce accurate or reliable financial information
4. Information and Communication				
5. Monitoring				
Are all components operating together in an integrated manner? Do the combination of internal control deficiencies represent a major deficiency when aggregated across all five components? If yes, explain.*		N		
Is the overall internal control system effective? <Y/N>*		N		
Basis for conclusion		Due to a material weakness in the Control Activities component, these components are not functioning properly and the overall internal control system is not effective.		
* If there is a major deficiency, management must conclude that the internal control system is not effective.				

Figure 19.   Overall Internal Control System Assessment (after COSO Illustrative Tools, 2013)

This template allows the DON MICP to consolidate all internal control information reported by commands into one place. The type of objective, for example, external financial reporting, is listed along with risk assessment considerations. Using the MICM risk assessment requirements, this template can document major deficiencies. For example, a high, combined risk was identified in the Control Activities component and determined to be a major deficiency that resulted in a material weakness. This deficiency is explained in the Control Activities component cell. All the components are evaluated to judge whether or not all components are operating together in an integrated fashion. This template also documents the basis for whether or not the overall internal control system is effective.

Consolidating all of the information into one place may make it easier for all stakeholders to use it. This template may expand MIC Coordinators' view of how deficiencies may affect other areas during self-assessments. Having a summary view of four MICM documentation requirements on one template may also help management at the command level and FMO make better decisions.

Another benefit of having a summary view of internal control deficiencies in a format that external auditors understand from their experience in auditing the private sector is that it may help DON external financial audits go smoother. Using a tracking number system that simplifies how each internal control deficiency is mapped to each component and principle may prevent external auditors from examining and inquiring more than necessary in attempts to determine whether or not the internal controls are effective.

5. Recommended Tracking Number System

The recommended templates may not only improve MIC Coordinators' ability to conduct self-assessments by using a more thorough internal control framework based on industry and federal standards, but also improve commands' monitoring and tracking corrective action plans. Tracking deficiencies properly is important for

compliance as well as for decision makers, who rely on the information to understand what areas need the most attention and monitoring.

The recommended tracking number system accounts for the major DON commands listed in the MICM. The MICM lists 18 Major Assessable Units (MAU), as shown in Figure 20 that report internal control deficiencies to FMO (SECNAV, 2008). Identification numbers (ID #'s) can be created to track the origin of each deficiency and be linked to all 18 MAUs. For instance, numbers 1 through 18 can be assigned to the 18 MAUs listed in Figure 20 in order from top to bottom. The Assistant for Administration to the Under Secretary of the Navy can be assigned the number one all the way down through the 18th MAU.

AAUSN	Assistant for Administration to the Under Secretary of the Navy
ASN(FM&C)	Assistant Secretary of the Navy (Financial Management & Comptroller)
ASN(I&E)	Assistant Secretary of the Navy (Installations & Environment)
ASN(M&RA)	Assistant Secretary of the Navy (Manpower & Reserve Affairs)
ASN(RD&A)	Assistant Secretary of the Navy (Research, Development & Acquisition)
AUDGEN	Auditor General of the Navy
CHINFO	Chief of Information
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
DON CIO	Department of the Navy Chief Information Officer
JAG	Judge Advocate General
NAVINSGEN	Naval Inspector General
NCIS	Director, Naval Criminal Investigative Service
OGC	General Counsel of the Department of the Navy
OLA	Chief of Legislative Affairs
ONR	Chief of Naval Research
OPPA	Director, Office of Process and Program Assessment
OSBP	Director, Office of Small Business Programs

Figure 20.   DON MIC Major Assessable Units (after SECNAV, 2008)

Besides the 18 MAUs, subordinate levels may be assigned ID #'s. Members of the DON MIC Senior Assessment Team may use the recommended templates to roll up information to FMO. The MICM lists the DON MIC Senior Assessment Team, as show in Figure 21. The Senior Assessment Team may be assigned an ID # on the next tier of numbers listed after the MAUs. Similar to the

MAUs, numbers of 01 through 12 may be assigned in order from top to bottom based on Figure 21.

ASN(FM&C), FMB	Office of the Under Secretary of the Navy (Financial Management and Comptroller), Office of Budget
HQMC	Headquarters Marine Corps
DFAS	Defense Finance and Accounting Service (Arlington and Cleveland)
NAVAIR	Naval Air Systems Command
NAVFAC	Naval Facilities Engineering Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
SPAWAR	Space and Naval Warfare Systems Command
CFFC	Commander, Fleet Forces Command
CNIC	Commander, Navy Installations Command
BUPERS	Bureau of Naval Personnel
ONR	Office of Naval Research
Advisors	Executive, non-voting advisors from the Naval Audit Service and appropriate business management (non-FM) areas

Figure 21.   DON MIC Senior Assessment Team (after SECNAV, 2008)

A tracking number system can begin by focusing on what external auditors are looking for, namely how internal controls relate to compliance requirements. Instead of starting the tracking number with the associated DON MIC MAUs or Senior Assessment Team, DON may consider using a tracking approach designed to help external auditors and management understand the big picture of each material internal control weakness. For instance, DON may consider labeling the ID #'s with the component number first, principle number second, attribute number third, branch of military service fourth, major assessment command fifth, senior audit team sixth, and any further details thereafter. This type of tracking system may help external auditors and FMO trace the root of deficiencies. An example ID #, as shown in Figure 22, may be C3.P11.A3.N.0.5-0001.
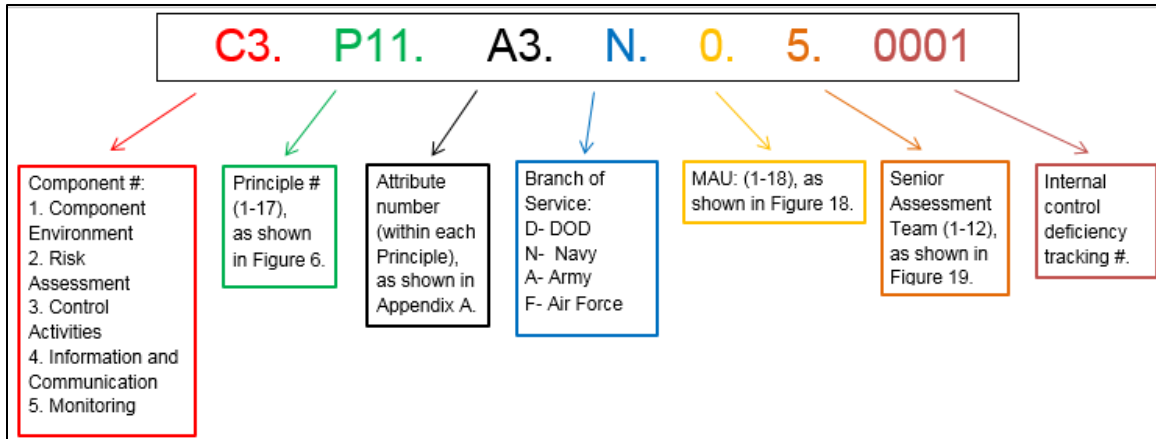
Figure 22.   Example ID #

Using a number system that helps external auditors follow DON's tracking system may also help commands track deficiencies in an organized fashion on the Deficiency Summary. For tracking and spacing purposes, the recommended templates abbreviate the identification numbers of each component as C1 through C5, each principle as P1 through P17, and each attribute as A1-A7. The ID # in Figure 22 uses the NAVSEA scenario and represents a deficiency in the third federal internal control component, Control Activities. The deficiency is associated with the 11th principle and its third attribute.

The "N" for DON may be beneficial for future tracking if the entire DOD later adopts the templates because the Army may use "A" and the Air Force may use "F." All branches of the military may eventually roll up into a "D" for Department of Defense. The deficiency originates from NAVSEA, the fifth Senior Assessment Team and not from one of DON's 18 MAUs. The remaining numbers on Figure 22 of the Example ID # give commands an ability to track in a way that meets their needs. A zero can be placed in the fifth or sixth part of the tracking number if it does not apply to one of the numbered MAUs or Senior Assessment Teams. A deficiency number is assigned in the final part of the tracking number. The following section provides recommendations based on the analysis and findings.

C.   RECOMMENDATIONS BASED ON ANALYSIS AND FINDINGS

This section provides recommendations based on the analysis and findings. Implementing the recommendations may help commands meet the Green Book's application requirements, help commands present internal controls to external auditors more effectively, and focus on the most critical principles.

