AN ANALYSIS OF HOW CYBERSECURITY RELATES TO FINANCIAL AUDITABILITY

by

Francis R. Lust Sr.

A Capstone Project Submitted to the Faculty of

Utica College

August 2017

in Partial Fulfillment of the Requirements Course CYB-695

Master of Science in
Cybersecurity

Abstract

The United States Department of Defense (DoD) has yet to comply with the Chief Financial Officers Act of 1990, which requires the DoD to produce auditable financial statements. The purpose of this research is to study the financial and efficiency losses organizations within the DoD suffer by researching the DoD's reliance on legacy IT systems and current internal business controls. This research will explore the relationship between financial auditability and cybersecurity in an effort to take advantage of commonalities within both disciplines to find areas of efficiencies and true cost savings.

This research will focus on the problems preventing the DoD's compliance with federal regulations, such as unsupported journal vouchers. The DoD is a large and complex federal agency, which relies on hundreds of financial information systems. Some these financial information systems are legacy financial information systems, which have evolved over many years and now include complex and entwined functionality. In some cases, replacing the financial information system successfully is simply not feasible. This research project will involve techniques to mitigate the impact of relying on legacy financial information systems.

An important part of this research will focus on the Financial Improvement and Audit Readiness (FIAR) guidance and best practices to implement strong internal business controls and cybersecurity controls to achieve audit readiness (FIAR, 2017). The research methodology is to compare the strengths and weaknesses of the legacy IT systems from an internal business controls perspective and a cybersecurity perspective. In addition, this research project includes the impact of human behavior, as it relates to financial auditability.

Keywords: Cybersecurity, Financial Auditability, Internal Controls, Audit readiness, DoD Legacy Systems, Unsupported Journal Vouchers, FIAR Guidance, CUECs, CSOCs, Michael Sanchez

Acknowledgements

First, there are far too many wonderful people to list here by name, many of whom have had a direct impact upon my entire educational career. However, I would like to acknowledge my wife and my children for their continued support and their many sacrifices, as challenges and deadlines approached. I would like to acknowledge the several local, state, and federal law enforcement professionals, who have shared their expertise and offered their encouragement, in my pursuit of higher education. I would like to acknowledge the long list of educators, who were not only able to teach, but able to inspire. Many of these educators proved to be an invaluable resource in providing both the confidentiality and the highly technical information, which was critical in closing numerous criminal cases throughout my law enforcement career. Finally, I would like to acknowledge those few, but exceptional supervisors, within my chain of command and throughout my professional career, who have shown true leadership, professionalism, and integrity by their own example, and who have created a specialized working environment for their employees to learn, grow, and achieve.

Table of Contents

Introduction

In the history of the world, auditing financial records traces back centuries to an era long before the advent of computer systems (Pava, n.d.). However, it was the development of the railroad and the transportation of goods that made auditing a requirement for businesses (Pava, n.d.). In the beginning, achieving auditability required manual processes, which means humans must record or enter the data by hand, instead of using a more efficient and more visible automated process, which is available today (Kutz, Gregory, 2002). Manual processes lead to human error, duplication of data, and the inability to integrate data with other computer systems easily (Kutz, Gregory, 2002). The inability to integrate data with other computer systems means the computer systems cannot share data correctly (Kutz, Gregory, 2002). The error-ridden manual processes add a high cost factor to normal business operations (Kutz, Gregory, 2002).

The advent of automated computer systems was far from a quick fix to manual auditing because auditors did not immediately adopt and implement computer systems into the auditing process. Auditors needed time to assure themselves that computerized systems were reliable. The first computers were limited in terms of memory size and processing power, which made it impossible to create the sophisticated systems available today (Shelly, Cashman, & Forsythe, 1985). In order to process data in the central processing unit of a computer system, the computer system must be able to hold the operating system instructions, the application instructions, and the data within the main memory of the computer system's central processing unit. (Shelly, Cashman, & Forsythe, 1985). In addition, the cost of early computer systems was out of reach for most businesses (Ensmenger, 2003).

However, the audit world gradually came to accept computer systems. Whether through systematic or manual processes, auditing now relies on general accepted auditing principles. The

necessary standards for financial reporting by all organizations are general accepted auditing principles, which are a collaboration of public and private concepts (Financial Accounting Foundation, n.d.). The Financial Accounting Standards Board sets financial standards for public and private organizations (Financial Accounting Foundation, n.d.). The Government Accounting Standards Board sets financial standards for government organizations (Financial Accounting Foundation, n.d.). Financial reporting is the universal method of communicating the condition of public or private organization's financial statements (Financial Accounting Foundation, n.d.). Standards are necessary to ensure all entities are describing the financial statements of their respective organizations in the same manner.

Legacy information technology (IT) systems are IT systems that no longer serve a useful purpose when modern technology is implemented (DSecretary of the Army, 2016). For the purposes of this research, legacy systems will include automated systems as well as manual processes. A manual process must exist prior to automation because the manual process is the basis for the automation. The challenge is to automate the process with increased efficiency, increased accuracy, and reduced overall cost. Manual processes and system processes that are no longer auditable in today's business environment are legacy processes. For example, timesheets require specific data elements for auditability purposes, such as the date signed by the employee, the date signed by the approver, and the name of the approver. If there is only one date on the timesheet or the handwritten approver's signature is not legible, the manual process is a legacy process in today's business environment. In the timesheet example, if there were provisions to accept digital signatures that are electronically timestamped and legible, the timesheet would be auditable and the manual process would no longer be a legacy process.

There is an important effort within the U.S. Army to improve their network services, as described in the following excerpt:

> Critical to this effort is the elimination of legacy information technology (IT) hardware, software, and services. Legacy IT is IT that has no functional benefit to the Army's network upon delivery of modernized technology. Legacy IT includes duplicate networks, equipment replaced during integration with the Joint Information Environment, unnecessary and unused software, and IT services that no longer fulfill a requirement. Elimination of costs associated with operating and maintaining unnecessary legacy IT will increase resources available to operate the modernized network. (DSecretary of the Army, 2016, p. 1)

Missing from the United States (U.S.) Army's definition is the age of the legacy systems. For example, a poorly designed IT system, which does not interface well with other dependent IT systems, could be a legacy system very soon after deployment. With a failure rate of 50% to 80%, many systems never make it to deployment (Dorsey, 2005). Legacy systems and business processes may not necessarily be old, but systems and processes that no longer serve a useful purpose in today's business environment are legacy (DSecretary of the Army, 2016).

Internal business controls are steps taken by management and employees to provide the necessary oversight and assurance that business objective are being met (Kutz, 2014). Internal business controls consist of efficiency of business operations, reliability of data, and compliance with applicable statues (Kutz, 2014). Management can set business priorities, define business objectives, and design internal controls, but it is the organization's staff that implements and operates internal business controls (Kutz, 2014). In other words, internal business controls are dependent on capable and engaged personnel.

Background

The United States federal government is comprised of many agencies and offices. For example, the U.S. Army is a unique agency within the federal government. The U.S. Army is partly under the purview of the Assistant Secretary of the Army (OASA) Financial Management & Comptroller (FM&C) (HQDA Org, 2014). As compared to smaller entities, such as the Department of Defense, Office of the Inspector General (DoDIG), the U.S. Army is a large government organization with a significant level of complexity. The size and complexity of the U.S. Army is evident by the significant number of Secretariat Offices and U.S. Army Staff, which includes service members, civilians, and contractors. In addition, the U.S. Army relies on many legacy IT systems to produce a financial statement, which becomes part of the Department of Defense's financial statement. As of 2016, the U.S. Army's inability to report correct financial information has affected the entire Department of Defense (DoD) (Paltrow, 2016).

In January of 1990, Congress passed the Chief Financial Officers Act of 1990, which required government agencies to produce "…complete, reliable, timely, and consistent financial information…" (United States Congress, 1990, p. 1). While the DoD has made some progress, the DoD has yet to comply with the Chief Financial Officers Act of 1990. The Financial Improvement and Audit Readiness (FIAR) team first provided guidance to DOD organizations, such as the U.S. Army, United States Navy, United States Air Force, United States Marine Corp, Defense Logistics Agency, and others in December of 2005 (FIAR, 2005). The FIAR team discussed the 11 material weakness that the DoDIG identified (FIAR, 2005). A material weakness is an internal control that is not operating effectively and has the potential to affect the accuracy of an organization's financial statement (FIAR, 2005; Center for Audit Quality, n.d.). The 11 material weaknesses identified by the DoDIG relate to the following:

- Financial management systems
- Transactions within government agencies
- Unsupported adjustments
- Reconciliation with the United States Treasury
- Activities that create risks to the environment
- Depreciation of DOD owned property
- DoD property issued to contractors
- Valuation of inventory
- Method of tracking operating materials and supplies
- Total cost to achieve the mission
- Reconciliation of obligations (FIAR, 2005, p. 22)

Additional cybersecurity controls are necessary to discover and mitigate the effects of material weaknesses. Cybersecurity controls are a subset of general IT controls because general IT controls include more than just those IT controls that focus on cyber security risk (Waterman, 2017). The Under Secretary of Defense (Comptroller) provided the DoD management with five steps to improve financial management, such as discovery and correction, validation, assertion, assessment, and audit (FIAR, 2005). Management's responsibility is to review controls, standard operating procedures, and processes to identify system deficiencies (FIAR, 2005). In addition, management's responsibility is to implement corrective action plans (CAPs) and validate that new controls are working (FIAR, 2005; OMB Circular A-123, 2004). Once validation of the new controls is complete, management must assert the reliability of the organization's financial systems, processes, and financial statements (FIAR, 2005). The DoDIG's responsibility is to assess the effectiveness of the new control and audit as necessary (FIAR, 2017).

In 2005, there was progress in reducing unsupported journal vouchers (JVs). Journal vouchers serve a legitimate purpose in the auditing world, which is to provide an auditable record of the underlying financial transactions (Investor Words, 2017). Supported JVs provide enough information for auditors to trace the JVs back to the original obligating document, which must contain sufficient transaction level details (DoDIG-113, 2016). Unsupported JVs indicate there is not enough documentation for auditors to determine whether the underlying transactions are legitimate (DoDIG-113, 2016). The DoDIG reported a reduction in unsupported JV's from 2.3 trillion dollars in 1999 to just 250 billion dollars in unsupported JVs in 2005 (FIAR, 2005). The reduction in unsupported JVs in 2005 was misleading and temporary because unsupported JVs increased significantly from the amounts reported in 2005 (DoDIG_2016_113, 2016).

The inability to support a JV with sufficient documentation is what results in the unsupported JV classification (DoDIG D_2008_084, 2008). The basic process begins with the generation of some type of key supporting document (KSD), which creates a future obligation. When the requirements contained within the initial KSD are satisfied, a disbursement matching the initial obligation must occur. The initial KSD will contain all the detail necessary to support the obligation. However, the data elements from the initial KSD may pass through many computer systems and lose some data elements before the disbursement occurs. "There are a variety of systems that must be considered in audit readiness efforts, including but not limited to: general ledger systems, source/feeder systems, system interfaces, disbursing systems, reporting systems, and property management systems (FIAR, 2017, p. 47). Each system will have interfaces with input control points, processing control points, and output control points (FIAR, 2017). If each interface works correctly through each system, the disbursement, which is the actual funds paid out, can occur correctly. However, if some of the system interfaces or controls

points are broken the disbursement may occur incorrectly or not at all. Auditability requires sufficient controls in place to maintain the integrity of the data throughout each processing step.

The Defense Civilian Personnel Data System (DCPDS) is a DoD example of the number of systems and interfaces data must process through correctly. The DCPDS is a custom-off-the-shelf human resources data system, which is web-based and customizable (DCPAS, 2017). The DCPDS is a complex system, which supports 26 functional areas of human resources records management (DCPAS, 2017). The DCPDS contains process rules exceeding 500,000 and nearly 2 million pay and benefit algorithms, all of which must communicate with more than 40 external systems (DCPAS, 2017). The DCPDS is a good example because it is typical of the level of complexity and interconnectivity within DoD information systems. There are certainly many opportunities for data to process incorrectly and lead to an unsupported JV.

Statement of the Problem

In 2015, the DoDIG published a finding that the OASA FM&C and the Defense Finance Accounting Service (DFAS) were unable to support 6.5 trillion dollars in journal vouchers in fiscal year 2015 (DoDIG-113, 2016). The DoDIG attributed the primary issue to deficient IT systems (DoDIG-113, 2016). The government accounting service that currently processes the U.S. Army General Fund's financial transactions is DFAS. According to the DoDIG, the OASA FM&C, which is the reporting entity and the DFAS, which is the service provider did not correct the system deficiencies responsible for the errors that made JV adjustments necessary (DoDIG-113, 2016). The 6.5 trillion dollars in unsupported JVs represents a sharp increase from the 250 billion dollar amount of unsupported JVs discovered in 2005. In addition, this sharp increase is indicative of a much larger problem, which requires a more in-depth analysis to determine and to mitigate the root cause of this problem.

In considering other large Department of Defense organizations, such as the United States Navy, there are additional financial and efficiency losses. The Navy did not design its legacy financial systems with enough visibility of the transaction level detail necessary to achieve auditability (DODIG_051, 2012). Large organizations can suffer financial and efficiency losses, due to the use of legacy IT systems (Kelly, Holland, Gibson, & Light, 1999; Thornton, 2017). To correct the financial and efficiency losses, the Navy has implemented an enterprise resource planning (ERP) system which will provide "financial transparency" and increase "effectiveness and efficiency" throughout the Navy's financial systems (DODIG_051, 2012, p. 1). An ERP system combines many business processes, such as financial records, human resources, and other day-to-day business processes into one cohesive system (Microsoft, 2017b). However, ERP systems alone cannot provide the entire solution because the input data

is dependent on the quality of the organization's internal business processes and controls (DODIG_051, 2012). ERP systems can provide a platform the achieve audit readiness, but an ERP cannot "…guarantee audit readiness…" (DODIG_051, 2012, p. 1). In another example, the U.S. Army uses many legacy IT systems to process business data (McNermey, 2003). The U.S. Army's inability to provide auditable financial records has led to trillions of dollars in unsupported journal vouchers (DoDIG-113, 2016). According to the DoDIG, the unsupported JVs are the result of a failure of the OASA FM&C and DFAS to prioritize system deficiencies properly (DoDIG-113, 2016). The unsupported journal vouchers indicate a need for further research to determine and to mitigate to root cause of the unsupported JVs. Financial records are auditable or clean when an auditor's review results in an unqualified or unmodified opinion, asserting that the auditor finds the financial records to be compliant with general accepted auditing principles (Farlex, 2012). Auditable records are necessary to support the reliability of financial statements.

