



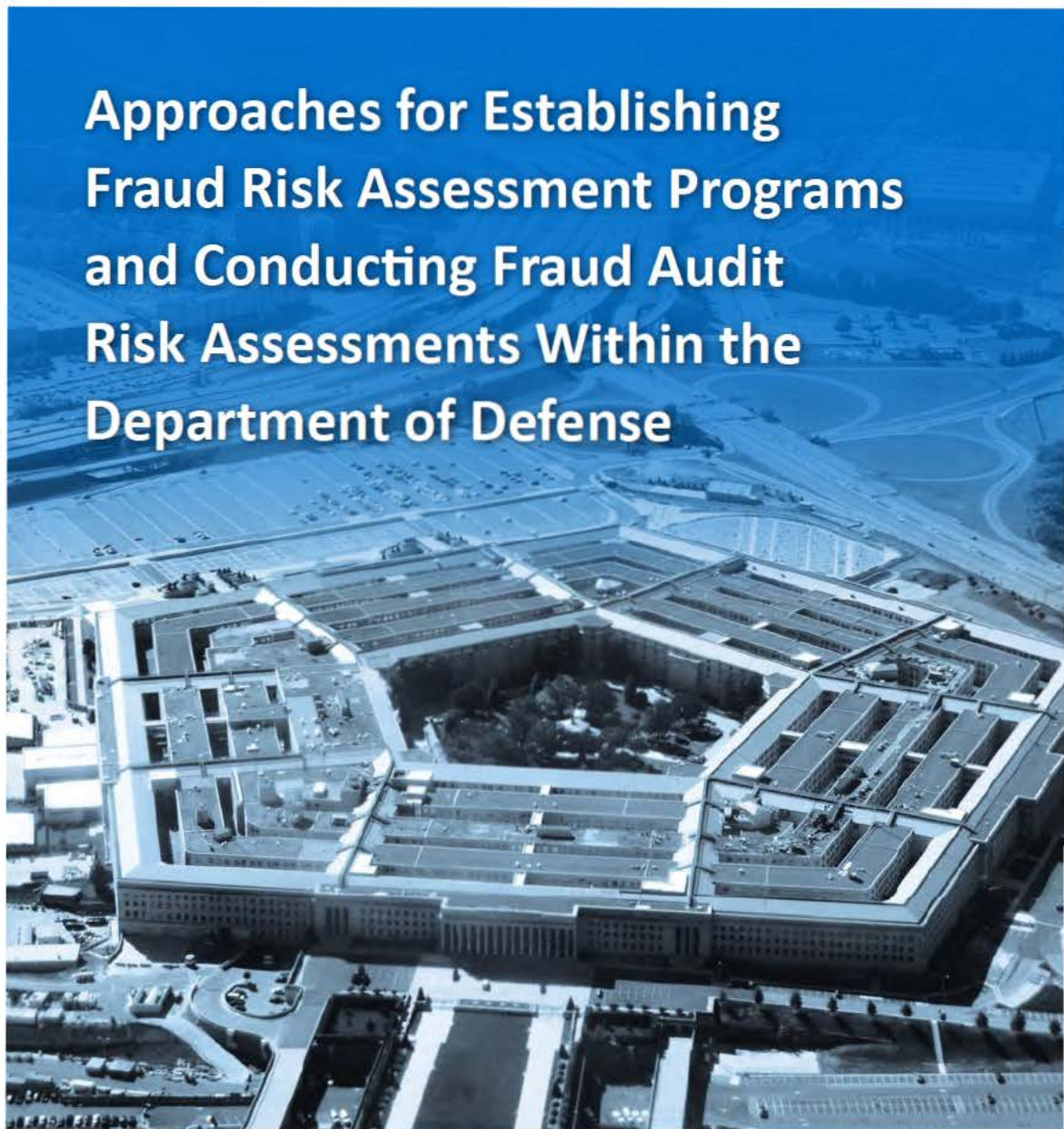
INSPECTOR GENERAL

U.S. Department of Defense

JULY 17, 2014



Approaches for Establishing Fraud Risk Assessment Programs and Conducting Fraud Audit Risk Assessments Within the Department of Defense



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 17 JUL 2014		2. REPORT TYPE		3. DATES COVERED 00-00-2014 to 00-00-2014	
4. TITLE AND SUBTITLE Approaches for Establishing Fraud Risk Assessment Programs and Conducting Fraud Audit Risk Assessments Within the Department of Defense				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Defense Inspector General, 4800 Mark Center Drive, Alexandria, VA, 22350-1500				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 158	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



For more information about whistleblower protection, please see the inside back cover.



Results in Brief

Approaches for Establishing Fraud Risk Assessment Programs and Conducting Fraud Audit Risk Assessments Within the Department of Defense

July 17, 2014

Objective

The objective of the review was to identify approaches for establishing fraud risk assessment programs and conducting fraud risk assessments within the DoD. The review focused on various DoD activities including procurement, retail, and financial operations.

What We Found

We identified numerous innovative approaches for conducting fraud risk assessments. Of the 33 DoD organizations we interviewed,* 13 were conducting entity-wide risk assessments, 26 were conducting fraud risk assessments when performing audit-related work, 23 were providing fraud awareness training, and 3 were concentrating on internal control evaluations.

DoD entities are encouraged to modify any of the described approaches to suit their specific mission, size, and fraud vulnerabilities. The approaches were developed through research and interviews with 100 subject matter experts representing DoD organizations, academic institutions, private companies, and nonprofit organizations.

* For some DoD organizations, more than one component participated in this review.

What We Found (cont'd)

Fraud risk assessment approaches developed by the Marine Corps Nonappropriated Funds Audit Service; Army and Air Force Exchange Service, Audit Division; and the Army Audit Agency are highlighted within this report. Additionally, entity-wide fraud risk assessment approaches developed by the DoD Investigative Organizations; Naval Exchange Service Command, Office of Internal Audit; and the Naval Sea Systems Command Office of the Inspector General are also discussed in detail. The report also contains information on auditor and entity-wide fraud risk assessment approaches developed by external DoD organizations.

We used documentation obtained from the subject matter experts to develop example documents included in the report Appendixes. Example documents include audit organization fraud risk assessment policies, financial statement audit fraud interview questionnaire, and an entity-wide fraud risk assessment report. The report also provides information on auditor fraud brainstorming and interviewing techniques and DoD fraud case study examples.

Management Comments and Our Response

We have incorporated draft report comments received from the Commander, Naval Sea Systems Command; Naval Audit Service; Defense Health Agency; Defense Information Systems Agency, Office of the Inspector General; Air Force Office of Special Investigations; and Board of Regents of the University System of Georgia. No further comments are required.



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500**

July 17, 2014

MEMORANDUM FOR SEE DISTRIBUTION

**SUBJECT: Approaches for Establishing Fraud Risk Assessment Programs and
Conducting Fraud Audit Risk Assessments Within the Department of Defense
(Report No. DODIG-2014-094)**

We are providing this report for your information and use. We have incorporated draft report comments received from the Commander, Naval Sea Systems Command; Naval Audit Service; Defense Health Agency; Defense Information Systems Agency, Office of the Inspector General; and Board of Regents of the University System of Georgia. This report contains no recommendations; therefore, written comments are not required.

This was a self-initiated review. To assist DoD's efforts to prevent, detect, and mitigate fraud risks, we identified approaches for conducting fraud risk assessments for DoD entities and audit organizations. The review focused on various DoD activities including procurement, retail, and financial operations. We also describe fraud risk assessment approaches developed by DoD organizations.

We present a variety of models for DoD organizations and auditors to consider when evaluating fraud risk. DoD entities are encouraged to modify any of the described approaches to suit their specific mission, size, and fraud vulnerabilities. Example documents include audit organization fraud risk assessment policies, financial statement audit fraud interview questionnaire, and an entity-wide fraud risk assessment report. The report also provides information on auditor fraud brainstorming and interviewing techniques and DoD fraud case study examples.

We appreciate the courtesies extended to the staff. Please direct questions to Carolyn R. Davis at (703) 604-8877 (DSN 664-8877). If you desire, we will provide a formal briefing on the results.

Carolyn R. Davis
for Randolph R. Stone
Deputy Inspector General
Policy and Oversight

Distribution:

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
Assistant Secretary of the Air Force (Financial Management and Comptroller)
Commandant of the Marine Corps
Director, Defense Commissary Agency
Director, Defense Contract Management Agency
Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, Missile Defense Agency
Director, Tricare Management Activity
Naval Inspector General
Auditor General, Department of the Army
Auditor General, Department of Navy
Auditor General, Department of the Air Force

Contents

Introduction

Objective	1
Background	1

Successful Brainstorming for Auditors 10

American Accounting Association Top Seven Brainstorming Practices	12
Grant Thornton, LLP, Fraud Brainstorming Approaches for Auditors	12
TDoD Fraud Brainstorming Approaches	17

DoD Audit Organizations' Approaches for Performing Fraud Risk Assessments 18

Marine Corps Nonappropriated Funds Audit Service Fraud Risk Assessment Approach	18
Army and Air Force Exchange Service, Audit Division, Fraud Risk Assessment Approach	22
Army Audit Agency Fraud Risk Assessment Approach	29
Summary of DoD Audit Organizations' Approaches for Conducting Fraud Risk Assessments	34

Auditor Fraud Risk Assessment Special Considerations 35

Special Fraud Risk Considerations When Auditing Health Care Organizations	35
Special Fraud Risk Considerations When Auditing Government Contracts	36

Contents (cont'd)

Approaches for Conducting Entity-Wide Fraud Risk Assessments _____ 37

Fraud Risk Assessment Benefits for DoD Organizations	37
DoD Investigative Organizations' Fraud Risk Assessment Approaches	39
Navy Exchange Service Command Fraud Risk Assessment Approach	40
Naval Sea Systems Command Fraud Mitigation Framework	44
NAVSEA, Office of Inspector General, Contract Fraud Risk Assessment and Mitigation Branch, Fraud Risk Assessment Approach	47
Professional Organization Guidance on Managing the Business Risk of Fraud	49
Australian National Audit Office Fraud Risk Management Process	55
Australian National Audit Office Fraud Risk Assessment Approach	57
Association of American Medical Colleges	58
Smart Insights, LLC Fraud Risk Assessment Approach	62
Texas Tech Fraud Risk Assessment Approach	63
Grant Thornton Approach for Enterprise Risk Management	67
Grant Thornton Fraud Risk Assessment Approach	70
Summary of Entity-Wide Approaches for Conducting Fraud Risk Assessments	72

Summary of DoD and External Organizations' Fraud Initiatives _____ 74

DoD Entities and External Organizations' Fraud Risk Assessment Approaches, Fraud Awareness Training, and Internal Control Evaluations	74
Department of Defense	77
Department of the Army	84
Department of the Navy	84
Department of the Air Force	88
External Organizations	89

Contents (cont'd)

Appendixes

Appendix A. Scope and Methodology	93
Appendix B. Example Naval Audit Service Performance Audit Fraud Risk Policy	96
Appendix C. Example Naval Audit Service Fraud Risk Assessment Work Paper	104
Appendix D. Example DoD OIG, Fraud Interview Questionnaire – Financial Statement Audit	108
Appendix E. Example IIA, AICPA, ACFE, Fraud Risk Assessment Framework	110
Appendix F. Example Smart Insights Group, LLC, Internal Control Evaluation Questionnaire	114
Appendix G. Example Grant Thornton Client Report and Heat Map	123
Appendix H. Example NAVSEA, Office of the Inspector General, Contract Fraud Risk Assessment and Mitigation Branch, Organization Fraud Risk Assessment Report	131
Appendix I. Procurement Fraud Personality Risk Profiles	138
Appendix J. Organization Tool for Evaluating Fraud Control Program	143
Appendix K. Suggested Reading	146

Acronyms and Abbreviations	148
-----------------------------------	------------

Introduction

Objective

The objective of the review was to identify approaches for establishing fraud risk assessment programs and conducting fraud audit risk assessments within the DoD. The review focused on various DoD activities including procurement, retail, and financial operations. Information in this report should be used as a resource for DoD organizations interested in improving their current methods for assessing fraud risk. The document also serves as a useful teaching tool to enhance auditors' understanding of the fraud risk assessment process and educate DoD entities about the value of entity-wide fraud risk assessment programs. Each of the risk assessment approaches presented can be modified to suit an organizations' mission, size and specific fraud vulnerabilities.

Background

Fraud Risk Assessments Benefits for DoD

Fraud risk assessments help to mitigate the risk of fraud occurring within DoD programs and operations. To assist DoD's efforts to prevent, detect, and mitigate fraud, we identify approaches for conducting fraud risk assessments for DoD auditors and DoD organizations. We also describe numerous fraud risk assessment approaches developed by DoD organizations. The suggested approaches were obtained through interviews with 100 subject matter experts from within DoD, the public and private sectors, and published research (refer to Appendix A for a list of organizations participating in this review). The technical experts represented 45 organizations located in 16 states and the District of Columbia. Individuals contributing to this review included auditors, forensic auditors, investigators, attorneys, academics, and engineers. Additional information within this document includes auditor fraud brainstorming and interviewing techniques, example fraud risk assessment policies, and case study examples. Although we do not endorse a specific approach, we are presenting a variety of models for DoD organizations and auditors to consider when evaluating fraud risk.

Significant Threat of Fraud Within DoD

Fraud within the DoD presents a significant threat to the organization's mission and efforts to ensure warfighter safety. Because of the size and complexity of DoD programs and operations, opportunities to commit fraud are always present.

Advances in technology, along with the ongoing development of new fraud schemes, reinforces the need for DoD organizations to be continuously alert to fraud, perform periodic fraud risk assessments, and provide fraud awareness training to all employees. Fraud risk assessments benefit all organizations by offering a cost-effective method to evaluate fraud risks, identify entity-wide improvements, educate employees about fraud, and improve internal controls. Audit organization fraud risk assessments support DoD efforts to prevent and detect fraud through analyzing internal controls, considering fraud schemes and indicators, and developing recommendations for management to reduce the likelihood of fraud.

Individuals attempting to defraud DoD include contractors, subcontractors, civilian employees, and individual service members. Fraudulent activities range from complex procurement schemes to theft in retail operations. The following examples of recent fraud cases illustrate the challenges facing the Department:

- A construction company paid a \$2 million fine and \$1.1 million to settle allegations of submitting false claims to the government.
- DoD contractors and Navy employees were sentenced to pay more than \$3 million for a widespread bribery and corruption scheme.
- A pharmaceutical company paid \$45 million to resolve criminal and civil allegations of drug misbranding.
- A former Army Major was sentenced to 18 months in prison for a bribery scheme relating to DoD contracts in Kuwait.

When organizations do not conduct periodic fraud risk assessments, they are often reactive when fraud occurs and are left to answer questions such as:

- Why did this happen?
- How did this happen?
- How significant is the damage to our reputation?
- What is the effect on the trust of the public, elected officials, and key stakeholders?
- How can we prevent this from happening in the future?
- Why did the auditors not alert management to internal control weaknesses and fraud vulnerabilities?

Definition of Fraud

Fraud is defined in various ways. The generally accepted government auditing standards (GAGAS) describes fraud as:

A type of illegal act involving the obtaining of something of value through willful misrepresentation. Whether an act is, in fact, fraud is a determination to be made through the judicial or other adjudicative system and is beyond the auditor's professional responsibility.

Black's law dictionary also describes fraud as:

A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment.¹

Definition of Fraud Risk Assessments

It is important for DoD organization's to understand the differences between enterprise-wide risk assessments and fraud risk assessments. Although both approaches contain similarities, the objectives, outcomes, and benefits to an organization differ. Enterprise-wide risk assessments are focused on identifying risks associated with achieving program goals, maximizing program performance, or future risks, such as reductions in budgets or personnel. In comparison, a fraud risk assessment is an evaluation of potential instances of fraud that could impact an organization's ethics and compliance standards, business practice requirements, financial reporting integrity, and program goals and program performance.²

Auditor Responsibility for Assessing Fraud Risk

Auditors are required to assess the risk of fraud when conducting their work in accordance with GAGAS, American Institute of Certified Public Accounts (AICPA), and the Institute of Internal Auditors (IIA), International Professional Practices Framework. Auditing standards also require auditors to maintain their professional skepticism and remain alert to fraud indicators at all phases of an audit. To maximize the benefit to DoD, fraud risk assessments should not be considered only routine exercises, or just a way to document compliance with auditing standards or internal policies and procedures. Instead, auditors should conduct robust discussions about fraud indicators and schemes and in-depth analyses of internal controls to identify weaknesses when conducting fraud risk assessments.

¹ Black's Law Dictionary, 9th edition, 2009.

² Pricewaterhouse Coopers, "A practical guide to risk assessment, How principles-based risk assessment enables organizations to take the right risks," 2008.

GAGAS

The December 2011 Revision of GAGAS acknowledges the auditor's responsibility to assess fraud risk when conducting performance audits:

In planning the audit, auditors should assess risks of fraud occurring that is significant within the context of the audit objectives. Audit team members should discuss among the team fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud. Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives.

For financial statement audits, GAGAS incorporates the AICPA Statements on Auditing Standards. GAGAS establishes requirements for performing financial audits in addition to the requirements contained within the AICPA standards. Auditors should comply with these additional requirements, along with the Statements on Auditing Standards guidance when citing GAGAS in their reports.

AICPA

AICPA Auditing Standard, Section 316, "Consideration of Fraud in a Financial Statement Audit," requires auditors to assess the risk of fraud. Members of the audit team should discuss the potential for material misstatement due to fraud through an exchange of ideas or brainstorming discussion. Additionally, when applying professional judgment to assess fraud risk, the following risk attributes should be considered.

- The *type* of risk that may exist, that is, whether it involves fraudulent financial reporting or misappropriation of assets.
- The *significance* of the risk, that is whether it is of a magnitude that could lead to result in a possible material misstatement of the financial statements
- The *likelihood* of the risk, that is, the likelihood that it will result in a material misstatement in the financial statements

- The *pervasiveness* of the risk, that is, whether the potential risk is pervasive to the financial statements as a whole or specifically related to a particular accounting assertion, financial statement accounts or types of transactions.

IIA, International Professional Practices Framework

The January 2013 version of the IIA, “International Professional Practices Framework, Performance Standards, Risk Assessment,” Section 2120A2, states that the internal audit (IA) activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.

Federal Organization’s Responsibility for Minimizing the Potential for Waste, Fraud, and Mismanagement

Office of Management and Budget Circular A-123, “Management’s Responsibility for Internal Control,” December 2004, states that management has a fundamental responsibility to develop and maintain effective internal controls. Programs must operate and resources must be used consistent with agency missions, in compliance with laws and regulations, and with minimal potential for waste, fraud, and mismanagement. Managers should define the control environment and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance internal control. The risk assessment is a critical step in the process to determine the extent of controls. Management is then responsible for redesigning or improving upon those controls. Management is also responsible for communicating the objectives of internal control and ensuring the organization is committed to sustaining an effective internal control environment.

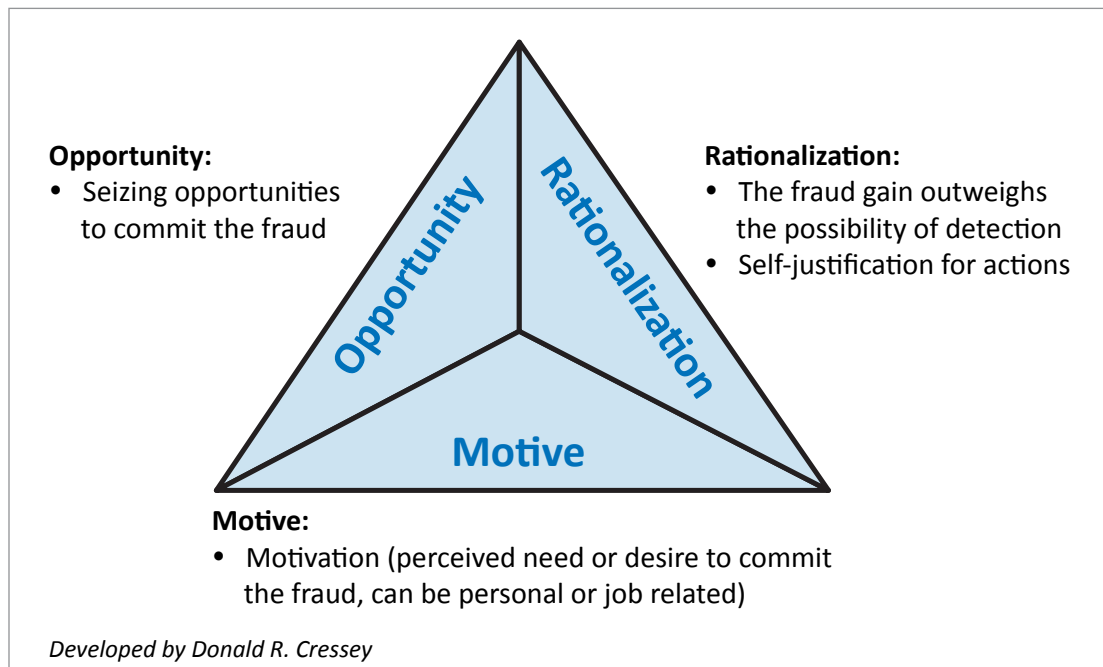
DoD Guidance on Safeguarding Against Waste, Fraud, Abuse and Mismanagement of Resources

DoD Instruction, 5010.40, “Managers’ Internal Control Program Procedures,” May 2013, assigns responsibility and prescribes procedures for the execution of the program within the DoD. This guidance requires DoD employees to determine whether a financial reporting material weakness is a significant deficiency, or a combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. An internal control deficiency should be considered a material weakness if it significantly weakens established safeguards against waste, fraud, abuse, and mismanagement of resources.