1.   Add 17 New Principles to MICM to Meet Green Book's Application Requirements

The first recommendation is to update the MICM with the 17 principles using the recommended templates. This is important for several reasons. DON may benefit from a tool that commands can use to improve the effectiveness of their internal control programs, which also helps DON comply with new GAO requirements and make processes more auditable. The recommended templates may offer DON more than improved compliance during external financial audits. The recommended templates may also help commands more effectively communicate with external auditors, mitigate risks, deter fraud, and meet long-term objectives.

The MICM can either be modified to map internal controls to each principle or supplemented with templates based on the Green Book using the Illustrative Tools. A recommendation is to augment the MICM with the 17 principles and COSO templates adapted for DON use because it would allow the MICM to meet the Green Book's documentation requirements and may help the DON MICP expand its internal control capabilities.

2.   Help Commands Present Internal Controls to External Auditors

The second recommendation is to use a recognizable format on MICP documentation and templates with which external auditors are familiar. Private sector entities often tailor the templates from COSO Illustrative Tools to conduct organizational self-assessments. From a perception standpoint, supplementing the MICM with tailored Illustrative Tools from Green Book application requirements may show external auditors that DON is not only committed to

complying with federal internal control guidance and policies, but also committed to using current best practices from industry to improve internal controls.

Furthermore, having templates congruent with private sector templates may help in preventing external auditors from examining deeper into areas of uncertainty when commands are unable to effectively communicate how they have implemented internal controls. Presenting documentation in a manner that is easily understood by external auditors may be beneficial when commands are providing supporting documentation as evidence that internal controls are in place and being used. The templates may reduce or eliminate ambiguity of how commands implement internal controls in accordance with the federal standards of internal control found in the Green Book.

In practice, most commanders may not regularly reference the Green Book or consider how the Green Book may help them achieve command objectives through building more effective internal control systems. Having templates that simplify how to report their internal controls in a way that meets the revised Green Book's application requirements may help external auditors understand how DON internal control processes are being implemented effectively. Commanders may feel threatened by external auditors in part because they may be uncertain as to how to communicate how they implement their internal controls on a daily basis in a way that external auditors will understand how it complies with the Green Book.

Upcoming external financial audits are a new procedure for which commanders need to prepare. Even though they may be implementing internal controls properly, they may be uncertain as to how to communicate what they do in auditor terminology since this is not a typical commander's area of expertise. Commanders may perceive the external financial audit as an FMO problem that is interrupting their commands operations by having to prepare internal control documentation for external auditors. Uncertainty on how to tie in their internal controls to new Green Book application requirements may only exacerbate the

threatening perception of the external auditors if a tool is not in place to help prepare them with communicating their internal control program effectively.

To address this uncertainty on how to effectively present internal controls, the recommended templates add a tracking number system and mapping process that may help commands document and describe how their internal controls are in compliance with the Green Book. This may help commands more effectively portray that they are using current internal control guidance to help them achieve their organizational objectives. If external auditors buy in to the commands' explanations on how they are effectively implementing internal controls, then perhaps external financial audits may go smoother.

External auditors may look favorably on the recommended documentation methodology that entails four templates based on the COSO Illustrative Tools and a tracking number system geared toward helping them map internal control deficiencies. The recommended templates are even more stringent than the COSO Illustrative Tools' recommended Yes (Y) or No (N) answers in various cells. This approach may provide commands with more thorough documentation and findings, which may help prevent external auditors from delving deeper into internal control deficiencies. The increased tractability from the recommended templates and tracking number system may give external auditors confidence that MIC Coordinators are going beyond just "checking the box" yes or no.

3. Focus on Most Critical Principles: Control Activities' Principles 10–12

The third recommendation is to implement the 17 internal control principles to meet GAO's FY 2016 compliance requirements into its MICP. However, this implementation may be cumbersome, especially if attempting to perfect every principle at once. FMO may consider beginning with supplementing the MICM with the 17 principles. Perhaps the most plausible approach is to begin by monitoring the implementation of the most crucial principles.

FMO may consider focusing first on the most critical principles that most private sector organizations concentrate on when preparing for audits. Specifically, the three principles within the Control Activities internal control component are the main principles on which organizations spend the most time. The reason for this is that design issues related to control activity have been subject to increased audit scrutiny since they provide the first line of defense in preventing and detecting material misstatements (Prawitt & Tysiac, 2013).

As far as the remaining 14 principles related to the other four internal control components, DON is already addressing many of them. For instance, programs are in place to set the proper tone at the top on important issues like ethics, proactive leadership, fraud, waste, and abuse. Therefore, DON has further incentive to shift attention from principles already being addressed to the most critical principles that have caused the most audit scrutiny for the private sector in this relatively new COSO Framework presented in May 2013.

D.   SUMMARY

This chapter developed templates that are designed to supplement the MICM and may help bridge the gaps by aligning the MICM with the Green Book using COSO's Illustrative Tools. Other potential recommendations for further research were discovered during this research and are discussed in Chapter VI, Summary, Conclusions, and Areas For Further Research. The following chapter concludes this research and provides recommended areas for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. SUMMARY, CONCLUSIONS, AND AREAS FOR FURTHER RESEARCH

A. INTRODUCTION

This chapter begins with a summary of the background that motivated this research study. It provides a conclusion and briefly discusses the findings based on the analysis related to the research question. This chapter also suggests four areas for further research.

B. RESEARCH SUMMARY AND CONCLUSION

The purpose of this research was to examine the Department of the Navy's (DON) Managers' Internal Control Program's (MICP) capability in relation to external financial audits. This research highlighted that the MICP's Manual, hereafter referred to as the MICM, did not meet the minimum requirements found in the *Standards of Internal Control for the Federal Government* (Green Book) primarily because the MICM does not give guidance on The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 17 principles of effective internal control.

DON may benefit from a tool that commands can use to improve the effectiveness of their internal control system, which also helps DON comply with new Government Accountability Office (GAO) requirements and make processes more auditable. This research utilized a content analysis and examined the relationship between the MICM, Green Book, and COSO's Illustrative Tools. Gaps in the MICM were identified and their relevance was reviewed in relation to internal audits, external financial audits, and financial auditability. Recommended templates were developed to help bridge this gap by supplementing the MICM with the 17 principles. Recommendations were made based on this analysis and findings to expand the MICP's internal control capability to help commands prepare for external financial audits.

The answer to the research question based on the literature review and content analysis of the internal control framework between the MICM, GAO, and COSO's Illustrative Tools is as follows:

- Research Question: How would updating the MICP's capabilities to current internal control guidance help commands achieve audit readiness?

DON may benefit from templates that commands can use to improve the effectiveness of their internal control programs, which also helps DON comply with new GAO requirements and make processes more auditable. The MICP may benefit by adopting the current framework into its program, manual, and guidance by supplementing the MICM with the recommended templates. The recommended templates may help commands improve their internal controls to meet their objectives and help them prepare for external financial audits that will test their internal controls before issuing an audit opinion.

Adding the 17 principles into the MICM may help commanders refocus on the right internal control processes, controls, and documentation practices since the 17 principles are what the private and public sectors are currently transitioning to in efforts to incorporate all of the COSO Internal Control—Integrated Framework. Expanding the MICP's capabilities to include the 17 principles into its MICM and training guidance may help commands build and maintain effective internal control systems.

The MICM's omission of the 17 new principles could be identified during internal audits upon checking commands' documentation against the Green Book. External auditors could determine the omission of the 17 new principles, which are a part of the minimum requirements by the Green Book, to be a material weakness in DON's internal control systems and automatically disqualify DON from receiving a clean audit opinion on its financial statements. Thus, the internal control gap of missing the 17 principles of internal control could severely impact DON's audit readiness on its path toward achieving financial auditability. The next section provides areas for further research.

C. AREAS FOR FURTHER RESEARCH

1. Area #1: Communicating with External Auditors

FMO is responsible for preparing commands for financial audits, and a paradigm shift is needed to embrace the volume, intensity, and tempo of a Schedule of Budgetary Activity (SBA) audit. Previously, commands have centered on inspections and their perspective "has been shaped by their experience responding to segment assertion activities" (Cook, 2015) because the focus has been on people and performance in an effort to produce permanent records. Going forward, commanders must adjust their focus to reasonableness by focusing on processes, controls, and documentation toward an outcome of continuous improvement (Cook, 2015).