The inability to provide auditable records of budgetary resources, commonly known as Statements of Budgetary Resources is not a new problem for the U.S. Army (Smithberger, 2016; DoDIG_2015_144, 2015). This inability to provide clean or auditable Statements of Budgetary Resources has existed since before Congress required all federal agencies to be audit ready by passing the Chief Financial Officers Act in 1990 (Smithberger, 2016). However, the 6.5 trillion dollars in JV adjustments occurred as recently as fiscal year 2015. This fact indicates previous research has not provided a suitable solution to mitigate the risk of unsupported JV adjustments. In 2017, independent public accountants (IPAs) found system control deficiencies within the U.S. Army's IT systems (GAO_17_85, 2017). In addition to general control deficiencies in access controls, segregation of duties, and configuration management, the IPA for the Army

"…identified information system general control deficiencies in security management and information contingency planning" (GAO_17_85, 2017). The U.S. Army is currently reviewing its use of legacy IT systems in an effort to improve IT services, increase security, and reduce costs (DSecretary of the Army, 2016). Keeping pace with evolving technology requires continual research and understanding in order to develop and implement sufficient mitigation techniques to minimize the impact on the organization's financial statement.

Examining the relationship between cybersecurity and financial auditability will hone in on some vulnerabilities presented by the reliance on legacy IT systems, help to mitigate risks, and find areas of true cost savings. This study will explore methods to improve an organization's underlying business processes and auditability through more effective cybersecurity controls and monitoring activities. Organizational leaders, business managers, financial managers, accountants, IT professionals, cybersecurity professionals, and analysts can benefit from the research. In addition, every user can benefit from this research because the organization's users are performing the internal business controls and the cybersecurity controls, which are in place to mitigate the risk to the organization's financial statement. The lines of financial auditing and cybersecurity have blended is such a way that every member of the organization must be at least some exposure and understanding, from entry level to the top of leadership.

Purpose of the Study

The purpose of this research is to examine the financial and efficiency losses organizations within the Department of Defense suffer by researching the DoD's reliance on legacy IT systems and current internal business controls. The research methodology is to compare the strengths and weaknesses of the legacy IT systems from an internal business

controls and cybersecurity perspective. In 2010, the FIAR team began providing guidance and continual updates to the DoD on methodology and best practices to achieve audit readiness (FIAR, 2017). An important part of this research will focus on the FIAR Guidance (FIAR, 2017). Through this research, one can better understand the importance of the relationship between effective cybersecurity controls and financial auditability.

Research Questions

The three questions this research will investigate are as follows:

Q1. What is the relationship between financial auditability and cybersecurity?

Q2. What aspects of legacy IT systems create risk factors to the Department of Defense Organization's financial statement?

Q3. How can the Department of Defense Organization's mitigate financial risk when use of legacy IT systems is necessary?

Literature Review

The capability of producing an unmodified auditor's opinion of financial records has eluded the DoD for over twenty-five years. Many professionals from various entities inside and outside the DoD have worked tirelessly on improving the quality of the DoD's financial reporting. The DoD is a complex organization made up of a large number of other defense organizations. To receive an unmodified auditor's opinion, each organization within the DoD must be able to provide an unmodified auditor's opinion. This project will research peer-reviewed sources, United States Government Accountability Office (GAO) reports, DoDIG reports, testimony before Congress, scholarly journal articles, FIAR guidance, National Institute of Standards and Technology (NIST) publications, The Federal Information Security Management Act, and the Federal Information System Controls Audit Manual (FISCAM) standards. In addition, this project will research decisions made by authorized officials over the past 25 years. Examination of the above research provides a representative view the effort by the DoD to produce auditable financial records.

Auditors focus on IT systems, internal business process controls, and cybersecurity controls at the reporting entity and any other entity that processes the data (FIAR, 2017). In addition, all IT systems that process the data, including micro-application IT systems must be auditable (FIAR, 2017). Microsoft Excel formulas can be simple or complex (Microsoft, 2017a). For example, many organizations use Excel spreadsheets as part of their data processing, but Excel spreadsheets are not secure and Excel spreadsheets are not easily auditable (Host Analytics, 2015). In fact, data in Excel spreadsheets is not always accurate (Host Analytics, 2015). Though not auditable as part of a financial processing system, Excel formulas can provide reporting entities with real value when conducting monitoring activities.

The relationship between cybersecurity and auditability is important when considering legacy business processes, legacy IT systems, ERP systems, financial managers and other employees, technological growth, and cultural changes. The goal of this research is to examine the risks and vulnerabilities the DoD is experiencing in its effort to provide clean and auditable financial records from a cybersecurity perspective and from an auditability perspective. In addition, this research will evaluate best practices to mitigate the risks of the DoD providing unreliable financial statements from both perspectives.

Cybersecurity controls.

Simply stated, cybersecurity controls are those IT controls that focus on risk to an organization from a cybersecurity standpoint, which is "…a relatively new pain point in corporate audits" (Whitehouse, 2015, p. 1). Cybersecurity or "…information technology security, focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change, or destruction" (University of Maryland University College, 2017, p. 1). Many public and private organizations collect, store, and transmit sensitive information, which the organizations must be protect from an increasing number of cyber-attacks, regardless of the where the data is located. (University of Maryland University College, 2017). Organizations must protect all forms of the sensitive data "…such as: data-in-transit and data-at-rest" (Bhadauria, Borgohain, R. Biswas, & A. Sanyal, 2014, p. 189).

Cybersecurity and auditing are no longer mutually exclusive functions because both disciplines involve mitigating risk to the organization. According to Worth MacMurray, senior vice president at compliance services provider GAN Integrity, aligning cybersecurity professionals and auditors is an important function of a chief compliance officer (Whitehouse, 2015). Sandy Herrygers, a partner and IT specialist at Deloitte finds that cybersecurity programs

include financial reporting controls, operational controls, and processing controls, while auditing is more narrowly concerned with system controls that impact financial reporting (Whitehouse, 2015).

In a survey conducted by KPMG in 2014, nearly half of the United States audit committee members surveyed indicated their audit committee oversees their organization's cyber security risk (Bell, 2014). According to Bell, management should use a dashboard or scorecard and conduct periodic risk assessments to monitor cyber activity (Bell, 2014). In addition, the main areas of cybersecurity risks are around "…cyber security leadership and governance, human factors or 'people risks', legal and regulatory compliance, business continuity, operations and technology, and information risk" (Bell, 2014, p. 1). These main areas of cybersecurity risk are the focus of cybersecurity controls.

Accountability

Every organization is accountable to someone or some entity. For example, a small business is accountable to its customer base, its suppliers, the Department of Commerce in the state where the business is licensed, the Internal Revenue Service, and perhaps some others depending on the business sector. There are many regulations, which are applicable to a large federal organization, such as the Department of Defense. In fact, taxpayer dollars, which the United States Congress appropriates, wholly fund the DoD (Higgs, 2007). In addition, the DoD maintains all levels of classified and unclassified information, which the DoD must safeguard whether at rest or while in transit (Bhadauria, et al., 2014). This research will present a few of the federal regulations, which are applicable to internal controls, financial management, auditability, and cybersecurity at the DoD.

Chief Financial Officers Act of 1990. The Chief Financial Officers Act of 1990 was a legislative effort to improve the federal government's methods and internal controls, which were in place to reduce waste and to provide fully auditable financial statements across all agencies within the federal government (Radin, 1998). There have been many additional legislative attempts to strengthen the effort to improve financial management and audit readiness across the federal government. For example, there is the Government Performance and Results Act enacted in 1993, the Government Management Reform Act of 1994, the Paperwork Reduction Act of 1995 the Information Technology Management Reform Act of 1996, and the Federal Financial Management Improvement Act of 1996. Each new legislative effort was an attempt to improve accountability, but it is the Chief Financial Officers Act of 1990 that requires each federal agency to provide an annual financial statement that is auditable (Radin, 1998).

The Government Performance and Results Act enacted in 1993. The United States Congress enacted the Government Performance and Results Act in 1993 to correct the disadvantages that federal financial managers were experiencing with program efficiency and effectiveness (United States Congress, 1993). The lack of federal program effectiveness made it difficult for Congress to oversee federal programs and make correct decisions on spending (United States Congress, 1993). In addition, federal program waste and ineffectiveness contributed to the erosion of taxpayer confidence in the federal government (United States Congress, 1993). The objective of the Government Performance and Results Act was to restore public confidence by mandating the federal government to increase transparency, improve federal financial management, become more effective and accountable, and to measure the performance of federal programs (United States Congress, 1993). Congress included provisions in the Government Performance and Results Act that required the Director of the Office of

Management and Budget (OMB) to prepare verifiable annual performance reports on program activity for each federal agency (United States Congress, 1993).

The Government Management Reform Act of 1994. The United States Congress enacted the Government Management Reform Act of 1994 to improve government efficiency (United States Congress, 1994). The four main areas Congress addressed in the Government Management Reform Act were pay limitations, human resource management, streamlining management, and financial management (United States Congress, 1994). The Federal Financial Management Act of 1994 is the financial management part of the Government Management Reform Act of 1994 (United States Congress, 1994). The Federal Financial Management Act required each federal agency to provide auditable financial statements no later than March 1, 1997 (United States Congress, 1994). In addition, the Secretary of the Treasury and Director of the OMB were required to submit to the President of the United States and the United States Congress, an audited financial statement covering the entire executive branch of the United States government (United States Congress, 1994).

The Paperwork Reduction Act of 1995. Congress enacted the Paperwork Reduction Act of 1995 to reduce the public's burden of maintaining and storing federal paperwork (United States Congress, 1995). The goal of the Paperwork Reduction Act was to improve federal government efficiency and reduce costs by maintaining more information in electronic format (United States Congress, 1995). By using an electronic format, the government reduces the costs associated with storing and producing large amounts of information. In addition, an electronic format allows the government to share information with the public more efficiently (United States Congress, 1995). Of course, freely sharing more information with the public and storing

more information in electronic format increases the federal government's exposure to hacking activities and other nefarious activities.

The Information Technology Management Reform Act of 1996. The Information Technology Management Reform Act of 1996 provides several new requirements for the Director of the OMB, involving the oversight of federal information technology development (United States Congress, 1996a). In fact, the Information Technology Management Reform Act of 1996 gives Director of the OMB wide latitude in monitoring and overseeing the use and development of information technology throughout all federal agencies (United States Congress, 1996a). The Director of the OMB must improve the procedures to acquire and implement information technology systems, develop a process to track and evaluate all major federal information technology systems, and mitigate risks associated with the use of federal information technology systems (United States Congress, 1996a). In addition, the Information Technology Management Reform Act of 1996 requires the Director of the OMB to review policy and keep Congress informed about federal information technology systems (United States Congress, 1996a). One of the communication tools the Director of the OMB uses to manage these requirements are the OMB Circulars (The White House, 2017). The OMB Circulars contain the guidance federal agencies must follow for a period of two or more years (The White House, 2017). Each circular has a specific numbered sequence, which identifies the circular (The White House, 2017).

The Federal Financial Management Improvement Act of 1996. The Federal Financial Management Improvement Act of 1996 requires federal agencies to use information technology systems that comply with the many federal regulations and accounting standards (United States Congress, 1996b). In addition, audits are necessary to ensure the integrity of the data processed

with federal information technology (United States Congress, 1996b). When auditors find non-compliance issues with federal information technology systems, the Federal Financial Management Improvement Act of 1996 requires remediation through the implementation of corrective action plans (United States Congress, 1996b). The Director of the OMB must report to Congress on any agency failing to meet compliance of the Federal Financial Management Improvement Act of 1996 within the allotted period (United States Congress, 1996b). Clearly, the legislative branch is demanding accountability from federal agencies for the receipt of federal funding through taxpayer dollars. In addition, the series of legislative changes demonstrates the increasing importance of cybersecurity and auditability with respect to the federal information technology systems.

Financial Management Regulation. The Under Secretary of Defense (Comptroller) publishes The Financial Management Regulation (FMR), which applies to all DoD agencies (DoD_700014_R, 2017). The FMR contains over seven thousand pages and there are 16 volumes covering the financial management areas as follows:

- General Financial Management Information, Systems, and Requirements
- Budget Formulation and Presentation (Chapters 1-3)
- Budget Formulation and Presentation (Chapters 4-19)
- Budget Execution – Availability and Use of Budgetary Resources
- Accounting Policy
- Disbursing Policy
- Reporting Policy
- Form and Content of the DoD Audited Financial Statements
- Military Pay Policy – Active Duty and Reserve Pay

- Military Pay Policy – Retired Pay
- Civilian Pay Policy
- Travel Policy
- Contract Payment Policy
- Reimbursable Operations Policy
- Reimbursable Operations Policy – Working Capital Funds
- Special Accounts, Funds and Programs
- Non-appropriated Funds Policy
- Administrative Control of Funds and Anti-deficiency Act Violations
- Security Cooperation Policy
- Department of Defense Debt Management (DoD_700014_R, 2017, pp. I-3)

The FMR is a compilation of all federal regulations applicable to the DoD. The FMR provides detail on specific requirements that federal agencies must meet. The regulations within the FMR apply to all federal employees as well as all those individuals and business entities dealing with the federal government (DoD_700014_R, 2017). Volume 1 of the FMR, entitled *General Financial Management Information, Systems, and Requirements* is most applicable to this research project. Volume 1 emphasizes that financial management systems must be integrated, reliable, available, and comply with accounting principles (DoD_700014_R, 2017). Agencies within the DoD must take affirmative steps to comply with all applicable requirements of the FMR, including internal business processes and external business process (DoD_700014_R, 2017). In addition, the requirement to comply with the FMR is applicable to both manual and automated systems (DoD_700014_R, 2017). The FMR specially requires federal agencies to comply with the Director of the OMB's policies (DoD_700014_R, 2017). The FMR is a good

place to find specific information about nearly any topic concerning the DoD financial management.

The Office of the Under Secretary of Defense (Comptroller) maintains the FMR online. The Office of the Under Secretary of Defense (Comptroller) publishes revisions by the month, as needed. All files, including archived files are searchable. Actively maintaining the FMR provides continuously updated information for all stakeholders within the DoD. The Office of the Under Secretary of Defense (Comptroller) welcomes all questions and comments concerning FMR regulation, which arrive to the website by email (DoD_700014_R, 2017).

Financial Audit Manual. The GAO and the President's Council on Integrity & Efficiency first published the Financial Audit Manual (FAM) in 2001 and revised in both 2004 and 2008 to keep pace with increases in technology and auditing standards recommended by the American Institute of Certified Public Accountants (AICPA) (GAO-08-585G, 2008). The FAM currently consists of three volumes (GAO-08-585G, 2008). The FAM volume 1 describes effective methods and guidance to conduct audits of federal agencies and produce financial statements (GAO-08-585G, 2008). The FAM volume 2 provides effective auditing tools that auditors and financial managers can use to improve financial management (GAO-08-585G, 2008). The FAM volume 3 provides a variety of steps federal agencies can use for accounting and reporting (GAO-08-585G, 2008). The FAM incorporates important requirements and guidelines from a variety of sources into one manual for use by auditors and financial managers.

