JOURNAL OF GOVERNMENTAL & NONPROFIT ACCOUNTING
Vol. 10, No. 1
2021
pp. 26–49

American Accounting Association
DOI: 10.2308/JOGNA-17-001

Integrated Business Intelligence and Analytics: The Case of the Department of the Navy

Robert J. Eger III
Naval Postgraduate School

Christy Smith
University of New Haven

ABSTRACT: From a stakeholder perspective, this study explores the viability of data analytics as a tool in government fraud prevention. Using an interview methodology, we analyze the implications of business intelligence and analytics fraud tools on procurement stakeholders. We find that implementing and integrating business intelligence and a fraud program streamlines processes by consolidating information and presenting data within a unique program. The functioning data analytics program increases our stakeholders' confidence level without alleviating their responsibility to perform due diligence in their management functions. Our stakeholders recognized a potential increase in workload; however, they acknowledged no perceived increase in undue administrative burden.

JEL Classifications: M48.

Data Availability: Data are available from the authors.

Keywords: business intelligence and analytics; fraud; interviews.

I. INTRODUCTION

Practitioner's use of business intelligence and analytics (BIA) has gained traction in accounting and finance during the past two decades. Recent studies have demonstrated the role of BIA capability to support advanced management accounting and control

We thank Raymond J. Lanclos III, Amilcar Menichini, Thurman B. Phillips, Juanita M. Rendon, and Rene G. Rendon for their outstanding research guidance and assistance throughout this endeavor. We thank Raymond J. Lanclos III and Thurman B. Phillips for providing us exceptional data collection.

Robert J. Eger III, Naval Postgraduate School, Graduate School of Defense Management, Department of Financial Management, Monterey, CA, USA; Christy Smith, University of New Haven, Henry C. Lee College of Criminal Justice and Forensic Sciences, Department of Public Administration, West Haven, CT, USA.

Editor's note: Accepted by Vaughan S. Radcliffe.

Submitted: January 2017
Accepted: November 2020
Published Online: March 2021

systems (Elbashir, Collier, and Sutton 2011), regulatory compliance, and risk management (Nasar and Bomers 2012; Starr, Newfrock, and Delurey 2003). This prior research explains the significant investments in BIA by organizations to unlock the potential of large data warehouses in accruing benefits (Anderson-Lehman, Watson, Wixom, and Hoffer 2004; Appelbaum, Kogan, and Vasarhelyi 2017). In the fraud context, BIA can be used to create fraud prediction models that assist auditors in improving portfolio management and audit planning decisions and identify firms for potential fraud investigation (Chen, Chiang, and Storey 2012; LaValle, Lesser, Shockley, Hopkins, and Kruschwitz 2011).

BIA principally seeks to know how managers can make better decisions once they have better data and analytic tools for decision making (Davenport and Harris 2007). An implicit assumption underpinning this literature is that organizations capture value while continuing to function as before (Davenport, Harris, and Morison 2010). These managerial and organizational activities lead to our exploratory research question: How does BIA's prospective implementation affect stakeholders? We propose that BIA influences stakeholders and various other user and provider groups in anomaly detection (fraudulent behavior). How and what affects the stakeholder is a puzzle that we investigate through structured and unstructured questions posed in an interview process. Prior literature has explored the stakeholder concept in two fundamental aspects: the first is the attitude of corporate validity, where the corporation is managed, or should be managed, for the benefit of the stakeholder, broadly defined to include customers, suppliers, owners, employees, and local communities; and the second is a guardian attitude where managers in the corporation are trustees of the firm acting in the interest of stakeholders, where survival and safeguarding the firm are paramount (Evan and Freeman 1993). Our work adds to the latter, broadening the work of Rezaee (2005), Hogan, Rezaee, Riley, and Velury (2008), Greenlee, Fischer, Gordon, and Keating (2007), and Ugrin and Odom (2010) into the governmental sector. We add to this literature by interviewing four groups, including data analytic users, fraud investigators, fraud auditing stakeholders, and data analytic providers. Each group provided at least two participants for the interviews. Using this broad interviewing approach, we narrow our exploratory investigation to those stakeholders impacted by the U.S. Navy procurement system.

Our study leads to an important finding that the implementation and integration of a BIA fraud program reveals procedural, not policy implications. Why this observation? BIA streamlines processes by consolidating information and presenting data within a single package, supporting the prior literature findings that BIA allows for large amounts of raw data to improve operational and/or strategic performance through an increase in interpretation (Vasarhelyi and Halper 1991; Vasarhelyi, Kogan, and Tuttle 2015). Once the streamlining of processes is in place, procedural safeguards are needed to assure the maximization of employee response to potential wrongdoing (Miceli, Near, Rehg, and Van Scotter 2012). Our findings infer that the knowledge gain of functioning data analytics increases the confidence level of our stakeholders without alleviating their responsibility to perform due diligence in their management functions or adding undue administrative burden. Our results regarding undue burden and due diligence help the audit community address the costs and benefits associated with Big Data burdens on stakeholders, one of the concerns raised in Appelbaum et al. (2017) as a challenge in audit engagements.

Our exploratory analysis leads our stakeholders to conjecture that proactively protecting critical resources (money, manpower, and time) from fraudulent activities is the essential aspect of a BIA program for fraud. The inference is that BIA is perceived to identify fraudulent activities before they occur, freeing up resources for more efficient use.

The organization of the remainder of the paper is as follows. We provide an overview of BIA in Section II. We identify the stakeholders, critical issues, and managerial implications of using BIA in

anomaly detection in the U.S. Navy in Section III. To assist us in our exploration, we offer a conceptual model in Section IV. We then define our interview methodology in Section V. Results are presented in Section VI. Using our interviewers, in Section VII we provide a discussion of how and why the effects of BIA anomaly detection are perceived to impact stakeholders in U.S. Navy procurement. We conclude in Section VIII by linking the interview information with BIA anomaly detection in the U.S. Navy.

II. BIA OVERVIEW

Traditionally, *business intelligence and analytics* (BIA) is an umbrella term to describe concepts and methods that improve decision making through the use of fact-based support systems. BIA's primary objectives are to enable interactive and easy access to diverse data, enable manipulation and transformation of these data, and provide managers and analysts the ability to conduct appropriate analyses and perform responses (Turban, Sharda, Aronson, and King 2008; Wixom, Watson, and Werner 2011).

According to Beyer (2011), the trend of Big Data over the past decade has quietly descended on many communities, from government and e-commerce to health and sports organizations. The umbrella of BIA covers a range of techniques to provide both strategic advantage and enhance control and monitoring. Given the enormous amount of information contained within current-generation information systems, processing some on a real-time basis, the progressive shift in practice toward the maximum possible degree of automation provides the technological basis for business transaction monitoring. This monitoring affords gains in reducing anomaly detection costs compared to earlier collecting and processing of traditionally structured payroll, employee, supplier, and product information, often collected and analyzed via relational database management systems.

III. ANOMALY DETECTION AND STAKEHOLDERS

The U.S. federal government has been using relational systems for anomaly detection as a means of battling fraud, waste, and abuse issues for many years (GAO 2006, 2013; OIG 2009). The current process—relying on auditor investigations, relational data inquires, and whistle-blowers—has been effective but is initiated only after the commission of a crime. The idea of moving the federal government from a "pay and chase" into a preventive process creates the ability to leverage responsiveness through BIA, thereby assisting detection and enforcement in fraudulent behavior (Hughes 2011; Lemon 2012). Given the significant amount of volume, variety, and velocity of data, in combination with the structured and unstructured nature of the data, benefits, and costs in anomaly detection and fraud prevention accrue to the government (Maurno 2013).

Benefits to the federal government amass in the multifaceted process using data integration and analytical approaches. Given that BIA encompasses rules-based, distributional, predictive, and linkage analytics, benefits come in a variety of forms, with the most critical achieving early responsiveness to fraudulent behavior (Lemon 2012). Using rules-based analytics, which involves a series of business rules that apply conditional statements to address logical questions (Davenport and Harris 2007), allows a filter for activities and transactions to uncover anomalies. Distributional analytics can discover anomalies within data patterns, detecting abnormal individual and aggregate patterns that reveal unknown anomalies (Slavakis, Kim, Mateos, and Giannakis 2014). Predictive analytics uses attributes of past (known) fraudulent behaviors to predict future fraud behavior.