DON personnel may struggle with this change, as old habits are hard to break. Internal auditors may often be perceived as inspectors, and this can cause commanders to feel threatened. Even in the private sector a stereotype exists that views internal auditors as police in the hunt to identify negative findings in an organization's internal controls (Haas et al., 2006). Communicating, both orally and in writing, is crucial to maximizing resources because key stakeholders should understand the needs of the audit function (Haas et al., 2006).

2. Area #2: Developing an Internal Auditing Capability Model

DON may benefit from the internal auditing profession to improve its internal control systems and internal audits in preparing for financial audits. DON may be able to expand its MICP's capabilities by adopting internal auditing and internal control best practices from professional associations, academic textbooks, consulting firms, and professional journals.

DON may be able to gain insight from internal auditing consulting firms like Protiviti and the "Big 4" on how to improve internal control capabilities during internal audits. Internal auditing firms assist large corporations in the private sector in preparing for financial audits. DON may benefit by implementing

87

lessons learned from the private sector to expand the MICP's capabilities and, in turn, this may assist commands' preparations for external financial audits.

Protiviti is a globally respected internal audit consulting firm that provides solutions to over 40 percent of Fortune 1000 and Fortune Global 500 corporations. Protiviti bases its research on the internal audit functions of leading companies around the world, and their work is often cited in publications from the Institute of Internal Auditors (IIA) (Protiviti, n.d.).

Besides Protiviti and the "Big 4," DON may look to the leading professional association in the field, The Institute of Internal Auditors (IIA). IIA has developed an Internal Auditing—Capability Model (IA-CM) with five levels that may help commands optimize its internal auditing capabilities.

3. Area #3: Educating the DON Workforce on the Importance of Internal Control and Internal Auditing in Auditability

DON workforce may not value the importance of internal control and internal auditing as related to auditability as much as FMO. Research regarding how FMO can improve its internal control and internal auditing training may be beneficial in helping commands prepare for external financial audits. Since an external auditor cannot give a clean audit opinion to DON's financial statements if they find one or more material weaknesses in an organization's internal control system, FMO may benefit by expanding the MICP's training on internal control and internal auditing. Building and sustaining effective internal controls through regular internal audits may enhance commands' preparations for external financial audits.

4. Area #4: Provide a Single website

Many of the new principles may be practiced by DON already. Instead of changing any of the existing DON programs in place, DON may consider developing a website to consolidate all supporting documentation from existing programs that address issues associated with the 17 principles. A single online location that stores and links all supporting documentation to the recommend

templates may be beneficial to external auditors and, more importantly, decision makers.

Having a single website to upload supporting documentation may also help external auditors quickly validate DON's audit readiness efforts without having to delve deeper into various programs scattered across commands. This may reduce the duration and costs of external auditors. For example, one website could contain all GAO reports and follow up reports, FMO's high-level internal control and audit readiness assessments, and command-level supporting documentation. All documents may be uploaded into a single location online to simplify the validation process for external auditors. Furthermore, decision-makers may benefit from more efficient access to information, increased accountability, and the ability to monitor weaknesses more closely.

D.   SUMMARY

This chapter discussed the background that motivated this research study. This chapter provided a conclusion and briefly discussed the findings based on the analysis related to the research question. This chapter also discussed recommended areas for further research.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. MIC PLAN

Organization Name
Managers' Internal Control (MIC) Plan

This plan is updated (indicate frequency, i.e., annually, quarterly, etc.)

Last Update: (Enter actual date of last update)

MIC Senior Official: (This person will sign the organization's certification statement)

- Identify the MIC senior official by name, title and position within the organization.
- Identify to whom the position reports.
- Indicate how the responsibility is assigned and how often the position changes staffing.

MIC Coordinator:

- Identify the MIC coordinator by name, title and position within the organization. Identify to whom the position reports.
- Indicate how the responsibility is assigned and how often the position changes staffing.
- Indicate if this is a full-time or part-time function.

Alternate MIC Coordinator:

- Identify the alternate MIC coordinator by name, title and position within the organization.
- Identify how the position reports to the Coordinator.
- Indicate how the responsibility is assigned and how often the position changes staffing.
- Indicate if this is a full-time or part-time function.

Overview of the Managers' Internal Control Program within the Organization:

Address all five elements of the GAO standards: Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring, and how they are being addressed within your organization. For each discussion

area, if published information already exists, it is unnecessary to repeat it within the document. Instead, attach or reference the location and source of the relevant information, so it can be easily obtained.

Control Environment

Mission
- Identify your organization's mission - what your organization is working to accomplish.

Attach/Reference: location and/or copy of published mission statement

Strategic Plan
- Identify your organization's strategic plan.

Attach/Reference: location and/or copy of the Strategic Plan

Organization Structure
- Describe at a high level how your organization is structured—the hierarchy, functional divisions, programs, staffing, etc.
- Discuss how key areas of authority and responsibility are defined. Identify how lines of reporting are established.
  - Identify the IC reporting chain of command within your organization
  - Identify the funding flow within your organization

Attach/Reference: organization chart, DON organizational manual, chapters, pages, etc. Indicate the date of the chart and frequency of update.

Risk Assessment

- Describe how your organization assesses the risks associated with accomplishing its mission. Is your organization performing risk assessments on operations, programs and administrative functions? (This section is simply a narrative overview of your risk assessment. The results of your risk assessment shall be included in the risk assessment documentation requirement.)

Control Activities

- Describe the methodology of how control activities are identified and developed, the types of policies and documented procedures that are in place to explain and outline how to ensure the effectiveness of the controls.

Information and Communications

- Describe how your organization communicates information up and down the chain of command. Include information on the significant channels of communication, such as type of channel (email, website, monthly reports, etc.), the typical subject matter; the target audience; and the frequency of the communication.

Monitoring

Control Activities

- Describe the major types and methods of monitoring activities/internal control assessment being performed by both internal and external entities. Include self-assessments, evaluations and risk assessments. Reference by assessable units, if different or applicable.
- List the total number of scheduled internal control assessments for upcoming MIC year. (This information is needed for the annual MIC certification statement).
- List the total number of completed internal control assessments for the previous MIC year. (This information is needed for the annual MIC certification statement).

Accomplishments

- Describe how management tracks the organization's accomplishments. Include a discussion on the types of performance measures and indicators (i.e., specific metrics) your organization has established to measure progress in accomplishing its objectives and goals.

Corrective Action Plans

- Include a brief description of your internal organization process (either manual or automated) for tracking progress against control deficiencies. This may currently be one of the functions of your internal Inspector General.

MIC Training

- Provide a high level overview of the training opportunities available within your organization.

- Indicate the minimum annual training requirements and how they are monitored. Reference databases, sources, etc.

Reporting Requirements:
- Indicate the schedule for internal reporting and review times within your organization necessary to meet the DON SOA requirement.

APPENDIX B.   SUGGESTED MICM TEMPLATES

Principle Evaluation

Principle Evaluation – Control Environment
Principle 1: Demonstrates Commitment to Integrity and Ethical Values –The oversight body and management should demonstrate a commitment to integrity and ethical values.
Attributes   - Tone at the Top – The oversight body and management demonstrate the importance of integrity and ethical values through their directives, attitudes, and behavior.   - Establishes Standards of Conduct – Management establishes standards of conduct to communicate expectations concerning integrity and ethical values. The entity uses ethical values to balance the needs and concerns of different stakeholders, such as regulators, employees, and the general public. The standards of conduct guide the directives, attitudes, and behaviors of the organization in achieving the entity's objectives.   - Adherence to Standards of Conduct – Management establishes processes to evaluate performance against the entity's expected standards of conduct and address any deviations in a timely manner.

Summary of Controls to Effect Principle 1

Deficiencies Applicable to Principle 1				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 1:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 1, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 1 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 1 present?				
Is Principle 1 functioning?				

* Note: Record deficiencies in Deficiency Summary Template.

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 2: Exercises Oversight Responsibility
—The oversight body should oversee the entity's internal control system.