The FAM volume one. The FAM volume one provides a methodology for performing a financial audit, which includes the planning phase, the internal controls phase, the testing phase, and the reporting phase (GAO-08-585G, 2008). In the planning phase, auditors gather information about the organization's financial process cycle, discuss the scope of the audit, list

the internal controls, and evaluates all the regulations the organization must observe to maintain compliance (GAO-08-585G, 2008). In the internal controls phase, auditor further examine the organization's internal controls more closely to determine if the internal controls are implemented, and test the internal controls for compliance with financial reporting and compliance with regulatory guidance (GAO-08-585G, 2008). In the testing phase, auditors request the key supporting documents, which provide evidence that internal controls are working (GAO-08-585G, 2008). In the testing phase, auditors normally draw a representative and random sample the entire population, which auditors use to conduct detailed tests of the internal controls (GAO-08-585G, 2008). In the reporting phase, auditors document the results of the audit (GAO-08-585G, 2008). The audit report is a compilation of the auditor's activities, which forms the auditor's opinion of the organization's financial statement and the auditor's opinion of the organization's compliance with regulations (GAO-08-585G, 2008).

The FAM volume two. The FAM volume two includes many tools and procedures to assist auditors with conducting financial statement audits for federal organizations (GAO-08-586G, 2008). Much of an auditor's work builds upon the work of other auditors, who have performed similar audits (GAO-08-586G, 2008). In addition, the auditors have wide latitude and discretion in what areas to focus on and which tools or procedures to use, which makes the FAM volume two useful in planning and executing the audit (GAO-08-586G, 2008). The FAM volume two contains many agreed upon procedures, standardized written documentation, business letter templates, and reporting templates, which auditors use to perform and document audits (GAO-08-586G, 2008). Essentially, the FAM volume two contains a wealth of standardized information consisting of reusable documents and charts to help auditors standardize the audit work (GAO-08-586G, 2008).

The FAM volume three. The FAM volume three provides an abundance of detailed checklists for auditor to use when auditing federal organizations. The FAM volume three contains two categories of checklists, which are the checklist for federal accounting and the checklist for federal reporting. The two checklists help auditors use an organized and systematic approach to testing and reporting. In addition, the two checklists provide excellent documentation. While the two checklists are thorough, there are no requirements for auditors or organizations to use either of the checklists. Auditors are free to develop their own checklists. In fact, auditors are free to test any aspect of the organization's business processes and financial management processes. In addition, classified material is auditable, so long as auditors working with classified material have the appropriate government clearances in place and follow all procedures for handling classified material (GAO-07-1173G, 2007).

Federal Information Security Management Act. The Federal Information Security Management Act became law in 2002 (NIST, 2017). According to the Federal Information Security Management Act, all federal agencies must implement information security programs across each agency to support military, civilian, and contractors charged with operating federal information systems (NIST, 2017). When combined with the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996, the legislator's message regarding the protection of federally managed information becomes increasing clear (NIST, 2017).

The Office of Budget and Management. Among other requirements, the FMR requires financial management systems to comply "…with such policies and requirements as may be prescribed by the Director of the Office of Budget and Management" (OMB) (DoD_700014_R, 2017, pp. 4, Volume 1). The OMB publishes and updates Memorandums and Circulars to keep

federal agencies informed of new and existing requirements, which pertain to federal information systems. In July of 2016, the OMB updated *OMB Circular A-130 – Managing Information as a Strategic Resource* to keep federal officials abreast of information security risks and other vulnerabilities present (OMB A-130, 2016). In 2014, the Federal Information Security Management Act became the Federal Information Security Modernization Act, which required the OMB to update and strengthen *OMB Circular A-130* to reflect technological advances (NIST, 2017). The updates to *OMB Circular A-130* place more responsibility for security and privacy on federal agencies (NIST, 2017). For example, the updates to *OMB Circular A-130* encourage the sharing of non-classified government information with the public in an open fashion, while providing increased safeguarding of individual privacy and the private information the government collects (OMB A-130, 2016). The *OMB Circular A-130* is a subsequent document to *OMB Circular A-123* (OMB Circular A-123, 2004). The OMB dictates the information security standards that federal agencies must meet in order to protect entrusted information, which federal legislation requires.

Federal Information System Controls Audit Manual. The FISCAM is an all-inclusive manual for federal information systems and the controls supporting the integrity of data contained within the federal information systems **(GAO_092-32G, 2009)**. Many of the controls published in the FISCAM are from the NIST Special Publication 800-53, which is all about information system controls. Chapter three of the FISCAM contains many of the cybersecurity controls and chapter four of the FISCAM contains the business process controls. The FISCAM methodology includes planning, testing, and reporting **(GAO_092-32G, 2009)**.

FISCAM chapter three. Chapter three of the FISCAM contains information system controls around cybersecurity domains, such as security management, access controls,

configuration management, contingency planning, and segregation of duties. Security management covers controls to ensure users receive periodic security awareness training. Access controls ensure there is an appropriate level of restriction regarding physical and logical access to network hardware and software resources. Configuration management ensures that changes to systems receive proper authorization and documentation. Contingency planning ensures that information system resources are secure, that organizations can continue critical operations, and that organizations can reconstitute all operations efficiently. Segregation of duties ensures that incompatible duties do not exist between users, or that sufficient monitoring is in effect whenever a business need requires users to have incompatible duties. It is not by coincidence that auditors tend to focus on the above listed cybersecurity domains (GAO_092-32G, 2009).

FISCAM chapter four. Chapter four of the FISCAM focuses on business process controls, such as completeness, accuracy, validity, confidentiality, and availability. Completeness ensures that the information system processes all transactions only once and that the output is correct. Accuracy ensures that all transactions are correct, timely, and produce reliable output. Validity ensures that the transactions are authentic, receive proper authorization, and that the output is correct. Confidentiality ensures unauthorized access does not occur and there is protection in place for all output. Availability ensures that users are able to access all pertinent data when necessary (GAO_092-32G, 2009).

The planning phase. The planning phase is where auditors begin the audit. Since each organization is different, auditors must spend time planning their way forward. The goal is to acquire an understanding of the reporting entity, the service organizations, the relevant laws and regulations, the systems and networks, the risks, the critical control points, and other areas that

spark the auditor's interest. Auditors accomplish these objectives by conducting research, reading previous audit reports, asking the organization for documents, and by interviewing some of the organization's employees. Under audit conditions, the auditors have wide discretion to probe any part of the organization (GAO_092-32G, 2009).

The testing phase. The testing phase is where auditors ask for key supporting documents, which support that a cybersecurity control or a business process control is operating effectively. For example, a timesheet is a key supporting document, which supports the fact that an employee worked at a specific time and on a specific date. Simply providing the timesheet passes one of the tests in the testing phase. However, the existence of the timesheet does not indicate that the total hours are correct. Auditor's conduct many additional test on key supporting documents (GAO_092-32G, 2009). In the timesheet example, the employee must attest to the total hours prior to the supervisor certifying the total hours, which is the passing criteria in the testing phase. In addition, if the timesheet contains leave or overtime, the reporting entity must provide a key supporting document for each instance, along with the attestation by the employee and the prior approval by the supervisor (GAO_092-32G, 2009). The above actions of the employee and the supervisor represent the necessary segregation of duties for time and attendance (GAO_092-32G, 2009). In other words, employees cannot certify their own time and attendance. As presented in this example, the testing phase can soon become very detailed for auditors. In addition, the testing phase can be cumbersome for organizations that are missing key supporting documents. This example demonstrates the type of detail necessary for auditors to determine whether the controls are operating effectively or if potential vulnerabilities exist (GAO_092-32G, 2009).

The reporting phase. The reporting phase of the audit is when auditors provide the organization with feedback on the testing phase (GAO_092-32G, 2009). Auditors will use the testing results to evaluate and support any findings (GAO_092-32G, 2009). If controls are operating effectively and risk to the organization is minimal, the auditor's opinion is likely to be favorable. If the auditor's report on findings, the organization will need to design and execute corrective action plans. Auditors will evaluate the effectiveness of the controls and conclude all reporting requirements (GAO_092-32G, 2009).

The FISCAM auditors are well versed in the FISCAM methodology and FISCAM controls. The FISCAM controls include internal business controls and cybersecurity controls (GAO_092-32G, 2009). The FISCAM auditors are able to help agencies implement the FISCAM methodology throughout the agency by discovering financial process deficiencies and issuing CAPs. Agencies can avoid findings from a full financial audit by using the FISCAM methodology to discover and correct financial process deficiencies early. In addition to improving the overall financial process, agencies can avoid spending dollars in the future to correct deficiencies. The cost to correct financial deficiencies may grow much higher as the financial deficiencies age because many other systems will receive and process the incorrect data, which will likely need manual correction.

Independent public accountant. The Independent public accountant (IPA) is a more inclusive term because it includes certified public accountants and independent public accountants licensed prior to December 31, 1970 (Stowe, 1995). The use of IPAs is a complex process that requires a technical understanding of federal regulations by those responsible for contracting with IPAs on behalf of the federal government (Stowe, 1995). There is no pre-defined format for an IPA audit. In fact, an IPA may request to see any part of the workflow

process, speak to any member of the organization, or examine any document prior to rendering an opinion on the status of an organization's financial statements. Thus, each financial auditor can take a different approach to the examination depending upon the systems, processes, and controls present, as well as the discretion of the individual IPA. In addition to auditing internal controls and business processes, the IPA must audit system controls and cybersecurity controls (Whitehouse, 2015). The Chief Financial Officers Act of 1990 requires that the DoDIG or an independent auditor conduct all federal audits (United States Congress, 1990; FIAR, 2017).

Fighting the audit process is unproductive because the audit process is a tool that organization's use to help identify root problems and implement correction plans. According to the Department of Homeland Security, it is effective to use risk assessment and testing to find unknown problems, identify the root cause of the problems, implement CAPs, and test the effectiveness of the CAPs. The commitment of organizational leadership is a necessity. Leadership commitment sets the tone for the organization and keeps employees focused on the problem in a collaborative way. Achieving auditability goals is tedious work that requires changes in business processes, which depends on the dedication all personnel within the organization (Norquist, Sherry, Bedker, & Janssen, 2014).

Legacy IT Systems

Some legacy systems are over 30 years old and still processing data (Deloitte, 2013b). When legacy systems first became operational, cybersecurity was not a huge concern. Since that time, there have been many attacks on information systems and many of those attacks have been fruitful for the attackers. In April of 2015, cyber professionals at The United States Office of Personnel Management became aware that an advance persistent attack had been present on the United States Office of Personnel Management's information system for nearly a year (Koerner,

2016). The United State Office of Personnel Management typically deals with approximately 10 million attacks per month, though many attacks are routine throughout many other information systems (Koerner, 2016). General IT controls that were sufficient to mitigate risk when legacy systems were developed are no longer adequate. For example, an eight-character password was an acceptable IT control 25 years ago, but eight-characters is no longer of sufficient length to protect one's user credentials (Deloitte, 2013a). It would take nearly a year for a fast computer to break an eight-character password containing a number and symbol, but human behavior and technological advances combine to make the eight-character password ineffective (Deloitte, 2013a). Humans are unable to retain more than seven numbers in short-term memory, so humans typically select easy to remember passwords, which are easier to break (Deloitte, 2013a). The inability to protect user credentials adequately poses a serious risk to the organization's financial statement (Deloitte, 2013a). Today, cybersecurity is of great concern and financial auditability relies on effective cybersecurity controls (Bell, 2014).

The DoD's financial management first made the high-risk series in 1995. In February of 2017, the GAO published a high-risk series update to the GAO's 2015 report. The update on the DoD's financial management since the 2015 report has positive and negative points. According to the GAO report, the DOD and Congress cannot make proper decisions concerning DoD operations without reliable financial information. The GAO report cites continued internal control issues as a cause affecting operational efficiencies and effectiveness. In addition, the GAO reports that reliance on legacy systems will continue to be an obstacle in the DoD's effort to obtain a clean auditor's opinion on the DoD's financial statements because of the non-standardized data that legacy systems produce. According to the GAO report, other obstacles to a clean or unmodified DoD audit are a "…decentralized environment, cultural resistance to

change, lack of skilled financial management staff, lack of effective processes, systems, and controls, incomplete corrective action plans (CAPs), and ineffective monitoring and reporting" (GAO_17_317, 2017, p. 280). In addition to legacy systems, there are many other legacy factors and legacy processes to consider when making efforts to improve the DoD's financial management and auditing readiness (GAO_17_317, 2017).

The DoD cannot simply replace all legacy systems because some legacy systems provide functionality not available in systems that are more modern (Peled, 2016). In 1995, the DoD decided to replace the Defense Civilian Personnel Data System (DCPDS) because DCPDS was costly, difficult to use, and DCPDS was outdated (Peled, 2016). What the DoD failed to realize was that highly customized routines were built into DCPDS, but after spending $300 million taxpayer dollars on a replacement, the DoD decided not to replace DCPDS and DCPDS is still in use today (Peled, 2016). This example shows why it is necessary to do a cost analysis on all factors relating to legacy systems and to prioritize the replacement of legacy systems. The high cost of adding a tremendous amount of specialized functionality to a commercial off the shelf IT system is often overwhelming from a time, a labor, and a financial perspective. It is important to consider the DCPDS example along with the memo issued by the Secretary of the United States Army in 2016, which requires the divesting of legacy information technology no longer required (DSecretary of the Army, 2016).

The DoD is not the only large government agency to have trouble managing investments in new technology, while maintaining and supporting legacy IT systems. For example, the Social Security Administration relies on hundreds of Common Business Oriented Language legacy applications written over 40 years ago. These Common Business Oriented Language legacy applications total approximately 60 million lines of code. Finding personnel to maintain

these Common Business Oriented Language legacy applications is becoming increasingly difficult, due to separation and retirement. Many younger developers have never written a single line of Common Business Oriented Language code. In addition, the risks of replacing all the Common Business Oriented Language legacy applications are greater than the benefits. Since replacement is not always the best option from a risk standpoint, ensuring the necessary strong internal business controls and cybersecurity controls remain in place is a requirement (GAO_14_308, 2014).