Why Fraud Happens

In 1950, Donald R. Cressey, a criminologist, examined why people commit fraud. Donald Cressey's work resulted in the development of the Fraud Triangle (see Figure 1), which uses the elements of opportunity, motivation, and rationalization to explain why people commit fraud. Organizations have limited control over fraudster's³ pressures and rationalizations. However, proactive steps can be taken to significantly reduce opportunities to commit fraud.⁴

Figure 1. The Fraud Triangle



Opportunity

Fraud is more likely to occur in organizations where there is a weak system of internal controls, poor security over assets, little fear of exposure and likelihood of detection, or unclear policies regarding acceptable behavior. The Chartered Institute of Management Accountants, "Fraud risk management, A guide to good practice," 2008, states that, "Research shows that some employees are totally honest, some are totally dishonest, but that many are swayed by the opportunity to commit fraud."

Research shows that some employees are totally honest, some are totally dishonest, but that many are swayed by the opportunity to commit fraud.

³ The definition of a fraudster is a person who commits fraud. Source: [Dictionary.com](https://www.dictionary.com)

⁴ Donald R. Cressey, "Other People's Money," Montclair: Patterson Smith 1973, and Naval Sea Systems Command, Office of Inspector General, Presentation, "Acquisition Fraud Awareness Training," not dated.

There must be something to steal and a way to steal it. Anything of value is something to steal, including both DoD tangible assets such as inventory items, and intangible assets such as government patents and copyrights. Any weakness in a system, for example, lack of oversight, provides opportunities to steal from DoD. Of the three elements of the Fraud Triangle, opportunity is often the most challenging to detect, but is fairly easy to control through improvements to internal controls and changes to policies or procedures.

Rationalization

Many people obey the law because they believe in it and/or are afraid of being shamed or rejected by their friends and family if they are caught. However, some people are able to rationalize fraudulent actions as:

- Necessary – especially when done for the organization,
- Harmless – because the victim is large enough to absorb the impact, or
- Justified – because the victim deserved it or because they were mistreated.⁵

There are two aspects of rationalization: One, the fraudster concludes that the gain to be realized from fraudulent activities outweighs the possibility for detection. Two, the fraudster needs to justify committing the fraud. Justification can relate to job dissatisfaction or perceived entitlement, or saving one's family, possessions, or status. Rationalization is usually detected by observing the fraudster's comments or attitudes.⁶

Motive

In simple terms, motivation is based on either greed or need. Many people are faced with the opportunity to commit fraud, and only a minority of the greedy or needy do so. In general, greed is the number one cause for fraud along with problems with debt and gambling. Personality and temperament, including how frightened people are about the consequences of taking risks also influences their decisions. Some people with good principles fall into negative behavior patterns and develop tastes for the fast life, which tempts them to commit fraud. Others are motivated only when faced with personal and professional ruin.⁷

⁵ Chartered Institute of Management Accountants, "Fraud risk management, A guide to good practice," 2008.

⁶ Naval Sea Systems Command, OIG, Presentation, "Acquisition Fraud Awareness Training," not dated.

⁷ Chartered Institute of Management Accountants, "Fraud risk management, A guide to good practice," 2008.

Case study examples of DoD specific frauds are discussed in Figures 2 and 3. The examples are for illustrative purposes and highlight the presence of motivation, opportunity, and rationalization in each fraud scheme.

Figure 2. Case Study-Disclosure of Information

**Motivation, Opportunity and Rationalization in DoD
Improper Selection of Source Selection Information**

Case Facts – A DoD employee responsible for assisting the contracting officer with funding, performance, and technical issues relating to a DoD program admitted to Federal investigators that he disclosed contractor bid and source selection information to a company bidding on a new contract. The employee gave the company the information so they would have a competitive advantage during contract bidding.

Motivation – In exchange for the information, the company provided the employee with a new car.

Opportunity – The contracting officer was overwhelmed with their workload and paid little attention to contract awards less than \$3 million.

Rationalization – The employee had been passed over for promotion several times and believed he was mistreated and not valued by DoD.

Outcome – The employee was prosecuted in Federal court and received a maximum sentence of 20 years in prison and a fine of \$250,000.

Figure 3. Case Study-Trafficking Counterfeit Parts and Money Laundering

Motivation, Opportunity and Rationalization in DoD Counterfeit Parts

“I have to buy China and risk fake parts to compete. ...It’s my biz.” Fraudster Instant Message, 2008

Case Facts – During a 5-year period, a DoD parts supplier purchased counterfeit semiconductors from sources in Hong Kong and China. The individual went to great lengths to conceal the true origin of the parts and sold them as legitimate and reliable components for use in submarines and complex machinery.

Motivation – The supplier was motivated by money. Through the sale of about 14,000 counterfeit parts, they were paid several million dollars.

Opportunity – Counterfeit parts are difficult to detect once they enter the DoD supply chain. Globalization of the supply chain has resulted in many suppliers receiving goods from second- and third-tier suppliers. Quality assurance tests may not detect all counterfeit parts because manufacturers are skilled at making parts appear authentic.

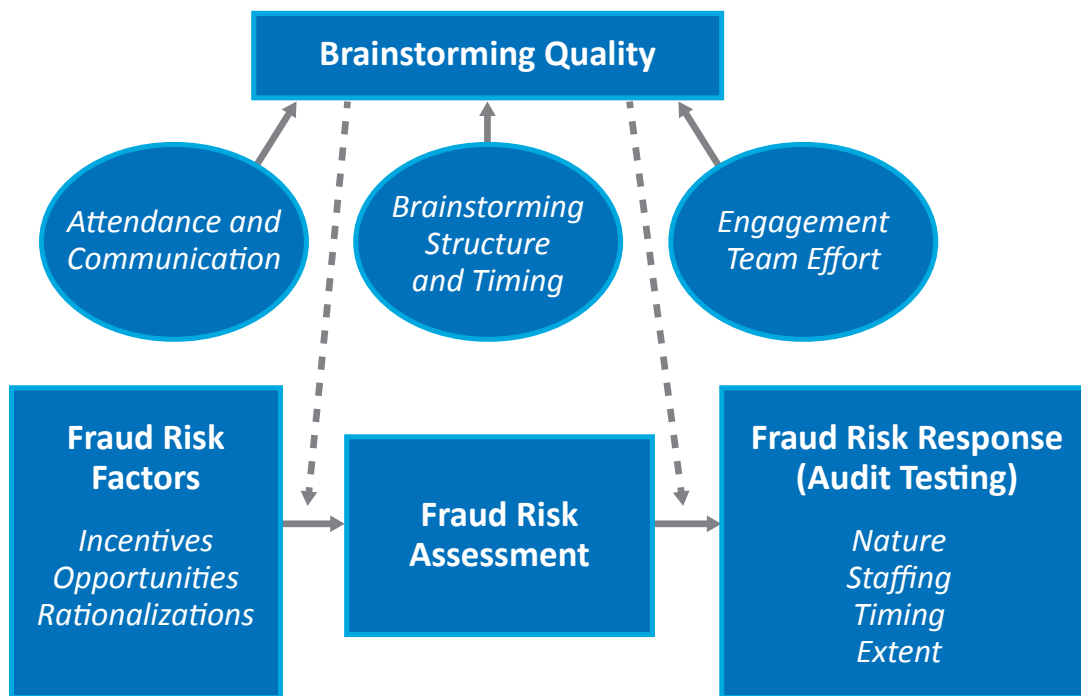
Rationalization – Because the scheme was successful over time, the fraudster believed their chances of getting caught were minimal or nonexistent.

Outcome – The fraudster was indicted on eight counts that included conspiring to traffic in counterfeit goods, conspiring to traffic in counterfeit military goods, trafficking in counterfeit goods, and conspiring to commit wire fraud and money laundering. When convicted, they were sentenced to 75 years in Federal prison.

Successful Brainstorming for Auditors

Most approaches for conducting auditor fraud risk assessments require auditors to brainstorm fraud indicators and schemes associated with their audit objectives. American Accounting Association⁸ research shows that important tangible benefits are achieved through high-quality brainstorming sessions.⁹ In contrast, research also suggests that some engagement teams will incur the cost of brainstorming without receiving the intended benefits of the interaction. Quality brainstorming plays an important role in improving the link between auditors, fraud risk assessments, and their subsequent testing including the design of audit procedures. Figure 4 illustrates a model of audit teams' use of brainstorming in their consideration of fraud. This model is based on psychology and accounting research and the AICPA Statement on Auditing Standards Number 99, "Consideration of Fraud in a Financial Statement Audit" framework.

Figure 4. Auditors' Use of Brainstorming in the Consideration of Fraud



⁸ The American Accounting Association is a voluntary organization of persons in accounting education and research that promotes worldwide excellence in accounting education, research and practice.

⁹ American Accounting Association, "Auditors' Use of Brainstorming in the Consideration of Fraud: Reports from the Field," Joseph F. Brazel, North Carolina State University, Tina D. Carpenter, University of Georgia, J Gregory Jenkins, Virginia Polytechnic Institute and State University, 2010.

Brainstorming Quality

Brainstorming quality is directly affected by team members' attendance and communication, structure and timing of the session, and engagement team effort. As more members of the engagement team attend and participate in the brainstorming session, there will be greater diversity and more sharing of information. This should improve the overall quality of the session and the responsiveness of fraud judgments. The structure and timing of team discussions also contributes to the quality of team judgments. Sessions held earlier in the planning process positively influence auditors' fraud judgments as the engagement team will have more time to implement the ideas endorsed during the session. Engagement team effort is another determinant of the quality of teams' brainstorming sessions. Auditors are encouraged to identify risks and potential audit responses prior to brainstorming. These efforts should enhance each team member's involvement in the fraud audit process, augment their client-specific knowledge, and improve their contributions to the brainstorming session.

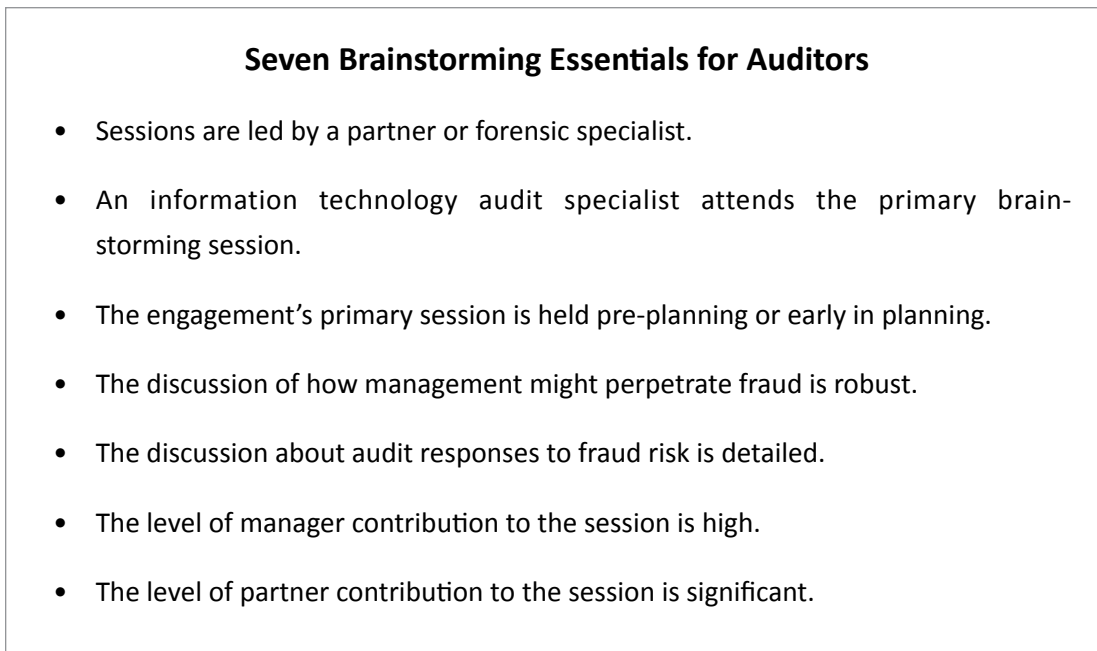
Fraud Risk Factors, Fraud Risk Assessment, Fraud Risk Response

AICPA Statement on Auditing Standards Number 99, "Consideration of Fraud in a Financial Statement Audit," provides guidance to improve the likelihood that auditors will detect fraud using a multi-phase approach. First, auditors collect information related to the risk of material misstatement due to fraud. Using such information, auditors brainstorm to identify fraud risk factors (e.g., incentives, opportunities, rationalizations), synthesize this information to develop a fraud risk assessment, and develop a response to the risk assessments such as altering the staffing of the engagement, or modifying the nature, timing, and extent of audit procedures. Brainstorming sessions are intended to aid auditors in linking fraud risk factors to risk assessments and, in turn, foster the development of appropriate audit responses. As such, the approach depicted in Figure 4 indicates that brainstorming should influence both phases of the fraud decision-making process such that the relations among fraud risk factors, risk assessments, and responses are positively moderated by the quality of the brainstorming session.

American Accounting Association Top Seven Brainstorming Practices

Researchers identified seven brainstorming practices that significantly improve brainstorming quality.¹⁰ Most importantly, they are all controllable inputs that can be easily fostered by management. Figure 5 lists the top seven brainstorming practices for auditors.

Figure 5. Top Seven Brainstorming Practices for Auditors



Grant Thornton, LLP, Fraud Brainstorming Approaches for Auditors

The Importance of Ensuring Sufficient Rigor

If conducted with sufficient rigor the fraud brainstorming session is central to identifying and responding to fraud risks. Ordinarily in the first year, the meeting has such rigor, but in subsequent periods, if sufficient rigor is not sustained, there is a risk that it could become a routine exercise and what the audit team learns over time is not brought to the discussion.

¹⁰ American Accounting Association, "Auditors' Use of Brainstorming in the Consideration of Fraud: Reports from the Field," Joseph F. Brazel, North Carolina State University, Tina D. Carpenter, University of Georgia, J Gregory Jenkins, Virginia Polytechnic Institute and State University, 2010.

The meeting facilitator should not arrive at the brainstorming session with a preconceived notion of the final outcome and a mindset that was closed to new ideas, and must give full consideration to the value of new ideas.

Partner, Grant Thornton, LLP

When conducting fraud brainstorming sessions, it is important that team members and session leaders remain focused on the attributes discussed in Figure 6.

Figure 6. Attributes of Rigorous Brainstorming¹¹

Attributes of Sufficient Rigor

- Devoting sufficient time to the fraud risk brainstorming meeting.
- Ensuring active participation by partner, manager, and subject matter experts.
- Focusing on risks of material misstatement of fraud, as opposed to all fraud risks.
- Stressing the importance of professional skepticism and the specific areas where it is needed.
- Holding robust discussions about how the team will respond to identified fraud risks and tailoring the audit procedures to reflect those decisions.
- Reinforcing the concept that the risk assessment process does not end with the meeting; and if during the course of the audit, additional fraud risks are identified, they should be brought to the attention of the partner, and the audit procedures adjusted, as necessary.

¹¹ Grant Thornton, "DoD Office of Inspector General, Conducting Fraud Risk Assessments Within DoD, Project No. D2012-DIPOAI-00227.000," Grant Thornton Survey Responses, April 2013.

Methods to Achieve Sufficient Rigor

Preparing for the Session

When preparing for a brainstorming session, the session facilitator should review the applicable auditing standards and be familiar and able to discuss various aspects of the consideration of fraud:

- The three conditions that generally accompany fraud (that are, incentive/pressure, opportunity, and an attitude that permits rationalization),
- management's unique ability to perpetrate fraud,
- the possibility of concealed fraud, and
- the potential existence of collusion.

A brainstorming session leader who has prepared sample responses to these prompts or considered past examples of fraud is better equipped to jump-start a stalled brainstorming session or keep a fraud discussion on track. Brainstorming sessions conducted immediately after the engagement team kick-off meetings allow the participants to use information discussed during the kick-off meeting to form questions/comments regarding fraud while the understanding of the organization is still fresh.

Devoting Sufficient Time to the Fraud Risk Brainstorming Meeting

When conducting brainstorming sessions, it is important to allow ample time for the session. The free flow of ideas and connections among team members with different perspectives can often take circuitous routes that do not result in as much value-added to the process if time is too short or the process is rushed. The process is designed to promote free form thinking from an unbiased perspective, but the session can benefit from some level of advance preparation on the part of the meeting facilitator. This advance preparation can bring sufficient focus to the situation to increase the likelihood of considering the breadth of relevant factors.

Ensuring Active Participation

Active participation by audit managers, auditors, and specialists ensures that team members with the most experience provide guidance and input during the discussions. However, discussions are often more interactive when nonleadership

members of the team lead the discussions. Members of the leadership of the audit team should interject in the discussion when necessary. This approach allows for a free exchange of information rather than a lecture type discussion.

Keeping the Discussion Fresh

It is important to keep fraud discussions fresh from year to year or engagement to engagement to ensure that participants in the discussion continue to think “out of the box” and consider the possibility of fraud from diverse perspectives. An effective strategy for encouraging creativity and new perspectives is to rotate the staff both leading and participating in the discussion. By assigning different staff to lead the fraud discussion year after year, the fraud brainstorming session may assume a different direction or tone, as the new staff leading the discussion may have a fresh viewpoint on the auditee’s susceptibility to fraud.

Ranking Fraud Risks

Developing a risk ranking during the session is essential. The ranking of risk areas requires a full understanding of how each business area functions. Based on that understanding, auditors must consider the likelihood of fraud based on the type of business function, the factors influencing the business environment, and the controls in place. Determining the relative risk of each area requires not only a thorough analysis of these factors but also professional judgment based on years of experience. Materiality is an important concept in auditing, when it comes to considering fraud, one must use caution as the occurrence of seemingly small fraud in terms of dollar amount can have much larger implications for the organization. These larger implications can include the assessment of management integrity and whether management representations can be accepted, as well as the potential legal and reputational implications of relatively small amounts of fraud.

Balancing Costs and Benefits

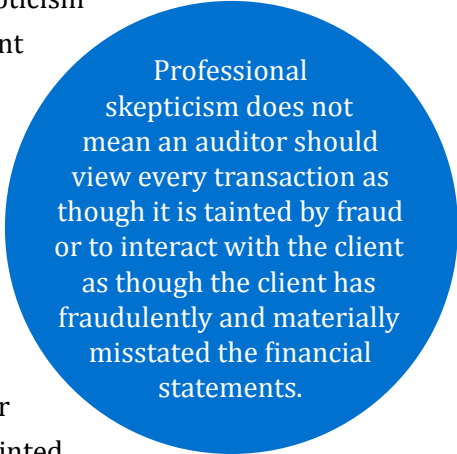
To balance the costs and benefits, the auditor must be able to estimate the level of effort required to analyze an area. The level of effort determines the expected cost. This expected cost must be compared to the combination of the potential cost of fraud in an area and the probability of fraud occurring, as was done when determining a risk ranking. This risk ranking is subjective and, again, based not only on a thorough analysis but also professional judgment based on years of experience.

Identifying High-Risk Areas

Holding robust discussions on how the team will respond to identified fraud risks and tailoring the audit procedures to reflect the decisions is essential. Areas of heightened risks may be identified by the audit team, during the fraud risk assessment process and brainstorming sessions. It is an effective practice to have a team member document in writing those areas including reasons why the team determined the area to be of high risk. A subsequent meeting should be held with the engagement management team to decide the level of focus for each of those areas and the audit response/tests that should be included within the audit programs.