Attributes

- Oversight Structure—The entity determines an oversight structure to fulfill responsibilities set forth by applicable laws and regulations, relevant government guidance, and feedback from key stakeholders. The entity will select, or if mandated by law will have selected for it, an oversight body. When the oversight body is composed of entity management, activities referenced in the Green Book as performed by "management" exclude these members of management when in their roles as the oversight body.

- Provides Oversight for the System of Internal Control—The oversight body oversees management's design, implementation, and operation of the entity's internal control system. The oversight body's responsibilities for the entity's internal control system include the following:

  – *Control Environment*—Establish integrity and ethical values, establish oversight structure, develop expectations of competence, and maintain accountability to all members of the oversight body and key stakeholders.

  – *Risk Assessment*—Oversee management's assessment of risks to the achievement of objectives, including the potential impact of significant changes, fraud, and management override of internal control.

  – *Control Activities*—Provide oversight to management in the development and performance of control activities.

  – *Information and Communication*—Analyze and discuss information relating to the entity's achievement of objectives.

  – *Monitoring*—Scrutinize the nature and scope of management's monitoring activities as well as management's evaluation and remediation of identified deficiencies.

- Input for Remediation of Deficiencies—The oversight body provides input to management's plans for remediation of deficiencies in the internal control system as appropriate.

Summary of Controls to Effect Principle 2				
Deficiencies Applicable to Principle 2				
ID #	Internal control deficiency description	Evaluate severity of each internal control deficiency: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 2:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 2, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 2 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 2 present?				
Is Principle 2 functioning?				

* Note: Record deficiencies in Deficiency Summary Template.
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 3: Establishes Structure, Responsibility, and Authority
—Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

Attributes

- Organizational Structure—Management establishes the organizational structure necessary to enable the entity to plan, execute, control, and assess the organization in achieving its objectives. Management develops the overall responsibilities from the entity's objectives that enable the entity to achieve its objectives and address related risks.
- Assignment of Responsibility and Delegation of Authority—To achieve the entity's objectives, management assigns responsibility and delegates authority to key roles throughout the entity. A key role is a position in the organizational structure that is assigned an overall responsibility of the entity. Generally, key roles relate to senior management positions within an entity.
- Documentation of the Internal Control System —Management develops and maintains documentation of its internal control system.

  – Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

  – Management documents internal control to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, capable of being communicated to those responsible for their performance, and capable of being monitored and evaluated by the entity.

  – The extent of documentation needed to support the design, implementation, and operating effectiveness of the five components of internal control is a matter of judgment for management. Management considers the cost benefit of documentation requirements for the entity as well as the size, nature, and complexity of the entity and its objectives. Some level of documentation, however, is necessary so that the components of internal control can be designed, implemented, and operating effectively.

Summary of Controls to Effect Principle 3

ID #	Internal control deficiency description	Evaluate severity of each internal control deficiency: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

Deficiencies Applicable to Principle 3

Evaluate deficiencies within Principle 3:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 3, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>		
Evaluate Principle 3 using judgment.**	Y/N	Explanation/Conclusion	
Is Principle 3 present?			
Is Principle 3 functioning?			

* Note: Record deficiencies in Deficiency Summary Template.

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 4: Demonstrates Commitment to Competence
—Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

Attributes

- Expectations of Competence—Management establishes expectations of competence for key roles, and other roles at management's discretion, to help the entity achieve its objectives. Competence is the qualification to carry out assigned responsibilities. It requires relevant knowledge, skills, and abilities, which are gained largely from professional experience, training, and certifications. It is demonstrated by the behavior of individuals as they carry out their responsibilities.
- Recruitment, Development, and Retention of Individuals—Management recruits, develops, and retains competent personnel to achieve the entity's objectives. Management considers the following:
  • Recruit - Conduct procedures to determine whether a particular candidate fits the organizational needs and has the competence for the proposed role.
  • Train - Enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.
  • Mentor - Provide guidance on the individual's performance based on standards of conduct and expectations of competence, align the individual's skills and expertise with the entity's objectives, and help personnel adapt to an evolving environment.
  • Retain - Provide incentives to motivate and reinforce expected levels of performance and desired conduct, including training and credentialing as appropriate.

- Succession and Contingency Plans and Preparation—Management defines succession and contingency plans for key roles to help the entity continue achieving its objectives. Succession plans address the entity's need to replace competent personnel over the long term, whereas contingency plans address the entity's need to respond to sudden personnel changes that could compromise the internal control system.

Summary of Controls to Effect Principle 4

Deficiencies Applicable to Principle 4				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 4:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 4, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 4 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 4 present?				
Is Principle 4 functioning?				

* Note: Record deficiencies in Deficiency Summary Template.
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 5: Enforce Accountability

—Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Attributes

- Enforcement of Accountability—Management enforces accountability of individuals performing their internal control responsibilities. Accountability is driven by the tone at the top and supported by the commitment to integrity and ethical values, organizational structure, and expectations of competence, which influence the control culture of the entity. Accountability for performance of internal control responsibility supports day-to-day decision making, attitudes, and behaviors. Management holds personnel accountable through mechanisms such as performance appraisals and disciplinary actions.

- Consideration of Excessive Pressures—Management adjusts excessive pressures on personnel in the entity. Pressure can appear in an entity because of goals established by management to meet objectives or cyclical demands of various processes performed by the entity, such as year-end financial statement preparation. Excessive pressure can result in personnel "cutting corners" to meet the established goals.

Summary of Controls to Effect Principle 5

Deficiencies Applicable to Principle 5				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 5:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 5, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 5 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 5 present?				
Is Principle 5 functioning?				

* Note: Record deficiencies in Deficiency Summary Template.

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 6: Define Objectives and Risk Tolerances

—Management should define objectives clearly to enable the identification of risks and define risk tolerances.

Attributes

- Definitions of Objectives—Management defines objectives in specific and measurable terms to enable the design of internal control for related risks. Specific terms are fully and clearly set forth so they can be easily understood. Measurable terms allow for the assessment of performance toward achieving objectives. Objectives are initially set as part of the objective-setting process and then refined as they are incorporated into the internal control system when management uses them to establish the control environment.

- Definitions of Risk Tolerances—Management defines risk tolerances for the defined objectives. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerances are initially set as part of the objective-setting process. Management defines the risk tolerances for defined objectives by ensuring that the set levels of variation for performance measures are appropriate for the design of an internal control system. *note: Management defines risk tolerances in specific and measurable terms so they are clearly stated and can be measured. Risk tolerance is often measured in the same terms as the performance measures for the defined objectives. Depending on the category of objectives, risk tolerances may be expressed as follows:

- Operations objectives—Level of variation in performance in relation to risk.

- Nonfinancial reporting objectives—Level of precision and accuracy suitable for user needs, involving both qualitative and quantitative considerations to meet the needs of the nonfinancial report user.

- Financial reporting objectives—Judgments about materiality are made in light of surrounding circumstances, involve both qualitative and quantitative considerations, and are affected by the needs of financial report users and size or nature of a misstatement.

- Compliance objectives—Concept of risk tolerance does not apply. An entity is either compliant or not compliant.

Summary of Controls to Effect Principle 6				
Deficiencies Applicable to Principle 6				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 6:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 6, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 6 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 6 present?				
Is Principle 6 functioning?				

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 7: Identify, Analyze, and Respond to Risks
—Management should identify, analyze, and respond to risks related to achieving the defined objectives.

Attributes

- Identification of Risks—Management identifies risks throughout the entity to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.
- Analysis of Risks—Management analyzes the identified risks to estimate their significance, which provides a basis for responding to the risks. Significance refers to the effect on achieving a defined objective.
- Response to Risks—Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective.
  Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance. These risk
  responses may include the following:
  • Acceptance - No action is taken to respond to the risk based on the insignificance of the risk.
  • Avoidance - Action is taken to stop the operational process or the part of the operational process causing the risk.
  • Reduction - Action is taken to reduce the likelihood or magnitude of the risk.
  • Sharing - Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.

Summary of Controls to Effect Principle 7			
Deficiencies Applicable to Principle 7			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)	List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N) / Comments/Compensating Controls	
Evaluate deficiencies within Principle 7:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 7, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>		
Evaluate Principle 7 using judgment.**	Y/N	Explanation/Conclusion	
Is Principle 7 present?			
Is Principle 7 functioning?			