Decentralized environment. A decentralized environment has legacy attributes in today's enterprise resource planning efforts. An example of a decentralized environment is each agency within the DoD being responsible to interpret FIAR guidance independently and to take action to correct audit findings (GAO_17_317, 2017). The GAO acknowledges there is some progress within the DoD in correcting audit findings, but attributes the absence of significant progress to the DoD's decentralized environment (GAO_17_317, 2017). A decentralized environment can lead to duplicative work and unnecessary expense (GAO_17_317, 2017). For example, there is a cybersecurity requirement under the security management domain, which requires each user to complete security awareness training at least annually. In a decentralized environment, each organization must spend time and resources satisfying this requirement for each of its information system users. In a centralized environment, the human resources department can ensure each employee that comes aboard completes security awareness training as part of the onboarding process. In addition, the human resources department can direct all employees to take security awareness training within a specific period each calendar year as a condition for continued employment. Most new employees will be out of cycle and take the security awareness training twice within the first year, but that does not violate the security

management requirement. The benefit is that each employee will always meet the security management requirement irrespective of how many systems the employee accesses. While the system information owners will still need to monitor this requirement, violations to the security management requirement should be very few. This type of centralized approach ensures all DoD employees are meeting requirements, while the DoD resources are not wasted.

Many legacy systems are products of a decentralized environment as managers make efforts to resolve financial management system needs independently. While it may be tempting to continue using legacy systems instead of replacing legacy systems, there are many factors to consider. In fact, the DoD often spends many more dollars maintaining legacy systems than anticipated (Eiband, Eveleigh, Holzer, & Sarkani, 2013). In order to make to correct decisions, management must evaluate each legacy system independently. There is a framework to assist management in making the correct decision about a particular legacy system (Eiband et al, 2013). The three main factors to consider when evaluating legacy systems are the available documentation, the available subject matter experts, and the feasibility of integrating the legacy IT systems with other necessary IT systems (Eiband et al, 2013). The GAO reported a $7.3 billion in less spending on development and modernization since 2010, while there has been an increase in operation and maintenance of legacy systems (Powner, 2016). Spending more on legacy systems and less on modernization is not sustainable over the long term.

Cultural resistance to change. Cultural resistance to change contributes to legacy business process instead of ushering in needed changes. There is an important relationship between the organizational climate and the leadership style, which effects employee's emotions. More importantly, studies have found that the employee's emotions affect the employee's willingness to accept change. When organizational climate and leadership style is out of

alignment, the result is poor employee performance. When employees perform poorly, the agencies must spend more dollars to achieve the agency's objective. Keeping organizational climate and leadership style in alignment can help keep costs from increasing (Haakonsson, Burton, Obel, & Lauridsen, 2008).

Organizational change requires leadership support from the top of the agency, but there are factors that cause employees to resist change, even when change is necessary. On such factor is self-interest. When employees find benefit for themselves in the required change, they are much more likely to tolerate the change. The psychological factor is the employee's perception of how the change affects job security and other related employee concerns. Another factor is the employee's preconception of the loss of control of organizational resources or workflow procedures. There are many factors relating to the employee's perception of the change, which has a significant impact on the employee's willingness to accept the change (Trader-Leigh, 2002).

Lack of skilled financial management staff. The lack of skilled financial management staff is a concern within the federal government (Lunney, 2016). Acquisitions within the federal government have increased as much as seventy-five percent from 2000 to 2005 (Kathuria, 2009). During the same period, the workforce handling acquisition for the federal government has not increased (Kathuria, 2009). As experienced acquisition professionals retire from government service, the employees left behind lack the needed experience to meet increasing job expectations (Kathuria, 2009). Without a sufficient acquisition workforce, the federal government must rely on contractors to fill the gap (Kathuria, 2009). However, the loss of an experienced workforce and the reliance on contractors leaves the government more susceptible to fraud and unscrupulous contractors, who could take advantage of the situation (Kathuria, 2009).

An important consideration when awarding government contracts is the selection of contractors and contracting companies, who operate ethically as part of their business model or founding principles. In an annual survey of chief financial officers for the Association of Government Accountant's in 2008, reported the highest risk was the governments "…inability to employ the proper amounts of workers and the leaders in financial management not really being on the same page as managers" (Armul, 2009, p. 10). From the standpoint of fraud, waste, and abuse, the loss of experienced personnel can be catastrophic.

Lack of effective processes, systems, and controls. The lack of effective processes, systems, and controls combine to create huge vulnerabilities from a data integrity, auditing, and reporting perspective (GAO_17_317, 2017). The DoD is operating a financial accounting system that cannot provide the data needed to produce useful reports (Armul, 2009). Information systems that are no longer useful are the definition of legacy systems (DSecretary of the Army, 2016). There are faulty accounting codes and processing differences between a variety of data processing systems, which contribute to difficulties in sharing information with partners and stakeholders (Armul, 2009). In some cases, obtaining an unmodified auditor's opinion cannot occur without upgrading the DoD's financial accounting system (Armul, 2009). After an audit of the Department of Homeland Security, KPMG LLC auditors reported that "…long standing procedural, control, personnel, and cultural issues…" are preventing an auditable financial management process (Armul, 2009, p. 8). Reforming the financial management process is a necessity, but an unqualified audit opinion is still years into the future for the DoD (Armul, 2009). Effective processes, systems, and controls are all required before an organization can produce a useful and auditable financial statement.

Incomplete corrective action plans (CAPs). The IPAs issued over 700 notice of findings and recommendations to the DoD after the 2015 full audit (GAO_17_85, 2017). This is not good news for the DoD because the GAO report indicates that after 25 years of attempting to comply with the Chief Financial Officers Act of 1990, the DoD is still years away from achieving a clean audit opinion. In addition to finding the DoD incapable of producing auditable financial statements, the GAO finds the DoD's decision-making ability, with respect to its mission and operations, adversely effected. Each time an IPA issues a notice of findings and recommendations, the receiving entity must address the notice of findings and recommendations with a complete CAP, implement the CAP, test the design of the CAP, test the effectiveness of the CAP, and then close the CAP under the oversight of the FIAR Office (FIAR, 2017). The process to respond to a single notice of findings and recommendations results in a large amount of work and a significant amount of time. There can be additional difficulties responding to notice of findings and recommendations. For example, even a well-documented CAP may be ineffective if the CAP does not address the notice of findings and recommendations correctly, which means there will need to be a rework of the entire process. In addition, the reporting entity must track the status of a CAP throughout the process. The GAO found that the U.S. Army, United States Navy, and United States Air Force have experienced difficulty in tracking CAPs, which has resulted in lost or incomplete CAPs (GAO_17_85, 2017). It is important to take the time to study the notice of findings and recommendations and write a CAP that will correct the deficiency from the onset of the process.

The Newport News Standard. In August of 2012, the Defense Contract Audit Agency provided guidance seeking more access to contractor's internal work products and audits. However, this new guidance was in opposition to the long-standing precedence from the Fourth

Circuit of the United States Court of Appeals in Richmond, which already decided that internal contractor documents were out of the Defense Contract Audit Agency's scope. The Newport News standard is the result of the case brought by the United States against the Newport News Shipbuilding & Dry Dock Company. The Newport News standard limits government access to contractor's internal documents (Napoleon et al, 2013).

Ineffective monitoring and reporting. The Defense Contract Audit Agency has the responsibility to oversee DoD contracts and to make sure the DoD spends its contracting dollars wisely. With a 70 percent increase in government spending from 2003 to 2013, ensuring government contracting dollars are not wasted is an important safeguard. The Newport News standard is the result of legal decisions, which prevent the government from exercising unfettered access to contractor's internal audit documents. Still, the GAO is pushing for more access to contractor's audit documents improve efficiency and to better monitor internal controls. The GAO report creates incentive for the Defense Contract Audit Agency to reach further into the contractor's internal process, which could lead to unintended consequences. Contractors could cut back or even do away with their internal auditing processes to prevent overreach by the Defense Contract Audit Agency. Instead of increasing audit efficiency and monitoring, this kind of government overreach could have the opposite effect (Napoleon & Henry, 2013).

In addition, the GAO found monitoring and the use of FIAR guidance to test and fix deficiencies in internal business controls to be necessary for the DoD to become auditable (GAO_17_317, 2017). For example, FIAR guidance defined seven deficiencies within the DoD as the inability "…to:

(1) Produce a universe of transactions

(2) Reconcile its Fund Balance with Treasury (FBWT) (i.e., balance its checkbook)

(3) Provide supporting documentation for material adjustments to its financial records

(4) Validate the existence, completeness, and rights of its assets

(5) Establish an auditable process for estimating and recording its environmental and disposal liabilities

(7) Implement critical information technology controls for its financial systems. (GAO_17_317, 2017, p. 285)

The above requirements are necessary to achieve auditability. The inability to balance the DOD's checkbook is the opposite of auditable. In addition, the lack of supporting documentation for transactions means the need for the disbursements are not verifiable and that an unsupported journal voucher may be necessary.

Financial Risk Mitigation

The Office of Management and Budget Circular A-123 describes management's responsibility to implement effective internal controls (Lippuner, 2014). Effective internal controls are those management activities that mitigate those operational weaknesses, which are adverse to the organization's mission (OMB Circular A-123, 2004). Management is responsible for the use of tools to help, policies, and procedures to mitigate potential vulnerabilities and risks to the organization (OMB A-130, 2016). Internal business controls are a necessity when it comes to financial risk mitigation. With today's advances in technology, cybersecurity controls are merely a subset of all internal business controls (GAO_092-32G, 2009). For example, the importance of keeping user credentials private cannot be understated. However, one's user credentials are among the cybersecurity controls, which did not exist prior to the advent of computer systems. In addition, the procedures to issue and track user credential are internal business controls located in the user entities standard operating procedure.

Internal business controls and cybersecurity controls have increasingly blended as technology advances. The user entity's financial statement is at risk when business and cybersecurity controls are not operating effectively. Although federal regulation, federal guidance, and logic dictate the importance of internal business controls, many financial managers view federal guidance on internal business controls as just a compliance requirement or unnecessary work rather than an important job function (Lippuner, 2014). One must take a larger view across the entire agency to accomplish financial risk mitigation across the entire agency (Lippuner, 2014). A larger view includes a thorough examination of the user entity's risk management framework, FIAR, internal business process interfaces, system interfaces, and the internal controls in place at the user entity level and each subsequent processing level.

Risk management framework. The purpose of risk management framework is to provide guidelines for a more dynamic approach to protecting federal information systems in today's more sophisticated and more vulnerable environment. The basis for risk management is the NIST Special Publications and the Federal Information Processing Standard. NIST issues Special Publications, which the federal information processing standards require agencies to follow. The goal of risk management framework is to secure federal information systems against reasonable or anticipated risks. The federal risk management framework includes six steps, which are categorize, select, implement, assess, authorize, and monitor (Joint Task Force Transformation Initiative, 2016a).

Categorize. Categorizing the information system includes all the data contained within the information system and all the data transmitted by the information system. The responsible party to categorize the system is the system Information Owner. There are many supporting roles, such as the Chief Information Officer, the Senior Information Security Officer, the

Information Security Officer, and the Risk Executive. Categorization considers the impact on the organization from potential adverse vulnerabilities, which could affect the organization. The categorize step provides a detailed description of all software, hardware, and network architecture. The categorize step must be consistent with the organization's risk management strategy (Joint Task Force Transformation Initiative, 2016a).

Select. Selection is the process of identifying the standard or baseline security controls that are in place at the organization (Joint Task Force Transformation Initiative, 2016a). The primary responsibility falls on the Chief Information Officer, Senior Information Security Officer, or Information Security Architect (Joint Task Force Transformation Initiative, 2016a). Security controls could be physical controls or logical controls (Joint Task Force Transformation Initiative, 2016a). In addition, documentation of the security controls is necessary (Joint Task Force Transformation Initiative, 2016a). An example of a physical control is the smart card needed to unlock the electronic door lock mechanism to access a computer terminal. An example of a logical control is the two-factor authentication process necessary to access the application. In some cases, the same smart card could be part of a physical control and part of a logical control. Each organization will have many security controls and it is necessary to monitor the security controls continuously (Joint Task Force Transformation Initiative, 2016a). The standard or baseline security controls require system specific security controls for each active information system (Joint Task Force Transformation Initiative, 2016a).

Implement. Implementation of security controls are the responsibility of the Information Owner and supported by the Information Security Engineer. The goal of the implement step is to examine each of the identified controls and ensure that the identified controls are appropriately addressing weaknesses. In addition, the implement step will include all the documentation for

the security controls and the implementation of the security controls. The security controls must meet minimum information assurance requirements to support the organization's mission (Joint Task Force Transformation Initiative, 2016a).

Assess. The primary responsibility for the assessment step in the risk management framework is the Security Control Assessor. The assess step is where the Security Control Assessor provides a complete plan to assess each security control within the information system. In addition, the Security Control Assessor provides a report, which includes findings and recommendations. The organization must take remedial action on all findings provided by the Security Control Assessor and update the security plan appropriately (Joint Task Force Transformation Initiative, 2016a).

Authorize. The primary responsibility for the authorize step belongs to the Information Owner. The Information Owner will put the security authorization package together to submit to the organization's authorizing official. The report should include all risks to the organization, such as the mission, the organizational functions, and the organization's reputation. The authorizing official for the organization will review the report and determine if the risk to the organization is at an acceptable level. If the organizational risk is acceptable, the plan receives authorization from the authorizing official (Joint Task Force Transformation Initiative, 2016a).

Monitor. The Information Owner has responsibility for the monitor step in the risk management framework. The Information Owner must determine the impact of any proposed changes to the information system before implementation. The Information Owner must develop a monitoring strategy for the security controls that are most critical to the security of the information system. The Information Owner will provide feedback and update the security plan based upon continual monitoring of the security controls. The Information Owner will provide

feedback on the effectiveness of the security controls based upon the monitoring activities. In addition, continual monitoring will alert the Information Owner to any significant changes in the organization's security posture (Joint Task Force Transformation Initiative, 2016a).

Each security control is identified by categories, such as access controls, security awareness, audit and accountability, risk assessment, physical and environmental protection, contingency planning, configuration management, and many others (SP_800_53, 2015). In addition, there is a prioritization of each control into risk classifications of low, medium, and high (SP_800_53, 2015). The risk management framework consists of a continual life cycle and the risk management framework is the basis for many public and private organizational security risk management programs. For example, the US Navy defines NIST SP 800-53 as an overlay between financial audit and cybersecurity (Tann & Chae, 2016). According to the Navy, entities can manage and implement financial controls and cybersecurity controls at the same time and cover all the requirements for both financial audit and cybersecurity (Tann et al, 2016). There appears to be a blending of internal business controls and cybersecurity controls that organizations can use to the organization's advantage in streamlining and cost savings (Tann et al, 2016).