Stressing the Importance of Professional Skepticism

It is critical to reinforce that the fraud risk assessment process does not end with the meeting. If during the course of the audit, additional fraud risks are identified, they should be brought to the attention of the audit manager and the audit procedures adjusted, as necessary. During the brainstorming sessions the team is reminded to maintain professional skepticism during all phases of the audit. AICPA, Statement on Auditing Standards 99, "Consideration of Fraud in a Financial Statement Audit," and GAGAS explain the importance of exercising professional skepticism while conducting an audit. Professional skepticism is an attitude that includes a questioning mind and a critical assessment of audit evidence. Professional skepticism does not mean an auditor should view every transaction as though it is tainted by fraud or to interact with the client as though the client has fraudulently and materially misstated the financial statements. The auditor should conduct the engagement with a mindset that recognizes the possibility that fraud could be present, regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity. Furthermore, professional skepticism requires an ongoing questioning of whether the information and evidence obtained suggests that fraud has occurred.¹²



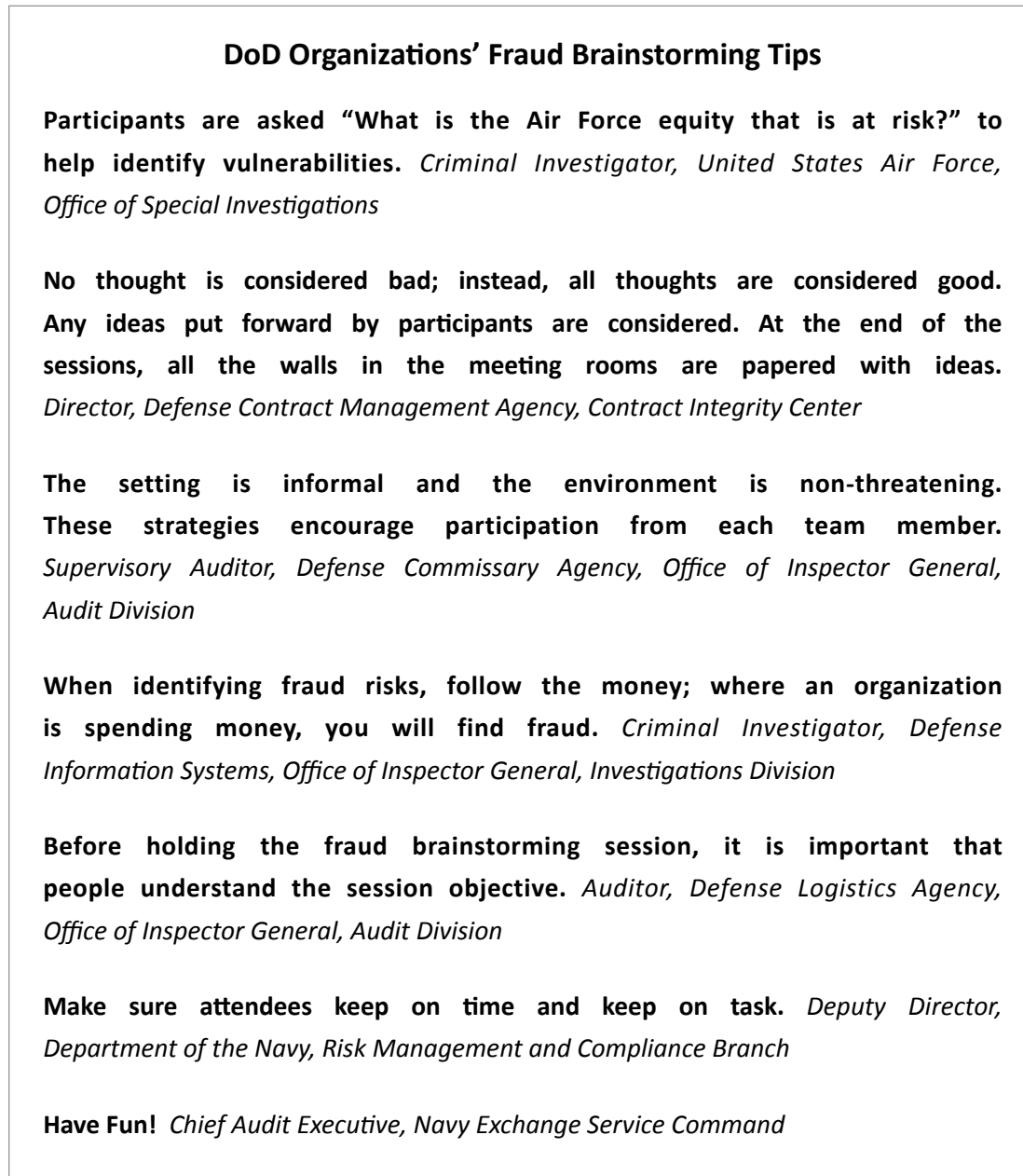
Professional skepticism does not mean an auditor should view every transaction as though it is tainted by fraud or to interact with the client as though the client has fraudulently and materially misstated the financial statements.

¹² Grant Thornton, "DoD Office of Inspector General, Conducting Fraud Risk Assessments Within DoD, Project No. D2012-DIPOAI-00227.000," Grant Thornton Survey Responses, April 2013.

DoD Fraud Brainstorming Approaches

Interviews with DoD subject matter experts disclosed that many organizations are using brainstorming sessions when conducting fraud risk assessments and control self-assessments (CSAs).¹³ Personnel providing guidance on effective brainstorming approaches includes attorneys, auditors, investigators, and risk management experts. Figure 7 summarizes DoD suggested fraud brainstorming approaches.

Figure 7. DoD Organizations' Brainstorming Practices



¹³ CSAs help to identify fraud risks, vulnerabilities, and opportunities to improve existing controls.

DoD Audit Organizations' Approaches for Performing Fraud Risk Assessments

DoD audit organizations developed numerous approaches for performing fraud risk assessments. Auditors can modify any of the fraud risk assessments examples presented in this document to suit their organization's size, mission, and structure. In addition to discussing fraud risk assessment approaches, other guidance discussed within this section includes:

- fraud interviewing approaches,
- general control environment questionnaires, and
- testing for fraud.

See Appendixes B and C for examples of fraud risk assessment policies and a fraud risk assessment work paper developed by the Naval Audit Service.

Marine Corps Nonappropriated Funds Audit Service Fraud Risk Assessment Approach

Key steps used by the Marine Corps Nonappropriated Funds Audit Service (MCNAFAS) when performing fraud risk assessments are audit team brainstorming sessions to identify fraud risks and Internal Control Questionnaires. For brainstorming sessions, team members review prior year work papers, when available, to determine whether previously identified fraud risk factors are applicable to the current audit objectives. Through team discussion, team members also identify new fraud risks and vulnerabilities. The brainstorming sessions reinforce the importance of professional skepticism and set the tone for the engagement.

Networking within your organization and with your audit peers is an effective way to stay current on fraud trends within your industry.

Audit Director, MCNAFAS

Internal Control Questionnaires

MCNAFAS developed internal control questionnaires to gather information about the auditee's general control environment. Sometimes, auditors modify the questionnaires to include information about the process being reviewed to gain an understanding of the program or activity and assist in evaluating control effectiveness. If the questionnaires disclose areas where controls are weak, team members consider the area for additional testing during fieldwork. Figure 8 provides an example of control environment questions. See Appendix D for a DoD Office of Inspector General, (OIG),¹⁴ Office of the Deputy Inspector General for Audit, example fraud interview questionnaire for a financial statement audit.

¹⁴ In this document, the terms Inspector General (IG) or Office of Inspector General (OIG) refers to all Inspector General Offices, to include statutory and nonstatutory entities.

Figure 8. Auditor Questionnaire

General Control Environment Questionnaire	
1.	Can management override a control? If yes, explain.
2.	How does senior management communicate its commitment to sound internal control and their expectation regarding the employees' role?
3.	Does management receive frequent and timely updates from the budget function, accounting function, internal and external audits, and compliance functions? If yes, explain.
4.	Is the structure appropriate to manage activities and accomplish goals? If no, explain.
5.	Are the reporting relationships appropriately organized and periodically reviewed? If no, explain.
6.	Are the appropriate number of people and resources allocated to key functions/activities? If no, explain.
7.	Are job descriptions current, accurate, and understood? If no, explain.
8.	What mechanism exists to identify any new laws or regulations or changes to existing ones?
9.	What has management done to effectively encourage employees to communicate control breakdowns, overrides, or potential regulation or policy violations?
10.	Has management established a code of conduct and other policies regarding acceptable business practices, conflicts of interest, and standards for ethical and moral behavior?

Effective Fraud Interviews

It is helpful for auditors to remember that effective communication requires active listening skills. Auditors at MCNAFAS and Grant Thornton, LLP (Grant Thornton) consistently integrate employee interviews within their fraud risk assessment approaches. Both organizations emphasize that interviewing techniques are essential for achieving high-quality fraud interviews. Figure 9 summarizes interview strategies recommended by both organizations.

Figure 9. Interviewing Techniques

Strategies for Effective Fraud Interviews

Interviews with Management and Employees

Audit team members interview both managers and employees to gather information about fraud risks, assist with evaluating controls, and obtain information about potential fraudulent activities. This strategy provides employees opportunities to raise any concerns they might have regarding management fraud. When conducting employee and management interviews, auditors should use care and good judgment in any discussions about fraud with all personnel and not insinuate that fraud is present or imply that an employee or manager is under suspicion of fraud.

Setting the Tone for Discussion

An important consideration when preparing for a fraud interview session is to set the proper tone for the discussion. Because of the sensitive nature of a discussion of fraud and the potential for interview participants to become shy or refrain from voicing their opinions, it is a good idea to indicate that the interview session is required by AICPA, Statement on Auditing Standard 99, "Consideration of Fraud in a Financial Statement Audit," and that no one is suspected of or being accused of fraud when conducting a financial statement audit.

Asking Follow-Up Questions

When conducting fraud interview sessions, it is critical to keep an open mind and to ask follow-up questions. Many frauds have been allowed to continue too long because of the failure to ask the next question. Responses to interview questions may be less complete than expected. If so, requests for additional clarification or amplification are often necessary. Other times, responses may be different from what was expected or about areas other than what was asked. In those situations, rather than continue to the next question from a pre-determined list, it is important to probe further. The person being interviewed may feel uncomfortable providing information directly that could lead to uncovering a potential issue. But with sufficient diligence in following up on responses, the auditor is more likely to fully identify suspect situations or irregularities. This is not possible without listening fully to responses and responding with relevant follow-up questions.

Army and Air Force Exchange Service, Audit Division, Fraud Risk Assessment Approach

The Army and Air Force Exchange Service (AAFES), Audit Division, fraud risk assessment approach provides an example of a straightforward and effective method for auditors to use when conducting their work. When conducting their analysis of internal controls over a process or program, team members consider “What Could Go Wrong?” to help identify fraud risks and assign risk rankings of high, moderate, or low. When fraud risks are identified, auditors evaluate their results to determine whether additional audit testing is needed for higher risk areas.

When conducting fraud risk assessments, auditors need to think about internal controls and ask themselves:

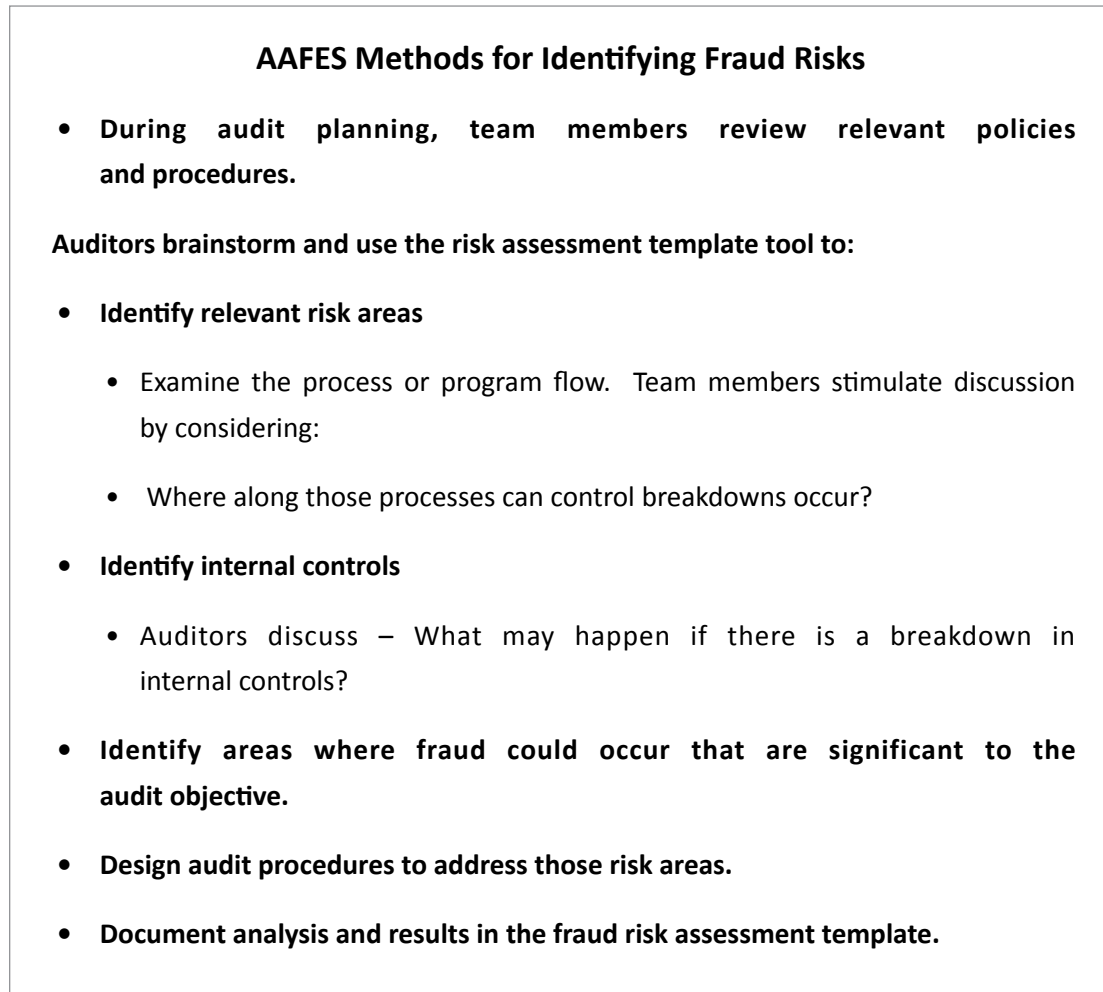
What do I need to measure? And, what is the potential for fraud?

Audit Director, AAFES

AAFES Fraud Risk Assessment Overview

The AAFES fraud risk assessment approach is summarized in Figure 10. A key concept in the approach is the importance of critical thinking when evaluating controls and identifying control weaknesses. AAFES requires auditors to conduct a fraud risk assessment during audit planning to ensure that auditors remain alert to fraud risks throughout the audit process.

Figure 10. AAFES Fraud Risk Assessment Approach



AAFES Fraud Risk Assessment Example

When completing the fraud risk assessment template, auditors are required to perform a detailed analysis of the reviewed area. This example is presented for illustrative purposes only. Refer to Table 1 to view the assessment in its entirety.

1. **Document the fraud risk assessment objective.** A clear and concise objective statement should be developed to ensure all team members understand the expected outcome of the analysis.

Objective Statement. To ensure adequate reporting of sales and accurate billing.

2. **Document the process flow.** During this step, auditors document the process they are reviewing. Team members should consider conducting employee and management interviews and/or reviewing the organization's policies and procedures when performing this step.

Process Flow. Student applies for free/reduced meals.

3. **Analyze Process Control Points/Internal Control Over Process.** For each step documented in the process flow, auditors analyze and document the related internal controls. If multiple controls are developed by an organization, this information should be documented on the fraud risk assessment template.

Process Control Points/Internal Controls Over Process. Local installation or community commander approves/denies application based on income guidelines set by the Secretary of Agriculture.

4. **Risk Details/What Could Go Wrong?** During this step, team members review each control and brainstorm to identify potential control weaknesses by asking themselves; "What could go wrong?" It is important for the team to consider previous audit results, prior frauds, and apply their education, training, and experience when performing this analysis.

What Could Go Wrong? Student approved for incorrect meal plan and/or student approved even though they were not eligible.

5. **Risk Level.** Auditors assign risk rankings based upon the information documented in the risk details section of the template. The AAFES approach uses risk rankings of high, moderate, or low.

Risk Level. Low. The Exchange would still be reimbursed for meals sold regardless of student eligibility.

6. **Audit Procedure.** The team members develop audit procedures to address identified risks. When completing this step, auditors remember that additional procedures may not be necessary for lower risk areas. It is important that auditors should rely on their professional judgment and experience when making this determination.

Audit Procedure. None required. Risk is low. The Exchange is not involved in the approval process for free/reduced meals and reimbursement is not affected.

7. **Fraud Test.** The audit team develops fraud tests for moderate or high-risk areas. For the AAFES fraud risk assessment approach, audit procedures documented in the fraud risk template are used to test for fraud.

Fraud Test. Review facility personnel costs and personnel cost transfers to ensure that the desired goal for personnel costs is 50 percent below sales and that school meal associates are being effectively used in the summer months when school is closed.

Table 1. AAFES Fraud Risk Assessment Example

SUBJECT AREA: School Meal Program

OBJECTIVE: To ensure adequate reporting of sales and accurate billing.

Process Flow	Process Control Points (Internal Controls Over Process)	Risk Details (What Could Go Wrong?)	Risk Level (High, Moderate, or Low)	Audit Procedure	Fraud Test
Student applies for free/ reduced meals.	Local installation or community commander approves/denies application based on income guidelines set by the Secretary of Agriculture.	Student approved for incorrect meal plan and/or student approved even though they were not eligible.	Low – The Exchange would still be reimbursed for meals sold regardless of student eligibility.	None required. Risk is low. The Exchange is not involved in the approval process for free/reduced meals and reimbursement would not be affected.	None required.
Student purchases meal using cash, coupons, or Horizon FastLane Point of Sales School prepayment system (Horizon System).	Coupons issued in sets of ten to a book. Books are serial numbered and number controlled by each type of coupon. Coupons are only issued at one retail location which is designated by the Exchange General Manager. This is usually the Cashier's Cage at the main store.	Students receive more than the monthly allotted number of coupons and hands them out to friends.	Low – All schools are currently using the Horizon System. On the occasion, coupons are necessary, the students can only be issued one month of coupons at a time (2 Books). Each book has a serial number (and the coupons have the same serial number) and is number controlled. Coupons are only sold at one location.	None required. Risk is low.	None required.
	Account in the Horizon System is established annually by the parent at the Cashier's Cage in the main store. Where applicable, the account is set up to reflect free or reduced meals and is charged accordingly in the Horizon System.	Student allows others to use their Horizon FastLane account to charge meals.	Low – Accounts are set up by the parents. A user name and password are created for logging into the system. Each students is given a PIN that is used when purchasing meals. The US Department of Agriculture (USDA) allows three charges to a student's account. To limit excessive charging, a "reminder note" will be sent home when the students account drops below the equivalent of three meals.	None required. Risk is low. Reimbursement for meals served would not be affected.	None required.

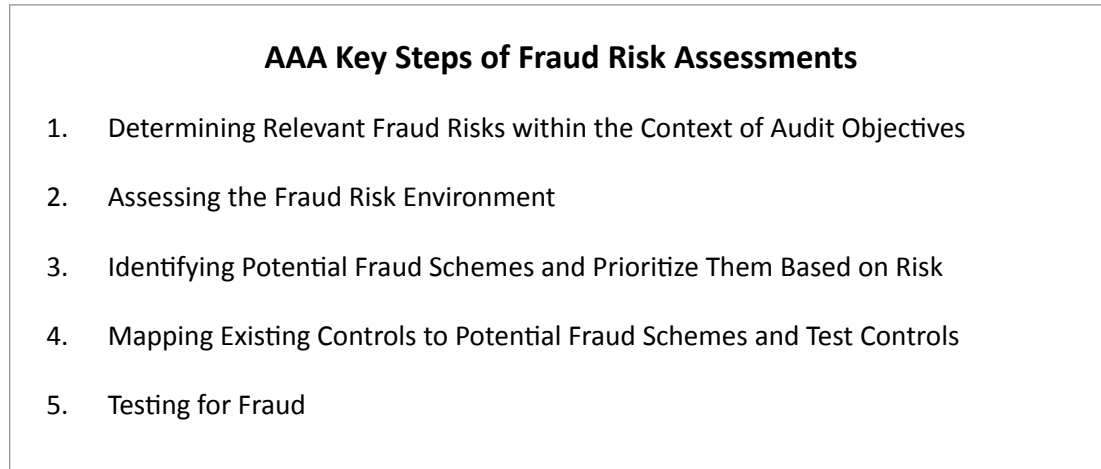
Process Flow	Process Control Points (Internal Controls Over Process)	Risk Details (What Could Go Wrong?)	Risk Level (High, Moderate, or Low)	Audit Procedure	Fraud Test
	Local installation or community commander approves/denies application based on income guidelines set by the Secretary of Agriculture.	Account set up in Horizon System is for the incorrect meal plan.	Low – The Exchange would still be reimbursed for meals sold regardless of the meal category.	None required. Risk is low. The Exchange is not involved in the approval process for free/reduced meals and reimbursement would not be affected.	None required.
Daily/Monthly sales data sent to Self Defense Force for consolidation and completion of Office of Management and Budget Form Number 0564-0284 (USDA Food and Nutrition Service, School Lunch/Breakfast/Snack Claim for Reimbursement).	Daily/Monthly sales (breakfast, lunch, and a' la carte) are recorded in a spreadsheet by each cafeteria. The information from each cafeteria is sent to the Staff Dietician at the end of the month.	Data entry errors. Meals misclassified resulting in the incorrect reimbursement rate being used.	Moderate to High – Misclassification of meals could result in the Exchange being over/under compensated for actual meals served.	Determine the process for capturing and reporting sales to Exchange Headquarters.	Same as Audit Procedure.
	Staff Dietician then consolidates the information from each cafeteria into two spreadsheets (one for Europe and one for Pacific) showing totals by exchange and for the Region.	Data entry errors. Incorrect formulas. Meals misclassified resulting in the incorrect reimbursement rate being used.	Moderate to High – Misclassification of meals could result in the Exchange being over/under compensated for actual meals served.	Determine the process for consolidating and reporting the number of meals served to FA. Review sales data submitted to the consolidated spreadsheet created by the Staff Dietician.	Same as Audit Procedure.
	Staff Dietician then completes the USDA form and sends the information to Family Assistance (FA).	Data entry errors. Incorrect formulas. Meals misclassified resulting in the incorrect reimbursement rate being used.	Moderate to High – Entry errors, incorrect formulas, and meal misclassification could result in the Exchange being over/under compensated for actual meals served. Incorrect billing could result in decreased reimbursements from USDA in the future.	Compare data on consolidated spreadsheet to information included on USDA form.	Same as Audit Procedure.