In contrast, social network analytics uses associative link analysis to enable immediate reactions when links are discovered, preventing or limiting the impact of fraudulent behavior (Maurno 2013). Using these analytical approaches requires an enterprise perspective (Kearney 2013). The ability to integrate analytical programs to prevent government fraud is perceived to have a substantial impact on government spending, with savings attributable to fraud reduction.

The potential costs associated with BIA are nontrivial. Beyond the identifiable direct costs of software and hardware integration, BIA proponents request organizations to consider the impact of their actions and decision making on their various stakeholders. From a normative view, an organization needs to consider the various stakeholders and balance their divergent interests (Agle et al. 2008; Freeman 1984; Frooman 1999; Ullmann 1985). The standard categorizations of stakeholders are on a priority rank, those identified as primary stakeholders versus those identified as secondary stakeholders (Clarkson 1995). Primary stakeholders are those actors who enjoy a direct and contractually determined relationship with the organization, whereas secondary stakeholders are actors at the boundaries of the firm who may be affected by the firm's actions but lack any contractual connection (Collier and Roberts 2001; Carroll 1991).

IV. CONCEPTUAL FRAMEWORK

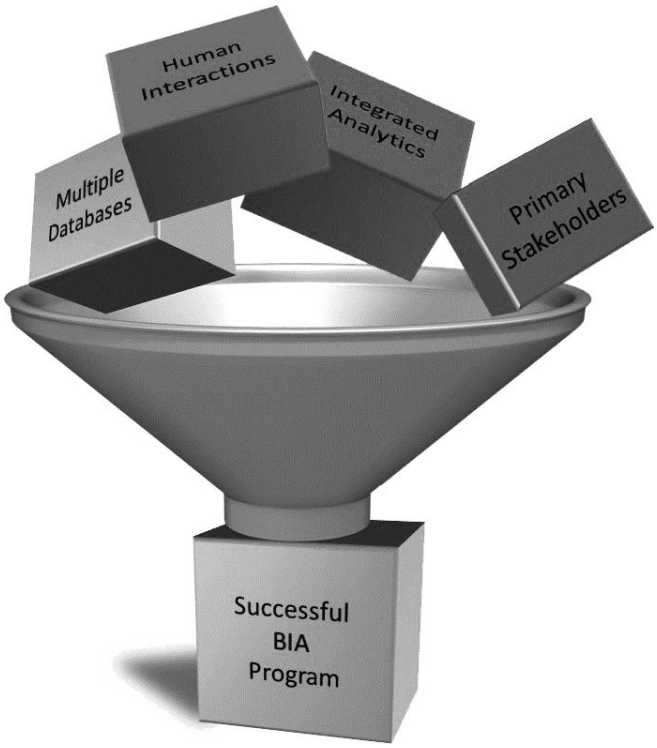
Drawing on the literature, decision making with data focuses on interpretations from hints in the data (Chater, Tenenbaum, and Yuille 2006). Drawing inferences depends on inductive reasoning, either heuristic-based (pattern matching) or rules-based processes, such as rational choice (Ferreira, Garcia-Marques, J. Sherman, and S. Sherman 2006). For fairly simple decisions, pattern matching is very quick. The decisionmaker merely executes actions similar to those applied in the past. Klein (2008) argues that if the match between the current and previous is positive, the decision is implemented. If not, changes occur with a second round of evaluation taking place. If the decision is perceived as very complex, decisionmakers evaluate the similarity of the situation relative to those stored in memory, determining whether more information is required. After assessment, the decisionmaker chooses a course of action, with an evaluation of the potential outcomes (Klein and Klinger 1991).

BIA research illustrates that the decisionmaker employs these cognitive processes, based on the complexity of the problem, drawing conclusions for the business problem at hand. Included in a business problem, such as accounting or auditing, the decisionmaker then must understand the systems in use, how those technologies work, and have an appreciation for the limitation of the analytic techniques being used (Huang, Eades, and Hong 2009).

Focusing on this prior research, we offer a framework to guide our methodology and analysis. The framework, as identified in Figure 1, incorporates the theoretical insights obtainable from BIA's rules-based, distributional, predictive, link, and analytic approaches (Richards 2016; Vo, Thomas, Cho, De, and Choi 2018).

We conceptualize the framework to have four components—multiple databases, primary stakeholders, integrated analytics, and human interactions—combining into a successful BIA program. Stakeholders are those actors that engage under the BIA umbrella. These stakeholders are groups involved in the approaches associated with minimizing anomalies for an organization. Let us consider the stakeholders surrounding the rules-based heuristic. This group focuses on business rules within the anomaly detection process (Simpao, Ahumada, Gálvez, and Rehman 2014). The second primary stakeholder group is composed of those who

FIGURE 1
Conceptual Framework for a BIA Program



discern anomalies within data patterns, thereby detecting abnormal individual and aggregate patterns, uncovering previously unknown anomalies (Chen et al. 2016). The third are those professionals tasked with using past attributes to predict future behavior (Gunasekaran et al. 2017). The role of the last group of the primary stakeholders is to investigate networks and associative links to enable immediate reactions in the prevention or control of the anomaly behavior (Aggarwal 2011).

With the stakeholders identified, our conceptual framework shows a mixing of two additional elements, integrated analytics and human interactions. Integrated analytics mixing allows for the unique characteristics of data and processes that are quite varied to be used in anomaly detection. Prior work shows that integrated analytics can assist in the collection of data in a structured format (Alblawi and Alhamed 2017). However, there is a significant variety of multiple databases (i.e., free-form text, social graphs, and operational data) to be integrated. The last element in the mix is human interactions. Here, individual interactions, with both stakeholders and data integration, are influenced by ability and knowledge. Human interactions necessitate abilities to engage with exploratory and demand-driven processes with the goal of clear communication, often to an audience with little background in analytical techniques. The human element must produce high-confidence outcomes while preserving institutional memory by tracking the experiences of past decisions and allowing repeatability across investigations (Fisher, DeLine, Czerwinski, and Drucker 2012). Interactions of primary

stakeholders with each other, with data integration, and with human interactions combine into a successful program.

Application to the U.S. Navy

Applying our conceptual framework to procurement in the U.S. Navy, we look at four primary stakeholders in the U.S. Navy. We begin with the acquisition professionals who play a fundamental role as primary stakeholders, given their immersion in the Federal Acquisition Regulation (FAR), which is the principal set of rules regarding government procurement in the United States. The acquisition profession includes positions such as contracting officers, contracting officers' representatives, program managers, technical experts, and financial managers. These professionals have been identified as the first line of defense in preventing fraud, like internal auditors in firms (Rezaee 2005), given their involvement in rules-based anomaly prevention.

Our second group is the U.S. Navy procurement fraud investigation services. This group's mission is to assess abnormal patterns in revealing anomalies. These fraud investigators view fraud as "a knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment, a misrepresentation made recklessly without belief in its truth to induce another person to act, and unconscionable dealing" (Garner and Black 2009).

Our third group is the U.S. Navy auditors. Although the role of the auditor is elusive concerning fraud detection (Chong 2013; Humphrey, Turley, and Moizer 1993), government auditing professionals are primary stakeholders given that they are the last line of protection in the prevention or detection of fraud. Government auditing professionals have a responsibility to thoroughly review U.S. Navy records to determine whether there exists diversion of funds or over-invoicing of goods and services. In this vital role, what impacts government auditing professionals are aspects of the BIA program influencing existing policy and procedures. Unlike real-time continuous auditing (Appelbaum et al. 2017; Gonzalez and Hoffman 2018; Pathak, Chaouch, and Sriram 2005; Weins, Alm, and Wang 2017), the U.S. Navy's audit procedures are manual, and therefore are labor and time intensive. These constraints limit audit frequency to an annual occurrence. As a result, management and stakeholder reliance on financial information regarding procurement choices can lead to adverse resource allocation decisions.

Our final group is internal and external to the U.S. Navy—subject matter experts. Subject matter experts determine the composition of existing technology (Dooley, Levy, Hackney, and Parrish 2018) and address modifications essential for a BIA procurement fraud prevention program. As primary stakeholders, industry experts assure that the BIA industry's perspective is incorporated (Dooley et al. 2018) while offering subject matter experts that affect integration.