Financial Improvement and Audit Readiness. The FMR now requires federal agency to take steps to achieve audit readiness (DoD_700014_R, 2017). The Financial Management and Improvement (FIAR) team is an organization that provides the United States Department of Defense (DoD) with the continued guidance necessary to achieve audit readiness (FIAR, 2017). The FIAR team defined audit readiness as "…having the capabilities in place to allow an auditor to scope and perform a full financial statement audit that results in actionable feedback" (FIAR, 2017, p. 1). The FIAR team identified financial reporting objectives from the Financial Audit

Manual published by the GAO (FIAR, 2017). Using financial reporting objectives from the Financial Audit Manual helps government organizations identify significant risks, which are part of a financial audit (FIAR, 2017). Organizations achieve financial reporting objectives through the organization's internal controls, cybersecurity controls, and the organization's ability to produce key supporting documents (KSDs) (FIAR, 2017).

An example of a cybersecurity control in the access control domain is an access request form used to provision system access because it includes the request, the authorization, and the user privileges. In addition, the access request form is also part of business internal controls, which collaborate with other controls to ensure necessary business operations (Atoum, Otoom, & Abu Ali, 2014). When an employee initiates and routes a form requesting access to a system, the actual completed access request form is the KSD. A form is complete when specific required fields are supplied, such a name, date, purpose, system name, access level, authorization, and subsequent approvals. In addition, this is an example of the type of detail needed to establish audit readiness (DoD_700014_R, 2017; FIAR, 2017). Other examples of KSDs are completed forms, such as security awareness certificates, leave request forms, overtime request forms, heath benefits forms, life insurance forms, timecards, and many other completed forms. The point is that when an auditor requests a KSD, the organization must be able to produce the KSD in a timely manner (FIAR, 2017). A second requirement is that the KSD produced by the organization must be complete and must contain specific criteria, which demonstrates to the auditor that the internal control or cybersecurity control is operating effectively (FIAR, 2017).

Internal business process controls interfaces. Internal business process controls are tasks that entity's embed into the business processes and not part of entity level controls (FIAR, 2017). Most of internal business controls are manual processes, which are controls that

employees perform as opposed to automated controls (FIAR, 2017). For example, a paper process inventory is a manual process control and an internal business process control (FIAR, 2017). Each internal business process control must interface correctly with an automated system. If the interface is not operating correctly because of control weaknesses, then some necessary information can be lost, which could result in the need for an unsupported JV to balance financial records (DoDIG D_2008_084, 2008).

System interfaces. System interfaces are where the communication and interactions between systems and between humans occur (Fosse & Delp, n.d.). There are many interfaces to consider and the interface can be exclusively between systems or the interface can be between a system and a human. For example, the icon menu screen on a smart phone is an interface between a system and a human. Unless there is a latency issue, users are not generally aware of when system interfaces occur, such as when a user connects to a web site. Latency is the route miles a packet must travel between connections, which is noticeable to the user when there is heavy network congestion or some other factor causing the poor network performance (Gottlieb, 2012). These system interfaces happen with no technical knowledge of the user and no technical control by the user. When processing data, each system must have controls around the input, controls around the processing, and controls around the output (FIAR, 2017). To ensure the data processes correctly, the output data must reconcile against the input data (FIAR, 2017).

Controls

There are many controls needed to operate an organization efficiently (FIAR, 2017). To understand the need for controls, one can consider a process with missing controls. For example, payroll processing with no input controls will simply create a disbursement equal to the total number of hours times the configured rate of pay. If either the total number of hours or the rate

of pay is incorrect, the disbursement and the organization's financial statement will be incorrect. Even if the total hours are correct and the rate of pay is correct, but the payroll processing system is not processing correctly, the disbursement will still be incorrect. To prevent incorrect disbursements, organizations typically institute many internal business controls, processing controls, interface controls, cybersecurity controls, and other controls. An example of an internal business control is the requirement for the supervisor to review and certify the timecard. An example of a processing control is to ensure the amount of the disbursement does not exceed the mandatory maximum amount of pay. An example of an interface control is the service provider ensuring that someone from the reporting entity with the authority to certify timecards has certified the timecard before submitting the timecard for processing. An example of a cybersecurity control is an access control in place to ensure non-repudiation by the supervisor certifying the timecard.

Some of the other types of controls are written procedures organizations document in the standard operating procedure (FIAR, 2017). When service providers external to the organization perform some of the organization's business processes, there are additional controls that are necessary (FIAR, 2017). For example, there are service organization controls, complimentary subservice organization controls, and complimentary user entity controls (FIAR, 2017). Each organization the touches the data must at least be aware of the above named controls (FIAR, 2017).

Standard operating procedure. Each organization must have a standard operating procedure in place. A standard operating procedure (SOP) is documentation, which represents a control and spells out the organization's policies and procedures, to ensure that all personnel follow the same procedures (Roberts, 2013). For example, segregation of duties, physical

security, information system access, and other procedures to prevent fraud are available in the SOP documentation (Roberts, 2013). Standard operating procedures are an important part of every organization because they provide standardization in both manual and automated processes (Roberts, 2013). In addition, an authorized and signed SOP is an audit requirement (FIAR, 2017).

An example of a standardized procedure is the procedure for IT system access. Every organization that uses an information system provides personnel with access to the IT system through some procedure. To standardize the procedure, an SOP would provide all the detailed procedures the organization follows to provide user access to the information system, maintain user access to the information system, and remove user access from the information system (GAO_092-32G, 2009). Without an SOP, the criteria to obtain, maintain, and remove user access may vary significantly (Office of Environmental Information, 2007). Some users may have access to areas of the system that violate segregation of duties (GAO_092-32G, 2009). Other users may have left the organization years prior, but continue to have access to the system (GAO_092-32G, 2009). Even worse, users that have left the organization may no longer be logging to the account and the organization may not be monitoring activity on the user account (GAO_092-32G, 2009). Failing to remove and monitor user accounts leaves the information system susceptible to attack by insiders or outsiders (GAO_092-32G, 2009).

Outsourcing. Outsourcing is contracting between an organization and an outside service provider to perform some processing services previously done in-house (Eliot, 1994; Pine, 2017). The outsourcing agreement is usually in the form of a service level agreement, which is a document explaining the understanding between an organization and a service provider (Hale, Grimaila, Mills, Haas, & Maynard, 2010). After reaching an agreement, each organization's

leadership signs the proposed service level agreement. The service level agreement is a control between two organizations that provides all the specifics about the services that will be outsourced (Pine, 2017). A service level agreement does not relieve the reporting entity from financial reporting responsibility, though it may lessen the financial risk (Ren, Busch,, U.S.A.F., & Prebble, 2010).

The benefits to outsourcing. There are sound reasons to employ this strategy, such as improving efficiency and increasing profit (Pine, 2017). Outsourcing legacy processing or current in-house processing can free up internal staff to tackle the development of newer and more efficient IT systems (Eliot, 1994). Outsourcing high cost processing to a less expensive and more efficient solution can free up organizational funding for other organizational business needs (Eliot, 1994). Outsourcing provides the flexibility needed when existing staff is unable to adapt to technological advances (Eliot, 1994).

The risks to outsourcing. There are risks associated with outsourcing, such as the loss of control over critical business processing (Eliot, 1994). Whether outsourcing legacy information systems or more useful information systems, the increased vulnerability can have a demoralizing effect on both IT staff and management (Eliot, 1994). For example, IT staff may have difficultly turning the control of organizational data over to an outside vendor, especially when the organization is ultimately responsible for the handling of the data (Eliot, 1994). IT staff may feel less appreciated and decide to leave the organization because of outsourcing (Eliot, 1994). In another example, an outside vendor could decide to outsource some of the work to a third party (FIAR, 2017). In addition, there must be interfaces between each organization and the creation of more interfaces inherently creates more risks (FIAR, 2017). To ensure the reliability of the data, each involved entity must consider cybersecurity when designing and

implementing interface controls (GAO_092-32G, 2009). Having a service level agreement in place is a necessary control, but a service level agreement alone cannot eliminate all the risks associated with outsourcing (Pine, 2017).

The supply chain risk. Consideration of the supply chain risk must be part of every outsource strategy. Providing other entities with critical or sensitive information even for the purposes of data processing introduces new risk. At the DoD, this responsibility falls on the Chief Information Officer for Risk Management Activities, who must consider supply chain risk with respect to the DoD's IT systems. The DoD relies heavily on commercial systems that are part of a global supply chain. These commercial systems include hardware and software and pose additional risk to the DoD information systems (House of Representatives, 2017).

Internal controls and Service organization controls. The Statement on Standards for Attestation Engagements Number 16 (SSAE 16) report is a report about the internal controls of a service organization (SSAE 16, 2015). The SSAE 16 report is the interface between the DoD and several data processing systems, which are DoD service organizations (SSAE 16, 2015). The value of the SSAE 16 report is the standardization the SSAE 16 provides. DoD financial managers and auditors only need to consult one document to obtain a complete understanding of the standardized controls the service organization expects each reporting entity to implement. A fair analogy is a Java compiler, which produces bytecode that can interface with several different computing platforms, after passing through the Java Virtual Machine. The SSAE 16 is the basis for the service organization controls (SOC 1) report and auditors may either test the controls themselves or obtain a SOC 1 report opinion (SSAE 16, 2015). The SOC 1 reports "…are specifically intended to meet the needs of entities that use service organizations (user entities) and the CPAs that audit the user entities' financial statements (user auditors), in evaluating the

effect of the controls at the service organization on the user entities' financial statements" (SOC 1, 2017, p. 1). Obtaining the SOC 1 opinion is the preferred method because it reducing duplicative testing (SSAE 16, 2015).

The reporting entity maintains responsibility of its financial statement regardless of which organizations process the data or any portion of the data (DoD_700014_R, 2017; FIAR, 2017). For example, the reporting entity may choose to process all of the data or may outsource some of the data processing to a service organization (FIAR, 2017). In fact, a service organization may choose to outsource a portion of the reporting entity's data processing to a third organization, which is a subservice organization (FIAR, 2017). The reporting entity maintains some control over the processing through various service level agreements. It is important to consider that there are input control points, processing control points, and output control points with each system that touches the data, whether the system is a manual process or an automated process (FIAR, 2017). Input control points are the part of the system where data enters, such as a data input screen or a data input file (FIAR, 2017). Processing control points are all the system-processing controls that ensure the integrity of the processing (FIAR, 2017). Output control points are the part of the system where processed data leaves the system (FIAR, 2017). Auditors and financial managers must use a variety of controls to test, monitor, and reconcile the data before and after the data passes through each interface (GAO_092-32G, 2009).

The significance of internal controls, system controls, and cybersecurity controls becomes increasingly important as the number of entities processing the data increases (FIAR, 2017). Specifically, it is important to know which entity is responsible for operating the controls and whether the entity is operating a shared control (FIAR, 2017). For example, the reporting entity may choose to operate the internal controls governing the employee accessions and the

employee separations completely and not outsource any part of the accessions and separations process. In another example, the reporting entity and the service organization may operate shared controls governing the accessions and separations process, which means there must be communication and understanding between the two parties (SSAE 16, 2015). In another instance, the reporting entity may outsource the continuity of operations plan to a service organization and not operate any of the controls governing the continuity of operations. Regardless of which entity is operating the controls, it is important is to map all of the controls, test the design of the controls, implement the controls, and test the effectiveness of the controls (FIAR, 2017). In addition, it is important to reconcile the data after processing, monitor the effectiveness of the controls on a periodic basis, and document the monitoring activities (FIAR, 2017).

Complimentary subservice organization controls. Complementary subservice organization controls (CSOCs) are controls that a subservice has in place to align with the service organization controls (FIAR, 2017). In other words, the work that a service organization outsources to a subservice organization must have controls in place that meet the same requirements as the original service organization (FIAR, 2017). As an example, a DoD agency may outsource payroll processing to agency B, which is service organization. Agency B may outsource some of that work to agency C. The guidance from the FIAR office is that there must be controls in place at agency C, which align and operate effectively with agency B (FIAR, 2017). This alignment of controls is crucial because alignment ensures there are no gaps in the input controls, processing controls, and output controls at the reporting entity level, service organization level, or the subservice organization level (FIAR, 2017). The accuracy of the resulting financial statements remains the responsibility of the original DoD agency or reporting

entity. An example of a control gap within the system interface is an employee timesheet that processes through the payroll-processing center, but no one certifies the timesheet. Although no human certified the timesheet, the hours on the timesheet may still be correct. However, the risk of incorrect hours on the timesheet increases when no human certifies the timesheet. In addition, if the hours on the timesheet are incorrect then the DoD's financial statement is affected. To protect the DoD's financial statement, there must be aligned controls at the DoD agency level, the service organization level, and the subservice organization level (FIAR, 2017).

Complimentary user entity controls. Complimentary user entity controls (CUECs) "… are those controls for which management of the service organization assumes will be in place at user entities in regards to the actual services being performed by the service organization" (Nickell, 2017, p. 1). In this context the term "user entity" and reporting entity" are the same entity. The above statement from the service organization obligates management to take steps to ensure the CUECs are in place and operating effectively at the reporting entity level (Nickell, 2017). An example of a CUEC is the use of a system access form. The system access form is the control form and the reporting entity ensures that the control form has all data elements complete, and that there is authorization for the control form, prior to routing the control form to the service organization. Upon receipt of the control form, the service organization verifies the authorization of the control form, ensures the control form originated from the reporting entity, and grants the reporting entity's employee the correct access the system. In order for the service organization to process the work correctly, the reporting entity must provide accurate data through the effective use CUECs (FIAR, 2017). Without the system access form CUEC, there is a significant risk of unauthorized access to the system, which could result in financial consequences for the reporting entity (FIAR, 2017).

What may not be quite so obvious about CUECs is that there are many CUECs within the SOP. While the word CUEC may not be anywhere in the SOP, each CUEC should be mapped to a policy or procedure in the SOP (FIAR, 2017). The primary CUEC domains are access controls, configuration management, continuity of operations, security management, and segregation of duties (GAO_092-32G, 2009). There may be more than one CUEC within a domain (FIAR, 2017). For example, there are several CUECs within the access controls domain and each will be part of physical access or logical access to an information system (FIAR, 2017). In addition, CUECs are IT system controls, but those system controls are not limited to just what the service provider defines as CUECs. The organization should map each CUEC back to the procedure or policy within the SOP that refers to the CUEC (FIAR, 2017). This mapping exercise will let financial managers and auditors know where the CUECs are and how the CUECs operate. These CUEC domains are about how an organization maintains both internal controls and cybersecurity controls to mitigate risks to the organization (GAO_092-32G, 2009).

There are those in leadership, who do not believe CUECs are necessary to implement, especially when a service organization actually does the processing (DoDIG_2016_054, 2016). In 2014 for example, there was a finding by the DoDIG indicating the United States Navy's management of the Invoice, Receipt, Acceptance, and Property Transfer information system did not design and implement CUECs for three United States Navy commands because the United States Navy's management thought the Defense Logistics Agency was operating those controls (DoDIG_2016_054, 2016). In addition, the United States Navy did not view the responsibilities and procedures for system change management as being important (DoDIG_2016_054, 2016). This example demonstrates why it is necessary to map all CUECs and to identify the entity responsible to operate each CUEC. If leadership does not view CUECs as being important, there

is little hope that financial management employees will see the importance of CUECS (Haakonsson, Burton, Obel, & Lauridsen, 2008). In addition, the risk of financial misstatement increases significantly when neither entity is operating the controls.