Process Flow	Process Control Points (Internal Controls Over Process)	Risk Details (What Could Go Wrong?)	Risk Level (High, Moderate, or Low)	Audit Procedure	Fraud Test
USDA billed for pattern meals served during a given month.	FA completes USDA invoice based on information received from the Staff Dietician.	Incorrect billing amount.	Low – FA creates a monthly invoice and bills USDA based on the totals calculated by the Staff Dietician.	Compare data sent to FA to USDA invoice completed by FA and submitted to the USDA for reimbursement.	Same as Audit Procedure.
	USDA reimbursements, both cash and commodity, are entered into the FA quarterly spreadsheet.	Date entry errors. Incorrect formulas.	Low to Moderate – USDA reimbursements are calculated by the Staff Dietician; however, if FA enters the wrong reimbursement amount into their quarterly spreadsheet, this will have an affect on the billing to DoDEA.	Compare USDA monthly invoices to amounts included in FA quarterly spreadsheet.	Same as Audit Procedure.
FA completes quarterly spreadsheet using Report Management and Distribution System, Hyperion, Strawman Report, and Integrated Ledger Accounting System.	Program sales and expenses are taken from various sources and included on quarterly spreadsheet. Reimbursements from USDA (both cash and commodity) are also included. The remaining balance is the program gain/shortfall.	Date entry errors. Incorrect formulas.	Low to Moderate – One data entry error/ incorrect formula could have a snowball effect impacting the total reimbursement of program operations.	Compare information obtained from various sources to the data entered into the quarterly spreadsheet.	Same as Audit Procedure.
		Personnel costs inflated and/or personnel costs not transferred to other food facilities during the summer months.	High – School Meal Associates and the related personnel costs are not tracked during the summer months to ensure these associates are being utilized when schools are closed.	Review facility personnel costs and personnel cost transfers to ensure the desired goal for personnel costs is 50% below sales and school meal associates are being effectively utilized in the summer months when school is closed.	Same as Audit Procedure.
DoD Education Activity (DoDEA) billed quarterly for program shortfalls.	FA completes quarterly invoice to DoDEA based on program shortfalls after USDA reimbursement.	Incorrect billing amount.	Low – DoDEA invoice is created directly from FA's quarterly spreadsheet. The risk is in the completion of the spreadsheet and not in the creation of the invoice.	Compare quarterly results to invoices submitted to DoDEA.	Same as Audit Procedure.

Army Audit Agency Fraud Risk Assessment Approach

The Army Audit Agency's (AAA) fraud risk assessment methodology emphasizes the auditor's assessment of the fraud risk environment and the importance of auditor brainstorming in developing audit steps to identify fraud indicators and schemes. Figure 11 outlines AAA's fraud risk assessment methodology.

Figure 11. Key Steps for the AAA Fraud Risk Assessment Approach



Determining the Relevant Fraud Risks Within the Context of Audit Objectives

To identify relevant fraud risks within the context of the audit objectives, the audit team starts the fraud risk assessment process by asking themselves whether fraud is likely to occur within the operation or program being audited. Examples of topics considered during the team brainstorming meeting include the potential for the theft of cash or other assets, bribery and kickbacks, and personal financial gain. Auditors also apply their overall knowledge of a program or operation, previous audit results, and knowledge of current fraud trends to help identify fraud risks.

The AAA method emphasizes that not all DoD programs or operations are high-risk areas for fraud. For example, the potential for auditors to encounter fraud when conducting a property accountability audit is generally much higher compared to an audit of unit training. However, auditing standards and AAA procedures require written documentation of the auditors' fraud risk assessment analysis in the work paper files for both high-and low-risk areas.

Assessing the Fraud Risk Environment

When assessing the fraud risk environment, it is important for auditors to consider fraud risk indicators. The AAA approach assigns qualitative scores ranging from high, medium, or low and requires auditors to consider the likelihood and impact of each risk indicator. Figure 12 outlines heightened fraud risk factors presented in the 2011 Revision of GAGAS. AAA uses the Government Accountability Office examples in its fraud risk analysis.

Figure 12. Example Fraud Risk Factors

GAGAS Indicators of Heightened Fraud Risk	
1.	The audited entity's operations provide opportunities to engage in fraud.
2.	The entity's financial stability, viability, or budget is threatened by economic, programmatic, or entity operating conditions.
3.	Management's monitoring of compliance with policies, laws, and regulations is inadequate.
4.	The organizational structure is unstable or unnecessarily complex.
5.	Management's communication and/or support for ethical standards are lacking.
6.	Management is willing to accept unusually high levels of risk in making significant decisions.
7.	The entity has a history of impropriety; such as previous issues with fraud, waste, abuse, or questionable practices; or past audits or investigations with findings of questionable criminal activity.
8.	Operating policies and procedures are not developed or are outdated.
9.	Key documentation cannot be provided or does not exist.
10.	The entity's asset accountability or safeguarding procedures are inadequate.
11.	The entity has a history of improper payments.
12.	Management provides false or misleading information.
13.	There is a pattern of large procurements in a budget line with remaining funds at year end, in order to "use up all of the funds available."
14.	There are unusual patterns or trends in contracting, procurement, acquisition, and other activities of the entity or program under audit.

Identifying Potential Fraud Schemes and Prioritizing Based on Risk

If an auditor concludes that there is a high fraud risk environment, they are required to:

- **Identify potential fraud schemes.** When identifying fraud schemes, it is important that auditors brainstorm and remain open to all team member suggestions. Researching current and past fraud trends specific to a program or activity is also encouraged.
- **Prioritize fraud risk based on likelihood and impact.** Likelihood refers to the possibility of the event occurring, while impact pertains to the effect on the organization. When determining impact, it is important to consider both the potential for monetary losses and impact on the organization's reputation if the event occurred.

Mapping Existing Controls to Potential Fraud Schemes

Auditors identify controls to prevent fraud for each likely fraud scheme and then perform tests of controls. When performing this step it is important to:

- Apply auditor training and skills.
- Review key controls in the organization's internal control checklists.
- Review applicable regulations, standard operating procedures, and system user manuals to understand business operations and control processes.
- If the tests of controls disclose weaknesses, the auditor expands audit testing to determine impact or effect on the audit objective.

Additionally, other fraud risk assessment approaches recommend interviewing employees and managers responsible for the program or activity.

An illustrative example of AAA's identification of fraud schemes, fraud indicators, and mapping of internal controls to fraud schemes is provided in Figure 13. This example pertains to a review of the Defense Travel System (DTS) and is presented for illustrative purposes only.¹⁵

¹⁵ Army Audit Agency, "Fraud Risk Training," not dated.

Figure 13. AAA Fraud Risk Assessment Matrix

	Probability			Monetary Loss			Internal Controls
	H	M	L	H	M	L	
Fraud Schemes							
Altering bank account to divert travel payments to specific bank accounts.		X		X			Separation of Duties, Limit Permission Level 5 administrative power.
Altering routing lists to reroute travel vouchers to inappropriate approvers.	X				X		Limit Permission Level 5 administrative power.
Altering e-mail information to screen personnel from DTS communications with DTS profile owner and management.	X				X		Limit Permission Level 5 administrative power.
Amending previously settled vouchers to increase authorized lodging per diem rates, in addition to adding bogus expenses with no documentation.		X		X			Limit Permission Level 5 administrative power. Alter guidance to require supporting documentation.
Creating and approving authorizations and vouchers for temporary duty travel after the temporary duty travel is complete.		X			X		Limit Permission Level 5 administrative power. Alter guidance to require supporting documentation.
Fraud Indicators							
Multiple stamps by the same individual on a single voucher.							
Multiple DTS users with the same bank account government credit card information.							
High-dollar value travel vouchers with no documentation.							
Amendments to travel vouchers that are increased by more than 25% of the original cost of the voucher.							
Amendments to travel vouchers that are made more than 60 days after original approval.							
Amendments made to prior year travel documents.							
Multiple amendments to travel vouchers that contain the same traveler or approver.							
Vouchers filed more than 15 days after the end of the trip.							
Manual per diem rate changes in DTS.							

H - Indicates High

M - Indicates Medium

L - Indicates Low

Testing for Fraud

Procedures to test for fraud will vary for each engagement. When developing tests for fraud, it is important that auditors keep an open mind and think like a fraudster when performing their work. With fraud, it is important to remember that anything is possible. It is also an effective strategy to consult with forensic auditors and subject matter experts to assist with designing and executing fraud testing procedures. Figure 14 presents examples of audit tests to detect fraud.

Figure 14. Fraud Tests

Example Audit Tests to Detect Fraud

- Talk to lower level operating personnel about observing any unethical or suspect activities occurring within the past 12-18 months
- Observe operations and visit contractors' place of business
- Perform trend analysis
- Identify unusual data patterns
- Conduct ratio analysis
- Compare prices
- Evaluate justifications and approvals for sole-source acquisitions
- Evaluate compliance with sole-source selection criteria
- Check for document tampering or errors
- Identify and analyze duplicate transactions
- Compare invoiced quantities to purchased quantities
- Identify transactions occurring out of logical sequence
- Identify transactions furthest from the mean
- Analyze e-mails

Summary of DoD Audit Organizations' Approaches for Conducting Fraud Risk Assessments

Table 2 summarizes fraud risk assessment approaches developed by MCNAFAS, AAFES, and AAA. The table is intended to illustrate the similarities and differences between the various approaches for assessing fraud risk. DoD audit organizations should consider implementing one or more of these methods when performing their work. Each of the suggested procedures can be modified to suit an organization's mission, size, or audit specific objectives. Similarly, audit organizations are encouraged to develop other approaches for performing fraud risk assessments using information presented within this document as a resource.

Table 2. Summary of DoD Audit Organizations' Approaches for Conducting Fraud Risk Assessments

Audit Organization	Team Brainstorming to Identify Fraud Indicators and Schemes	Standardized Interview Questionnaire	Fraud Risk Assessment Template	Assign Risk Rankings	Assess Impact and Probability	Analyze Controls for Weaknesses	Develop Fraud Tests	Document Results
MCNAFAS	X	X		Strong, Medium, Weak		X	X	X
AFFES	X		X	High, Moderate, Low		X	X	X
AAA	X		X	High, Medium, Low	High, Medium, Low	X	X	X

Auditor Fraud Risk Assessment Special Considerations

Special Fraud Risk Considerations When Auditing Health Care Organizations

Healthcare Providers

Financial audit risks relating to healthcare provider organizations¹⁶ typically revolve around recognition of accounts receivables and revenue. In relation to accounts receivable, audit risks include overstatement of receivables due to inadequate assessment/reassessment of the methodology for establishing allowance for uncollectable accounts. In addition to an overall financial statement audit risk, revenue recognition may also be considered as an area for potential fraud as pressure to meet established revenue goals may lead to fraudulent reporting and recording of claims to healthcare payers. Typical schemes of provider revenue fraud include billing for services not provided to patients, falsification of claims (billing codes, dates, patient), incorrect collection of co-pays or deductibles, and improper use of prescription drugs. The magnitude of these risks (both overall audit risks and fraud risks) is assessed during the financial statement risk assessment process, including the brainstorming session during the planning phase of the audit.

Healthcare Payer

Financial statement audit risks related to healthcare payer organizations are often focused on estimates related to benefits due and payable. This included risks surrounding the methodology used to develop the estimates such as significant judgments and assumptions. In relation to fraud for healthcare payer organizations, the majority of the risks involve fraud committed against the company/agency from third parties (that is, applicants, beneficiaries, and healthcare providers) for fraudulent claims or abuse. Healthcare payer organizations must have robust quality assurance mechanisms to guard against fraudulent claims that may involve not only the claimant or healthcare provider, but also collusion between the claimant and the healthcare provider. The auditor should be sure to assess the impact during the overall risk assessment and fraud brainstorming sessions.

¹⁶ Grant Thornton, "DoD Office of Inspector General, Conducting Fraud Risk Assessments Within DoD, Project No. D2012-DIPOAI-00227.000, Grant Thornton Survey Responses," April 2013.

Special Fraud Risk Considerations When Auditing Government Contracts

Inadequate Government contract monitoring may lead to the misuse, abuse, and waste of Federal funds. During a performance audit, the auditor should determine the adequacy of the organizations' procedures to perform effective oversight, evaluate internal control effectiveness, and training in contract administration because these controls are fundamental in ensuring the proper and effective use of Federal funds to achieve program goals. Auditors should be attuned to the different types of fraud schemes that can occur during each stage of the procurement process.

Approaches for Conducting Entity-Wide Fraud Risk Assessments

There are numerous methods for conducting entity-wide fraud risk assessments. Approaches developed by DoD organizations and standard-setting bodies such as the AICPA, Association of Certified Fraud Examiners (ACFE), IIA, Australian National Audit Office, and public and private sector entities are presented in this section. While we are not recommending one specific approach, we are providing a range of options for DoD entities to consider when assessing fraud risk. Report users are also encouraged to review Appendix K, Suggested Resources, for additional information about these methods and related resources.

Fraud Risk Assessment Benefits for DoD Organizations

Table 3 provides information about the principles, benefits, and opportunities of conducting entity-wide fraud risk assessments. DoD organizations are encouraged to use the information as a tool to educate employees and agency managers regarding the benefits and opportunities of establishing fraud risk assessment programs. Most importantly, entity-wide fraud risk assessments provide a cost-effective way for organizations to mitigate fraud risks, identify control weaknesses, and educate employees about fraud.

For maximum benefit, entity-wide fraud risk assessments should not be considered as a check the box exercise.

Director, KPMG Forensic Practice

Table 3. Entity-Wide Fraud Risk Assessment Principles, Benefits, and Opportunities

Principles	Benefits	Opportunities
Responsibility for the fraud risk assessment process must be clearly established	- Organizational commitment and cooperation - Ownership of the process and output, resulting in greater quality of data - Accountability for taking risks	- Collaborate on key risk decisions - Drive consistency in approaches to assessing fraud risks
Fraud risk assessments begin and end with clearly defined objectives	- Defined scope for fraud risk assessment - Accountability for the achievement of objectives - Fraud risk discussion targeted in the context of specific objectives, risk appetite, and tolerance	Identification and evaluation of fraud risks is available for the organization
Fraud risk rating scales are defined in relation to the organization's risk tolerance	- Common basis for assessment of fraud risks - Assessment of the impact and probability of fraud risks in relation to stated objectives	Measure and monitor the organization's ability to achieve objectives
The organization forms a portfolio view of fraud risks to support decision making	- Prioritization of the organization's most significant fraud risks - Ability to view and manage fraud risks that span multiple functional areas - Clarity on the interrelationships between fraud risks and risk responses that may be required - Fraud risks are not merely avoided but understood, and risk informed decisions are made to seize opportunities	- Deliver integrated responses to multiple fraud risks - Identify immediate and longer term improvement opportunities - Prioritize deployment of capital and measurement of relative performance across various objectives or entities
Leading indicators are used to provide insight into potential risks	- Forward-looking analysis in relation to the overall portfolio of fraud risks - Analysis enables the detection of relevant changes in the environment that could impact the achievement of objectives and prompt action as necessary	- Reduce instances of fraud and associated losses - Use relevant fraud risk information to guide decision making

Adapted from Pricewaterhouse Coopers, "How principles-based risk assessment enables organizations to take the right risks," 2008.

DoD Investigative Organizations' Fraud Risk Assessment Approaches

DoD investigative organizations initiate entity-wide fraud risk assessments. Other stakeholders participating in the assessments include auditors and security personnel. DoD investigative organizations' approaches to identify and evaluate fraud risks include:

- Brainstorming sessions to identify fraud schemes that could potentially threaten DoD programs. Risk rankings are assigned by some organizations. Example rankings range from weighted risk scores based upon specific criteria to rankings of high, medium, or low.
- Analysis of internal and external fraud trends.
- Reviews of ongoing and prior fraud cases.
- Input from field office locations.
- Study of reports prepared by the ACFE to pinpoint emerging fraud trends.
- Installation-level fraud risk reviews designed to target risks within specific geographic areas.
- Evaluation of expenditures to identify higher risk programs.
- Analysis of programs with increased levels of congressional interest.

Once the assessments are complete, some organizations report their results to internal stakeholders and senior managers. This approach ensures communication of fraud trends and mission priorities throughout the organization. Additionally, DoD Investigative organizations are proactive with increasing employee's fraud awareness through fraud briefings and on-line training classes.

Figure 15 summarizes benefits of DoD investigative agencies' approaches for conducting fraud risk assessments. DoD entities should consider using these methods when assessing fraud risk within programs or operations. The suggested approaches can also be modified to align with an organization's mission, size, or known fraud vulnerabilities.

Figure 15. Advantages of DoD Investigative Organizations' Fraud Risk Assessments

Benefits of DoD Investigative Organizations' Fraud Risk Assessments

- Identify high-risk areas and trends.
- Results are used to develop fraud awareness training for employees.
- Communicate to senior management high-risk areas and vulnerabilities.
- Prioritize and help to plan the use of internal resources.
- Communicated to employees – “This is why we are doing what we are doing.”
- Focus fraud efforts on areas of high Congressional interest.
- For decentralized organizations, encourage communication and participation from employees working at contiguous and overseas locations.

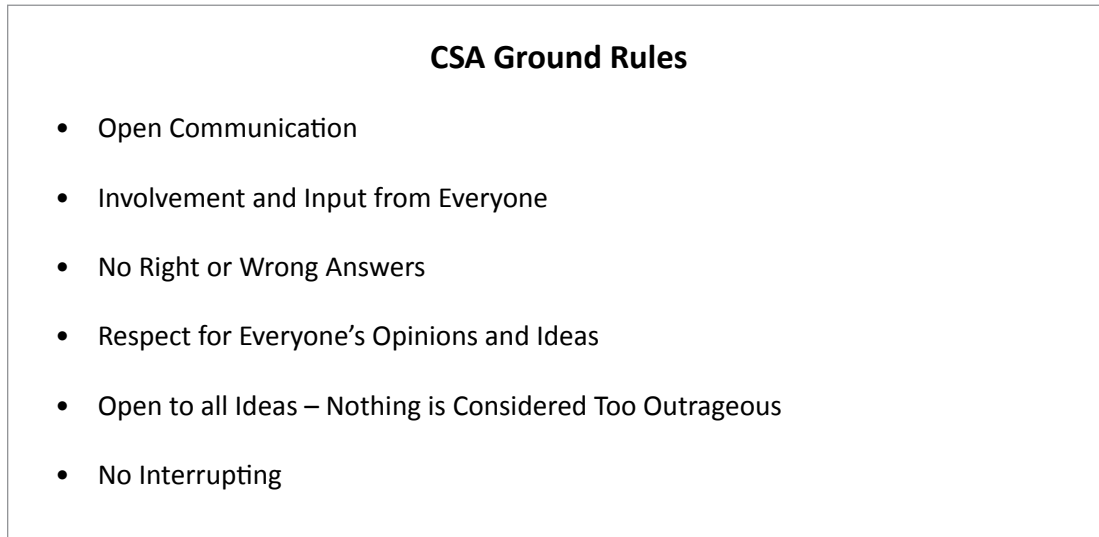
Navy Exchange Service Command Fraud Risk Assessment Approach

Navy Exchange Service Command (NEXCOM), Internal Audit representatives facilitate CSAs. A CSA is a process through which internal control effectiveness is examined and assessed to provide reasonable assurance that all business objectives are met. Previous CSA review areas include cash and credit card operations, purchase cards, and inventory controls. At the start of each assessment, Internal Audit conducts fraud awareness training. The training emphasizes a range of topics that include fraud indicators and key components of internal controls.¹⁷ Representatives from the review areas are also provided information about the CSA, objectives, and approach.

¹⁷ The Committee of Sponsoring Organizations defines internal control key components as the control environment, risk assessment, control activities, information and communication, and monitoring.

To ensure a productive CSA, facilitators emphasize the information in Figure 16 to participants prior to discussing internal controls and identifying potential control gaps.