All these groups, both internal to the U.S. Navy and external, bring human interactions and abilities to engage with exploratory and demand-driven processes. The goal of these interactions is clear communication to an audience with little background in the BIA system. The human element needs to assure high confidence in anomaly detection, expressing the how and what questions of BIA as a function of combining institutional memory and external knowledge, ensuring repeatable outcomes across investigations (Fisher et al. 2012).

V. METHODOLOGY

To explore how and what questions affect a BIA fraud prevention program in the U.S. Navy, we use semi-structured interviews. To derive the questions for the interviews, we found it necessary to clarify our thinking by reviewing the literature on BIA development and implementation in private firms, a process like Horton, Macve, and Struyven (2004). To design

our questions, we assumed the implementation of the BIA fraud program when considering both the organizations' current and potential future states. In our development of the questionnaire, we considered the time required by the individual or group providing the information. We intended to have interviews that lasted from 30 minutes to one hour. We felt it would be essential to allow all interviewees the opportunity to receive an advance copy of the questionnaire. This process assisted in the minimization of the time required by the respondent(s). As we were designing the questionnaire, we felt that the variation in the expertise of our potential respondents necessitated different questionnaires. Two groups of interviewees, procurement fraud auditing professionals and procurement fraud investigating professionals, had identical questionnaires due to the similarities of their organizations.

Approval of our interview questionnaires was through the Institutional Review Board (IRB). The IRB approval occurred before providing our stakeholder and subject matter expert participants with the list of questions. We note that we conducted this research using the Department of the Navy personnel, which limited the personalization of questions and the number of interviewees. Before holding interviews with any of the stakeholders, we provided a statement to the purpose of our discussions. The purpose included an explanation that these interviews were to explore the viability of using data analytics software as a tool in procurement fraud prevention. Our method included strategies used in prior research (e.g., Marginson 2004) to ensure the validity and reliability of the data collected.

Communication with the stakeholders and subject matter experts included providing our objective for exploring the potential use of data analytics software in bringing an integrative approach to the active and passive detection of fraudulent procurements. In understanding existing data analytics technology and integration, we included subject matter industry experts to identify potential integration complexity, costs, and benefits.

Initial contact was made by email and telephone, where we outlined the objectives of the research, discussing research outputs, and provided an assurance of confidentiality (Yin 2014). The data collected include our interviews, follow-on emails, and follow-on telephone calls. Recording of the follow-on information was manual. The taped interviews were transcribed by a third party to enhance validity. After receiving the transcribed data, we reduced the data into manageable sets of information, determining themes, systematically presenting information, and describing meanings, while noting regularities, patterns, and explanations (Miles, Huberman, and Saldana 2014). We offer our interview instruments in the appendices.

VI. RESULTS

Our main objective is to explore the effect of BIA expansion into the U.S. Navy. We present an analysis of the identified stakeholders' responses to the interview questions following Tellis (1997) and Yin (1993), who recommend that the preparation of narrative accounts should be around the relevant topic, not the individual interview. The analysis focuses on our conceptual framework—databases, stakeholders, integration process, and human interactions—and how BIA fraud prevention plays a role in procurement fraud protection and what its impact might be. This leads to providing connections to each of the stakeholders and subject matter experts' roles in the potential transformation of the U.S. Navy's procurement fraud processes.

Implications on Stakeholders

How the implementation of a BIA fraud prevention process would impact the current stakeholders is an essential aspect of BIA. We define *processes* as the means and mechanisms

set in place through which organizations efficiently acquire goods and services (Lindsay, Downs, and Lunn 2003). We asked our interviewees several questions regarding what processes and procedures would be affected by the implementation of a BIA procurement fraud program, the methods needed for implementation, what changes to job requirements would be desired, and how this process would impact the organization.

Acquisition Stakeholders

Our first group is the acquisition stakeholders. The questions asked are available in Appendix A. Our questions were sent out before our interviews. This questionnaire led to a broader discussion with our acquisition stakeholders. Their engagement resulted in a refinement surrounding two potential areas that would be shaped by a BIA fraud procurement program: the reformation of existing processes and contractor performance management. This discussion led to unease about the additional administrative burdens the BIA fraud procurement could add.

Our stakeholders considered their current role in monitoring multiple databases as an essential issue of reformation. They surmised that a data analytics program could streamline the existing processes since it is using data from varying locations. The streamlining into a single place could change workload allowing identification of contracting trends and information. Acquisition Agency 2, Interviewee 1 said:

> Well, maybe you see that trend going up, and you stick that as a firm fixed price and on the next contract makes it a little bit easier and on that new contract, having that as a firm fixed price makes it less administratively burdensome on the contracting team. So I could see that potentially being helpful in that regard.

A data analytics program that identifies seasonal pricing trends may identify ideal times to agree on a fixed price for trending products reducing administrative burden, thereby lowering costs.

Consistently, interviewees saw the implementation of a BIA program as helping them to form better and faster decisions in the procurement process. Acquisition Agency 1, Interviewee 1 noted:

> This is simply providing them data to assist them in making that decision, and if they are uncomfortable with that decision, it would also suggest mitigation strategy. You know, what to do, who to talk to.

When asked about what would change in the process, opinions were quite direct. Acquisition Agency 1, Interviewee 1 said:

> Let me also put it to you this way; at present, you are aware that contracting officers have to go to four or five, perhaps more, websites—particularly for large acquisitions—to gain information about an offeror to on certain procurements check CPARs, check PPRS, check [SAM], formerly EPLS, maybe check [D&B] to see if they are a viable contractor. There is a number of places that they are supposed to go.

Acquisition Agency 1, Interviewee 3 followed up by saying that:

> We would hope that it [BIA] would streamline existing processes. Certainly, we are not looking to create a process that would slow down procurements.

A similar tone was heard from Acquisition Agency 2, Interviewee 1 when saying:

> But, we should have that visibility—I should be able to go to the Department of the Interior and see what they paid and if they got something for—you know, if we are buying the same thing. We have limited visibility into what their numbers really mean.

The other key area impacted with the implementation of a BIA program, from the acquisition professional's perspective, is the potential for the program to become a tool to monitor contractor performance proactively. One acquisition professional identified nonconforming products as their greatest challenge, more so than deliberate counterfeit products. As stated by Acquisition Agency 2, Interviewee 1:

> There are more people who give us the wrong item because they are stupid than give us the wrong item because they are trying to defraud us.

A BIA program helps identify these issues, either an item or a supplier, indicating to the acquisition professionals that they should proactively engage in a mitigation strategy. If the data analytics program assists in identifying trends in a supplier's behavior, fraudulent or not, the organization is provided information that implies a thorough inspection of the products delivered from that supplier. As stated by Acquisition Agency 1, Interviewee 3:

> I do certainly think it could be useful to maybe bring those things to the attention of the decision-makers and then make the decision if it meets—if it is actual fraud or if it is just an honest mistake or something like that.

The acquisition professional can inquire further by requesting traceability on the product submitted to the government. Only one of our interviewees' organizations had a department that internally tracks, but does not prohibit, suppliers suspected of improper behavior regarding supplies.

When discussing the impact on jobs and job requirements, there was a fear of an increase in administrative burden. Acquisition Agency 1, Interviewee 3 said:

> It would be something that they would have to understand to keep up on because I can see it very easily being put to the side when people are most focused on the mission and not necessarily entering data into a software program.

Although the potential of administrative burden exists, our interviewees found that overall the burden is small compared to the possible benefits. As stated by Acquisition Agency 1, Interviewee 2:

> So maybe a team of you guys kind of in the back room behind closed doors can go in and access the data, and it would be roughly transparent to us on the working floor. So, would it be burdensome to us? We may not even have to know about it. That is normally how fraud prevention works. You guys are behind the one-way glass kind of thing.

Acquisition Agency 1, Interviewee 1 commented that:

> If we would receive training or just awareness of what to look for and just like human trafficking. You know, we are not going to do it, but just make us aware. Train us on something, so if it does pop up if something smells funny, we want to know that hey, that smells funny for human trafficking or it smells funny for contract fraud. So just—and she pointed it out, but training for us.

Fraud Investigating Stakeholders

Interviews with members of the procurement fraud investigating profession highlighted the distinction between their processes for the generation of potential fraud cases and the investigative methods of the opening of a fraud case. The questions asked are available in Appendix B.