Summary

To summarize, this research examines the link between financial auditability and cybersecurity, the adverse effects of using legacy IT systems, and the available methods to mitigate the risk of using legacy IT systems. In addition, this research describes a problem that evolves and changes as the available technology and the environment evolve and change. The problem is the huge dollar amounts of unsupported JVs, which prevents the DoD from obtaining a clean auditor's opinion on the DoD's financial statements (DoDIG_2016_113, 2016). Through the legislative process, the American taxpayer has demanded more transparency beginning with the Chief Financial Officers Act of 1990 (United States Congress, 1990). However, the DoD has been unable to produce financial statements that satisfy auditors, which keeps the American taxpayer unconvinced. In addition, the DoD is unable to make informed operational decisions because of the untenable financial management (GAO_17_317, 2017). Despite the resources in place at the DoD to achieve audit readiness, the DoD is still years from obtaining the goal of a clean auditor's opinion (Armul, 2009). Although the billions of unsupported JVs were manageable in 2005, the trillions of unsupported JVs are not manageable today.

There is no single cause responsible for the creation of an unsupported JV. In fact the DoDIG has identified many contributing factors, such as legacy IT systems, a decentralized environment, cultural resistance to change, a lack of skilled financial management staff, a lack of effective processes, systems, and controls, incomplete CAPs, and ineffective monitoring and reporting (GAO_17_317, 2017). In short, the DoD must correct the DoDIG findings to mitigate

financial risk, achieve audit readiness, and produce clean financial statements, as the law requires (United States Congress, 1990). This research provides detailed information concerning applicable federal regulations and guidelines, the internal business controls, the cybersecurity controls, and the other factors contributing to unsupported JVs. In addition, this research explores the FIAR methodology, which is the DoD's way forward to auditability (FIAR, 2017). In order to reduce or eliminate the need for unsupported JVs, the DoD must achieve and sustain a true state of audit readiness.

Discussion of the Findings

The focus of this research is the relationship between cybersecurity and financial auditability. The need for financial auditability evolved long before the first business computer became available. Essentially, these two disciplines evolved separately in traditional isolation. Auditability evolved primarily out a business need to account for property in transit. Computing technology evolved out of a business need to reduce costs, increase efficiency, and increase accuracy. Because memory size and processing power are limiting factors for computing technology, engineers have found methods to increase main memory and processing power significantly, which has led to the increased computer system sophistication available today. The increased computer system sophistication has caused the lines between cybersecurity and financial auditability to become blurred. This research focuses on taking advantage of the overlap between cybersecurity and financial auditability to strengthen internal business processes, mitigate financial risk factors, and use the principles of audit readiness to comply with federal regulations. The goal is to take advantage of the overlap between cybersecurity and financial auditability to produce a financial statement that meets auditor scrutiny.

Cybersecurity and auditability

There is an overlap between cybersecurity and financial auditability, which parallels the evolution of information technology systems. As systems become more powerful, the systems are able to increase efficiency by tracking and processing more data. The increased efficiency increases the organization's reliance on information systems, which increases the number of systems needed to process data accurately. As the number of systems increase, the number of interfaces and control points increase. All of these advances in data processing bind

cybersecurity and financial auditability together in such a way that financial auditability cannot exist without strong cybersecurity controls to mitigate risks.

Cybersecurity and financial auditability both require strong internal business processes, which must be operating in order to be effective. In other words, the information system test of design can be excellent, while the information system test of effectiveness can fail because well-designed controls that humans or systems do not operate will not be effective. Implementing strong internal business controls and strong cybersecurity controls is necessary in order to rely on the output from information systems. In addition, a holistic approach to internal business controls and cybersecurity controls can prevent duplicative work and help organizations realize cost savings. These cost saving can materialize through a coordinated approach to strong controls and through the benefits of risk mitigation.

Cultural resistance to change. There is a natural resistance to change when the benefits of the change are not readily apparent. Employees' will consider how the change will affect the employees' day-to-day operation. Thus, an employees' perception of the change is significant. Top-level employees should communicate the need for the change, so that all stakeholders understand there is leadership support behind the change. In addition, leadership remains aware of the changes that are occurring within the organization. Having leadership buy-in will help diminish the resistance to the change and provide an avenue for dealing with resistance to the change, if necessary.

Another consideration is that change should never occur just for the sake of change, there must be a benefit to making the change. The best way to quantify the benefits of a change is to show a real cost savings. However, there are non-monetary benefits to change, such as compliance with new federal regulations. When considering a change, the desired benefit must

outweigh the risks that are present with every change. The change control board will formalize and document this process whenever a stakeholder submits a system change request, the configuration management CUEC. The same process is necessary when the organization implements an internal business control change. Whenever changes occur, all stakeholders should be aware of the reasons for the change to help quell the natural resistance to the change.

Lack of skilled financial management staff. The lack of skilled financial managers has become a serious issue in many organizations. In addition, the blending of auditability and cybersecurity has increased the need for a skilled financial management staff. With all the systems in use today, financial managers must have an understanding of the benefits and the limitations of information systems. When financial managers view information systems to be something for the IT department to handle exclusively, there is a disengagement between financial managers and IT personnel. This disengagement leads to financial managers to blame IT personnel for incorrect output data and contrariwise.

In order to process data correctly, it take knowledge and experience of the part of financial managers and IT personnel. In addition, each must have a working knowledge of the others field of expertise. If financial managers have weak controls that introduce incorrect input data, there will be an adverse effect on the output data, even if the system processes the data correctly. The same result will occur when the input data is correct, but the system processes the data incorrectly. In 2017, processing data from start to finish involves many information systems, internal controls, system controls, interfaces, and personnel, all of which must be operating correctly. Financial managers must have an understanding of the entire financial process and not just a subset of the financial process. Unfortunately, the federal government has experienced a loss of highly skilled and experienced financial managers, primarily due to

retirement. The federal government is jobs filling those jobs, but the new personnel lack the skill and experience at a time when the job expectations are increasing. In a 2013 report to Congressional Committees, the "GAO has also reported that substantive results are not yet apparent from DOD's efforts to develop two important resources—modern business information systems and a skilled workforce—for resolving its financial management weaknesses and achieving and sustaining audit readiness" (GAO_13_283, 2013, p. 137). Perhaps the corrective action plan should include the development of a succession plan to retain key institutional knowledge throughout anticipated periods of attrition.

Incomplete corrective action plans (CAPs). When a reporting entity becomes aware of a finding or a deficiency, a corrective action plan or CAP is necessary. However, each CAP is unique to the specific finding or deficiency. Some CAPs may be simple to implement and some may be more complex, but reporting entities must ensure that the CAP addresses the finding completely. As an example, there is a requirement that the reporting entity's management must sign all standard operation procedures and that standard operating procedures must be periodically updated (FIAR, 2017). If personnel were using a standard operating procedure that management did not sign, there would be a finding because management did not formally agree with the current standard operating procedure. The risk of personnel ignoring the current standard operating procedure increases because there is no formal direction from management. This finding would likely result in a CAP, which would require management to sign the standard operating procedure after providing each periodic update. The CAP would remain incomplete until management signs the updated standard operating procedure.

The previous example is relatively straightforward to read, understand, and implement. However, other findings are more complex, multivariate, and require much more time to design

controls, implement the controls, and test the controls. For example, suppose a finding indicates that the reporting entity has no controls over the authorization of a pay increases for employees, which are processed by a service provider. This finding would likely result in a CAP to ensure the reporting entity authorizes all pay increases prior to the processing of the pay increase by the service provider. In this case, the control will involve both entities and could be as relatively simple, such as an authorizing official within the reporting entity digitally signing a pay increase document and routing the pay increase document to the service provider for processing. Since this is an example of a shared control, the service provider must physically inspect the pay increase document for an authorizing official's digital signature and to ensure the routing to the service provider was took an acceptable path. If either condition is false, the service provider will reject the pay increase document and notify the reporting entity. After implementation of this type of CAP, there must be testing to ensure the new control is operating effectively.

The above examples show that CAPS do not need to be difficult, but CAPS require both entities to have a clear understanding of how the controls operate and who is conducting the periodic monitoring of the controls. Ensuring that CAPS address the findings and ensuring complete implementation of CAPs is necessary to mitigate the risk to the reporting entity. In addition, it is important to conduct testing to determine the effectiveness of the CAP. In the first example, a test would be to ask for a copy of the document that designates the system owner or system administrator, including all roles and responsibilities. The criteria for passing the test would be that the key supporting document is available within an acceptable timeframe. The test for the second example would be for the tester to ask for a specific sample of pay increase documents and check each sample for an authorizing official's digital signature. The criteria for passing the test would be to ensure the authorizing official's digital signature exists on the pay

increase document and to ensure the information system processes the pay increase document after the signature of the authorizing official. If the CAP is incomplete, the risk to the reporting entity is still present.

Legacy systems create risk factors

There are many risks to using legacy IT systems, many of which came into existence over fifty years ago. Legacy systems are systems that no longer serve a useful purpose. A legacy system could be a manual business system that no longer serves a useful purpose. For example, a slide rule is a legacy system today because an electronic calculator is so much more efficient. In fact, many people do not know how to use a legacy slide rule. Many legacy information systems became legacy systems as personal computers became more powerful. However, a legacy system does not need to be old to be a legacy system. A new information system that cannot process data reliably is a legacy system. A system that cannot process data reliably serves no useful purpose.

Legacy systems are expensive to replace. In fact, it is not possible to replace some legacy information systems because the systems serve very specific functions and the systems interface with so many other systems that the replacement cost is prohibitive. In addition, the cost to operate legacy systems is steadily increasing, which consumes much of the available research and development funding. A legacy system that costs too much to operate and too much to replace is a perplexing problem. Programmers can create newer interfaces to sit on top of the legacy systems, but the risks posed by the legacy systems remain.

In addition to the cost risk, there is a risk of reliability. Many information systems process the data before it becomes part of the entities financial statement. There are many interfaces and many control points along the way. There is a risk of data loss at each processing

step and through each interface. There are reconciliation procedures, which can catch data that processes incorrectly and provide an opportunity to restore any data loss, but these controls be operating effectively. If there is confusion about where the responsibility for reconciliation lies, there may not be any reconciliation occurring. With no reconciliations occurring, the data loss becomes permanent. Data loss can be the difference between a supported journal voucher and an unsupported journal voucher. Unsupported journal vouchers have an adverse effect on the reporting entity's financial statement. In some cases, the systems are not auditable because the systems cannot process data reliably.

Lack of effective processes, systems, and controls. Legacy systems contribute to a general lack of effective processes, effective systems, and effective controls. Whether the processes are manual or automated, and whether the processes are legacy are brand new, ineffective means the processes are not reliable. The same is true for manual or automated controls. Fortunately, implementing the FIAR guidance can strengthen ineffective processes and controls. Systems are a little more problematic because some systems are not auditable, which means the output data is not reliable. Just as it is not easy to add good security to a pre-existing information system, the same is true for adding auditability to an existing information system. If a system is not auditable, it may be necessary to replace the information system with a completely new system. However, information systems have many interfaces and some information systems interact with many other systems. The way an information system interacts with other systems may adversely affect the feasibility of a complete system replacement, such as the government's attempt to replace the Defense Civilian Pay System.

System interfaces that are not working correctly can lead to data loss. The loss of critical data can lead to an unsupported JV. A reasonable analogy for what seems to result in an

unsupported JV is the processing required to reduce the resolution of a high-resolution digital photo to transmit the photo over the Internet efficiently. The high-resolution digital photo represents the original key supporting document with all the supporting data. The reduced-resolution photo loses some of the high-resolution data, which makes the photo smaller and easier to transmit over the Internet. The low-resolution photo represents the data from the key supporting document after processing. In both cases, some of the original and irreplaceable digital information is lost. In the case of a digital photo, the loss of information prevents one from enlarging the photo with the same detail as the high-resolution photo. In the case of a JV, the loss of information prevents financial managers and auditors from supporting the JV with sufficient documentation. Unsupported JVs have a dramatic impact on the DOD's audit readiness and resulting financial statements.

Ineffective monitoring and reporting. Ineffective monitoring and reporting is an area where there is confusion over which entity is responsible for monitoring and reporting on the effectiveness of business process controls and cybersecurity controls. It is acceptable for the service provider to conduct monitoring activities and perform reconciliations on behalf of the reporting entity and it is acceptable for the service provider to expect the reporting entity to monitor the controls. Both methods are effective so long as both entities have a clear understand of which entity is responsible for monitoring controls and reporting. The service level agreement between the two entities should spell out the responsibilities of both entities. Regardless of which entity is responsible to monitor controls, the responsibility to provide a complete and accurate financial statement is ultimately the responsibility of the reporting entity.

Along with the responsibility to monitor controls is the responsibility to report on the results of monitoring. For example, monitoring activities lead to discovery on the effectiveness

of internal business controls and cybersecurity controls, but monitoring alone will have no effect on the discovery of deficiencies. Making the reporting entity aware of deficiencies provides an opportunity for the reporting entity to design and implement a corrective action plan to address the deficiency. This is a continual process because systems and processes change over time and each change has the potential to introduce new deficiencies. Of course, the procedure to request a system change includes studying the proposed change, anticipating the cost and the effect of the proposed change, and testing the system after implementation of the change, but those procedures cannot determine all unintended consequences. Without continually monitoring the information system in an effective way and reporting the results, the resulting data can soon become unreliable.

Mitigating financial risk

Mitigating risk is task that is never complete because the business environment is continually changing in many ways. CUECs can strengthen business processes and internal controls, which helps mitigate financial risk. However, just the fact that a CUEC is not in place at the entity level does not indicate there is an adverse impact upon the entity's financial statement. It could be that no person or entity took advantage of the vulnerability created by the missing implementation of the CUEC. However, the risk of financial misstatement still increases when CUECs are not in place and auditors still evaluate risk when developing audit opinions. While not having a CUEC in place may not actually effect the financial statement in question, missing CUEC implementation at the entity level will adversely affect the auditor's opinion.

Information systems may require several hundred processing control points to ensure the integrity of the data processed. However, if the reporting entity does not own the information

system, the reporting entity may have no control over most of these processing control points. Simply put, the reporting entity may never touch any part of the control point. Thus, CUECs are a subset of these hundreds of system control points. When the reporting entity does not own the system, the CUECs are mostly input control points and output control points, which are the areas of shared control points between the system owner and the reporting entity. In addition, there are some CUECs, such as security awareness training that the reporting entity operates entirely. Likewise, the system owner operates many of the processing control points completely, with no interaction from the reporting entity.