Figure 16. Ground Rules

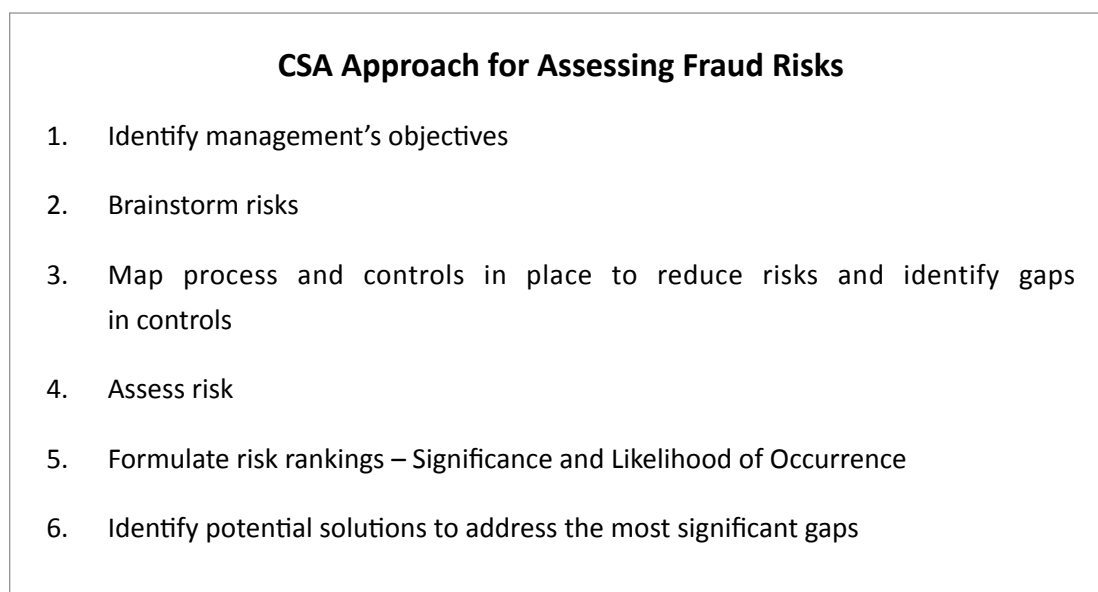


When the assessments are complete, the results are reported to management of the reviewed area. This information provides opportunities to address control gaps prior to an audit and helps to mitigate the risk of potential frauds. However, it is important to remember that CSAs cannot be expected to identify all existing control gaps and/or prevent fraud from occurring.

CSA Approach for Assessing Fraud Risks

Figure 17 summarizes the CSA approach for assessing fraud risks. It is important that DoD organizations complete the assessments in the order described to maximize results.

Figure 17. CSA Fraud Risk Overview



Risk Rankings

When assessing significance and likelihood of fraud risks, rankings of low, medium, and high are used by CSA participants. A low risk is considered unlikely to occur and would not materially impact the attainment of objectives. Medium risks are considered somewhat likely to happen and could impact the attainment of objectives. High risks are categorized as likely to occur and would significantly impact the attainment of objectives. For example, if an identified risk is likely to occur and could significantly impact the attainment of an objective, then the risk is considered high; therefore, controls would need to be put in place to reduce the risk.

Example CSA Risk Ranking

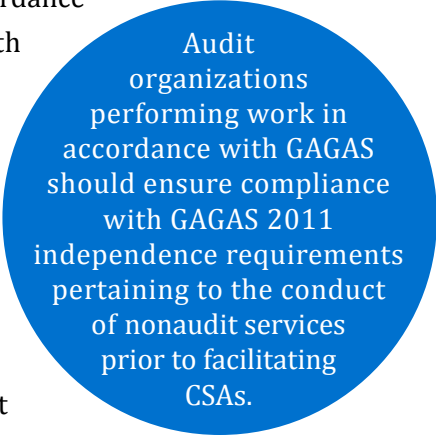
Table 4 depicts results of a CSA review of vending operations at a DoD retail operation.

Table 4. CSA Risk Ranking Template

Risks:	Controls:	Gaps:
1. Route drivers pilfer from sales receipts 2. Susceptibility of dollar bill changers 3. Pilfering vending merchandise 4. Misuse of government vehicles 5. Time and Attendance fraud 6. Inadequate key control 7. Inadequate inventory of vending machines 8. Inaccurate vending warehouse inventory 9. Inaccurate vending machine inventory 10. Inaccurate vending truck inventory 11. Inadequate staff to support vending operations 12. Inadequate control over spoilage 13. Truck change funds not properly tracked and controlled	Keys Supervisor retrieves keys from a lock box located at the Navy Lodge's administration for the vending house exterior door, office doors and the managers lock box. The lock box contains master keys for routes to include vending machines, building doors and duplicate keys. Route drivers will obtain keys from the red lock box located in the clerk's office for their respective routes. Drivers Drivers pull vending inventory merchandise for the day. The merchandise is verified by a vending clerk, supervisor or manager. Route order sheet is signed by driver and verifier. Once verified, driver's load their inventory items on their vending route truck to replenish truck inventory and fill machines.	Gap: Route driver money bags containing vending sales receipts at the end of the day are not locked. Gap: Money bag numbers are not tied to a particular vending machine. Gap: Lack of structured dollar bill changer audits. Gap: Documentation of unannounced change fund counts is not maintained. Gap: Consider outside training for upper level vending management.

Guidance for Audit Organizations Facilitating CSAs

Audit organizations performing work in accordance with GAGAS should ensure compliance with GAGAS 2011 independence requirements pertaining to the conduct of nonaudit services prior to facilitating CSAs. Auditors should review the GAGAS nonaudit service requirements to determine whether providing the service creates a threat to independence, either by itself or in the aggregate with other nonaudit services provided, with respect to GAGAS audits it performs. Auditors should document the results of their assessments in the work paper files.

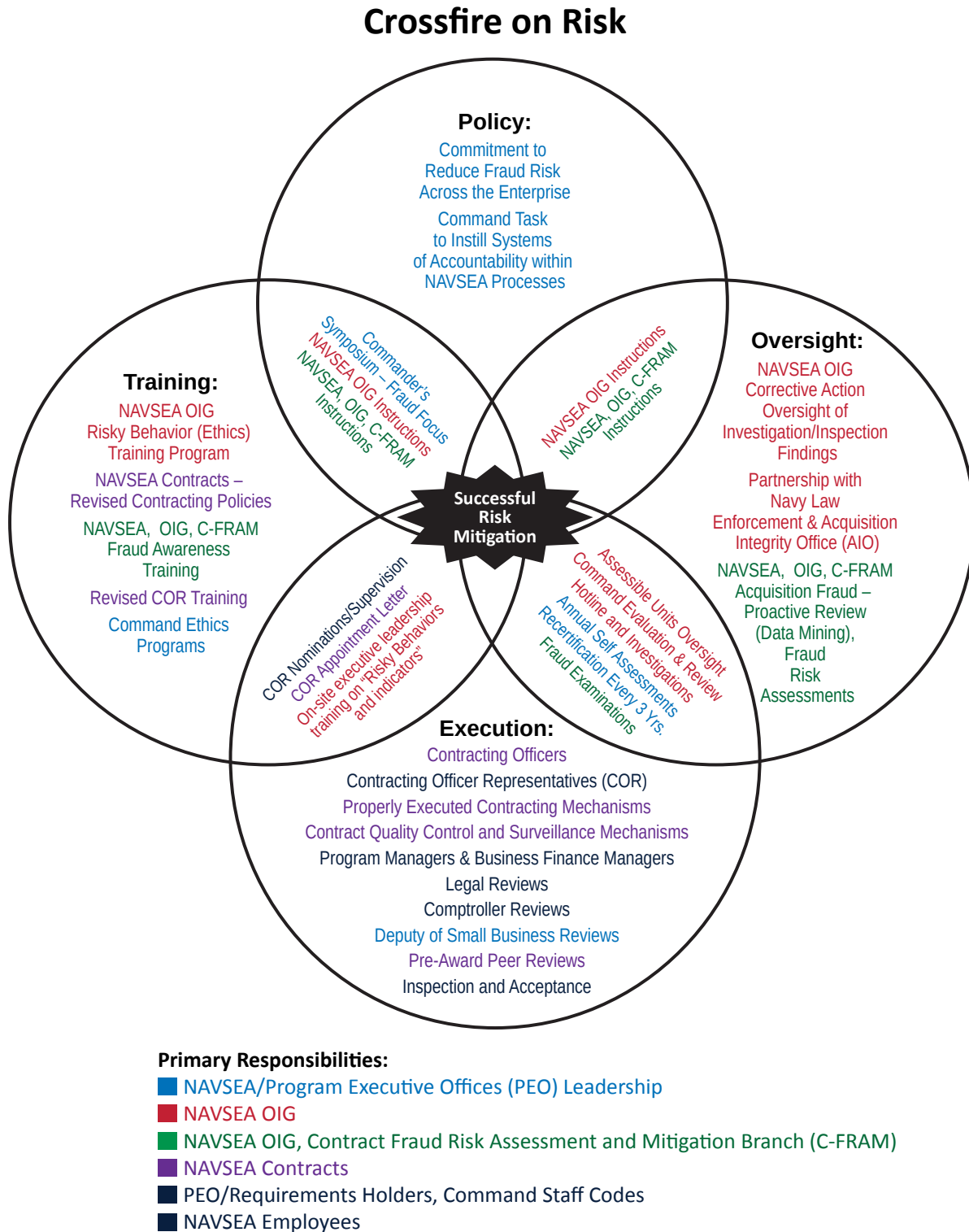


Audit organizations performing work in accordance with GAGAS should ensure compliance with GAGAS 2011 independence requirements pertaining to the conduct of nonaudit services prior to facilitating CSAs.

Naval Sea Systems Command Fraud Mitigation Framework

The Naval Sea Systems Command (NAVSEA) entity-wide approach to prevent and detect acquisition fraud consists of policy, training, and execution processes. Using an integrated approach, risk mitigation activities are included in policies, oversight and execution processes, and training efforts across the entire acquisition continuum. Figure 18 illustrates NAVSEA's fraud mitigation framework, which is also referred to as "Crossfire on Risk."

Figure 18. NAVSEA Risk Mitigation Framework

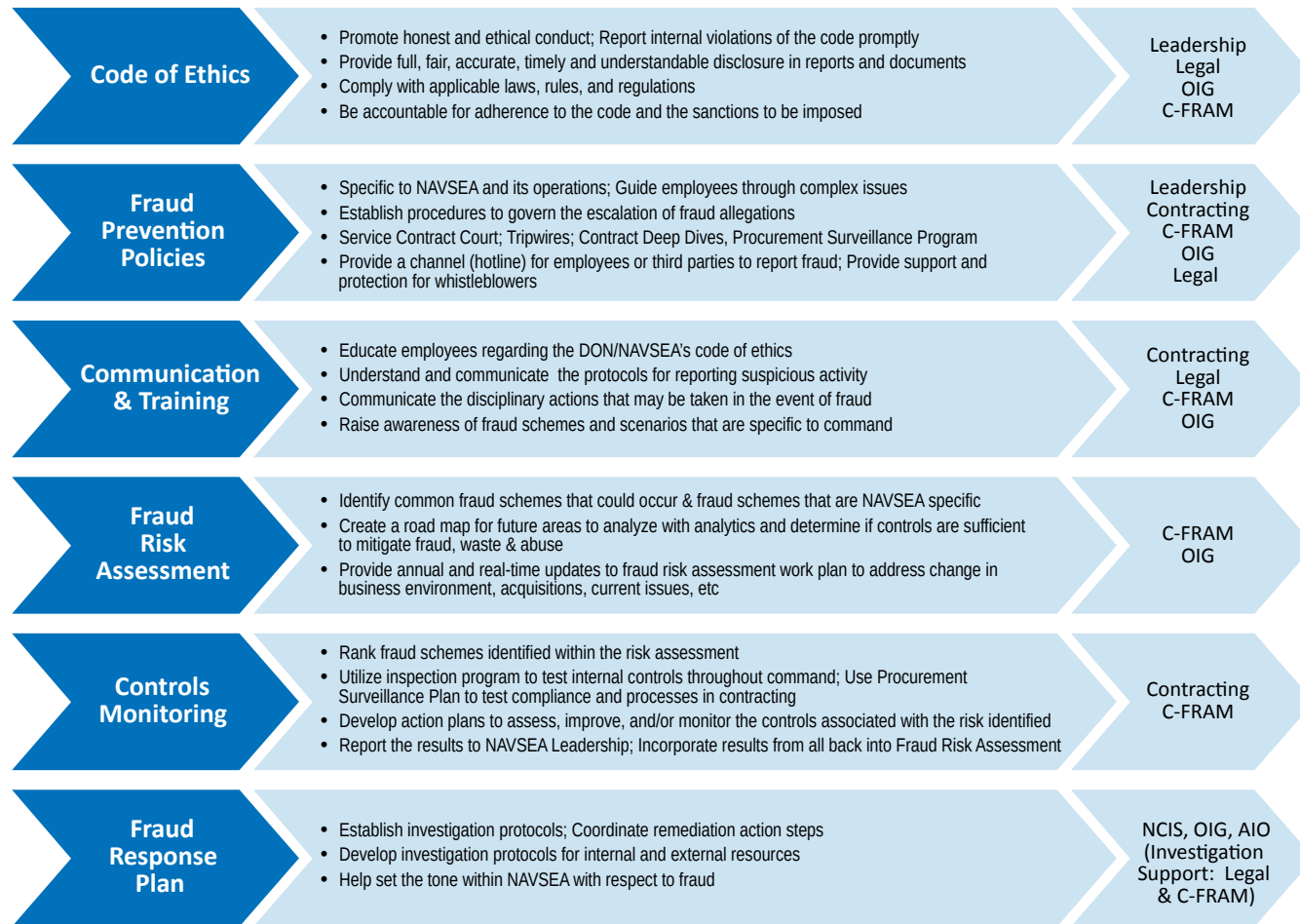


Individual Personal Responsibility at All Organizational Levels

Risk Mitigation must be included in Policies, Oversight and Execution Processes, as well as Training Across the Entire Acquisition Continuum

NAVSEA identifies elements of successful acquisition anti-fraud programs, based upon guidance developed by the ACFE. The model also emphasizes the importance of fraud risk assessments as a tool to determine if controls are sufficient to mitigate fraud, waste, and abuse within the organization. The model is illustrated in Figure 19.

Figure 19. Elements of a Successful Acquisition Anti-Fraud Program



C-FRAM – NAVSEA OIG, Contract Fraud Risk Assessment and Mitigation Branch

DON – Department of the Navy

NCIS – Naval Criminal Investigative Service

NAVSEA, Office of Inspector General, Contract Fraud Risk Assessment and Mitigation Branch, Fraud Risk Assessment Approach

The NAVSEA organization facilitates fraud risk assessments at local commands, leveraging Texas Tech University Systems' (Texas Tech) perception-based fraud risks assessment model.¹⁸ However, NAVSEA does not incorporate electronic polling within their assessments. All focus groups' discussions are facilitated by three NAVSEA employees that perform the roles of primary and secondary facilitators and scribes. At the end of the discussions, scribe notes are sent to participants to ensure accuracy.

Prior to the site visit, department managers are asked to identify a cross section of employees to participate in the fraud risk discussions and focus groups. Meeting topics include the acquisition process, internal control weaknesses, and potential fraud schemes. All focus group members possess a solid understanding of fraud indicators and schemes. Employees selected for participation are statistically significant; however, most answers provided by participants and analyzed by facilitators are qualitative rather than quantitative.

Example Fraud Risk Assessment Results

During one fraud risk assessment, discussions were held with 57 employees (approximately 20 percent were civilians) to obtain information about their perceived fraud risks. These employees were divided into four focus groups representing all major functional areas: Contracts, Finance, and Engineering. Additionally, team members conducted discussions with 1 composite group, consisting of 13 employees from all major functional areas, that were not included in the original focus group. Lastly, 14 individual interviews were completed with employees who self-identified as wishing to discuss issues with NAVSEA representatives and other employees from major functional areas.

Based on the information obtained from focus groups, composite groups, and individual interviews, the site visit team found common fraud vulnerabilities and suggested mitigation strategies for the Commanding Officer. Table 5 lists the fraud vulnerabilities with the mitigation strategies.

¹⁸ Texas Tech's fraud risk assessment approach is discussed on pages 63 through 66 of this report.

Table 5. *Fraud Vulnerabilities and Mitigation Methods*

Common Fraud Vulnerabilities	Mitigation Strategies
Possible fraudulent schemes	Assess Managers' Internal Controls Program Assessable Units and other processes to determine whether fraud vulnerabilities are identified and mitigated.
Contract management	Review contract surveillance plans on all current and future contracts. Assess and establish mitigation plans.
Financial review and payment system	Cross check with contracts and contracting officer's representative to verify costs incurred and work accomplished.
Contractor oversight	Identify and train contracting officer's representatives and appoint a representative for each contract per agency regulations. Timely review of invoices in the accounting system.

If a fraud risk assessment discloses high-risk areas or weak internal controls, NAVSEA conducts follow-up reviews. A report is sent to local command detailing the results of each review. See Appendix H for an example report.

Advantages of the NAVSEA Fraud Risk Assessment Approach

Figure 20 summarizes advantages of the NAVSEA approach for assessing fraud risks. DoD organizations are encouraged to consider incorporating some, or all, elements of this method when assessing fraud risks. The approach can also be modified to suit an entity's mission, size, or known fraud vulnerabilities.

Figure 20. *NAVSEA Fraud Risk Assessment Benefits*

Advantages of the NAVSEA Fraud Risk Assessment Approach

- The use of small discussion groups encourages participation from all attendees.
- The approach provides opportunities for fraud awareness training and discussion, to include questions and answer sessions with NAVSEA subject matter experts.
- Cross sections of employees from key business areas provide a range of fraud risk perceptions.
- Results of the assessment are provided to the command to assist with mitigating potential fraud risks.

Professional Organization Guidance on Managing the Business Risk of Fraud

The IIA, AICPA, and ACFE worked with subject matter experts in fraud risk management and developed a guide titled, “Managing the Business Risk of Fraud: A Practical Guide,”¹⁹ for conducting entity-wide fraud risk assessments. The three organizations identified the following key principles for establishing an environment to manage an organization’s fraud risk:

Principle 1: As part of an organization’s governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of senior management regarding managing fraud risk.

Principle 2: Fraud risk exposure should be assessed periodically by the organization to identify specific schemes and events that the organization needs to mitigate.

Principle 3: Prevention techniques to avoid potential fraud risk events should be established, where feasible, to mitigate possible impacts on the organization.

Principle 4: Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized.

Principle 5: A reporting process should be in place to solicit input on fraud and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and in a timely manner.

The Fraud Risk Assessment Team

The fraud risk assessment team should consist of individuals from within the organization with different knowledge, skills, and perspectives. If expertise is not available internally, external participants with expertise in applicable standards, key risk indicators, anti-fraud methodology, control activities, and detection procedures should participate. Within DoD, participation will vary depending on the risk assessment objective. For example, fraud risk assessments that are targeted to evaluate controls related to a procurement cycle will differ from

¹⁹ IIA, AICPA, ACFE, “Managing the Business Risk of Fraud: A Practical Guide,” not dated.

participants tasked with evaluating retail operations. Figure 21 contains examples of subject matter experts that should be considered when developing a fraud risk assessment team.

Figure 21. Recruiting Team Members²⁰

Recruiting Subject Matter Experts

After establishing your objective, consider recruiting experts such as:

- DoD personnel responsible for administering the Managers' Internal Control Program,
- accounting or financial personnel who are familiar with the financial reporting processes and internal controls,
- nonfinancial operations personnel to leverage their knowledge of day-to-day operations and issues within a program or process,
- legal and compliance representatives because fraud risk assessments may identify risks resulting in potential criminal, civil, and regulatory liability if the fraud or misconduct were to occur,
- team members from the auditing and investigations disciplines who can provide information about internal controls and fraud risks, and
- organization management to ensure their commitment to the process and understanding of fraud risks within their areas of responsibility.

Fraud Risk Assessment Approach Exercise

To protect itself from fraud, an organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization. A structured fraud risk assessment, tailored to the organization's size, complexity, and goals, should be performed and updated periodically. The assessment may be integrated with an overall organizational risk assessment or performed as a stand-alone exercise, but should include risk identification, risk likelihood, and significance, and risk response. Organizations should develop a framework to document their fraud risk assessment, refer to Table 6 for an example.

²⁰ DoD OIG, Office of Audit Policy and Oversight, modified this information from IIA, AICPA, ACFE, "Managing the Business Risk of Fraud: A Practical Guide," not dated.

Risk Identification

Fraud risk identification includes gathering external information from regulatory bodies, industry sources, and professional organizations. Internal sources for identifying fraud risks should include interviews and brainstorming with personnel representing a broad spectrum of activities within the organization, review of whistleblower complaints, and analytical procedures. An effective fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. The fraud risk assessment process should consider the potential override of controls by management as well as areas where controls are weak or there is a lack of segregation of duties.

Risk Likelihood and Significance

Assessing the likelihood and significance of each potential fraud risk is a subjective process. All fraud risks are not equally likely, nor will all frauds have a significant impact on every organization. Assessing the likelihood and significance of identified inherent risks²¹ allows the organization to manage its fraud risks and implement preventive and detective procedures. It is important to first consider fraud risks to the organization on an inherent basis or without consideration of known controls. By taking this approach, the fraud risk assessment team is better able to consider all relevant fraud risks and design controls to address the risks. After mapping fraud risks to relevant controls, certain residual risks will remain, including the risk of management's override of established controls. The team must evaluate the potential significance of those residual risks and decide on the nature and extent of the fraud preventive and detective controls and procedures to address such risks.