Investigators typically receive cases through two primary processes: qui tam (Broderick 2007; Caminker 1989) or the Defense Contract Audit Agency (DCAA). The qui tam, or whistleblower, is the best opportunity for case generation. As Fraud Investigative Agency, Interviewee 1 explained:

> It's usually, say an employee of Boeing or Northrop who sees fraud going on within their particular division of the company. You go, and you find an attorney who knows how to write and file qui tam lawsuits, and they file on your behalf. Your identity is sealed with the whole complaint, and then whatever military agency is affected . . . usually for these things, it is multiple agencies. The Army and the Air Force all do business, and the Navy does business with the same contractors. It will come down to us. I'll know who the complaint person is, but I am not allowed to release the name of the person who is filing the complaint.

Qui tam filings have restrictions with non-governmental employees. As indicated by Fraud Investigative Agency, Interviewee 1, the qui tam process was developed to encourage people to report fraud by protecting their identity, along with providing monetary incentives.

The second primary process that generates cases originates from the DCAA. Fraud Investigative Agency, Interviewee 1 summarized the process:

> They have their suspected irregularity form. It's a Form 2000 and if the auditors are just going in to do a standard, whatever it is they do, audit of these companies, when they see something that doesn't make sense, they will file a Form 2000, and those get filed with all the affected agencies who are—Army, Navy, Air Force.

Fraud investigators identified the possibility that as an investigating profession, with proper training and access to the BIA program, they would be able to generate their cases for investigation based on the data analysis created by the program, a proactive, not reactive opportunity. As offered by Fraud Investigative Agency, Interviewee 1:

> I think an agent with proper training would be able to navigate it and use it. So my answer to your number five is yes, I think the data analysis program would definitely help in detecting fraud.

Fraud investigators opined on what they want a BIA system to "red flag" and what linkages of data would be preferred. Fraud Investigative Agency, Interviewee 1 said:

> And you know one of the things that I see a lot in relationships, people from the contractor having some sort of direct or indirect, other relationship with people in the contracting office—which is a real red flag. Sometimes it's so indirect nobody really realizes it, but that's one of the other things, I have a case now that, it's most likely going to go nowhere, but I call it the felony Facebook friends case because when you look at, somebody made, like a family tree and there are so many last names that are the same and all the people, you know, there's people that work for the government, the customer, command, and they have relatives that work for the prime contractor, and yet nobody has said anything, and I know I'm not going to get a U.S. attorney to prosecute felony Facebook friends and relatives, but it's so bad. And that's something that nobody seems to care about, and I wish they did. You know, when we go and award a contract, we just see, oh, ABC Incorporated, they can do the job, and they have a good price, so let's award the contract to them. Nobody is looking deeper into who owns ABC Incorporated and who has stock in ABC Incorporated, and does anybody in our office have a conflict with it? Nobody does that. And is it because everybody already knows and they are giving the contract to ABC Incorporated because all of the family members work there?

We ask why this link analysis characteristic is essential in a BIA audit program. Investigative Agency, Interviewee 1 said:

> Depending on what the data analytics program can produce, I definitely think it would aid in detecting fraud. Because I would just, me personally would be curious to see what you would put together. I think that would generate more ideas for me.

Our interviewees in the investigating professions did not foresee any changes to the investigating processes with the implementation of a procurement fraud BIA program. They viewed the BIA program as an additional tool to augment how they receive cases, leaving the process in which they conduct their investigations unchanged. Investigative Agency, Interviewee 1 summed up their position on BIA fraud programs:

> I think if everybody had access to some sort of data analytics and we all worked together, we would probably be finding all sorts of fraud and saving money for the government.

This theme held for the desired job requirement. BIA fraud programs are an enhancement, not an increase in burden:

> We would still do the standard stuff, pull the contract, contract review, do interviews, get documents if auditors are appropriate, request audit assistance and it would go to the U.S. attorney's office and present it to the U.S. attorney

Procurement Fraud Auditing Stakeholders

In our discussions with members of the procurement fraud auditing profession, they noted that:

> Usually we don't generate the cases, but we provide a sort of technical know-how, a lot of technical things, or some data analysis stuff as well.

The questions asked of the members of the procurement fraud auditing profession are available in Appendix C.

The procurement fraud auditing profession emphasizes the potential implementation effects of BIA on two distinct types of audits: procurement audits and fraud audits. Procurement audits have a primary objective of testing the procurement process and the organization's compliance with internal controls, not the detection of fraud. For example, a procurement audit may test contracts to ensure proper solicitation. In procurement audits, the data are secondary. As stated by Procurement Fraud Auditing Agency, Interviewee 1:

> There is the procurement audits, and then there is like a fraud audit. Sometimes they overlap, but oftentimes a procurement audit, the goal is not to find fraud. That is sort of a side thing. Like we hope to detect it, but the primary thing is like, are you guys providing the following proper procedures.

Our interviewees said there are additional ways to generate audits. As stated by Procurement Fraud Auditing Agency, Interviewee 1:

> The process for generating audits, it is kind of organic in the sense that it can come from a lot of different places. It can come from an audit project manager who has an idea based on a previous audit. It can come from someone from a command requesting assistance. It could come from the auditor general having an idea.

With the delineation of frauds and their potential avenues of discovery, if the procurement fraud auditing professional is conducting a fraud prevention audit, the data analytics program

becomes important for two reasons. First, the auditor's work should not be redundant to the program. Second, the program might itself be generating leads.

> Where in sort of a more fraud focused audit, we go in, and in that case, we do need a lot more of the data because we get the data and then maybe data analysis working with the audit team, we will really be focusing on the highest risk cases and then attempt to develop an audit that will actually identify cases.

If this is the case, the procurement fraud auditor would report the incident to Navy Criminal Investigation Services (NCIS) for further investigation into the potential fraud allegations.

Regarding data generation:

> Navy instruction has access to like any data, Navy data we want. Now in practice, it is sometimes easier said than done, but if someone had a data like we were interested in contract data and they have some sort of system, in most cases, we request the data, and then they provide it in whatever ways like is convenient to them. We generally don't have direct access to many systems.

The BIA fraud program can alleviate some of these issues, as pointed out by Procurement Fraud Auditing Agency, Interviewee 1:

> Imagine if there is a data analytics tool that makes everyone have amazing contracts. In some sense, we are more likely to go out and find that people have less issues in their contracts in terms of certain anomalies. But that doesn't necessarily make our job easier. Right? It would just impact the types of results we would find. If it is overall, and we have access to it, and it is effective, then that would be—it would have two advantages that would be sort of possibly generating leads, and that would be the [NCIS] side, and then two, possibly identifying high-risk cases of areas to audit. Like hey, this command looks like it has a lot of anomalous contracts, or whatever.

Data Analytics Stakeholders

Discussions held with the data analytics industry professionals showed that the processes involved in the government deployment of a BIA program would not affect their industry. The questions asked are available in Appendix D.

From the industry's point of view, they were very forward with what they had seen as impairments to success when working with the federal government. As identified by Analytics Industry Vendor 2, Interviewee 1:

> So it is understanding what type of data you have access to start with . . . it is usually on the government's side where we don't have access to that. There is a lot of infighting and people protecting their data, and they are afraid if I give you my data, you are going to manipulate it or use it in a way that it is going to hurt me or look bad on me or something like that. So you have got to break down a lot of barriers, but—so I would say the first thing is understanding what data you have at your disposal and then understanding how you could use that data so you can have someone kind of advise you on; this would be great data for anomaly detection, this would be great data for link analysis or something like that. Then just going in there and trying to design those models around finding those types of things. You are going to have different data that if you are looking for bid-rigging, if that is something that is pretty pervasive, that is a whole different type of data set and type of analytical model than if you are looking for purchase card fraud or travel card fraud

> or something like that . . . what exactly are you going to do with those types of things and how—what kind of results are we going to expect out of this.

The industry professionals' opinion, for the development of a data analytics program, is that in-house knowledge, combined with a little training, will assure the success of the implementation. Analytics Industry Vendor 2, Interviewee 1 stated:

> We are going to give you a list of, a prioritized list of, these are the transactions that you need to look at or the procurement officers or the people or the vendors or whatever it is, that you need to look at. These are the associated probabilities of them being bad guys, and here is why, because they broke these rules, they were above these thresholds or whatever it is.