Many disagree about the importance of CUECs. Their position is that CUECs are not system controls and that internal business controls are sufficient. The problem is that the CUECs are an interface between the internal business controls and the information system controls. For example, annual security awareness training is a security management CUEC, but a user's level of security awareness does not affect the actual information system processing. IT personnel or the service provider may believe that the security management CUEC is not important. However, if a user infects the system with an advance persistent attack like the one found on the Office of Personnel Management information system, that security management CUEC becomes much more important. In addition, there can be a severe impact on the organization's financial statement. Not having a CUEC in place does not mean that an adverse action will occur, but it does increase the risk of an adverse action. As the risk to information systems increase, the reliability of the information system decreases. CUECs are preventative controls, which is why some may believe they are not necessary. Similarly, having all the CUECs in place does not guarantee that no adverse actions will occur.

Summary

To summarize, financial transactions begin with several required data elements and each data element must meet required specifications to be valid data. If all the valid data elements necessary to support the transaction are present, the transaction should flow through the first financial IT system without fail or exception. If any of the data elements are missing or invalid, the transaction will be rejected and not flow through the first financial IT system. All rejected transactions will need correction and reprocessing, which is the reconciliation process. Occasionally, there will be transactions that cannot flow through a financial IT system and processing will require a human to perform a manual work-around. Manual work-arounds are undesirable because manual work-arounds create additional risk, create additional work, and require additional documentation. In addition, each transaction must successfully process through several financial information systems before the transaction becomes part of the entity's financial statements. Each financial IT systems has input control points, processing control points, and output control points.

In order to avoid lost transactions and transactions with incorrect or missing data, a reconciliation process at key control points is necessary. Lost transactions or incorrect transactions create a need JVs to bring financial records into balance. When the documentation to support a JV is not available, the JV falls into the unsupported category because the validity of the transaction is uncertain. To receive an unmodified auditor's opinion, an organization must be able to show that its internal business controls and cybersecurity controls are operating effectively and sufficiently and that the risk to the organization's financial statement is minimal or acceptable

Recommendations

This challenging problem, that excessive unsupported journal vouchers are necessary to balance the books at the DoD, seems to have no single root cause. The DoDIG offered a variety of problems that combine into one perplexing challenge for the DoD. Thus, there are many avenues for further research. In addition, the advances in technology seem to add to the problems instead of reducing or eliminating the problems. The recommendations involve further study to find and mitigate to root cause of the following problems identified in this research project.

Systems

Further study of all systems, including legacy systems is recommended with the goal of reducing the number of necessary systems overall. Each required system will have an input interface and an output interface. Each system interface is an opportunity for an interface error, which can lead to an unsupported JV. Reducing the number of required systems will reduce the number of required system interfaces, which will reduce the opportunity for error. Reducing the number of systems will serve to create a more centralized environment, which will address the finding from the DoDIG concerning the DOD's decentralized IT environment. Legacy systems that are required will need strong internal business controls and strong cybersecurity controls to ensure data integrity.

Skilled Financial Management Staff

Skilled financial management staff is a necessity for improvement financial auditability. Human personnel must understand the importance of input controls, processing controls, and output controls. While a service level agreement may obligate another entity to operate some controls, it is not possible to outsource the responsibility for the integrity of the data. For

example, when a reporting entity outsources data processing, the service provider relies on the integrity of the input data because the service provider does not produce the input data. The service provider distributes the output data to the reporting entity and relies on the reporting entity to reconcile the output data. In some cases, a service level agreement may obligate a service provider to reconcile the output data, but in those cases, the service provider will reach out to the reporting entity as questions from the output data arise. Thus, even when the service provider is obligated to reconcile the output data, a shared control exists between the reporting entity and the service provider.

Financial Improvement and Audit Readiness

The DoD relies on FIAR guidance to help the DoD forge a path to audit readiness and auditable financial statements. The FIAR team is a vital resource for the DOD in the DoD's continual efforts to comply with federal regulations. Updating the FIAR guidance is part of a continual process to reflect new information and technological changes. In addition, FIAR guidance reflects changes and update to the Office of Management and Budget Circulars, which contain the latest updates to federal regulations. In addition to guidance, the FIAR team provides many tools for tracking corrective action plans and for analyzing huge amounts of data. The FIAR team includes experts in the fields of internal business controls, information system controls, financial processes, and auditing.

Complimentary User Entity Controls

The term complimentary user entity controls or CUECs is a relatively new term in the auditing world. As organizations or reporting entities began outsourcing some of their financial data processing, some control gaps became noticeable. Legitimate questions arose about which entity was responsible for controlling specific processes. Service providers make CUECs

available to the reporting entities to prevent control gaps. The output from the service provider is not reliable unless the reporting entity implements the CUECs. For example, if information system users have no training in security awareness, the likelihood of those users' actions affecting the integrity of the service provider's data increases. Implementing the security management CUEC, which requires the reporting entity to provide every user with security awareness training before the user accesses the information system, mitigates the risk to an acceptable level. A key point is that the service provider operates some CUECs entirely, the reporting entity operates some CUECs entirely, and both the service provider and the reporting entity operate other CUECs. There must be coordination between both entities to ensure there are no control gaps.

Monitoring

Continual monitoring is part of the audit readiness process and part of a robust standard operating procedure. In addition, monitoring must occur on a regular basis. While Excel spreadsheets are not easily auditable as part of a data processing system, Excel spreadsheets are useful for monitoring activities. For example, through analysis of accession reports, separation reports, and gross pay files, Excel formulas can automate processes to identify exceptions, which are difficult and time consuming to identify through manual processes. Exceptions on the accession report will identify new employees that should be on the gross pay file, but are not on the gross pay file. Exceptions on the separation report will identify separated employees that are on the gross pay file, but should not be on the gross pay file. Excel is a powerful tool and can analyze thousands of lines of data in a matter of seconds. In addition, Excel array formulas can save time by automating the process of finding and writing the exceptions to a new Excel

Worksheet for corrective action. The automation and increased efficiency is an example of the prodigious use of Excel formulas.

The benefit to using powerful Excel tools for monitoring activities is the ability to conduct an analysis of the entire data set instead of just a few samples, which makes identifying exceptions more likely. In addition, an automated process means there is less time spent conducting monitoring activities by manual means. Using the Excel spreadsheet for monitoring activities does not touch any part of the data processing, so there are no requirements to make the Excel spreadsheet auditable. However, precautions should be in place to protect personally identifiable information and to limit the access to those with a specific need to access the populated Excel spreadsheets. Conducting and documenting monitoring activities is part of compliance with FIAR guidance.

Conclusion

In conclusion, there is no single root cause, which is attributable to the inability of the DoD to comply with the Chief Financial Officers Act of 1990. Rather, there are many factors to consider when analyzing the perplexing problem of the DoD's inability to provide clean financial statements. From a technical standpoint, the primary factors are the use of legacy IT systems, the sheer number of IT systems in use, the decentralized IT environment that exists, the interfaces between the numerous IT systems, and the ineffective processes controls, business controls, and cybersecurity controls around the various IT systems. In addition, there are human factors to consider, such as the cultural resistance to change, the lack of skilled financial management personnel, the incomplete corrective action plans, and the ineffective monitoring and reporting. It almost seems like humans have begun turning over the entire financial business process to a menagerie of IT systems, all lacking the artificial intelligence required to provide auditable output, which was never the intent of developing information technology systems. When interfaces break and reconciliations fail, unsupported journal vouchers become necessary.

Resolving this type of problem requires a multi-faceted approach, which is a continual process because of evolving technology. For example, IT systems must undergo evaluation periodically to determine the cost verses the benefits of replacement. Legacy IT systems need measured replacement in order to keep the maintenance of legacy systems and development of new systems in balance with the available funding. The goal is to reduce the number of IT systems needed to process data slowly, and to use Enterprise Resource Planning as much as possible.

From a human standpoint, the personnel processing the financial information should have a basic understanding of the entire financial business process, not just a portion of the financial

business process. Understanding the entire financial business process will help ensure an understanding of needed process changes. In addition, human personnel from the reporting entity must be cognizant of the fact that the reporting entity is ultimately responsible for the integrity of the financial data. In addition, the reporting entity must verify that the data processed correctly, regardless of the service level agreement in place with service providers.

The final considerations are the need for strong internal business controls and cybersecurity controls. Simply appending internal business controls and cybersecurity controls to the end of an entity's standard operating procedure will not be effective; embedding internal business controls and cybersecurity controls within the standard operating procedure is necessary. There is some synergistic value in implementing internal business controls and cybersecurity controls together because some of the controls overlap each other. Taking advantage of any overlap in controls and implementing the controls together can save time and help keep costs down.

This research project has shown that considerations of all of the above factors are necessary to mitigate the challenges the D0D is facing. Implementing strong internal business controls and strong cybersecurity controls in the important domains of segregation of duties, security management, access controls, configuration management, and continuity of business operations, will help improve auditability. In addition, the use of financial information technology systems that meet auditability standards is a necessity.

References

America Institute of CPAs. (2017). *SOC 1 - SOC for service organizations:: Internal controls over financial reporting*. Retrieved from https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC1Report.aspx

Armul, K. E. (2009). Progress of federal financial management: The CFO Government Management Reform Act, and beyond. *Issues in Innovation, 3*(2), 14. Retrieved from https://search.proquest.com/docview/225155855?accountid=28902

Atoum, I., Otoom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Securtiy; Bradford, 22*(3), 251-264. Retrieved from https://search.proquest.com/docview/1660151917?accountid=28902

Bell, G. (2014, 3 27). *Cyber risk area of focus for audit committee.* Retrieved from KPMG-Institutes: http://www.kpmg-institutes.com/content/dam/kpmg/auditcommitteeinstitute/pdf/2014/cyber-risk-areas-of-focus-audit-committee.pdf

Bhadauria, R., Borgohain, R. Biswas, & A. Sanyal, S. (2014). Secure Authentication of cloud data mining API. *Acta Technica Coriniensis - Bulletin of Engineering, 7*(1), 183-191. Retrieved from https://search.proquest.com/docview/1503139722?accountid=28902

Center for Audit Quality. (n.d.). Guide to internal control over financial reporting. Washington, D.C., United States. Retrieved June 18, 2017, from http://www.thecaq.org/sites/default/files/caq_icfr_042513.pdf

DCPAS Department of Defense - Defense Civilian Personnel Advisory Service. (2017, July 8). *HR LOB Shared Service Center Catalog.* Retrieved from Office of Personnel Management: https://www.opm.gov/services-for-agencies/hr-line-of-business/shared-service-center-catalog/department-of-defense-defense-civilian-personnel-advisory-service-dcpas.pdf

Deloitte. (2013a, 7 11). *The 8-character password is no longer secure.* Retrieved from The Wall Street Journal: http://deloitte.wsj.com/cio/2013/07/11/the-8-character-password-is-no-longer-secure/

Deloitte. (2013b, October 1). *When companies become prisoners of legacy systems.* Retrieved from The All Street Journal: http://deloitte.wsj.com/cio/2013/10/01/when-companies-become-prisoners-of-legacy-systems/

DoD_7000.14_R Office of the Under Secretary of Defense (Comptroller). (2017, June). *DoD_7000.14_R - Financial Management Regulation - Combined_Volume 1-16.pdf.* Retrieved from http://comptroller.defense.gov/Portals/45/documents/fmr/Combined_Volume1-16.pdf

DoDIG. (2016, Feb 25). *DoDIG_2016_054 Navy controls for invoice, receipt, acceptance, and property transfer system needs improvement.* Alexandria: government. Retrieved from http://www.dodig.mil/pubs/documents/DODIG-2016-054.pdf

DoDIG D_2008_084. (2008). *Journal vouchers processed by the defense finanace and accounting service for the navy working capital fund.* Department of Defense. Arlington: Governemnt. Retrieved from http://www.dodig.mil/audit/reports/fy08/08-084.pdf

DoDIG_2012_051. (2012). *DodIG_2012_051 Navy enterprise resource planning system does not comply with the standard financial information structure and U.S. government standard general ledger DODIG-2012-051.* Government, Department of Defense | Inspector General. Alexandria: Government. Retrieved 6 2, 2017, from file:///C:/Users/Tecra/AppData/Roaming/Mozilla/Firefox/Profiles/zo49ojau.default/zotero/storage/RUNNQ4M9/dodig-2012-051.pdf

DoDIG_2015_144. (2015). *DODIG_2015_144, Summary of DoD Office of the Inspector General audits of DoD financial management challenges - DODIG-2015-144.pdf.* Government, Department of Defense | Inspector General. Alexandria: Government. Retrieved 6 1, 2017, from http://comptroller.defense.gov/Portals/45/documents/micp_docs/Reference_Documents/DODIG-2015-144.pdf

DoDIG_2016_113. (2016). *DODIG-2016-113, Army General Fund Adjustments Not Adequately Documented or Supported - DODIG-2016-113.pdf.* Alexandria: Department of Defense | Inspector General. Retrieved 5 12, 2017, from http://www.dodig.mil/pubs/documents/DODIG-2016-113.pdf

Dorsey, P. (2005, 4 26). *Top 10 reasons why systems projects fail.* Retrieved from Dulcian, Inc.: https://www.hks.harvard.edu/m-rcbg/ethiopia/Publications/Top%2010%20Reasons%20Why%20Systems%20Projects%20Fail.pdf

DSecretary of the Army. (2016, 6 22). *Memorandum for distribution subject: Army Directive 2016-18 (Divesting legacy information technology hardware, software, and services in support of the Army network).* Retrieved 5 31, 2017, from Army: http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/Army%20Directive%202016-18%20(Divesting%20Legacy%20IT)%20(Final).pdf

Eiband, M., Eveleigh, T. J., Holzer, T. H., & Sarkani, S. (2013). Reusing DoD legacy systems: Making the right choice. *Defense AR Journal, 20*(2), 154-173. Retrieved from https://search.proquest.com/docview/1440345343?accountid=28902

Eliot, L. B. (1994, July 11). Legacy systems, legacy options. *Computerworld, 28*(28), p. 86. Retrieved from https://search.proquest.com/docview/216020109?accountid=28902

Ensmenger, N. L. (2003). Letting the "computer boys" take over: Technology and the politics of organizational transformation. *International Review of Social History, 48*, 153-180. Retrieved from https://search.proquest.com/docview/203569275?accountid=28902

Farlex Financial Dictionary. (2012). *Accountant's Opinion*. Retrieved from TheFreeDictionary.com: http://financial-dictionary.thefreedictionary.com/clean+opinion