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 8: Assess Fraud Risk
—Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

Attributes

- Types of Fraud—Management considers the types of fraud that can occur within the entity to provide a basis for identifying fraud risks. Types of fraud are as follows:
  • Fraudulent financial reporting - Intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. This could include intentional alteration of accounting records, misrepresentation of transactions, or intentional misapplication of accounting principles.
  • Misappropriation of assets - Theft of an entity's assets. This could include theft of property, embezzlement of receipts, or fraudulent payments.
  • Corruption - Bribery and other illegal acts.
- Fraud Risk Factors—Management considers fraud risk factors. Fraud risk factors do not necessarily indicate that fraud exists but are often present when fraud occurs. Fraud risk factors include the following:
  • Incentive/pressure - Management or other personnel have an incentive or are under pressure, which provides a motive to commit fraud.
  • Opportunity - Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.
  • Attitude/rationalization - Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.
- Response to Fraud Risks—Management analyzes and responds to identified fraud risks so that they are effectively mitigated. Fraud risks are analyzed through the same risk analysis process performed for all identified risks. Management analyzes the identified fraud risks by estimating their significance, both individually and in the aggregate, to assess their effect on achieving the defined objectives. As part of analyzing fraud risk, management also assesses the risk of management override of controls. The oversight body oversees management's assessments of fraud risk and the risk of management override of controls so that they are appropriate.

Summary of Controls to Effect Principle 8				
Deficiencies Applicable to Principle 8				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 8:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 8, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 8 using judgment.**	Y/N		Explanation/Conclusion	
Is Principle 8 present?				
Is Principle 8 functioning?				

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 9: Identify, Analyze, and Respond to Change

—Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Attributes

- Identification of Change—As part of risk assessment or a similar process, management identifies changes that could significantly impact the entity's internal control system. Identifying, analyzing, and responding to change is similar to, if not part of, the entity's regular risk assessment process. However, change is discussed separately because it is critical to an effective internal control system and can often be overlooked or inadequately addressed in the normal course of operations.

- Analysis of and Response to Change—As part of risk assessment or a similar process, management analyzes and responds to identified changes and related risks in order to maintain an effective internal control system. Changes in conditions affecting the entity and its environment often require changes to the entity's internal control system, as existing controls may not be effective for meeting objectives or addressing risks under changed conditions. Management analyzes the effect of identified changes on the internal control system and responds by revising the internal control system on a timely basis, when necessary, to maintain its effectiveness.

Summary of Controls to Effect Principle 9				
Deficiencies Applicable to Principle 9				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 9:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 9, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 9 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 9 present?				
Is Principle 9 functioning?				

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle Evaluation – Control Activities
Principle 10: Design Control Activities —Management should design control activities to achieve objectives and respond to risks.
Attributes • Response to Objectives and Risks—Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities to fulfill defined responsibilities and address identified risk responses. • Design of Appropriate Types of Control Activities—Management designs appropriate types of control activities for the entity's internal control system. Control activities help management fulfill responsibilities and address identified risk responses in the internal control system. The common control activity categories listed in Figure 6 of the Green Book are meant only to illustrate the range and variety of control activities that may be useful to management. The list is not all inclusive and may not include particular control activities that an entity may need. • Design of Control Activities at Various Levels—Management designs control activities at the appropriate levels in the organizational structure. • Segregation of Duties—Management considers segregation of duties in designing control activity responsibilities so that incompatible duties are segregated and, where such segregation is not practical, designs alternative control activities to address the risk.

Summary of Controls to Effect Principle 10				
Deficiencies Applicable to Principle 10				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 10:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 10, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 10 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 10 present?				
Is Principle 10 functioning?				

* Note: Record deficiencies in Deficiency Summary Template
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 11: Design Activities for the Information System

—Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

Attributes

- Design of the Entity's Information System—Management designs the entity's information system to respond to the entity's objectives and risks.
- Design of Appropriate Types of Control Activities—Management designs appropriate types of control activities in the entity's information system for coverage of information processing objectives for operational processes. For information systems, there are two main types of control activities: general and application control activities.
- Design of Information Technology Infrastructure—Management designs control activities over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology. Information technology requires an infrastructure in which to operate, including communication networks for linking information technologies, computing resources for applications to operate, and electricity to power the information technology. An entity's information technology infrastructure can be complex. It may be shared by different units within the entity or outsourced either to service organizations or to location-independent technology services. Management evaluates the objectives of the entity and related risks in designing control activities for the information technology infrastructure.

- Design of Security Management—Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

- Design of Information Technology Acquisition, Development, and Maintenance—Management designs control activities over the acquisition, development, and maintenance of information technology. Management may use a systems development life cycle (SDLC) framework in designing control activities. An SDLC provides a structure for a new information technology design by outlining specific phases and documenting requirements, approvals, and checkpoints within control activities over the acquisition, development, and maintenance of technology. Through an SDLC, management designs control activities over changes to technology. This may involve requiring authorization of change requests; reviewing the changes, approvals, and testing results; and designing protocols to determine whether changes are made properly. Depending on the size and complexity of the entity, development of information technology and changes to the information technology may be included in one SDLC or two separate methodologies. Management evaluates the objectives and risks of the new technology in designing control activities over its SDLC.

115

Summary of Controls to Effect Principle 11

Deficiencies Applicable to Principle 11				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 11:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 11, represents a major deficiency** <Update Deficiency Summary Template >				
Evaluate Principle 11 using judgment.**		Y/N	Explanation/Conclusion	
Is Principle 11 present?				
Is Principle 11 functioning?				

* Note: Record deficiencies in Deficiency Summary Template
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 12: Implement Control Activities

—Management should implement control activities through policies.

Attributes

- Documentation of Responsibilities through Policies—Management documents in policies the internal control responsibilities of the organization.
- Periodic Review of Control Activities—Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology. Regulators; legislators; and in the federal environment, the Office of Management and Budget and the Department of the Treasury may also change either an entity's objectives or how an entity is to achieve an objective. Management considers these changes in its periodic review.

Summary of Controls to Effect Principle 12

Deficiencies Applicable to Principle 12				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 12:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 12, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 12 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 12 present?				
Is Principle 12 functioning?				

* Note: Record deficiencies in Deficiency Summary Template
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 13: Uses Quality Information
—Management should use quality information to achieve the entity's objectives.

Attributes

- Identification of Information Requirements—Management designs a process that uses the entity's objectives and related risks to identify the information requirements needed to achieve the objectives and address the risks. Information requirements consider the expectations of both internal and external users. Management defines the identified information requirements at the relevant level and requisite specificity for appropriate personnel.

- Relevant Data from Reliable Sources—Management obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Relevant data have a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. Sources of data can be operational, financial, or compliance related. Management obtains data on a timely basis so that they can be used for effective monitoring.

- Data Processed into Quality Information—Management processes the obtained data into quality information that supports the internal control system. This involves processing data into information and then evaluating the processed information so that it is quality information. Quality information meets the identified information requirements when relevant data from reliable sources are used. Quality information is appropriate, current, complete, accurate, accessible, and provided on a timely basis. Management considers these characteristics as well as the information processing objectives in evaluating processed information and makes revisions when necessary so that the information is quality information. Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.

Summary of Controls to Effect Principle 13				
Deficiencies Applicable to Principle 13				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls affecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 13:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 13, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 13 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 13 present?				
Is Principle 13 functioning?				

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 14: Communicate Internally
—Management should internally communicate the necessary quality information to achieve the entity's objectives.

Attributes

- Communication throughout the Entity—Management communicates quality information throughout the entity using established reporting lines. Quality information is communicated down, across, up, and around reporting lines to all levels of the entity.

- Appropriate Methods of Communication—Management selects appropriate methods to communicate internally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider follow:
  • Audience - The intended recipients of the communication
  • Nature of information - The purpose and type of information being communicated
  • Availability - Information readily available to the audience when needed
  • Cost - The resources used to communicate the information
  • Legal or regulatory requirements - Requirements in laws and regulations that may impact communication

Summary of Controls to Effect Principle 14				
Deficiencies Applicable to Principle 14				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 14:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 14, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 14 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 14 present?				
Is Principle 14 functioning?				

* Note: Record deficiencies in Deficiency Summary Template
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 15: Communicate Externally
—Management should externally communicate the necessary quality information to achieve the entity's objectives.