Integrated Analytics

To address integrated analytics, we use responses from our stakeholders in identifying the mixing of data and processes. Our interviewees find a varied and somewhat unique set of characteristics in an anomaly. Procurement Fraud Auditing Agency, Interviewee 1 identified the integrating of data and processes in BIA, saying:

> So you could have a system that is very good at detecting anomalies, but even with that system in place, in some sense the controls are preventative. Right? So in a control sense, we would still want controls there because we wouldn't just want you to be able to detect the problems when they arise, we want to make sure that the contracting officer is properly comparing receipts to payments or is providing good oversight of the contractor that—you know, there is proper separation of duties, and we would want that regardless of whether that procurement system was in place.

This interviewee argued that:

> We have a requirement that we need to check its reliability according to like the audit standards, but beyond that, once we get the data and we ensure it is reliable, we are just like using it and we are often relying on the command to access the data. So usually we will do either Cisco sample or a broad scope review where the goal isn't to pick out the problems, it is just to see how the processes are working.

Fraud Investigative Agency, Interviewee 1 observed the role of the process working in unison with data:

> What we're looking [in]to is a hybrid type of data analytics program that would encompass prescriptive, predictive social networking analytics as well as the typical data mine that's occurring.

Acquisition Agency 1, Interviewee 3 pointed out the importance of integration across organizations within the federal government:

> So if we have a repository of government agencies that have bought similar or the same materials, then we can see, okay, this is how this trends, this is how other agencies have paid. Then maybe we can say, we can validate some of this information or question some of this information based on what is in this repository. As opposed to going after the contractor and begging them to give us the information to validate that.

This process of working with data was emphasized by Analytics Industry Vendor 1, Interviewee 1:

> From a B.I. point of view, we have got reporting tools that can look at millions and millions of records and help you size up and ask questions. What is necessary is probably alerts. Right? Like I don't have time to go and look for my—I need it to tell me, right? So what I would say necessary, I would—I would think it would be alerts because the alerts and the rules should interpret data to some level? Maybe not completely, but for example, the—here is what I mean when I say that—if we look at this alternator example, do we know that alternator is going to fail—that is not the right one. Do we know the alternator is going to fail? Not necessarily. Do we know it could? Yes. So we know some things we know we should look at it, but it could be fine. Right? I mean, it is just telling us based on what it knows.

Human Interactions

Human interactions with BIA encompasses two subcategories for our study: training and data analysis. We define training as the action of teaching a person the skills required in the use of a data analytics program. The definition of data analysis is the process of interpreting the data output of a data analytics program and practically applying this output to procurement fraud prevention.

Our stakeholders identify how important interaction, through training and integration, is to the success of a BIA program. Acquisition Agency 1, Interviewee 2 stated:

> It doesn't do any good to have a tool in the toolbox if no one knows how to use it. So what is a key part for us is that it be integrated into our contract writing system.

Acquisition Agency 2, Interviewee 3 emphasized training and post-implementation support:

> You know, new billets are hard to come by so it would be ideal to have somebody who understands that is their job, who understands how to read trends and not just sharp trends but maybe trends that the untrained eye wouldn't necessarily catch. So I think that seems like a specialized position rather than putting the onus on contracts folks whose position it is to execute contracts and not to understand trends.

Fraud Investigation Agency, Interviewee 1 contrasted this view:

> I think an agent with proper training would be able to navigate it and use it.

Analytics Industry Vendor 2, Interviewee 1 noted that in-house training is available for obtaining the skills to understand what underlies the BIA fraud program:

> These are the associated probabilities of them being bad guys, and here is why, because they broke these rules, they were above these thresholds or whatever it is. So at that point, just a person that does investigations—I don't know if that is a law enforcement guy with a gun or that is an analyst—whatever that person is, they are just reading from a list of these are the guys I need to go and investigate and I am an investigator, I have been doing this for 20 years, I can go and do my job now.

Although the BIA program produces information that in-house training can alert the non-statistical person to:

> To get that list is very difficult. You are going to need guys that understand data very well; you are going to need data integration guys so they can take formats from different data

> sources and kind of mash them together and come up with a clean data set. You are going to need statistical analysts to kind of sit down and build these models and understand and interpret those models.

The result of users and generators of the information leads to awareness of who needs in-house training and who needs statistical knowledge. This point is made:

> So there is a number of people and skillsets that are needed to get to the point of providing that list, but once you get that list, the skillset that is needed is whoever is doing the investigations right now.

From this point, the human interactions of investigation with the data may not be so cumbersome. The underlying analysis may be complicated, but once the analyst assesses the data, an investigation occurs as is traditional.

VII. DISCUSSION

Our interview results mimic requirements associated with Big Data analytics best practices (Russom 2011; Waller, and Fawcett 2013). The U.S. Navy stakeholders identified many of the issues with BIA as observed in the management strategy literature (see Agle et al. 2008; Freeman 1984; Frooman 1999; Ullmann 1985) for successful implementation of systems. These issues include an appreciation and understanding of the system, in our case, what BIA is collecting, what is being detected by the BIA tool, and how the user can incorporate the tools into their toolbox. The literature shows that many people use technological enhancements without a full understanding of their role with the acquired tool, leading to suboptimal use (Yi, Jackson, Park, and Probst 2006).

The effect of BIA on our U.S. Navy stakeholders includes identification of some personnel as those expected to provide usable data analysis, having a deeper understanding of the fundamentals of the BIA system in its entirety. As one of our interviewees pointed out:

> Okay, there are two pieces. One piece is data or information, and a lot of people collect data or have data available. Okay? The other piece is the analysis. Nobody does the analysis. I mean, nobody.

As identified by this stakeholder, BIA seeks to advance current processes in the procurement fraud system by enhancing analysis and changing the benefits derived from data.

Many stakeholders' were focused on the post-adoptive use of BIA, in particular, the analysis aspect within the procurement of goods and services.

> We are all laughing because we have concluded that it would help, which is why we have this initiative to get funding to actually develop and deploy software and the program to do it that will integrate with our procurement system, our contract writing system.

Although all of our interviewees felt that a BIA fraud program would benefit them and the government, fear in the implementation or post-adoptive use, given their particular histories, is a vital aspect of the value of BIA. As pointed out by many of our interviewees, the issue of function and completeness was on all interviewees' minds, as noted:

> If we are going to get serious and put our hats on and say we need to put something together, it has got to work in real life.

The unresolved problems related to users' difficulties in engaging a specific technical feature, to fulfill a business task, was seen to potentially limit the continued and extended use of the BIA

fraud program. If system use problems are understood and resolved promptly, organizations gain more significant benefits from their new systems (Hsieh, Rai, and Xu 2011). As identified by one of our interviewees:

> So necessary I would say alerts are very necessary as a starting point number one, and then number two, I would call *ad hoc* access. Because once you have something, you may want to go and investigate more to figure that out a little bit better.

The ability to discern between an alert and a fraudulent issue within a BIA fraud program is a partial function of system access. System access, as pointed out by our interviewees, is not statistical expertise, it is that:

> All of us in the acquisition review chains are also obligated to look for procurement fraud indicators. The leadership is challenged to remain cognizant of any kind of indicators that would be out there.

As identified in the literature, a lack of timely responses to system use problems may negatively impact the task performance of both the individual users and organizations (Ceaparu, Lazar, Bessiere, Robinson, and Shneiderman 2004).

In the technical and analytical changes brought about by the BIA system, our stakeholders felt that technical personnel should be made available throughout the implementation of a BIA program to offer assistance and guidance. In the implementation of a fraud prevention BIA program, adequate levels of required personnel to address potential additional workload are important. Our stakeholders discussed workload a great deal, with the majority concluding that workload would potentially increase:

> We would have a whole bunch of potentially new cases, and right now, we don't have enough people to investigate it.

At the same time, regarding workload, we had our stakeholders indicating that the issue of workload may not be harmful:

> As long as it is [CAC] enabled, I think we are fine.

Our stakeholders questioned reporting parties of the BIA fraud analysis by saying:

> I know that if we suspect fraud of some sort on a false claim or something like that, we are required to report to the I.G. So I mean I think it is kind of a tough question because I think we are all kind of responsible for fraud prevention, it is just who do we—if we suspect it or if we are sure of it, who do we report it to?