Likelihood

The assessment of the likelihood of a fraud risk occurring generally includes analyzing the following information: past instances of a specific type of fraud and the prevalence of the fraud risk within the organization's industry. Other related factors that should be considered include the number of individual transactions, the complexity of the risk, and the number of people involved in reviewing or approving the process. Organizations can categorize the likelihood of potential frauds occurring using any reasonable approach; however, three categories are generally adequate: remote, reasonably possible, and probable.

²¹ Inherent risk is the risk before considering any internal controls in place to mitigate such risks. IIA, AICPA, ACFE, "Managing the Business Risk of Fraud: A Practical Guide," not dated.

Significance

The assessment of the significance of a fraud risk should include not only financial statement and monetary significance, but also significance to an organization's operations and reputation, as well as criminal, civil, and regulatory liability. Organizations can categorize the significance of potential frauds in as many categories as deemed reasonable, but three categories are generally adequate: inconsequential, more than inconsequential, and material.

Incentives and Pressures

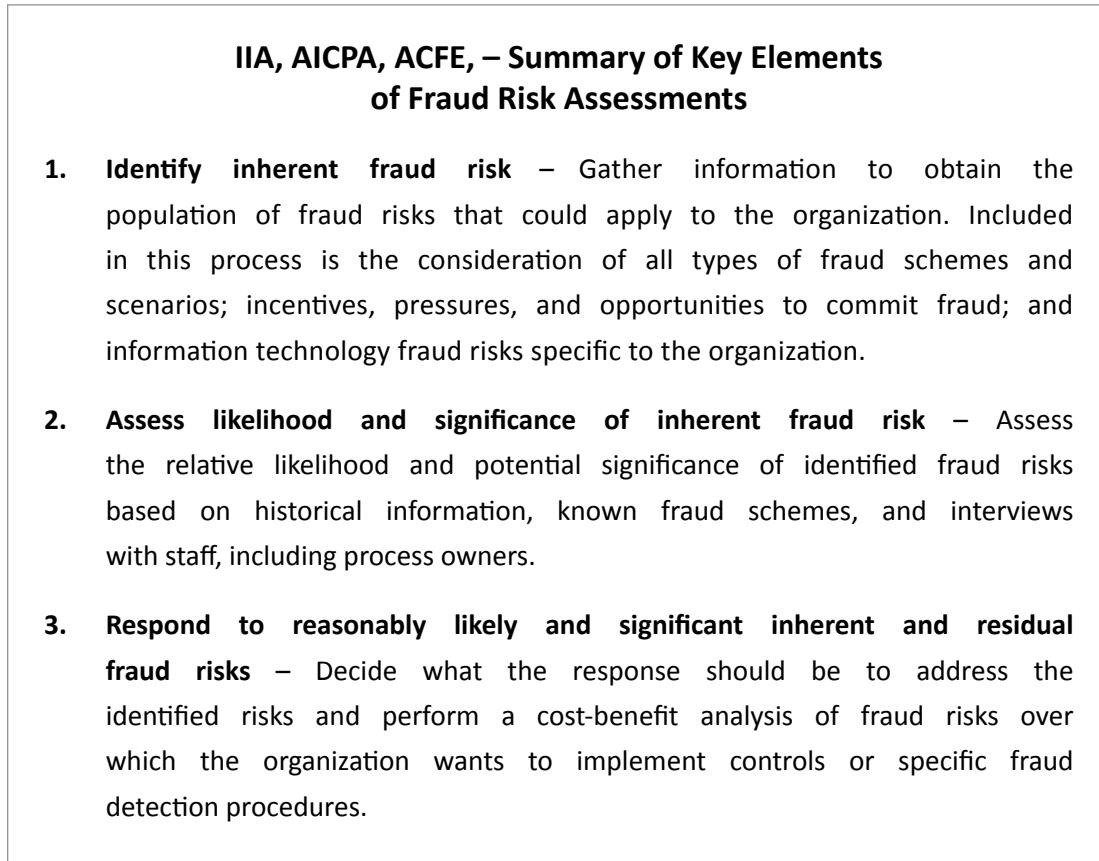
As part of the risk assessment process, the organization evaluates the incentives and pressures on individuals and departments and should use the information gained in that process to assess which individuals or departments were most likely to have incentive to commit a fraudulent act and, if so, by what means. This information can be summarized into the fraud risk assessment template and can help the organization design appropriate risk responses, if necessary.

Risk Response

Risk tolerance varies from organization to organization. Senior management or those charged with governance set the organization's risk tolerance level taking into consideration its responsibilities to all stakeholders. Some organizations want only to address fraud risks that could have a material financial statement impact, other organizations want to have a more robust fraud response program. Many organizations will state that there is a "zero tolerance" policy with respect to fraud. However, there may be certain fraud risks that an organization considers too expensive and time-consuming to address through controls. Consequently, the organization may decide not to put controls in place to address such risks. If a fraud is discovered, zero tolerance for fraud would be applied.

Figure 22 provides a summary of the professional organizations' key elements of fraud risk assessments. DoD organizations are encouraged to use this summary as a tool to educate employees and managers about the fraud risk assessment process.

Figure 22. Key Elements of Fraud Risk Assessments



Example Fraud Risk Assessment Framework

Organizations should document the results of the fraud risk assessment. Table 6 illustrates how the elements of fraud risk identification, assessment, and response are applied. For illustrative purposes, some information in this example was developed by the DoD OIG, Office of Audit Policy and Oversight, and also adapted from the State of North Dakota's, Fraud Risk Assessment Guidance.²² Appendix E contains another example illustrating potential revenue recognition risks within financial reporting.

Table 6. Example Fraud Risk Assessment

Identified Fraud Risks and Schemes	Likelihood	Significance	People and/or Department	Existing Anti-Fraud Controls	Controls Effectiveness Assessment	Residual Risk	Fraud Risk Response
Contract Award							
Contracts improperly awarded	Probable	Material	Contracting Official	Multiple supervisory reviews are required for each contract award.	Tested by management.	Potential for bribery or kickbacks to contracting employees. Bribery or kickbacks would be difficult to detect during management reviews.	Management monitors contract awards. Employees are aware of consequences of unethical behavior to include termination and other adverse actions.
Unauthorized or missing approvals	Probable	Material	Contracting Officer	Supervisory reviews of all awards are required.	Files are periodically reviewed by internal auditors and independent staff.	Adequately mitigated by controls.	Fraud risk response not required, adequately mitigated by controls.
Missing or incomplete file documentation	Probable	Material	Contracting Officer	All records are maintained electronically. System will not allow the contract award to process until all documentation is in the electronic record.	System controls are in place to monitor awards.	Possible override of system controls by contracting employees.	Information technology department conducts routine checks to test for control overrides.

²² Numerous audit organizations have also adapted this framework as a tool to assess the risk of fraud when performing their work.

Australian National Audit Office Fraud Risk Management Process

The Australian National Audit Office's fraud risk assessment process involves **communicating and consulting** with relevant employees at all levels within the organization during all stages of the risk assessment. This communication addresses issues relating to the risk itself, its causes, its impact (if known), and the measures taken to address it. The approach ensures that those accountable for implementing the risk management process and stakeholders understand the basis of decision making and the reasons particular actions were required.

Establishing the context involves articulating the organization's objectives and the external and internal parameters to be taken into account when managing risk. This process also establishes the scope and risk criteria for the remaining process.

Identifying fraud risks requires organizations to consider both internal and external fraud risks. Organizations are also encouraged to consider fraud risks that could emerge in the future, for example, fraud risks arising from a change to an information technology system or other significant changes in business processes. It is also important to consider fraud risks when evaluating the design of a new system or program. Identifying fraud risks at the system and program levels assists the organizations' efforts to assess overall organizational risk and to reflect these risks in their strategic planning objectives.

Because fraud is characterized by dishonesty and deception, the identification of fraud risks requires a skeptical mindset and involves asking probing questions during brainstorming such as:

- How might a fraudster exploit weaknesses in the systems of controls?
- How could a fraudster override or circumvent controls?
- What could a fraudster do to conceal fraud?

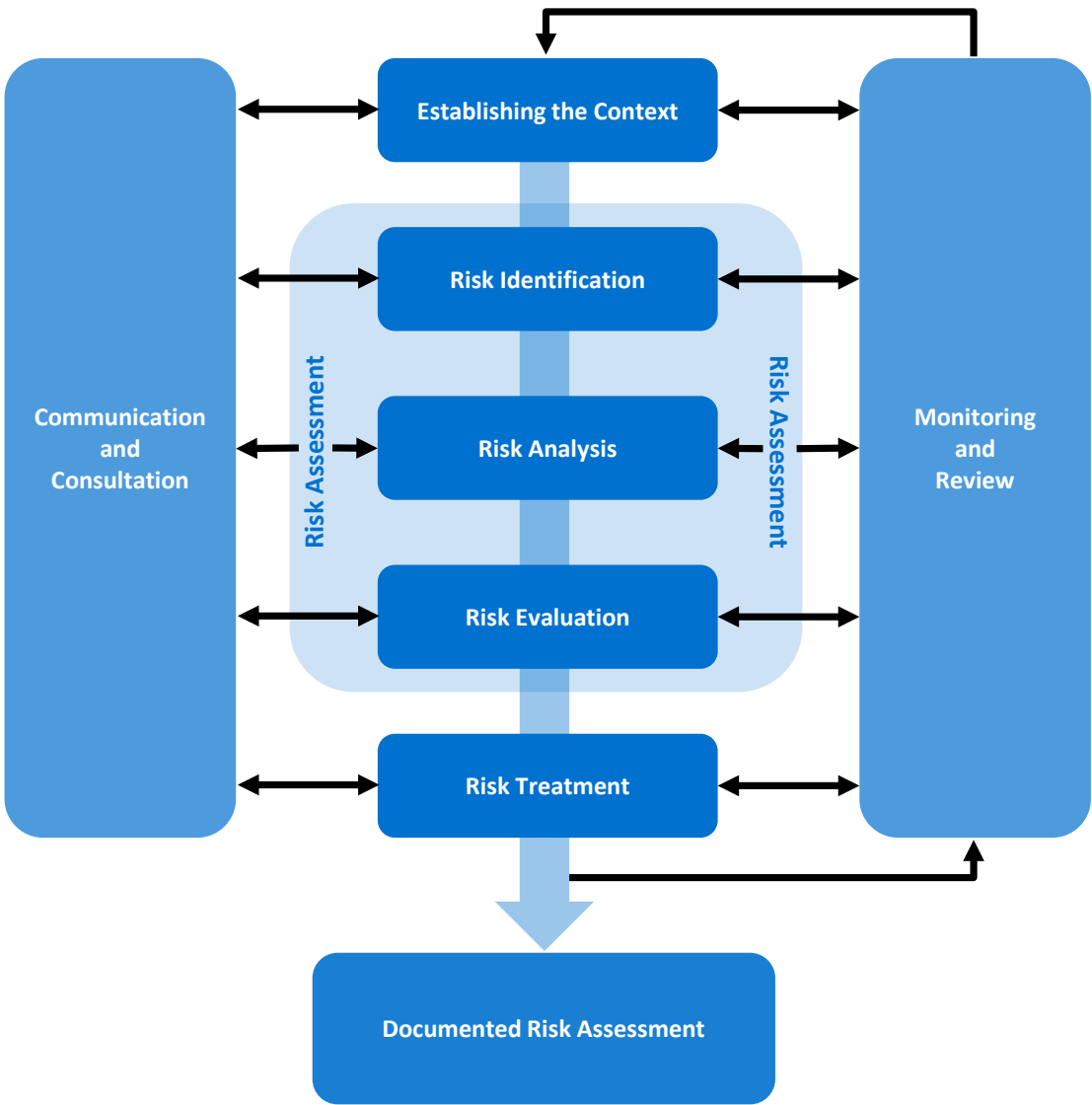
Documenting and assigning ownership of the risks and controls is important. The business area responsible for managing a particular fraud risk is identified and the timeframe for implementing any remedial action is clearly documented in risk management plans.

It is also **important to monitor and review** the fraud risk assessment regularly. A fraud risk assessment should be performed at least every 2 years and coincide with a review of the organization's overall fraud control plan. When an entity

undergoes a substantial change in structure or function, or when there is a significant transfer of responsibilities, the entity must undertake another fraud risk assessment in relation to the changed functions. An organization could also consider implementing an ongoing program to update the fraud risk assessment more frequently.

Organizations should actively monitor and review their identified fraud controls. Changes in the effectiveness or applicability of these fraud controls can impact the organization's fraud risk assessment to either increase or decrease fraud risk. Figure 23 illustrates the Australian National Audit Office's fraud risk management process.

Figure 23. Australian National Audit Office Fraud Risk Management Process



Source: Joint Australian/New Zealand International Organization for Standardization, Standard 3100:2009, Risk Management Principles and Guidelines

Australian National Audit Office Fraud Risk Assessment Approach

The Australian National Audit Office's fraud risk assessment approach provides a methodology to evaluate a program, function, or business area. Organizations begin the process by describing a specific fraud risk. At the end of the assessment, actions are developed to address each risk area. When using this methodology, it is important that organizations perform each of the steps in the sequence described in Table 7.

Table 7. Australian National Audit Office Fraud Risk Assessment Approach

Fraud Risk Description	The fraud risk is described; ensuring that both the cause and impact of the fraud risk happening is included in the description provided.
Fraud Risk Factors	The fraud risk factors are those conditions or actions which are most likely to cause the fraud risk to occur. This is generally a brief list of likely scenarios that could occur.
Inherent Likelihood	The inherent likelihood provides an indication of how often an identified risk might occur in the absence of any controls. This is generally measured using a five-point scale (that is, almost certain, likely, possible, unlikely, rare).
Inherent Risk Rating	The inherent risk rating provides a ranking for an identified risk once the likelihood and consequence of the risk has been considered in the absence of any controls. This is generally measured using a five-point scale (that is, severe, high, medium, low, very low).
Key Controls Identified	The key controls refer to those controls currently established within the entity to minimize the likelihood and consequence of the identified fraud risk from happening.
Residual Likelihood	The residual likelihood provides an indication of how often an identified risk might occur when taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale (that is, almost certain, likely, possible, unlikely, rare).
Residual Consequence	The residual consequence provides an indication of how serious the consequences would be if an identified risk occurred when taking into consideration the effectiveness or otherwise of the existing controls. This is generally measured using a five-point scale (that is, extreme, major, moderate, minor, insignificant).
Residual Risk Rating	The residual risk rating provides a ranking for an identified risk once the likelihood and consequence of the risk has been considered after taking into consideration the effectiveness of the existing controls. This is generally measured using a five-point scale (that is, severe, high, medium, low, very low).
Fraud Risk Owner	The fraud risk owner is the individual/group within the entity with accountability for managing the identified fraud risk.
Action Required	The action required relates to the identification of any further actions that the entity must undertake in relation to the identified fraud risk (that is, new controls to be established).

"Fraud Control in Australian Government Entities, Better Practice Guide, Australian National Audit Office and KPMG," March 2011, pages 36, 37, and 91.

Association of American Medical Colleges

The Internal Audit Division of the Association of American Medical Colleges (AAMC)²³ facilitates an annual enterprise-wide risk assessment, which includes an assessment of fraud risk. The organization's 35 auditable units participate in the review, which includes representatives from Finance, Information Technology, and Human Resources. The assessment also provides an opportunity for Internal Audit to educate other employees about fraud, and increase fraud awareness within the organization.

Quantifiable Fraud Risk Assessment

Both quantifiable and qualitative approaches are used to identify and evaluate fraud risks. For the quantifiable ranking, numeric values are assigned, ranging from a low of one to a high of five. Participants are also required to consider impact and opportunity when rating fraud risk, along with inherent and residual risks. For example, fraud risk in the Finance Department would be rated higher and have a more significant impact on the organization when compared to fraud risk at the on-site library. All business unit representatives are required to agree on the final risk rankings assigned. When the client rates the fraud risk as low (because of the presence of mitigating controls), but the auditors believe that the risk may be higher (for example, based on previous audits or audit experience), the auditors adjust the fraud risk scores up or down, as needed, after the business units complete their assessments.

During the fraud risk assessment discussions, Internal Audit asks business unit representatives about ways that *fraud could occur* versus where fraud is occurring. This approach helps to stimulate discussion and causes people to think about fraud. Additional topics discussed include opportunities for management fraud, employee fraud, unauthorized use or disclosure of sensitive information, theft of assets, and other illegal acts.

Table 8 depicts examples of the business units and risk attributes that are evaluated during the assessment. Business units/auditable units with interrelated functions and objectives are grouped in clusters.

²³ The AAMC is a nonprofit group of medical schools, hospitals, and academic societies. The organization provides assistance for members in the areas of education, research, and patient care.

Table 8. Business Units and Risk Attributes

Auditable Unit	Audit Name	Personnel	Financial	Process and Operational	Technology	Environmental	Governance	Fraud	Compliance	Reputational	Prior Audit Results	Total	Adjusted	Final Rating
Academic Affairs & Programs (Academic Affairs)														
	Academic Affairs											0		
Communications (Public Policy & Strategic Relations)														
	Communications											0		
Diversity Policy & Programs														
	Diversity											0		
Finance (Operations and Services)														
	General Accounting											0		
	Payroll											0		
Global Health Learning Opportunities (Operations and Services)														
	Global Health Learning Opportunities											0		
Government Relations (Public Policy and Strategic Relations)														
	Government Relations											0		
Health Care Affairs														
	Health Care Affairs											0		
Human Resources (Operations and Services)														
	Benefits											0		
	Human Resources											0		
	Compensation											0		
Information Technology (Operations and Services)														
	Data Integrity											0		
	Information Technology Services											0		
	Disaster Recovery											0		
	Information Technology Security/General Computer Controls											0		
	Reminder Sent	Response Received												

Qualitative Fraud Risk Assessment

The qualitative component of the fraud risk evaluation is an on-line Risk Assessment Survey, which is sent to all entity-wide risk assessment participants. Survey respondents have the option of identifying themselves or submitting their responses anonymously. The survey approach helps fill gaps in the quantifiable fraud risk assessment rankings. For example, the quantifiable assessments provide Internal Audit with numeric risk rankings, while the survey method provides insight regarding the thoughts behind the numbers. The survey also gives information on internal control improvement opportunities within the organization.

Figure 24 is an example of an online Risk Assessment Survey. The survey is intended for illustrative purposes only. DoD organizations are encouraged to develop surveys designed to target their specific programs, operations, or fraud vulnerabilities.

Figure 24. Survey Questions

Example Fraud Risk Assessment Survey Questions

1. In your opinion, what are the top risks or potential obstacles to achieving your operational objectives within your unit?
2. In your opinion, what are the top risks or potential obstacles to achieving your objectives within your cluster?
3. In your opinion, what are the top risks or potential obstacles that may prevent the organization from achieving our stated objectives?
4. Is there an obstacle, challenge or risk that “keeps you up at night?” If so, what are they, and why do they concern you?

Example Fraud Risk Assessment Survey Questions (cont'd)

5. Generally, where do you feel your unit is in terms of maturity of the internal control structure?
 - Initial: Controls of risks are ad-hoc, not in place, not working as intended or are easily overlooked or overruled.
 - Repeatable: Process to control risks is established and repeating, and controls documentation is lacking.
 - Defined: Process to control risks is established, repeating, documentation is in place to support the process.
 - Managed: Risks are managed systemically and reviewed at the enterprise level.
 - Optimized: Controls of risk are continuously improving and managed at an enterprise level.
6. Generally, how is your unit performing in relation to your stated objectives?
 - Always or nearly always, achieve objectives timely and without issue.
 - Periodically, our objectives are met timely and without issues.
 - It is often difficult to achieve process objectives timely and without issue.
 - Rarely are our objectives able to be met timely and without issue.
7. If you have any comments on risk or this survey, please add them below.

Advantages of Fraud Risk Assessment Surveys

Figure 25 highlights the advantages of using fraud risk assessment surveys. To maximize survey benefits, DoD organizations should ensure that they are not too long or time-consuming to complete. It is also important to request participation from both supervisory and nonsupervisory employees in the survey process. All participants should be reassured that their identities and responses remain confidential.

Figure 25. Survey Advantages.

Advantages of Fraud Risk Assessment Surveys

Fraud risk assessment surveys provide employees with ways to:

- Report fraud and/or fraud risks without their co-workers and supervisors in the same room or meeting.
- Identify fraud and/or fraud risks that may be occurring within their business units.
- Report suspect activity happening in other business units.

Smart Insights, LLC Fraud Risk Assessment Approach

The company²⁴ uses an Internal Fraud Risk Assessment Questionnaire that is intended to help identify gaps in an organization's anti-fraud program and processes. Benefits relating to this assessment approach are:

- provides an inexpensive, cost-effective means of identifying areas that are vulnerable to fraud,
- helps to proactively identify areas that are susceptible to fraud that could adversely impact an entity's financial position and/or reputation,
- pinpoints opportunities to save money or drive operational improvements,
- detects internal controls and/or processes that need improvements, and
- increases the confidence of the organizations clients and stakeholders.