Attributes

- Communication with External Parties—Management communicates with, and obtains quality information from, external parties using established reporting lines. Open two-way external reporting lines allow for this communication. External parties include suppliers, contractors, service organizations, regulators, external auditors, government entities, and the general public.
- Appropriate Methods of Communication—Management selects appropriate methods to communicate externally. Management considers a variety of factors in selecting an appropriate method of communication. Some factors to consider follow:
  • Audience - The intended recipients of the communication
  • Nature of information - The purpose and type of information being communicated
  • Availability - Information readily available to the audience when needed
  • Cost - The resources used to communicate the information
  • Legal or regulatory requirements - Requirements in laws and regulations that may impact communication

Summary of Controls to Effect Principle 15				
Deficiencies Applicable to Principle 15				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 15:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 15, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 15 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 15 present?				
Is Principle 15 functioning?				
* Note: Record deficiencies in Deficiency Summary Template ** If there is a major deficiency, management must conclude that the internal control system is not effective.				
.				

Principle 16: Perform Monitoring Activities
—Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

Attributes

- Establishment of a Baseline—Management establishes a baseline to monitor the internal control system. The baseline is the current state of the internal control system compared against management's design of the internal control system.
  The baseline represents the difference between the criteria of the design of the internal control system and condition of the internal control system at a specific point in time. In other words, the baseline consists of issues and deficiencies identified in an entity's internal control system.
- Internal Control System Monitoring—Management monitors the internal control system through ongoing monitoring and separate evaluations. Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change. Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring.
- Evaluation of Results—Management evaluates and documents the results of ongoing monitoring and separate evaluations to identify internal control issues. Management uses this evaluation to determine the effectiveness of the internal control system. Differences between the results of monitoring activities and the previously established baseline may indicate internal control issues, including undocumented changes in the internal control system or potential internal control deficiencies.

Summary of Controls to Effect Principle 16				
Deficiencies Applicable to Principle 16				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 16:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 16, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 16 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 16 present?				
Is Principle 16 functioning?				

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Principle 17: Evaluate Issues and Remediate Deficiencies
—Management should remediate identified internal control deficiencies on a timely basis.

Attributes

- Reporting of Issues—Personnel report internal control issues through established reporting lines to the appropriate internal and external parties on a timely basis to enable the entity to promptly evaluate those issues.

- Evaluation of Issues—Management evaluates and documents internal control issues and determines appropriate corrective actions for internal control deficiencies on a timely basis. Management evaluates issues identified through monitoring activities or reported by personnel to determine whether any of the issues rise to the level of an internal control deficiency. Internal control deficiencies require further evaluation and remediation by management. An internal control deficiency can be in the design, implementation, or operating effectiveness of the internal control and its related process. Management determines from the type of internal control deficiency the appropriate corrective actions to remediate the internal control deficiency on a timely basis. Management assigns responsibility and delegates authority to remediate the internal control deficiency.

- Corrective Actions—Management completes and documents corrective actions to remediate internal control deficiencies on a timely basis. These corrective actions include resolution of audit findings. Depending on the nature of the deficiency, either the oversight body or management oversees the prompt remediation of deficiencies by communicating the corrective actions to the appropriate level of the organizational structure and delegating authority for completing corrective actions to appropriate personnel. The audit resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that (1) corrects identified deficiencies, (2) produces improvements, or (3) demonstrates that the findings and recommendations do not warrant management action. Management, with oversight from the oversight body, monitors the status of remediation efforts so that they are completed on a timely basis.

Summary of Controls to Effect Principle 17

Deficiencies Applicable to Principle 17

ID #	Internal control deficiency description	Evaluate severity of each internal control deficiency: (Do other controls effecting this principle compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
Evaluate deficiencies within Principle 17:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across Principle 17, represents a major deficiency** <Update Deficiency Summary Template >	<Explanation>			
Evaluate Principle 17 using judgment.**	Y/N	Explanation/Conclusion		
Is Principle 17 present?				
Is Principle 17 functioning?				

* Note: Record deficiencies in Deficiency Summary Template

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Deficiency Summary

Summary of Deficiencies								
ID #	Source of each internal control deficiency		Internal Control Deficiency Description	Risk Type and Level (Inherent, Control, or Combined; Low (L), Moderate (M), or High (H)	Deficiency type: Material Weakness (MW), Reportable Condition (RC) or Item-to-be-Revisited (IR); Is it a major deficiency? (Y/N)	Point of Contact	Corrective Action Plan & Date	Impact on Present/ Functioning	List other applicable internal control deficiencies from other principles that may have impacted this internal control deficiency
	Component	Principle							

This is an example Deficiency Summary template. Management may tailor to include additional columns to document other relevant information.

129

Component Evaluation – Control Environment				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
1. **Demonstrate Commitment to Integrity and Ethical Values**—The oversight body and management should demonstrate a commitment to integrity and ethical values.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
2. **Exercise Oversight Responsibility**—The oversight body should oversee the entity's internal control system.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

Component Evaluation – Control Environment				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
3. **Establish Structure, Responsibility, and Authority**—Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
4. **Demonstrate Commitment to Competence**—Management should demonstrate a commitment to recruit, develop, and retain competent individuals.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

Component Evaluation – Control Environment				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
5. **Enforce Accountability**—Management should evaluate performance and hold individuals accountable for their internal control responsibilities.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency**: (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Explanation/Conclusion		
Evaluate deficiencies across the Control Environment component:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across the Control Environment component, represents a major deficiency**				
Evaluate the Control Environment component using judgment based on the principles and listed deficiencies**		Yes/No		Explanation/Conclusion
Is the Control Environment component present?				
Is the Control Environment component functioning?				

* Note: Record deficiencies in Deficiency Summary Template.

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Component Evaluation — Risk Assessment				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
6. **Define Objectives and Risk Tolerances**—Management should define objectives clearly to enable the identification of risks and define risk tolerances.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
7. **Identify, Analyze, and Respond to Risks**—Management should identify, analyze, and respond to risks related to achieving the defined objectives.				
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

133

Component Evaluation — Risk Assessment

		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
8.	**Assess Fraud Risk**—Management should consider the potential for fraud when identifying, analyzing, and responding to risks.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
9.	**Identify, Analyze, and Respond to Change**—Management should identify, analyze, and respond to significant changes that could impact the internal control system.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Explanation/Conclusion		
Evaluate deficiencies across the Risk Assessment component:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across the Risk Assessment component, represents a major deficiency**				
Evaluate the Risk Assessment component using judgment based on the principles and listed deficiencies**		Yes/No		Explanation/Conclusion
Is the Risk Assessment component present?				
Is the Risk Assessment component functioning?				

* Note: Record deficiencies in Deficiency Summary Template.

** If there is a major deficiency, management must conclude that the internal control system is not effective.

Component Evaluation — Control Activities			
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
10. **Design Control Activities**—Management should design control activities to achieve objectives and respond to risks.			
ID # — Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
	Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
11. **Design Activities for the Information System**—Management should design the entity's information system and related control activities to achieve objectives and respond to risks.			
ID # — Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
	Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

135

Component Evaluation — Control Activities

	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
12. **Implement Control Activities –** Management should implement control activities through policies.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)	List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Explanation/Conclusion		
Evaluate deficiencies across the Control Activities component:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across the Control Activities component, represents a major deficiency**			
Evaluate the Control Activities component using judgment based on the principles and listed deficiencies**	Yes/No		
Is the Control Activities component present?			
Is the Control Activities component functioning?			

* Note: Record deficiencies in Deficiency Summary Template.
** If there is a major deficiency, management must conclude that the internal control system is not effective.

Component Evaluation — Information and Communication				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
13	**Use Quality Information –** Management should use quality information to achieve the entity's objectives.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
14	**Communicate Internally –** Management should internally communicate the necessary quality information to achieve the entity's objectives.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	

137

Component Evaluation — Information and Communication

		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
15	**Communicate Externally –** Management should externally communicate the necessary quality information to achieve the entity's objectives.			
ID #	Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
		Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
		Explanation/Conclusion		
Evaluate deficiencies across the Information and Communication component:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across the Information and Communication component, represents a major deficiency**				
Evaluate the Information and Communication component using judgment based on the principles and listed deficiencies**		Yes/No		
Is the Information and Communication component present?				
Is the Information and Communication component functioning?				