This questioning of whom to report to should not change under BIA, so the issue appears to be that of procedural clarity when implementing the BIA program.

Our stakeholders showed their hesitation for the implementation of a program too quickly. As one of our stakeholders notes:

> [BIA] would be rolled out or deployed in an incremental fashion, we wouldn't just have them come to work on Monday, and they turn on the screen and there it is?

Adding to the incremental thought of implementation and process, our stakeholders were positive about the BIA fraud program as helpful and possibly a solution to many of the disjointed systems and processes. Relevant to our stakeholders is clarity in reporting, process improvement, and speed of implementation. This continuous process review allows our stakeholders to identify and

account for previously unforeseen process implications, ensuring their operating procedures remain productive and efficient. This questioning of a new process is analogous to issues identified in the change management literature (see Freeman 1984).

When we probed the impact of the BIA fraud program, our stakeholders responded to the potential effects:

> The program that you are describing would be more procedural than policy impact because the contributing officers are required to check all these things. It is more a procedural change than a policy change.

Before the implementation of a procedural change can take place, identification of the scope is paramount (Balogun and Hailey 2004). Every participating stakeholder group needs to examine its capability to engage in the collaboration system (BIA) and identify the services that need to be involved in the change process (Balogun and Hailey 2004). As recognized by our stakeholders:

> Developing and implementing continuous process monitoring and reviewing programs that incorporate the data analytics program into routine operations are needed to assure alignment with current processes.

Our stakeholders recommended the incorporation of training within the change to a BIA fraud program:

> We would have requisite training for these people so they would know how to use the information.

Furthermore:

> If you are going to plug numbers in—so I could see that, depending on who that information needs to be shared with, that person obviously is going to have a lot of requirements for NDAs [Non-Disclosure Agreements] and for certain training that they have to go through to make sure that they understand procurement integrity and things like that, but it is nothing that the rest of us don't already have to do.

Our stakeholder is pointing out that currently, they already have a basis for training as procurement professionals. However, as pointed out:

> I haven't had training in a long, long time because there's just never money in the budget for me to have training that I would want.

Overcoming these barriers is key to success in the BIA fraud program.

VIII. CONCLUSION

Fraud and the battle to prevent it affect critical U.S. Navy resources like money, human resources, and time. The current process of fraud prevention in the U.S. Navy is reactive, not proactive. As in the CRIME acronym offered in Rezaee (2005), where he maintains the importance of corporate governance's vigilance in its role as a defense against financial statement fraud, BIA augments the preventive process where management and technology can improve anomaly detection. The preventive process moves the U.S. Navy away from post-fraud detection or whistleblowing. As technology progresses, BIA offers a chance to align government with the commercial sector's battle to prevent fraudulent behavior by focusing on data anomalies as indicators of potential fraud through the use of business intelligence and analytics (BIA). These analytic tools are at the forefront of proactively reducing fraud.

In this study, we report on an exploratory analysis of the viability of a BIA fraud program from a stakeholder perspective. Our focus is on reviewing the implications of BIA fraud tools on federal procurement stakeholders in the U.S. Navy. We use a developed framework that seeks to demonstrate the role of multiple databases, integrated analytics, stakeholders, and human interactions as a way to implement a BIA program. Through an interview methodology, we explore the potential impacts of BIA fraud programs on government stakeholders in the procurement process. We find that the implementation, from our stakeholders' perspective, is that a BIA program has more procedural than policy implications. As a procedural issue, BIA is relating to a set of actions that is the authorized, permissible, or a conventional way of doing something. Our stakeholders demonstrated a desire to have clarity regarding the use of the BIA program, how the BIA program would impact their current jobs, what the BIA fraud program's goals were, and how the goals and processes would become part of the culture of the U.S. Navy procurement professional.

The knowledge gained in this study is that the BIA program is perceived to streamline processes by consolidating information and presenting data within a unique program. The functioning BIA program is seen to increase the confidence level of our stakeholders without alleviating their responsibility to perform their due diligence in their management functions. Our stakeholders recognized a potential increase in workload; however, they acknowledged that there is no perceived increase in undue administrative burden.

Audit and investigative agencies communicated their ability to use a data analytics program as one of many tools in their toolbox. These stakeholders indicate minimal policy ramifications directly resulting from the implementation of a BIA fraud program. There may be an increase in their workload with the additional identification of fraudulent cases generated. However, the potential benefits from the BIA fraud program outweigh the possible workload change. The audit and investigative stakeholders contend that the best data analytics program is a complement, not a substitute, for the human element required of audit and investigative agencies.

Through the use of established data analytics techniques currently employed in the commercial sector, addressing the issue of fraud with the implementation of BIA software and hardware aids in detecting anomalies associated with fraud schemes. The detection of these anomalies raises red flags within the processes of multiple stakeholders, sparking a further proactive investigation into the underlying cause of the red flag. Data analytics software allows for the near-instantaneous analysis of vast amounts of data that would have previously sat dormant, thereby enabling fraud scheme detection within government processes, and it provides the flexibility to detect previously unknown fraud schemes.

Our stakeholder interviewees imply that by using a data analytics software program in the prevention of fraud, the critical resources of money, manpower, and time could be protected from fraudulent activities in a proactive manner. This proactive approach identifies fraudulent activities before they are carried out and reduces costs to the taxpayers associated with lost resources due to fraud. These critical resources can then be available for more efficient use.

We acknowledge that our findings are just the beginning of the needed research into the practicality of a specific data analytics program implementation across the entire U.S. Department of Defense (DoD), not only our focus on the U.S. Navy. The DoD is an expansive organization that utilizes vast amounts of resources with many organizations that span across its agencies. A data analytics program that focuses on fraud would be most beneficial if it used all sources of available data generated by the DoD.

While we believe that this study contributes to the literature by identifying the managerial implications of BIA, this research has limitations. First, all of our interviewees focused on the

perceived benefits and costs associated with a BIA fraud prevention program, not actual costs. Second, our information is limited (by U.S. Navy policy) to groups that are within procurement, not all U.S. Navy professionals. Finally, a cost-benefit analysis that encompasses the implementation, maintenance, and training costs of a BIA fraud prevention program, along with the potential cost savings generated, should be accomplished before the implementation of the program.

REFERENCES

Aggarwal, C. C. 2011. An introduction to social network data analytics. In *Social Network Data Analytics*, edited by C. Aggarwal. Boston, MA: Springer.

Agle, B. T., T. Donaldson, R. E. Freeman, M. C. Jensen, R. K. Mitchell, and D. J. Wood. 2008. Dialogue: Toward superior stakeholder theory. *Business Ethics Quarterly* 18 (2): 153–190. https://doi.org/10.5840/beq200818214

Alblawi, A. S., and A. A. Alhamed. 2017. *Big Data and learning analytics in higher education: Demystifying variety, acquisition, storage, NLP and analytics*. Proceedings of the IEEE Conference on Big Data and Analytics (ICBDA), 124–129, Kuching, Malaysia.

Anderson-Lehman, R., H. J. Watson, B. H. Wixom, and J. A. Hoffer. 2004. Continental Airlines flies high with real-time business intelligence. *MIS Quarterly Executive* 3 (4): 163–176.

Appelbaum, D., A. Kogan, and M. A. Vasarhelyi. 2017. Big Data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory* 36 (4): 1–27. https://doi.org/10.2308/ajpt-51684

Balogun, J., and V. H. Hailey. 2004. *Exploring Strategic Change*. Harlow, U.K.: FT Prentice Hall.

Beyer, M. 2011. *Gartner says solving "Big Data" challenge involves more than just managing volumes of data*. Available at: https://www.businesswire.com/news/home/20110627005655/en/Gartner-Says-Solving-Big-Data-Challenge-Involves-More-Than-Just-Managing-Volumes-of-Data#

Broderick, C. O. 2007. Qui tam provisions and the public interest: An empirical analysis. *Columbia Law Review* 107: 949–1001.