²⁴ Smart Insights, LLC, is a consulting firm based in the District of Columbia. The company specializes in procurement and supply chain management, human capital, and organizational risk.

Participants are instructed to carefully review each question prior to assigning a final score, take their time developing their response, and provide comments or notes, as needed.

The following scoring legend is used to evaluate each question:

- A score of 0 represents an entity that has not implemented any of the recommendations.
- A score of 100 represents an entity that has designed and implemented processes, but has not tested them within the past twelve months.
- A score of 200 is given to an entity that has designed, implemented, tested, and determined the processes to be operating effectively within the most recent 12-month period.
- Any score less than 200 serves as a reminder that there is an opportunity for improvement.

For illustrative purposes, responses to the Internal Control Questionnaire were prepared using information contained in Department of the Navy, Bureau of Medicine and Surgery, Instruction 5370.04, "Navy Medicine Anti-Fraud Program," April 1, 2010 (see Appendix F). The scores assigned were based on fictitious information and are not related to a specific DoD organization or program.

Texas Tech Fraud Risk Assessment Approach

Members of the Internal Audit Department oversee entity-wide fraud risk assessments at Texas Tech locations. As facilitator's, the auditor's role consists of gathering information about fraud risks and reporting the results of each assessment to senior management. The fraud risk assessments are conducted in accordance with the International Standards for the Professional Practice of Internal Auditing. Related benefits are educating employees about fraud and increasing fraud awareness at participating campuses.

The Perception-Based Fraud Risk Assessment Approach

Texas Tech's fraud risk assessment process was developed by seasoned audit staff. Internal Audit named their methodology the Perception-Based Approach for Assessing Fraud Risk. Experienced employees and subject matter experts from each campus are selected to participate in fraud risk ranking sessions.

A cross-cutting methodology is used to identify employees representing a range of departments that includes accounting, payroll, accounts receivable, and business managers from various components.

During assessment planning, the audit team uses the ACFE Fraud Examiner's Manual to select fraud schemes for discussion and risk ranking for each session. This information is included in a Glossary of Fraud Schemes, which is not provided to participants in advance. At the start of each fraud risk assessment, fraud statistics from the most recent ACFE report on occupational fraud²⁵ are also discussed. Additionally, facilitators explain each fraud scenario in the Glossary of Fraud Schemes to participants. To educate employees about fraud, auditors use real-life examples to demonstrate how each fraud type could occur at their location and provide information about relevant fraud indicators. The employee's role in assisting with detecting and preventing fraud is also emphasized.

Electronic Polling Software Results

During one Texas Tech fraud risk assessment, the auditors initially focused on schemes related to corruption, asset misappropriation, and financial statement fraud. Nonfinancial fraud schemes were purposely excluded because they planned to focus on this type of fraud when facilitating future assessments. Financial statement fraud was also eliminated because most of the pressures and incentives related to private companies and did not exist in an academic environment. Other criteria used to identify the fraud schemes included:

- likelihood of occurrence
- auditors' prior knowledge and experience with fraud at the location

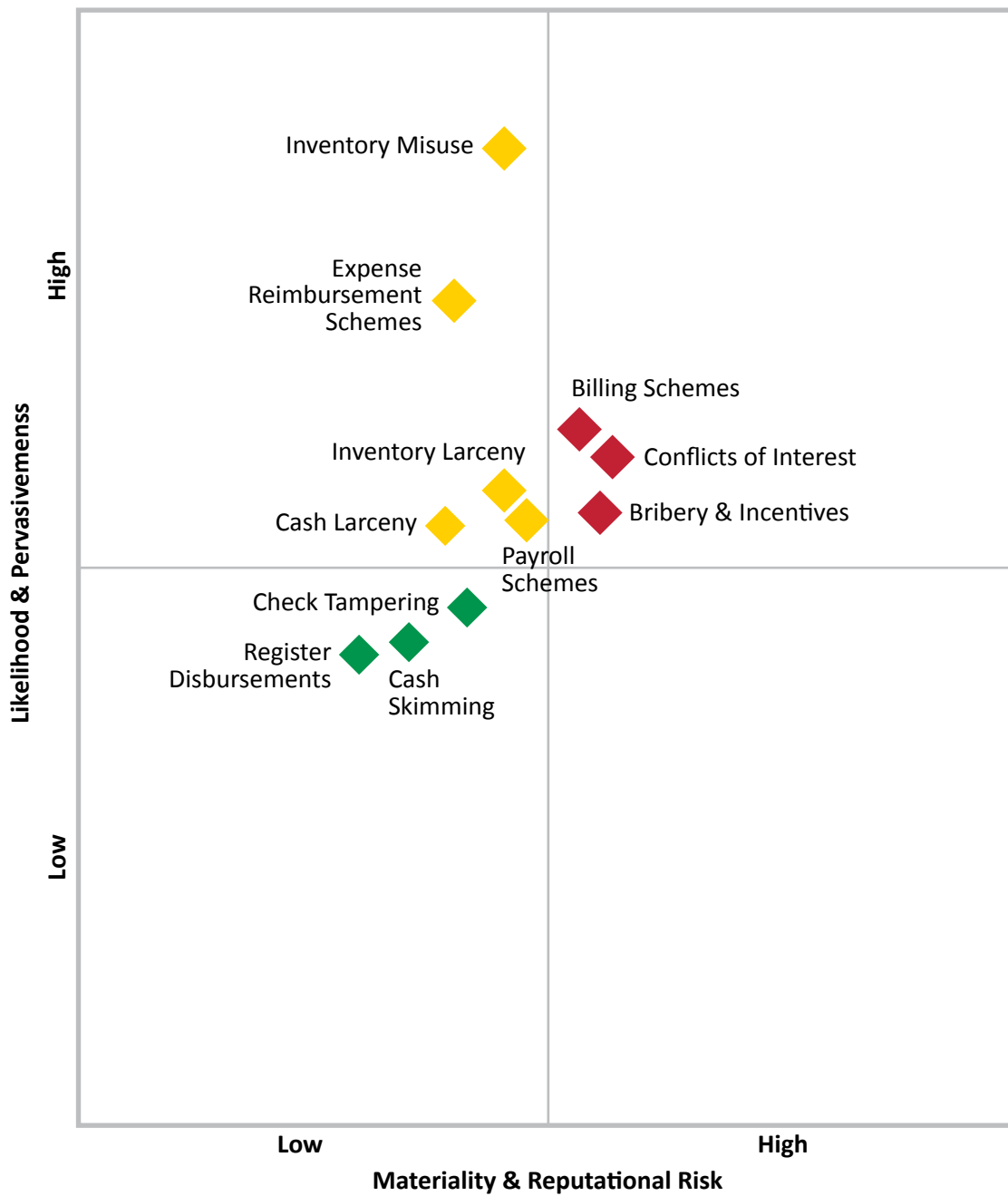
The engagement consisted of nine risk assessment sessions where the perceptions of 52 Texas Tech employees regarding the likelihood, pervasiveness, materiality, and reputational risks of 24 different types of fraud schemes were polled. After each fraud scheme was explained, the participants ranked the schemes using electronic polling software.

Figure 26 depicts a heat map²⁶ fraud risk perceptions of the Texas Tech Administration employees who provided input for the fraud risk assessment.

²⁵ The ACFE's "Report to the Nations on Occupational Fraud and Abuse," details the survey results of Certified Fraud Examiners that were requested to provide information on fraud cases that met specific criteria. The data is compiled in a comprehensive report and offers insights about prevention and detection methods.

²⁶ A heat map is defined as a two-dimensional representation of data in which values are represented by colors. A simple heat map provides an immediate visual summary of information. Source: [SearchBusinessAnalytics.com](https://www.searchbusinessanalytics.com)

Figure 26. Example Texas Tech Heat Map



- ◆ Red – Perceived to have high likelihood and probability as well as high materiality and reputational risk
- ◆ Yellow – Perceived to have high likelihood and probability, but a low materiality and reputational risk
- ◆ Green – Perceived to have a low likelihood and probability and a low materiality and reputational risk

Advantages of the Perception-Based Fraud Risk Assessment Approach

Figure 27 highlights the benefits of Texas Tech's Perception-Based Approach for Assessing Fraud Risk. DoD organizations should consider implementing electronic polling software, or comparable technology, when performing fraud risk assessments. Similar to online surveys, both approaches allow anonymous responses from employees.

Figure 27. Benefits of the Texas Tech Approach

Benefits of the Perception-Based Fraud Risk Assessment Approach

- Electronic polling allows participants to remain anonymous when evaluating fraud risks. Because people may not be comfortable or open discussing fraud in the presence of their managers, anonymity encourages more truthful responses.
- Live interaction helps facilitators gauge participants' understanding of the fraud schemes and indicators before risk rankings are submitted.
- The polling software can be embedded within Fraud Awareness Briefings to obtain additional information about employee's fraud perceptions. This data can be analyzed to identify trends and compare results at different business units within an entity.

Additionally, electronic polling enables a greater number of employees to participate in the fraud risk assessment process. As a result, more information is received, in less time, when compared to meetings with small groups, or one-on-one discussions about fraud risks.

Grant Thornton Approach for Enterprise Risk Management

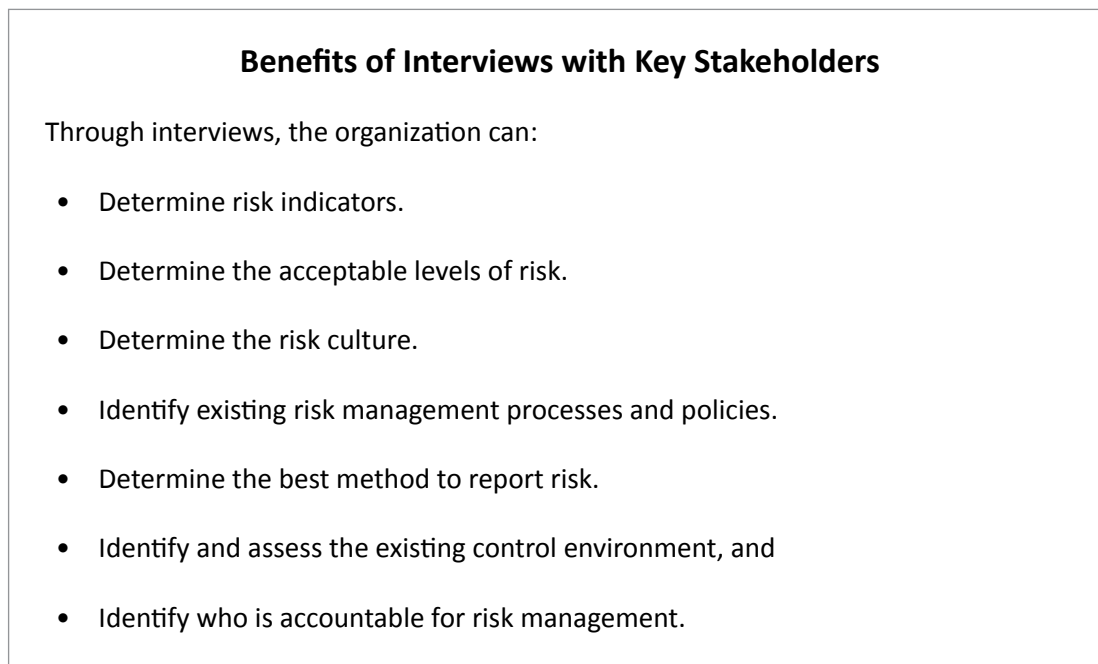
A fraud risk assessment is an integral part of enterprise-wide risk assessment. It is the responsibility of management to identify, measure, and reduce fraud risks to acceptable levels. As part of an ongoing, systematic, and recurring enterprise fraud risk assessment, the fraud risk assessment should consider internal and external fraud risks at all levels enterprise-wide. Additionally, it should prioritize fraud risk by significance, likelihood, and exposure.

The following information describes the five tasks that should be performed when developing a successful enterprise risk management program.

Task 1 – Establish a Framework

To establish the framework and governance structure the organization should collect and review information regarding the organization, including organization structure, roles and responsibilities, policies and procedures, audit reports, existing enterprise risk management documentation, and other organizational artifacts. After reviewing these materials, the agency should perform interviews with stakeholders, focusing on key risk areas, including organizational, financial, political, technological, market, legal, and security. Figure 28 describes the benefits of conducting interviews with stakeholders.

Figure 28. Interview Benefits



Using the information collected, the organization should develop the components of the framework, identify a governance structure that will complement the organization and culture, and develop the enterprise risk management architecture needed to support the program. Once the framework and governance structure are defined, the organization should develop the risk management policy and the policy for risk identification, assessment, measurement, mitigating, monitoring, and reporting.

Task 2 – Risk Identification

Leveraging information gathered during stakeholder interviews in Task 1, the organization should develop a methodology to identify and categorize risks across the enterprise, measure the intensity of the elements that drive each risk, and assess the organization's exposure to these elements. The benefits achieved through this effort will provide the organization with a shared language about its risks, promoting a more risk-aware environment that is equipped to respond quickly if a problem occurs.

Additionally, it is recommended that the Fraud Prevention Check-Up published by the ACFE be used as a tool for establishing a baseline in determining how well an organization understands its risk for fraud. The Fraud Prevention Check-Up is a survey that asks key questions related to fraud risk oversight, ownership, assessment, risk tolerance and management, anti-fraud controls, and fraud detection. The Fraud Prevention Check-Up is available on the ACFE's website at www.ACFE.com.

Task 3 – Risk Prioritization and Evaluation

The identification of risks leads to questions on how to best mitigate risks. The organization should identify possible responses and actions based on its' risk aversion appetite. The organization should first develop risk prioritization and evaluation policies, procedures, and business boundaries with clear objectives for enterprise risk management activities. These policies and procedures are guided by the risk aversion, or the extent to which management is willing to accept risk, which in risk evaluation is achieved by defining individual risk tolerance.

Task 4 – Risk Management

Effective risk management involves creating feasible corrective actions for control deficiencies and gaps identified, as well as understanding findings in the broader context of the organization's strategic goals. The organization should concentrate first on developing responses to high-frequency, high-severity events by assisting management with creating a risk response for factors that contribute to the risk's occurrence, evaluating response benefits versus the long-term costs, and defining quantifiable corrective actions that can be implemented and monitored.

Task 5 – Risk Monitoring, Reviewing and Reporting

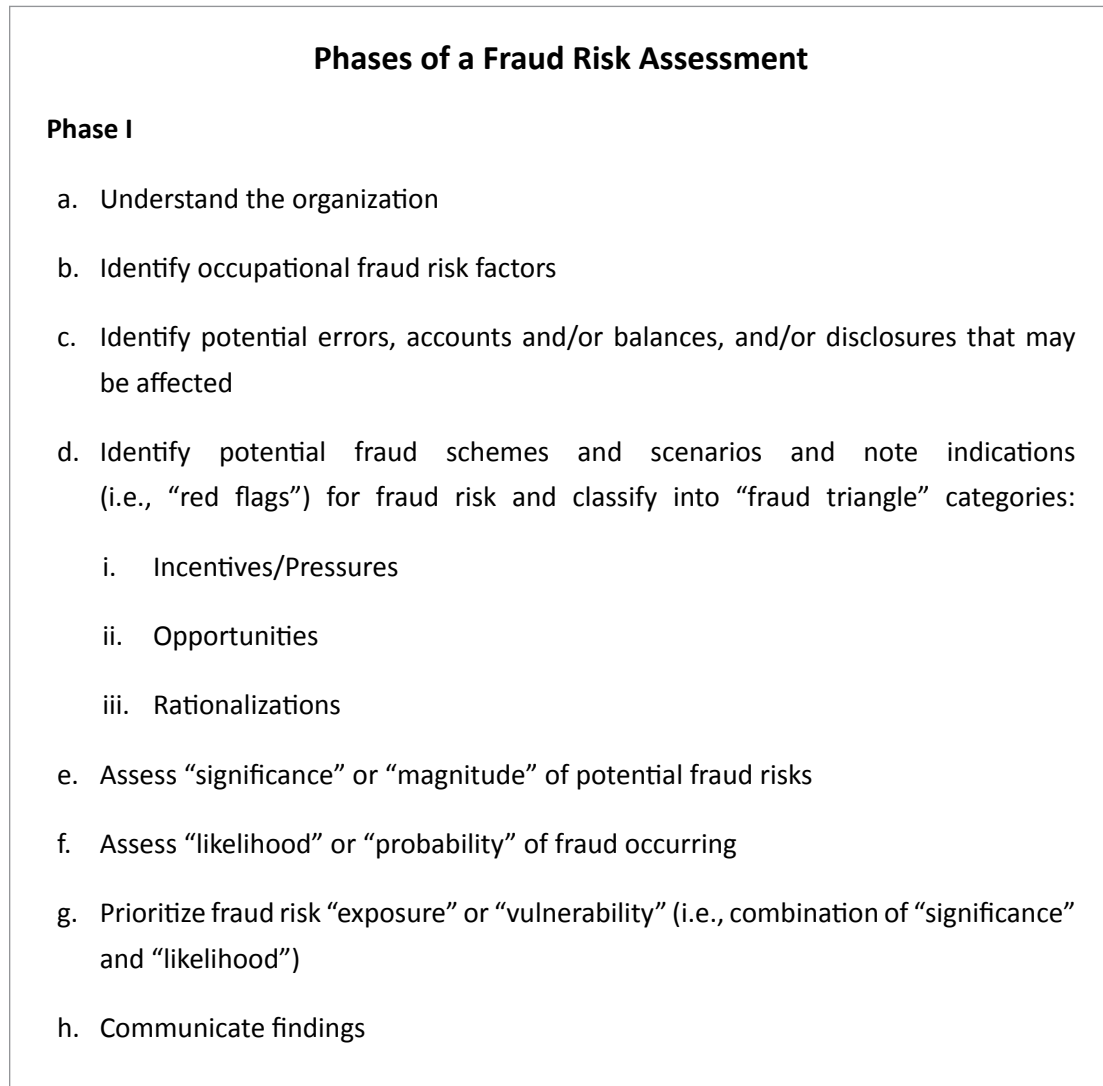
The organization's risk policy should contain clear objectives and guidance for risk monitoring, review, and reporting linked to overall business strategies. In addition, it should provide direction on communication of risks to senior management, execution on risk mitigation decisions, and procedures for monitoring remediation activities and the identified risks. The following should be monitored and reported:

- key risk ratings or profiles that classify and describe all risks,
- key performance indicators that measure impact of risks on performance,
- risk rates and modeling to measure risk concentration and interdependencies,
- top-level key risk indicators to provide an early signal of increasing risk exposures, and
- testing and validation results (stress testing and control testing).

Grant Thornton Fraud Risk Assessment Approach

Grant Thornton's fraud risk assessment approach consists of three phases, summarized in Figure 29. It is important for DoD organizations to complete each step in the sequence in Figure 29 if they elect to use the Grant Thornton approach. Additionally, the approach can be modified to suit an organization's size, structure, and known fraud vulnerabilities.

Figure 29. Grant Thornton Fraud Risk Assessment Phases



Phases of a Fraud Risk Assessment (cont'd)

Phase II

- a. Understand management's objectives related to fraud risk management, including tolerance for acceptable residual fraud risks
- b. Identify anti-fraud measures, programs, procedures, policies and internal controls
- c. Perform walk-throughs, as needed
- d. Document as requested
- e. Evaluate effectiveness of anti-fraud measures, programs, procedures, policies and internal controls to mitigate prioritized fraud risks
- f. Identify any "gaps" or weaknesses
- g. Prepare recommendations for improvements
- h. Communicate findings and recommendations

Phase III

- a. Identify anti-fraud measures, programs, procedures, policies and internal controls to be tested for compliance
- b. Sample and test anti-fraud measures, programs, procedures, policies and internal controls
- c. Evaluate results
- d. Identify any "gaps" or weaknesses
- e. Prepare recommendations for improvements
- f. Communicate findings and recommendations

The fraud risk assessment documentation will generally include written reports, documentation of procedures, recommendations, and proposed next steps. For an example client report and illustrative heat map of fraud risks, see Appendix G.

Summary of Entity-Wide Approaches for Conducting Fraud Risk Assessments

Table 9 summarizes the key attributes, similarities, and differences of the various fraud risk assessment approaches discussed within this section. As emphasized throughout this report, each of the suggested approaches can be modified to suit an organization's mission, size, or specific fraud vulnerabilities. DoD organizations are also encouraged to develop other approaches for performing fraud risk assessments using information presented within this report as a resource.