* Note: Record deficiencies in Deficiency
Summary Template.
** If there is a major deficiency, management must conclude that the
internal control system is not effective.

Component Evaluation — Monitoring			
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
16 **Perform Monitoring Activities –** Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.			
ID # Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
	Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
17 **Evaluate Issues and Remediate Deficiencies –** Management should remediate identified internal control deficiencies on a timely basis.			
ID # Internal control deficiency description	**Evaluate severity of each internal control deficiency:** (Do the controls of other principles within and across components compensate this internal control deficiency?)		List other internal control deficiencies associated with other principles that may impact this deficiency
	Is this a major deficiency? (Y/N)	Comments/Compensating Controls	
	Explanation/Conclusion		
Evaluate deficiencies across the Monitoring component:* Evaluate if any internal control deficiency or combination of internal control deficiencies, when considered across the Monitoring component, represents a major deficiency**			
Evaluate the Monitoring component using judgment based on the principles and listed deficiencies**	Yes/No		
Is the Monitoring component present?			
Is the Monitoring component functioning?			

* Note: Record deficiencies in Deficiency Summary Template.
** If there is a major deficiency, management must conclude that the internal control system is not effective.

139

Overall Internal Control System Assessment

Overall Internal Control System Assessment			
Name of Organization:			
Type of Objective:	Risk Assessment Considerations		
Operations			
Reporting			
Compliance			
Internal Control Component # (1-5):	Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
1. Control Environment			
2. Risk Assessment			
3. Control Activities			
4. Information and Communication			
5. Monitoring			
Are all components operating together in an integrated manner? Do the combination of internal control deficiencies represent a major deficiency when aggregated across all five components? If yes, explain.*			
Is the overall internal control system effective? <Y/N>*			
Basis for conclusion			

* If there is a major deficiency, management must conclude that the internal control system is not effective.

140

LIST OF REFERENCES

Allen, B. B. (2014). Lean risk assessments. *Internal Auditor, 71*(5), 24–25.

American Institute of Certified Public Accountants. (2002). Management antifraud programs and controls: Guidance to help prevent and deter fraud. *AICPA*. Retrieved from http://www.mtsu.edu/audit/Management_Antifraud_Programs_and_Controls_1_.pdf

American Institute of Certified Public Accountants. (2005). Management override of internal controls: The Achilles' heel of fraud prevention. *AICPA*. Retrieved from http://www.aicpa.org/ForThePublic/AuditCommitteeEffectiveness/DownloadableDocuments/achilles_heel.pdf

Association of Certified Fraud Examiners. (2004). *2004 report to the nation on occupational fraud and abuse*. Austin, TX: ACFE, 18.

Association of Government Accountants. (2006). *PAR: The report we hate to love. AGA CPAG Research Series Report, 6*(18).

The Big 4 Accounting Firms. (2015). The Big 4 accounting firms. Retrieved from http://www.big4accountingfirms.org/

Blair, D. R. (2011, September 23). *Financial management and internal control challenges at the Department of Defense. Statement to the Subcommittee on Government Organization, Efficiency, and Financial Management*. Retrieved from *http://www.dodig.mil/iginformation/IGInformationReleases/DoDIG_Testimony_Final%20(HOGR-20110923).pdf*

Bokhari, T., Simon, J., & Gathings, T. (2014). A next-generation vendor risk management program. *RMA Journal, 97*(4), 20–26.

Bresnahan, K. (2007). Sustaining internal control programs: What to do in the long run. *The Journal of Government Financial Management, 56*(1), 45–48. Retrieved from http://search.proquest.com/docview/222379892?accountid=12702

Brook, D. A. (2011). Exploring the value of financial statement audits. *The Journal of Government Financial Management, 60*(1), 38–43.

Chen, Y., Smith, A. L., Cao, J., & Xia, W. (2014). Information technology capability, internal control effectiveness, and audit fees and delays. *Journal of Information Systems, 28*(2), 149–180.

Committee of Sponsoring Organizations of the Treadway Commission. (2013a). *Executive summary*. Vol. 1 of *Internal control, integrated framework*. Durham, NC: Committee of Sponsoring Organizations of the Treadway Commission.

Committee of Sponsoring Organizations of the Treadway Commission. (2013b). *Framework and appendices*. Vol. 2 of *Internal control, integrated framework*. Durham, NC: Committee of Sponsoring Organizations of the Treadway Commission.

Committee of Sponsoring Organizations of the Treadway Commission. (2013c). *Illustrative tools for assessing effectiveness of a system of internal control*. Vol. 3 of *Internal control, integrated framework*. Durham, NC: Committee of Sponsoring Organizations of the Treadway Commission.

Committee of Sponsoring Organizations of the Treadway Commission. (2013d). *Internal control over external financial reporting: A compendium of approaches and examples*. Vol. 4 of *Internal control, integrated framework*. Durham, NC: Committee of Sponsoring Organizations of the Treadway Commission.

Commons, G. C. (2012). *Statement of the Honorable Gladys J. Commons, Assistant Secretary of the Navy, before the House Armed Services Committee Subcommittee on Oversight and Investigations on Department of Defense Auditability Challenges*. Retrieved from http://armedservices.house.gov/index.cfm/files/serve?File_id=0e62aebd-3a08-4870-9e5d-b3ad3db6a378

Congress of the United States of America. (1994, January 25). Government Management Reform Act of 1994. One Hundred Third Congress of the United States of America. Retrieved from: http://govinfo.library.unt.edu/npr/library/misc/s2170.html

Cook, C. E. (2015, January). Department of the Navy PPBE and fiscal review. Presented at Pentagon, Washington, D.C.

Cosmin, D. E. (2011). Enhancing assets' protection through an adequate monitoring of internal control system by internal audit. *Annals Of The University Of Oradea, Economic Science Series, 20*(2), 491–497.

Deloitte. (2004). *Internal audit services*. Unpublished manuscript. Retrieved from https://www.deloitte.com/assets/Dcom-Russia/Local%20Assets/Documents/ru_internalauditservices_050204.pdf

Department of Defense Inspector General. (2011, June 8). *Additional actions can improve Naval Air Systems Command's use of undefinitized contractual actions*, D-2011-068. Alexandria, VA: Author. Retrieved from http://www.dodig.mil/pubs/documents/D-2011-068.pdf

Department of Defense Inspector General. (2012, February 13). *Navy enterprise resource planning system does not comply with the Standard Financial Structure and U.S. Government Standard General Ledger*, D-2012-051. Alexandria, VA: Author. Retrieved from http://www.dodig.mil/audit/reports/fy12/DODIG-2012-051.pdf

Department of the Navy Naval Audit Service. (n.d.). Naval Audit Service. Retrieved from http://www.secnav.navy.mil/navaudsvc/Pages/default.aspx

Department of the Navy Office of the Chief of Naval Operations. (2014, May). *Fiscal Year 2014 Managers' Internal Control Program reporting requirements*. Washington, DC: Author. Retrieved from http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5200.1044.pdf

Executive Office of the President Office of Management and Budget. (n.d.). Office of Federal Financial Management Federal Financial Management Improvement Act (FFMIA). Washington, DC: Author. Retrieved from http://www.whitehouse.gov/omb/financial_ffs_ffmia

Executive Office of the President Office of Management and Budget. (2004, December 21). *OMB Circular A-123 - Management's responsibility for internal control*. Washington, DC: Author. Retrieved from http://www.whitehouse.gov/omb/circulars_a123_rev

EY. (2012, July). *The future of internal audit is now*. Unpublished manuscript. Retrieved from http://www.ey.com/Publication/vwLUAssets/Future_IA/$FILE/1204-1354105_Future%20IA%20whitepaper_FINAL.pdf

Gotbaum, J. (2001, January 4). Memorandum for the heads of executive departments and establishments, Chief Financial Officers, and Inspectors General. Executive Associate Director and Controller. Retrieved from http://www.whitehouse.gov/sites/default/files/omb/financial/ffmia_implementation_guidance.pdf

Haas, S., Abdolmohammadi, M. J., & Burnaby, P. (2006). The Americas literature review on internal auditing. *Managerial Auditing Journal, 21*(8), 835–844.