Caminker, E. 1989. The constitutionality of qui tam actions. *The Yale Law Journal* 99 (2): 341–388. https://doi.org/10.2307/796589

Carroll, A. 1991. The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons* 34 (4): 39–48. https://doi.org/10.1016/0007-6813(91)90005-G

Ceaparu, I., J. Lazar, K. Bessiere, J. Robinson, and B. Shneiderman. 2004. Determining causes and severity of end-user frustration. *International Journal of Human-Computer Interaction* 17 (3): 333–356. https://doi.org/10.1207/s15327590ijhc1703_3

Chater, N., J. B. Tenenbaum, and A. Yuille. 2006. Probabilistic models of cognition: Where next? *Trends in Cognitive Sciences* 10 (7): 292–293. https://doi.org/10.1016/j.tics.2006.05.008

Chen, H., R. H. Chiang, and V. C. Storey. 2012. Business intelligence and analytics: From Big Data to big impact. *MIS Quarterly* 36 (4): 1165–1188. https://doi.org/10.2307/41703503

Chen, Y., S. L. Kao, E.-S. Tai, H. L. Wee, E. Y. H. Khoo, Y. Ning, M. K. Salloway, X. Deng, and C. S. Tan. 2016. Utilizing distributional analytics and electronic records to assess timeliness of inpatient blood glucose monitoring in non-critical care wards. *BMC Medical Research Methodology* 16 (40): 1–9. https://doi.org/10.1186/s12874-016-0142-2

Chong, G. 2013. Detecting fraud: What are auditors' responsibilities? *Journal of Corporate Accounting & Finance* 24 (2): 47–53. https://doi.org/10.1002/jcaf.21829

Clarkson, M. 1995. A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review* 20 (1): 92–117. https://doi.org/10.5465/amr.1995.9503271994

Collier, J., and J. Roberts. 2001. An ethic for corporate governance? *Business Ethics Quarterly* 11 (1): 67–71. https://doi.org/10.5840/beq20011117

Davenport, T. H., and J. H. Harris. 2007. *Competing on Analytics: The New Science of Winning*. Boston, MA: Harvard Business Review Press.

Davenport, T. H., J. H. Harris, and R. Morison. 2010. *Analytics at Work: Smarter Decisions, Better Results*. Boston, MA: Harvard Business Press.

Dooley, P. P., Y. Levy, R. A. Hackney, and J. L. Parrish. 2018. Critical value factors in business intelligence systems implementations. In *Analytics and Data Science*, 55–78. Cham, Switzerland: Springer.

Elbashir, M. Z., P. A. Collier, and S. G. Sutton. 2011. The role of organizational absorptive capacity in strategic use of business intelligence to support integrated management control systems. *The Accounting Review* 86 (1): 155–184. https://doi.org/10.2308/accr.00000010

Evan, W. M., and R. E. Freeman. 1993. A stakeholder theory of the modern corporation: Kantian capitalism. In *Ethical Theory and Business*. 4th edition, edited by T. Beauchamp and N. Bowie, 75–93. Englewood Cliffs, NJ: Prentice Hall.

Ferreira, M. B., L. Garcia-Marques, J. W. Sherman, and S. J. Sherman. 2006. Automatic and controlled components of judgment and decision making. *Journal of Personality and Social Psychology* 91 (5): 797–813. https://doi.org/10.1037/0022-3514.91.5.797

Fisher, D., R. DeLine, M. Czerwinski, and S. Drucker. 2012. Interactions with Big Data analytics. *Interaction* 19 (3): 50–59. https://doi.org/10.1145/2168931.2168943

Freeman, R. E. 1984. *Strategic Management: A Stakeholder Approach*. Boston, MA: Pitman.

Frooman, J. 1999. Stakeholder influence strategies. *Academy of Management Review* 24 (2): 191–205. https://doi.org/10.5465/amr.1999.1893928

Garner, B. A., and H. C. Black. 2009. *Black's Law Dictionary*. 9th edition. St. Paul, MN: Thomson/West.

Gonzalez, G. C., and V. B. Hoffman. 2018. Continuous auditing's effectiveness as a fraud deterrent. *Auditing: A Journal of Practice & Theory* 37 (2): 225–247. https://doi.org/10.2308/ajpt-51828

Government Accountability Office (GAO). 2006. *Contract Management: DoD Vulnerabilities to Contracting Fraud, Waste, and Abuse. GAO-06–838R*. Washington, DC: United States Government Accountability Office.

Government Accountability Office (GAO). 2013. *High-Risk Series: An Update. GAO-13-283*. Washington, DC: United States Government Accountability Office.

Greenlee, J., M. Fischer, T. Gordon, and E. Keating. 2007. An investigation of fraud in nonprofit organizations: Occurrences and deterrents. *Nonprofit and Voluntary Sector Quarterly* 36 (4): 676–694. https://doi.org/10.1177/0899764007300407

Gunasekaran, A., T. Papadopoulos, R. Dubey, S. F. Wamba, S. J. Childe, B. Hazen, and S. Akter. 2017. Big Data and predictive analytics for supply chain and organizational performance. *Journal of Business Research* 70: 308–317. https://doi.org/10.1016/j.jbusres.2016.08.004

Hogan, C. E., Z. Rezaee, R. A. Riley, Jr., and U. K. Velury. 2008. Financial statement fraud: Insights from the academic literature. *Auditing: A Journal of Practice & Theory* 27 (2): 231–252. https://doi.org/10.2308/aud.2008.27.2.231

Horton, J., R. Macve, and G. Struyven. 2004. Qualitative research: Experiences in using semi-structured interviews. In *The Real Life Guide to Accounting Research*, 339–357. Amsterdam, The Netherlands: Elsevier.

Hsieh, J. J. P., A. Rai, and S. X. Xu. 2011. Extracting business value from IT: A sensemaking perspective of post-adoptive use. *Management Science* 57 (11): 2018–2039. https://doi.org/10.1287/mnsc.1110.1398

Huang, W., P. Eades, and S. H. Hong. 2009. Measuring effectiveness of graph visualizations: A cognitive load perspective. *Information Visualization* 8 (3): 139–152. https://doi.org/10.1057/ivs.2009.10

Hughes, P. 2011. Beating fraud is the bottom line. *Best's Review* 112 (8): 58.

Humphrey, C., S. Turley, and P. Moizer. 1993. Protecting against detection: The case of auditors and fraud? *Accounting, Auditing & Accountability Journal* 6 (1): 39–62. https://doi.org/10.1108/09513579310027512

Kearney, D. 2013. *Applying Data Analytics Logic to Supplier Management*. London, U.K.: Procurement Leaders.

Klein, G. 2008. Naturalistic decision making. *Human Factors* 50 (3): 456–460. https://doi.org/10.1518/001872008X288385

Klein, G., and D. Klinger. 1991. Naturalistic decision making. *Human Systems* 11 (3): 16–19.

LaValle, S., E. Lesser, R. Shockley, M. S. Hopkins, and N. Kruschwitz. 2011. Big Data, analytics and the path from insights to value. *MIT Sloan Management Review* 52 (2): 21–32.

Lemon, J. 2012. *How a hybrid anti-fraud approach could have detected and prevented fraud in government acquisition programs*. Available at: https://www.sas.com/en_us/insights/articles/risk-fraud/prevent-procurement-fraud.html

Lindsay, A., D. Downs, and K. Lunn. 2003. Business processes—Attempts to find a definition. *Information and Software Technology* 45 (15): 1015–1019. https://doi.org/10.1016/S0950-5849(03)00129-0

Marginson, D. E. 2004. The case study, the interview and the issues: A personal reflection. In *The Real Life Guide to Accounting Research*, 325–337. Amsterdam, The Netherlands: Elsevier.

Maurno, D. A. 2013. The latest fraud-finding tools. *Compliance Week* 10 (115): 38–39.