Financial Accounting Foundation. (n.d.). *The importance of generally accepted accounting principles (GAAP)*. Retrieved 6 11, 2017, from Accounting Foundation: http://www.accountingfoundation.org/cs/ContentServer?c=Page&pagename=Foundation%2FPage%2FFAFBridgePage&cid=1176164538898#section_2

Fosse, E., & Delp, C. L. (n.d.). Systems engineering interfaces: A model based approach. Jet Propulsion Laboratory, California Institute of Technology. Retrieved from http://www.omgsysml.org/System_Engineering_Interfaces-IEEE_2013.pdf

GAO_092_32G Government Accountability Office. (2009). *Federal Information System Controls Audit Manual (FISCAM.* Washington: government. Retrieved from http://www.gao.gov/assets/80/77142.pdf

GAO_13_283 Government Accountability Office. (2013, February). *High-risk series: An update.* Report to Congressional Committees, Washington. doi:http://www.gao.gov/assets/660/652133.pdf

GAO_14_308 United States Government Accountability Office. (2014, May). Information technology SSA needs to address limitations in management controls and human capital planning to support modernization efforts. *Report to the Chairman, Subcommittee on Social Security, Committee on Ways and Means, House of Representatives.* Washington, D.C., United States. Retrieved from http://www.gao.gov/assets/670/663057.pdf

GAO_17_317 Government Accountability Office. (2017). *Progress on many high-risk areas, while substantial efforts needed on others.* Government Accountability Office. Government Accountability Office. Retrieved from http://www.gao.gov/assets/690/682765.pdf

GAO_17_85 Government Accountability Office. (2017). DoD financial management: Significant efforts still needed for remediating audit readiness deficiences. (p. 76). Government Accountability Office. Retrieved from https://www.gao.gov/assets/690/682652.pdf

GAO-07-1173G - Untied States Governemnt Accountability Office & the President's Council on Integrity & Efficiency. (2007). *Financial Auditors Manual - Volume 3.* Washington: Government. Retrieved from http://www.gao.gov/assets/80/76993.pdf

GAO-08-585G - United States Government Accountability Office & the President's Council on Integrity & Efficiency. (2008). *Financial Audit Manual Volume 1.* Washington: Government. Retrieved from https://www.gao.gov/assets/80/77063.pdf

GAO-08-586G - United States Government Accountability Office & the President's Council on Integrity & Efficiency. (2008). *Financial Audit Manual - Volume 2.* Washington: Governemnt. Retrieved from http://www.gao.gov/new.items/d08586g.pdf

Gottlieb, A. (2012, 10 8). Addressing WAN latency issues in application performance. *Network World*. Framinham, MA, United States. Retrieved from http://www.networkworld.com/article/2223275/cisco-subnet/addressing-wan-latency-issues-in-application-performance.html

Haakonsson, D. D., Burton, R. M., Obel, B., & Lauridsen, J. (2008). How failure to align organizational climate and leadership style affects performance. *Management Decision, 46*(3), 406-432. doi:http://dx.doi.org/10.1108/00251740810863861

Hale, B., Grimaila, M., Mills, R., Haas, M., & Maynard, P. (2010). Communicating potential mission impact using shared mission representations. *Paper presented at the 120-XII.* Retrieved from https://search.proquest.com/docview/869617243?accountid=28902

Headquarters, Department of the Army, Office of the Administrative Assistant (OAA). (2014, 12 12). *OAA | HQDA Organizational Chart*. Retrieved May 31, 2017, from OAA | HQDA: http://www.oaa.army.mil/hqda.aspx

Higgs, R. (2007). Military-economic fascism: How business corrupts government, and vice versa. *The Independent Review, 12*(2), 99-316. Retrieved from https://search.proquest.com/docview/211221085?accountid=28902

Host Analytics. (2015). Five reasons to move off Excel for consolidation and close. Redwood City, California, United States. Retrieved from http://www.brittenford.com/wp-content/uploads/2016/03/Five-Reasons-to-Move-off-Excel-for-Consolidation-and-Close.pdf

House of Representatives. (2017, June 21). H.R 2810-fy18 national defense authorization bill. Washington, D.C., United States. Retrieved from http://docs.house.gov/meetings/AS/AS26/20170621/106126/BILLS-115HR2810ih-ETC.pdf

Investor Words. (2017). *What is a journal voucher? Definition and meaning.* Retrieved 6 1, 2017, from Investor Words: http://www.investorwords.com/16499/journal_voucher.html

Joint Task Force Transformation Initiative (b). (2015). *SP_800_53 Security and privacy controls for federal information systems and organizations.* NIST. Washington: Government. Retrieved from National Institute of STandards and Technology: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Joint Task Force Transformation Initiative. (2016a). *SP 800-37 Revision 1: NIST guide for applying the risk management framework to federal information systems: A security life cycle approach.* NIST. Washington: Government. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Kathuria, S. (2009, Summer). Best practices for compliance with new government contractor compliance and ethics rules under the Federal Acquisition Regulation. *Public Contract Law Journal, 38*(4), 803-856. Retrieved from https://search.proquest.com/docview/218709757?accountid=28902

Kelly, S., Holland, C., Gibson, N., & Light, B. (1999, 07). A business perspective of legacy systems. *Communications of the Association for Information Systems, 2*(7), 1-27. doi:1529-3181

Koerner, B. J. (2016, 10 23). Inside the cyberattack that shocked the US Government. *Wired* . New York, New York, United States. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

Kutz, G. (2014). *GAO-14-704G, STANDARDS FOR INTERNAL CONTROL IN THE FEDERAL GOVERNMENT - 665712.pdf.* Government, Government. Washington: United States Government Accountablity Office. Retrieved 17 5, 2017, from http://www.gao.gov/assets/670/665712.pdf

Kutz, Gregory. (2002). *GAO-02-873T DOD management: examples of inefficient and ineffective business processes.* Washington: Government Accountability Office. Retrieved 6 18, 2017, from http://www.gao.gov/assets/110/109449.pdf

Lippuner, D. (2014). Something's gotta give! *The Journal of Government Financial Management, 63*(1), 26-30. Retrieved from https://search.proquest.com/docview/1510293186?accountid=28902

Lunney, K. (2016, April 18). *OPM to agencies: Figure out how to close skills gap in the federal workforce.* Retrieved from Government Executive: http://www.govexec.com/management/2016/04/opm-agencies-figure-out-how-close-skills-gap-federal-workforce/127580/

McNermey, L. C. (2003). *Transforming the Army's legacy personnel systems.* U.S. Army War College, U.S. Army. Carlisle Barracks: U.S. Army War College. Retrieved May 31, 2017, from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA414511

Microsoft. (2017a). *Overview of formulas in Excel.* Retrieved from Microsoft Support: https://support.office.com/en-us/article/Overview-of-formulas-in-Excel-ecfdc708-9162-49e8-b993-c311f47ca173

Microsoft. (2017b). *What can an ERP system do for my business?* Retrieved 6 5, 2017, from Microsoft: https://www.microsoft.com/en-us/dynamics365/what-is-erp

Napoleon, V. J., & Henry, S. (2013). Defense contract audit agency's access to contractor internal audit reports: Is Newprot News still the standard? *Public Contract Law Journal, 42*(3), 517-547. Retrieved from https://search.proquest.com/docview/1368940429?accountid=28902

National Institute of Standards and Technology (NIST). (2017, 01 30). *Computer security division computer security resourse center: FISMA background.* Retrieved from NIST: http://csrc.nist.gov/groups/SMA/fisma/overview.html

Nickell, C. (2017). Complimentary user entity controls | SSAE 16 compliance | ssae16.org. Retrieved from https://socreports.com/glossary/79-complimentary-user-entity-controls-ssae-16-compliance.html

Norquist, D., Sherry, P., Bedker, L., & Janssen, S. (2014). DHS: The road to a 'clean' opinion. *The Journal of Financial Management, 63*(2), 38-46. Retrieved from http://www.kpmg-institutes.com/content/dam/kpmg/governmentinstitute/pdf/2014/dhs-clean-opinion.pdf

Office of Environmental Information. (2007, April). Guidance for preparing standard operating procedures (SOPs). Washington, D.C., United States. Retrieved from https://www.epa.gov/sites/production/files/2015-06/documents/g6-final.pdf

Office of Management and Budget. (2016). *OMB A-130: Managing information as a strategic resource.* government. Retrieved from https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf

Office of the Under Secretary of Defense (Comptroller) / Chief Financial Officer. (2017, April). *FIAR Guidance.* Retrieved June 1, 2017, from Government: http://comptroller.defense.gov/Portals/45/documents/fiar/FIAR_Guidance.pdf

Office of Under Secretary of Defense Comptroller in collaboration with the Finacial Improvement and Audit Readiness Committee. (2005). *FIAR - Defense financial*

improvement and audit readiness plan. Washington: Office of Under Secretary of Defense Comptroller. Retrieved 5 5, 2017, from http://comptroller.defense.gov/Portals/45/documents/fiar/FIAR_Plan_Dec_2005Complete.pdf

OMB A-123 Office of management and budget. (2004, 12 21). *OMB Circular A-123 - management's responsibility for internal control.* Retrieved from The White House: https://www.whitehouse.gov/omb/circulars_a123_rev

Paltrow, S. (2016). *U.S. Army fudged its accounts by trillions of dollars, auditor finds.* Manhattan: Reuters. Retrieved June 18, 2017, from http://www.reuters.com/article/us-usa-audit-army-idUSKCN10U1IG

Pava, M. L. (n.d.). *Auditing Accounting*. Retrieved 6 12, 2017, from Encyclopedia Britannica: https://www.britannica.com/topic/auditing-accounting

Peled, A. (2016, July 26). Do computers cut red tape? *The American Review of Public Administration, 31*(4), 414-435. doi:10.1177/02750740122065027

Pine, M. (2017, February 05). *Why Do Companies Outsource?* Retrieved May 03, 2017, from the balance: https://www.thebalance.com/why-do-companies-outsource-2553035

Powner, D. A. (2016). Federal agencies need to address aging legacy systems. *Testimony before the Committee on Oversight and Government Reform, House of Representatives.* United States Accountability Office. Retrieved from http://www.gao.gov/assets/680/677454.pdf

Radin, B. (1998, July/August). The government performance and results act (GPRA): Hydra-headed monster or flexible management tool? *Public Administration Review, 58*(4), 307-316. Retrieved from https://search.proquest.com/docview/197169086?accountid=28902

Ren, C. H., B. S., U.S.A.F., & Prebble, M. (2010). Improving the initiation of acquisition activities for automated information systems. *Defense AR Journal, 17*(4), 418-435. Retrieved from https://search.proquest.com/docview/762996105?accountid=28902

Roberts, W. (2013). Audit readiness: Sustaining the army's strength. *Army Sustainment, 45*(3), 13-16. Retrieved from https://search.proquest.com/docview/1355701109?accountid=28902

Shelly, G. B., Cashman, T. J., & Forsythe, S. G. (1985). *Structured COBOL flowchart edition.* Brea, California, United States: Anaheim Publishing Company, Inc.

Smithberger, M. (2016, 3 28). *Will the Pentagon ever be able to be audited?* Retrieved 5 31, 2017, from Project On Government Oversight: http://www.pogo.org/straus/issues/defense-budget/2016/will-the-pentagon-ever-be.html

SSAE 16 Office of the Under Secretary of Defense (Comptroller). (2015, May 29). What are SSAE 16 report and how do I use them to support my audit and A-123 compliance? *Presentation to American Society of Military Comptrollers Professional Development Institute*. Retrieved from http://www.asmconline.org/wp-content/uploads/2015/06/72-Keith-Kadiri.pdf

Stowe, A. M. (1995). Contracting for government financial statement audits. *The Government Accountants Journal, 43*(4), 28. Retrieved from https://search.proquest.com/docview/222366781?accountid=28902

Tann, A., & Chae, D. (2016, 6 2). Synergistic efforts between financial audit and cyber security. *Department of the Navy Chief Information Officer; Financial Policy and Systems*. Orland. Retrieved from http://www.pdi2016.org/wp-content/uploads/2016/06/82-Tann-Chae-Synergistic-Efforts-Between-Financial-Audit-and-Cyber-Security.pdf

The White House. (2017, July 15). *Office of Management and Budget: Information for agencies*. Retrieved from the WHITE HOUSE: https://www.whitehouse.gov/omb/information-for-agencies/circulars

Thornton, D. (2017, May 10). *DoD comptroller nominee: 'It is time to audit the Pentagon'*. Retrieved May 11, 2017, from FederalNewsRadio.com: https://federalnewsradio.com/hearingsoversight/2017/05/mccain-dods-inability-to-pass-an-audit-must-end/

Trader-Leigh, K. (2002). Case study: Identifying resistance in managing change. *Journal of Organizational Change Management, 15*(2), 138-155. Retrieved from https://search.proquest.com/docview/197611827?accountid=28902

United States Congress. (1990, 1 23). Chief Financial Officers Act of 1990. *United States Code*. (U. S. Congress, Ed.) Washington, DC, United States. Retrieved 6 4, 2017, from https://govinfo.library.unt.edu/npr/library/misc/cfo.html

United States Congress. (1993, 1 5). Government Performance & Results Act of 1993. Washington, D.C., United States. Retrieved from https://govinfo.library.unt.edu/npr/library/misc/s20.html

United States Congress. (1994, 1 25). Government Management Reform Act of 1994. Washington, D.C., United States. Retrieved from https://govinfo.library.unt.edu/npr/library/misc/s2170.html

United States Congress. (1995, May 22). Paperwork Reduction Act of 1995. Washington, D.C., United States. Retrieved from https://www.gpo.gov/fdsys/pkg/PLAW-104publ13/html/PLAW-104publ13.htm

United States Congress. (1996a, February 10). Information Technology Management Reform Act of 1996. Washington, D.C., United States. Retrieved from https://govinfo.library.unt.edu/npr/library/misc/itref.html

United States Congress. (1996b, September 28). Federal Financial Management Act of 1996. Washington, D.C., Unites States. Retrieved from https://www.congress.gov/bill/104th-congress/house-bill/4319

University of Maryland University College. (2017, July 5). *Introduction to cyber security: If you're new to cyber security, we've created a primer on this exciting field*. Retrieved 2017, from University of Maryland University College: http://www.umuc.edu/academic-programs/cyber-security/about.cfm

Waterman, S. (2017, April 3). What's in the NIST cybersecurity controls catalogue update? Washington, DC, United States: cyberscoop. Retrieved from https://www.cyberscoop.com/nist-cybersecurity-controls-catalogue-800-53-rev5-fisma/

Whitehouse, T. (2015, October 6). *Frustrating risk with the right internal control framework.* Retrieved 2017, from Compliance Week: https://www.complianceweek.com/news/news-article/frustrating-risk-with-the-right-internal-control-framework#.WWQmBYTyv3g