Hale, R. F. (2014, May 13). *Statement of the Honorable Robert F. Hale, Under Secretary of Defense (Comptroller)/Chief Financial Officer, before the United States Senate Committee on Homeland Security and Governmental Affairs*. Retrieved from http://comptroller.defense.gov/Portals/45/documents/micp_docs/Reference_Documents/Hale-testimony-2014-05-13.pdf

Hermanson, D. R., Smith, J. L., & Stephens, N. M. (2012). How effective are organizations' internal controls? Insights into specific internal control elements. *Current Issues In Auditing, 6*(1), A31-A50. doi:10.2308/ciia-50146

The Institute of Internal Auditors. (2009). *Internal Audit Capability Model (IA-CM) for the public sector*. Retrieved from https://na.theiia.org/iiarf/Public%20Documents/Internal%20Audit%20Capability%20Model%20IA-CM%20for%20the%20Public%20Sector%20Overview.pdf

The Institute of Internal Auditors. (n.d.). Definition of internal auditing. Retrieved March 22, 2015 from http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%BCdefinition

The Institute of Internal Auditors, The American Institute of Certified Public Accountants, and Association of Certified Fraud Examiners. (2008). Managing the business risk Of fraud: A practical guide. Retrieved March 28, 2015 from http://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf

Ionescu, l. (2011). Monitoring as a component of internal control systems. *Economics, Management & Financial Markets, 6*(2), 800–804.

Koutoupis, A. G. (2007). Documenting internal controls. *Internal Auditor, 64*(5), 23–27.

KPMG. (2014). *Transforming internal audit through critical thinking*. Retrieved from https://www.kpmg-institutes.com/content/dam/kpmg/advisory-institute/pdf/2014/transform-internal-audit-critical-thinking.pdf

Lenz, R., & Hahn, U. (2015). A synthesis of empirical internal audit effectiveness literature pointing to new research opportunities. *Managerial Auditing Journal, 30*(1).

Leung, P., & Cooper, B. (2006). The Americas literature review on internal auditing. *Managerial Auditing Journal, 21*(8), 809–810.

Liebesman, S. (2012). Revised thinking. *Quality Progress, 45*(4), 61–63. Retrieved from http://search.proquest.com/docview/1013474807?accountid=12702

Mulcahy, V. (2008). Reintroducing segregation of duties (with muscle). *The RMA Journal, 91*(1), 90–93, 99. Retrieved from http://search.proquest.com/docview/209774088?accountid=12702

Office of Financial Operations. (n.d.-a). *DON Managers' Internal Controls (MIC) Program.* Retrieved from http://www.fmo.navy.mil/Divisions/FMO4/don_managers_internal_control_program.html

Office of Financial Operations. (n.d.-b). *Internal Controls over Financial Reporting Program (ICOFR).* Retrieved from http://www.fmo.navy.mil/Divisions/FMO4/internal_controls_over_financial_reporting_program.html

Office of Financial Operations. (n.d.-c). *Financial Improvement and Audit Readiness (FIAR) Program.* Retrieved from http://www.fmo.navy.mil/Divisions/FMO4/financial_improvement_program.html

Office of the Under Secretary of Defense (Comptroller). (n.d.). Financial Improvement and Audit Readiness FIAR Plan. Retrieved from http://comptroller.defense.gov/fiar/fiar_plan.aspx

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer. (2014). Financial Improvement and Audit Readiness (FIAR) Plan status report. United States Department of Defense. Retrieved from http://comptroller.defense.gov/Portals/45/documents/fiar/FIAR_Plan_November_2014.pdf

Pitt, S. A. (2014). Internal audit quality: Developing a quality assurance and improvement program. Hoboken, NJ: John Wiley & Sons.

Porter, B., Simon, J., & Hatherly, D. J. (2014). *Principles of external auditing.* Hoboken, NJ: Wiley.

Prawitt, D. (2013). Put COSO Update to work. *Journal of Accountancy, 216*(1), 20.

Protiviti. (2006, June 19). *Internal auditing around the world vol. II.* Unpublished manuscript Protiviti Inc. Retrieved from http://itraining.protiviti.com/KnowledgeLeader/Content.nsf/Web+Content/ProtivitiBookletsVolumeIIIAPerformerProfiles!OpenDocument

Protiviti. (2014). *The updated COSO internal control framework* (2nd ed.). Protiviti, Inc. Retrieved from http://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf

Public Company Accounting and Oversight Board. (2007). Auditing Standard No. 5. Retrieved from http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx

PWC. (2014, March). *2014 state of the internal audit profession study.* Unpublished manuscript. Retrieved from http://www.pwc.com/en_M1/m1/publications/documents/pwc-state-of-the-internal-audit-profession-2014.pdf

Rendon, R. G., and Rendon, J. M. (in press). Auditability in public procurement: An analysis of internal controls and fraud vulnerability. *International Journal of Procurement Management.*

Richards, D. (2006). The future of the internal audit profession. *Managerial Auditing Journal, 21*(8), 869–871.

The Secretary of the Navy. (2008, June 2). *Department of the Navy Managers' Internal Control Manual* (SECNAV M-5200.35). Washington, DC: The Assistant Secretary of the Navy (Financial Management and Comptroller). Retrieved from http://www.fmo.navy.mil/documents/Divisions/FMO4/FIAR/MIC/SECNAV%20M-5200%2035%20PRINTED%20FINAL%20June%202008.pdf

The Secretary of the Navy. (2014, July 21). *Department of the Navy Managers' Internal Control Program* (SECNAVINST-5200.35F). Washington, DC: The Assistant Secretary of the Navy (Financial Management and Comptroller). Retrieved from http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5200.35F%20.pdf

The Secretary of the Navy. (n.d.). *Department of the Navy Managers' Internal Control Manual* (SECNAV M-5200.35). Washington, DC: The Assistant Secretary of the Navy (Financial Management and Comptroller). Retrieved from http://www.secnav.navy.mil/navaudsvc/Pages/default.aspx

Serbu, J. (2014). DOD awards contracts for its first large-scale financial audit. Retrieved on April 4, 2015 from http://www.federalnewsradio.com/522/3758534/DOD-awards-contracts-for-its-first-large-scale-financial-audit

Spillan, J. E. and Ziemnowicz, C. (2011). Who is in charge? Cases of not managing internal controls in nonprofit organizations. *Journal of Business, Society, & Government*, *(3)*1, 4–20.

Spoehr, W. D. (2012). Consequences of disconnects of 'tone at the top' at the institutional and operational level. *Financial Executive, 28*(10), 68–69.

Trudell, C. (2014). Internal audit's role in the risk assessment process at KeyCorp. *Journal Of Risk Management In Financial Institutions, 7*(4), 370–374.

Tsay, B. (2010). Designing an internal control assessment program using COSO's guidance on monitoring. *CPA Journal, 80*(5), 52–57.

United States Government Accountability Office. (2011, December). *Government auditing standards* (GAO-12-331G). Washington, DC: Comptroller General of the U.S. Retrieved from http://gao.gov/assets/590/587281.pdf

United States Government Accountability Office. (2014, June). *DOD financial management: The Defense Finance and Accounting Service needs to fully implement financial improvements for contract pay* (GAO-14-10). Washington, DC: Comptroller General of the U.S. Retrieved from http://www.gao.gov/products/GAO-14-10

United States Government Accountability Office. (2014, September). *Standards for internal control in the federal government* (GAO-14-704G). Washington, DC: Comptroller General of the U.S. Retrieved from http://www.gao.gov/assets/670/665712.pdf

Weaver. (2013, December). COSO 17 principles. Retrieved from http://weaver.com/blog/coso-framework%E2%80%99s-17-principles-effective-internal-control

Wells, J. T. (2006). When the boss trumps internal controls. *Journal of Accountancy, 201*(2), 55–57.

Whittington, R., & Pany, K. (2014). *Principles of auditing & other assurance services* (19th ed.). New York: McGraw-Hill/Irwin.

Whittington, R., & Pany, K. (2011). *Principles of auditing & other assurance services* (18th ed.). Boston: McGraw-Hill/Irwin.

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal*. Retrieved from http://wweb.uta.edu/faculty/subraman/EMBA-FTW2009/Articles/Fraud%20Diamond%20Four%20Elements.CPAJ2004.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1.   Defense Technical Information Center
       Ft. Belvoir, Virginia

2.   Dudley Knox Library
       Naval Postgraduate School
       Monterey, California