Miceli, M. P., J. P. Near, M. T. Rehg, and J. R. Van Scotter. 2012. Predicting employee reactions to perceived organizational wrongdoing: Demoralization, justice, proactive personality, and whistle-blowing. *Human Relations* 65 (8): 923–954. https://doi.org/10.1177/0018726712447004

Miles, M. B., M. A. Huberman, and J. Saldana. 2014. *Qualitative Data Analysis: An Expanded Sourcebook*. 3rd edition. Thousand Oaks, CA: Sage.
Nasar, M., and J. Bomers. 2012. Data management and financial regulation: Using a Big Data approach to regulatory compliance. *Business Intelligence Journal* 17 (2): 34–40.
Office of the Inspector General (OIG). 2009. *Summary of DOD Office of Inspector General Audits of Acquisition and Contract Administration. DOD IG Report No. D-2009-071*. November 18. Washington, DC: U.S. Department of Defense.
Pathak, J., B. Chaouch, and R. S. Sriram. 2005. Minimizing cost of continuous audit: Counting and time dependent strategies. *Journal of Accounting and Public Policy* 24 (1): 61–75. https://doi.org/10.1016/j.jaccpubpol.2004.12.004
Rezaee, Z. 2005. Causes, consequences, and deterrence of financial statement fraud. *Critical Perspectives on Accounting* 16 (3): 277–298. https://doi.org/10.1016/S1045-2354(03)00072-8
Richards, G. S. 2016. Business intelligence and analytics research: A peek inside the Black Box. *International Journal of Business Intelligence Research* 7 (1): 1–10. https://doi.org/10.4018/IJBIR.2016010101
Russom, P. 2011. *TDWI best practices report: Big Data analytics*. Available at: https://tdwi.org/research/2011/09/best-practices-report-q4-big-data-analytics.aspx?tc=page0&tc=assetpg&m=1
Simpao, A. F., L. M. Ahumada, J. A. Gálvez, and M. A. Rehman. 2014. A review of analytics and clinical informatics in health care. *Journal of Medical Systems* 38 (4): 1–45. https://doi.org/10.1007/s10916-014-0045-x
Slavakis, K., S. J. Kim, G. Mateos, and G. B. Giannakis. 2014. Stochastic approximation *vis-à-vis* online learning for Big Data analytics. *IEEE Signal Processing Magazine* 31 (6): 124–129. https://doi.org/10.1109/MSP.2014.2345536
Starr, R., J. Newfrock, and M. Delurey. 2003. Enterprise resilience: Managing risk in the networked economy. *Strategy and Business* 30: 70–79.
Tellis, W. 1997. Application of a case study methodology. *Qualitative Report* 3 (3): 1–19. https://doi.org/10.46743/2160-3715/1997.2015
Turban, E., R. Sharda, J. E. Aronson, and D. King. 2008. *Business Intelligence: A Managerial Approach*, 58–59. Upper Saddle River, NJ: Pearson Prentice Hall.
Ugrin, J. C., and M. D. Odom. 2010. Exploring Sarbanes-Oxley's effect on attitudes, perceptions of norms, and intentions to commit financial statement fraud from a general deterrence perspective. *Journal of Accounting and Public Policy* 29 (5): 439–458. https://doi.org/10.1016/j.jaccpubpol.2010.06.006
Ullmann, A. A. 1985. Data in search of a theory: A critical examination of the relationships among social performance, social disclosure, and economic performance of U.S. firms. *Academy of Management Review* 10 (3): 540–557. https://doi.org/10.5465/amr.1985.4278989
Vasarhelyi, M. A., and F. B. Halper. 1991. The continuous audit of online systems. *Auditing: A Journal of Practice & Theory* 10 (1): 110–125.
Vasarhelyi, M. A., A. Kogan, and B. M. Tuttle. 2015. Big Data in accounting: An overview. *Accounting Horizons* 29 (2): 381–396. https://doi.org/10.2308/acch-51071
Vo, Q. D., J. Thomas, S. Cho, P. De, and B. J. Choi. 2018. *Next generation business intelligence and analytics*. Proceedings of the 2nd International Conference on Business and Information Management, September, 163–168.
Waller, M. A., and S. E. Fawcett. 2013. Data science, predictive analytics, and Big Data: A revolution that will transform supply chain design and management. *Journal of Business Logistics* 34 (2): 77–84. https://doi.org/10.1111/jbl.12010
Weins, S., B. Alm, and T. Wang. 2017. An integrated continuous auditing approach. *Journal of Emerging Technologies in Accounting* 14 (2): 47–57. https://doi.org/10.2308/jeta-51857
Wixom, B. H., H. J. Watson, and T. Werner. 2011. Developing an enterprise business intelligence capability. *MIS Quarterly Executive* 10 (2): 61–71.
Yi, M., J. D. Jackson, J. S. Park, and J. C. Probst. 2006. Understanding information technology acceptance by individual professionals: Toward an integrative view. *Information & Management* 43 (3): 350–363. https://doi.org/10.1016/j.im.2005.08.006
Yin, R. K. 1993. *Applications of Case Study Research*. Newbury Park, CA: Sage Publishing.
Yin, R. K. 2014. *Case Study Research: Design and Methods (Applied Social Research Methods)*. Thousand Oaks, CA: Sage Publications.

APPENDIX A

Stakeholder Questions for the Acquisition Profession

- What are the organization's current methods of control for procurement fraud prevention?
- What office within the organization is currently in charge of procurement fraud prevention?
- What title does the organization have for the person who holds this position, and to which office within the organization does that person report?
- Would a data analytics program help the organization prevent government procurement fraud?
- What changes to the organizational work environment would be necessary if a data analytics program was incorporated into the procurement fraud prevention program?
- How would a procurement fraud data analytics program be utilized?
- What changes to job requirements or descriptions would be necessary for the person who oversees a procurement fraud prevention program using data analytics?
- What steps in the organization's procurement planning process would change if a data analytics procurement fraud prevention program was implemented?
- Would data analytics give the organization a higher confidence level that procedures were in place to proactively detect possible procurement fraud? Please explain.
- If a data analytics procurement fraud prevention program was implemented, what title should be given to the person holding the position to oversee the data analytics program within the organization?
- What organizational policies would be impacted by a data analytics program implementation?
- What type of information would the organization want included in a data analytics program for procurement fraud prevention?
- What steps would the organization take to utilize a data analytics procurement fraud prevention program?
- From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

APPENDIX B

Stakeholder Questions for the Procurement Fraud Investigating Professionals

- How is the organization currently alerted to the requirement for an investigation into fraudulent procurement activities?
- What are the organization's current investigative processes into procurement fraud?
- What are the organization's steps for procurement fraud prevention? Briefly describe each step and its level of success.
- What procedures in the organization's investigative process would change if the investigated entity implemented a data analytics program?

- What evidence would the organization need to aid in the detection of fraud in the procurement process?
- What methods would the organization utilize to gather information through a data analytics program for procurement fraud prevention?
- What type of information would the organization want included in a data analytics program to assist in procurement fraud prevention?
- What position or positions within the organization should have access to the investigated entity's data analytics program?
- If an investigated entity implemented a data analytics procurement fraud prevention program, how would the data be analyzed within the organization to help prevent procurement fraud?
- From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

APPENDIX C

Stakeholder Questions for the Procurement Fraud Auditing Professionals

- How is the organization currently alerted to the requirement for an investigation into fraudulent procurement activities?
- What are the organization's current investigative processes into procurement fraud?
- What are the organization's steps for procurement fraud prevention? Briefly describe each step and its level of success.
- What procedures in the organization's investigative process would change if the investigated entity implemented a data analytics program?
- What evidence would the organization need to aid in the detection of fraud in the procurement process?
- What methods would the organization utilize to gather information through a data analytics program for procurement fraud prevention?
- What type of information would the organization want included in a data analytics program to assist in procurement fraud prevention?
- What position or positions within the organization should have access to the investigated entity's data analytics program?
- If an investigated entity implemented a data analytics procurement fraud prevention program, how would the data be analyzed within the organization to help prevent procurement fraud?
- From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?

APPENDIX D

Stakeholder Questions for the Data Analytics Industry

- Are there currently commercial off-the-shelf data analytics programs available that are focused on procurement fraud prevention?
- Could a commercial off-the-shelf data analytics program effectively prevent government procurement fraud?
- What is the process for developing a data analytics program specifically designed for a government organization?
- Has the organization worked with the federal government before on any data analytics program implementation?
- If so, how was it implemented?
- What information would the organization need for the successful design and implementation of a data analytics program in a government organization?
- What is the shelf life of a data analytics program?
- What types of data do a government entity need to include to have an effective data analytics procurement fraud prevention program?
- What type of training would be necessary to interpret data generated from a data analytics procurement fraud prevention program?
- From an organizational standpoint, how could a data analytics program be implemented successfully in order to prevent government procurement fraud?
- From an organizational point of view, are there any issues not already discussed that should be considered in determining if a data analytics procurement fraud prevention program would be beneficial within the organization?