Table 9. Summary of Entity-Wide Approaches for Conducting Fraud Risk Assessments

Organization	Fraud Risk Assessment Attributes
DoD Investigative Agencies	- Brainstorming sessions help to identify fraud risks. - Review of current fraud trends and organization expenditures to identify high-risk areas. - For decentralized organizations, request input regarding specific trends occurring at various geographic areas. - Fraud efforts are focused on areas of high Congressional interest. - Assessment results are reported to investigative employees, senior management officials, and the Senior Executive Board.
Navy Exchange Service Command	- Use of CSAs to identify gaps in internal controls and potential fraud risks and vulnerabilities. - Fraud awareness training is provided to stimulate discussions with employees and educate them about the CSA process and goals. - CSA results are reported to management.
Naval Sea Systems Command	- Facilitate discussions with employees to identify fraud risks. - Fraud awareness training is provided during employee discussions. - Report of results prepared for management.
Institute of Internal Auditors, American Institute of Certified Public Accountants, Association of Certified Fraud Examiners	- Fraud risk assessment template used to identify and rank fraud risks. - Emphasize participation of subject matter experts in the fraud risk assessment process.
Australian National Audit Office	- Require the organization to involve relevant employees at all levels to participate in the fraud risk assessment process. - Emphasize the importance of documenting and assigning ownership of fraud risks and controls. - Require documentation of the assessment results.
Association of American Medical Colleges	- Online employee surveys encourage anonymous reporting of potential fraud risks or suspect activities. - Interviews with managers and employees help to quantify fraud risks. - Fraud awareness training is conducted during employee interviews.

Organization	Fraud Risk Assessment Attributes
Smart Insights, LLC	Internal Fraud Risk Assessment Questionnaires are used to identify gaps in an organization's anti-fraud program and processes.
Texas Tech	- Electronic polling software is used to identify high-risk areas. The approach permits employees to rate fraud risks anonymously. - A Glossary of Fraud Schemes is developed to provide employee fraud awareness training during the fraud risk assessment process. - Heat Maps are prepared to illustrate assessment results to management. - Report of fraud risk assessment results is prepared for management.
Grant Thornton	- Fraud risk assessments are considered a component of enterprise risk management. - Three-phase approach for conducting fraud risk assessments. Phase one emphasizes identifying fraud schemes and indicators. Phase two focuses on identifying weaknesses and reporting the results to management. Phase three consists of making recommendations for improvements.

Summary of DoD and External Organizations' Fraud Initiatives

DoD Entities and External Organizations' Fraud Risk Assessment Approaches, Fraud Awareness Training, and Internal Control Evaluations

We interviewed 82 subject matter experts from 33 DoD organizations. External participants represented both public and private entities and consisted of 18 subject matter experts from 12 organizations. During our review, we identified effective approaches for conducting audit and entity-wide fraud risk assessments, fraud awareness training activities, and internal control evaluations. We used documentation obtained from subject matter experts at Naval Audit Service; DoD OIG, Office of the Deputy Inspector General for Audit; AICPA; Smart Insights Group, LLC; Navy Bureau of Medicine and Surgery; Grant Thornton; NAVSEA; Council of the Inspectors General on Integrity and Efficiency, Training Institute (CIGIE); and the Australian National Audit Office to develop example documents included in Appendixes B through J.

During our interviews with DoD and external subject matter experts, we identified numerous innovative approaches for conducting fraud risk assessments. Of the 33 DoD organizations we interviewed, 13 were conducting entity-wide risk assessments, 26 were conducting fraud risk assessments when performing audit-related work, 23 were providing fraud awareness training, and 3 were concentrating on internal control evaluations. Table 10 indicates the focus of each participating DoD organization.

Table 10. Focus Areas of DoD Organizations

DoD Organization	Fraud Risk Assessment	Fraud Awareness Training	Internal Control Evaluations
Department of Defense			
Army and Air Force Exchange Service, Audit Division	X	X	
Defense Commissary Agency, OIG, Audit Division	X		
Defense Contract Management Agency, Contract Integrity Center	X*	X	
Defense Contract Management Agency, Internal Review	X		
Defense Information Systems Agency, OIG, Audit	X		
Defense Information Systems Agency, OIG, Investigations	X*	X	
Defense Logistics Agency, OIG, Audit Division	X		
Defense Logistics Agency, OIG, Investigations Division	X*	X	
Defense Logistics Agency, Office of General Counsel	X*,†		
DoD OIG, Office of the Deputy Inspector General for Audit	X	X	
DoD OIG, Defense Criminal Investigative Service	X*	X	
DoD OIG, Office of General Counsel		X	
DoD OIG, Office of the Deputy Inspector General for Policy and Oversight		X	
Missile Defense Agency, Internal Review	X		
Missile Defense Agency, Managers' Internal Control Program			X
Missile Defense Agency, Quality, Safety, and Mission Assurance	X*,‡	X	
National Geospatial Agency-Intelligence, OIG, Investigations	X*	X	
Office of the Undersecretary of Defense, Comptroller, Financial Improvement and Audit Readiness Division			X

* The organization is performing entity-wide fraud risk assessments. Organizations that do not have a notation indicated that they are performing fraud risk assessments during audits, evaluations, or internal reviews.

† Member of the DoD Counterfeit Parts Working Group.

‡ Representatives from these organizations provided information about the DoD Procurement Fraud Working Group's activities.

DoD Organization	Fraud Risk Assessment	Fraud Awareness Training	Internal Control Evaluations
Department of Defense (cont'd)			
Office of the Undersecretary of Defense, Acquisition, Technology, and Logistics, Defense Procurement & Acquisition Policy ‡		X	
Tricare Management Activity, Program Integrity Office	X*	X	
Department of the Army			
Army Audit Agency	X	X	
Army Criminal Investigation Command	X*	X	
Department of the Navy			
OIG Marine Corps	X		
Marine Corps Nonappropriated Funds Audit Service	X	X	
Marine Corps Risk and Compliance			X
Naval Audit Service	X	X	
Naval Criminal Investigative Service	X*	X	
Navy Exchange Command, Office of Internal Audit	X	X	
Naval Sea Systems Command, OIG	X*	X	X
Risk Management and Compliance Branch	X*	X	
Department of the Air Force			
Air Force Audit Agency	X	X	
Air Force Office of General Counsel ‡		X	
Air Force Office of Special Investigations	X*	X	

* The organization is performing entity-wide fraud risk assessments. Organizations that do not have a notation indicated that they are performing fraud risk assessments during audits, evaluations, or internal reviews.

† Member of the DoD Counterfeit Parts Working Group.

‡ Representatives from these organizations provided information about the DoD Procurement Fraud Working Group's activities.

Department of Defense

Army and Air Force Exchange Service Audit Division. Seventy-five percent of the staff members are Certified Fraud Examiners. All new hires are required to attend the ACFE test preparation course. The Audit Division invites employees from other AAFES disciplines to participate in the test preparation classes to include Loss Prevention, OIG, Finance Department, and buyers for stores. This approach helps to educate people throughout the organization about fraud. The Audit Division also developed a fraud risk assessment template. When performing their work, auditors are required to consider internal controls, fraud risks, and approaches to evaluate the effectiveness of the controls. Staff members conduct internal control audits at exchange stores, focusing on key control areas, such as over refunds, receipts, and damaged and defective goods. The Audit Division provides recommendations to management on ways to improve existing controls and store operations.

Defense Commissary Agency OIG, Audit Division. All audit staff participate in fraud brainstorming sessions. During the meetings, team members use a whiteboard to visually map the process they are auditing. A template was developed that requires auditors to evaluate the control risks, fraud indicators, potential for control overrides, control effectiveness, and impact on the organization. The Defense Commissary Agency developed the "Front End Audit Worksheet Information Guide" to assist senior managers' efforts to assess suspect financial transactions such as refunds, suspended transactions, or coupon misuse. The Audit Division provided examples of fraud indicators that were included in the Guide. In June 2012, the Director, Defense Commissary Agency, sent a memorandum to all employees emphasizing the importance of fraud prevention and discussed the role of the OIG in preventing and detecting fraud within the organization.

Defense Contract Management Agency, Contract Integrity Center. In 2007, the organization developed its first Strategic Plan for FY 2007-2012; the plan was most recently revised in July 2009. The purpose of the project was to identify fraud vulnerabilities and educate senior Defense Contract Management Agency leadership about the mission of the organization. This project was led by the Director, Contract Integrity Center, and participants included teams of attorneys working at various locations throughout the United States. The process started by examining the entity's fraud cases and assigning risk rankings of low, medium,

or high. The Director, Contract Integrity Center, then led discussions with smaller groups of attorneys and posed the question; "Fraud Happens, Why?" Brainstorming sessions were used to identify the organization's highest fraud risk activities and red, yellow, or green scores were assigned to each area. Next, high-risk areas received subsequent rankings such as high-risk/high-value, medium-high risk, and medium high-value. This information was used to develop the Contract Integrity Center Strategic Plan Goals, which included improving the capability of the entity's workforce to identify, report, and remediate fraud.

The organization also created a multifaceted fraud awareness training program. One of the more innovative training approaches are the on-line fraud training videos, similar to television soap operas, with cliffhangers at the close of each segment. Other web-based fraud resources include "Focus on Fraud" newsletters, fraud brochures, and fraud indicators and trends.

Defense Contract Management Agency, Internal Review. The Defense Contract Management Agency's Audit Manual requires auditors to be continuously alert to fraud when conducting their work and also includes information about fraud indicators. The Audit Team Leader coordinates discussions about fraud risk. The discussions are documented in the project files. All staff members participate in the Defense Contract Management Agency fraud training.

Defense Information Systems Agency, OIG, Audit. Auditors assess the potential for fraud, waste, and abuse when developing the annual audit plan. Areas considered include the amount of time since the last assessment; vulnerability to fraud, waste, and abuse; and external concerns. The team assigns scores to potential audit topics using the OIG Risk Assessment Tool. To evaluate the potential for fraud, auditors use risk rankings from high to low. Attributes of high-risk scores include assets that are easily converted to cash, high cost materials, and high potential for personal misuse. Information captured in the OIG Risk Assessment Tool is shared with audit staff to assist with audit planning.

Defense Information Systems Agency, OIG, Investigations. The organization conducted an entity-wide fraud risk assessment to develop a fraud awareness training program for Defense Information Systems Agency employees. Methods to identify fraud risks included an analysis of internal fraud trends, reviews of ongoing and previous fraud cases, and ACFE reports. Investigations staff also met

with more than 20 DoD and external organizations to obtain information about fraud training methods. A fraud awareness training video was developed, emphasizing procurement fraud. The video is continuously played throughout the entity's Headquarters, and at least 7,000 employees have seen the training. Investigators also conduct Fraud Awareness Briefings. Using video teleconference capabilities, briefing attendance ranges from twenty employees to six hundred. OIG Hotline submissions significantly increased with the organization's renewed emphasis on fraud awareness.

Defense Logistics Agency OIG, Audit Division. The Audit Division consists of a blend of staff members with diverse audit experiences that include other DoD audit organizations, private industry, and public accounting. As a result, fraud brainstorming sessions are enhanced through the team's collective knowledge and prior work experiences. Some offices prepare read-ahead briefing materials to encourage team members to think about fraud schemes and indicators before the brainstorming sessions and less senior auditors are required to review the DoD OIG Fraud Webpage²⁷ to enhance their fraud awareness. Types of information included in the pre-meeting briefing materials are the Defense Logistics Agency Management Internal Control Program, Statement of Assurance, AICPA and GAGAS guidance, and relevant ACFE fraud indicators. To promote discussion, members are encouraged to share their ideas, and an open forum approach is established. A fraud risk assessment template is used to summarize topics discussed during the brainstorming session and record ideas about potential fraud.

Defense Logistics Agency OIG, Investigations Division. The organization prepares an Annual Crime Vulnerability Assessment Plan. The plan's development begins with an informal meeting with Investigations senior management to discuss fraud indicators and trends. Risk rankings of high, medium, or low are assigned to each fraud category. The assessment results are shared with the Defense Logistics Agency Director, Senior Executive Board, and Investigations staff as a method to communicate priorities for the upcoming year. Investigations works closely with OIG Audit Division when performing their work. The ongoing partnership between the OIG components contributes to their success at detecting and preventing fraud.

²⁷ www.dodOIG.mil/resources/fraud/fraud_defined.html

Defense Logistics Agency, Office of General Counsel. The Office of General Counsel is an active member in the Counterfeit Parts Working Group.²⁸ Members include representatives from various DoD organizations and other Federal agencies such as Customs and Border Protection. Price, item, and supply are identified as significant fraud risks for counterfeit parts. DoD works with external vendors to develop statistical models to identify high risk areas and suppliers. The Defense Logistics Agency anti-fraud program has been in place for more than 20 years and includes on-line mandatory counterfeit parts training for all employees.

DoD OIG, Office of the Deputy Inspector General for Audit. The organization developed a predictive analytics pilot program using advanced data mining techniques. Program benefits included:

- increased internal and external collaboration and transparency,
- expanded accessibility and controls,
- verified audit and investigation outcomes, and
- consistent methodology and analysis techniques.

Planned focus areas were targeted at detecting fraud indicators in contracting, travel, and purchase card programs. Pilot participants included representatives from numerous DoD OIG components such as Audit, Defense Criminal Investigative Service, Information Systems Directorate, Hotline, and Office of General Counsel.

DoD OIG, Defense Criminal Investigative Service. This organization is the primary investigative arm of the DoD OIG and focuses its efforts on criminal/civil investigations involving the following areas: (1) procurement fraud and public corruption; (2) product substitution; (3) health care fraud; (4) illegal technology transfers, and (5) computer crime. From October 1, 2012 through March 31, 2013, the Defense Criminal Investigative Service investigations resulted in criminal fines, penalties, restitutions, and forfeitures totaling \$717.8 million. Defense Criminal Investigative Service representatives also participate as members of the National Intellectual Property Rights Center.

²⁸ The mission of the Counterfeit Parts Working Group is to detect and mitigate the risk of counterfeit parts within the DoD supply chain.

DoD OIG, Office of the Deputy Inspector General for Policy and Oversight.

The Investigative Policy and Oversight component was designated as the component responsible for receiving contractor disclosures in 2008. The Contractor Disclosure Program supports DoD's efforts to minimize the impact of fraud and criminal misconduct in areas such as counterfeit parts and materials, product substitution, and labor mischarging by:

- affording contractors a means of reporting certain violations of criminal law and violations of the civil False Claims Act and suspected counterfeit/nonconforming parts discovered during self-policing activities;
- providing a framework for government verification of matters disclosed; and
- providing an additional means for a coordinated evaluation of administrative, civil, and criminal actions appropriate to the situation.

During FY 2012 and 2013, 451 disclosures were received.

DoD OIG, Office of General Counsel. The organization supports the Defense Criminal Investigative Services' fraud investigative mission. Additionally, attorneys serve as liaison between DoD law enforcement agencies and fraud counsel at other DoD organizations including the Army and the Defense Logistics Agency. Staff members teach a variety of topics at the Defense Investigative Services' Special Agent Basic Training such as ethics, Freedom of Information Act, and subpoenas. The organization also played a role in developing suspension and debarment training for DoD law enforcement personnel.

DoD Procurement Fraud Working Group. The DoD Procurement Fraud Working Group is an ad hoc group composed of more than 30 members from various DoD organizations including; the four Defense Criminal Investigative Organizations, the three military service audit organizations, the four DoD Suspension and Debarment offices, the Defense Contract Management Agency, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Defense Contract Management Agency. In addition, representatives from the following non-DoD entities attend, Central Intelligence Agency, OIG, National Aeronautics and Space Administration, OIG, Intelligence Community OIG, Department of Justice – Criminal Division and Civil Division, and the U.S. Coast Guard. Monthly meeting focus on a wide range of procurement related topics, including proposed/new legislation, as well as emerging fraud trends. Until the

recent budgetary crisis, the Group had hosted an annual, week long fraud seminar that routinely attracted between 150 and 200 attendees that included detailed discussions of fraud and risk assessment related topics.

Missile Defense Agency, Managers' Internal Control Program. The Accounting Division oversees the Managers' Internal Control Program. A Risk/Control Assessment Template is designed to assist manager's evaluation and documentation of inherent risks and controls to mitigate the risks. The risk review also includes an assessment of fraud risks. The Missile Defense Agency contracted with an external vendor and developed online training to educate employees about risks, controls, and the Template.

Missile Defense Agency, Internal Review. Eighty percent of the auditors are Certified Fraud Examiners and hold certificates of forensic accounting. Staff holding Certified Fraud Examiner designations are required to receive annual fraud training to maintain their certifications. When Internal Review initiates an audit, team leads review Government Accountability Office, DoD OIG, and other Federal Office of Inspectors General reports to identify any fraudulent activity pertaining to the audit topic. Team leads are responsible for reviewing Missile Defense Agency Hotline inquiries and discussing case backgrounds with Internal Review senior management during audit planning. When instances of fraud or potential fraud are identified, auditors document the information in the project files. All audit programs contain specific steps to test for potential fraud.

Missile Defense Agency, Quality, Safety, and Mission Assurance. For counterfeit parts, engineers conduct risk assessments in the form of on-site reviews. Recently, 10 Missile Defense Agency contractors and 3 electronic parts distributors were evaluated for counterfeit risk. For on-site assessments of contractors, a detailed checklist is used to score the contractor's ability to avoid, detect, contain, and report counterfeit parts and train personnel. Industry best practices were used to develop the checklist categories that included procedures for supplier approval and selection. Answers to checklist questions help the Missile Defense Agency determine the risk of exposure of the agency to counterfeit parts. The Missile Defense Agency developed counterfeit parts training based upon the results of the assessments and meetings with stakeholders to identify vulnerabilities. The training includes information about the critical impact of counterfeit parts, counterfeit part types, procedures to detect and report suspect irregularities, and Missile Defense Agency and DoD requirements and expectations. .

National Geospatial Agency-Intelligence, OIG, Investigations. The Forensic Analysis Support Team completes an annual risk assessment that emphasizes the identification of fraud risks. The risk ranking approach begins with a team brainstorming session designed to generate ideas about vulnerabilities within the organization. Identified topics are ranked using the following criteria: potential dollars recovered, project completion time, and impact on fraud deterrence. Proposed projects are assigned a numeric ranking ranging from a high of five to a low of one. A weighted score is then assigned to each proposed project. The results of the fraud risk assessment are used to identify forensic audit projects for the upcoming year.

Office of the Undersecretary of Defense, Comptroller, Financial Improvement and Audit Readiness Division. The organization focuses on preparing DoD entities for financial audits of the Statement of Budgetary Resources. As part of this effort, personnel make site visits to DoD entities to educate nonfinancial employees about the importance of internal controls. Another area emphasized is ensuring that employees document internal control verifications to assist with audit preparedness.

Tricare Management Activity, Program Integrity Office. The organization is responsible for all worldwide anti-fraud activities for the Defense Health Program. About 100 contractor and government subject matter experts including healthcare, data analytics, and investigative representatives work to identify fraud schemes and trends. These proactive activities generate numerous referrals to law enforcement agencies. The organization publishes a newsletter for contractors to promote early identification of fraud schemes and minimize the loss of government dollars. Recognizing the importance of sharing information with the DoD investigative community, Program Integrity Office representatives attend and present information at task force meetings and healthcare fraud information sharing meetings. These meetings foster collaborative anti-fraud efforts across Government agencies and private organizations.

Department of the Army

Army Audit Agency. The audit organization updated the Detecting and Investigating Fraud Course to include training for auditors on conducting fraud risk assessments. The assessment methodology consists of the following steps:

- Determining relevant fraud risks within the context of audit objectives,
- Assessing the fraud risk environment,
- Identifying potential fraud schemes and methods to prioritize based on risk,
- Mapping existing controls to potential fraud schemes and testing controls, and
- Testing for fraud.

Additional training topics include approaches for working with DoD investigators and prosecutors, and fraud detection tools for auditors.

Army Criminal Investigation Command. As part of their training and education efforts, all Army Criminal Investigation Command offices conduct fraud awareness briefings. In FY 2011 and 2012 a total of 665 briefings were completed. The organization recently produced its first anti-fraud commercial, which aired on both the Pentagon Channel and the American Forces Network. For about 25 years, all 32 Army Criminal Investigations Command offices, including Germany, Korea, and Southwest Asia coordinated annual economic crime threat assessments. These assessments help each office develop approaches to target fraud and also identify high risks for specific geographic areas. Other stakeholders participating in the assessments include AAA, Army Internal Review, and Army Office of Security. Army Criminal Investigative Command Headquarters and field offices worked closely with AAA on numerous Southwest Asia anti-fraud efforts.

Department of the Navy

Inspector General of the Marine Corps. The purpose of the Risk and Opportunity Assessment is to provide the Marine Corps' input to the Navy Oversight Planning Board. The Board identifies and develops major risk categories within the Department of the Navy. The overarching risks are the susceptibility to fraud, waste, abuse, inefficiency, mismanagement, and statutory and regulatory

noncompliance. Direction for the assessment is provided by the Naval Audit Service and Naval OIG. The IG of the Marine Corps' input is based on the input of subordinate units. The organization also performs assessments of Marine Corps activities with multidisciplinary teams including representatives from the Readiness Division, IG of the Marine Corps, Counsel's Office, and Naval Audit Service.

Marine Corps Nonappropriated Funds Audit Service. The organization's auditors remain current on fraud trends through office subscriptions to ACFE, AICPA, and IIA publications. Auditors have access to software that allows them to view cashier activity and identify fraud indicators such as unusual refunds or purchases. Detailed fraud risk assessments, which include analysis of prior audit results, interviews with management, and internal control evaluations are performed during all audit engagements. Audit Directors from MCNAFAS, AAFES, and NEXCOM meet annually to discuss emerging fraud trends and significant events occurring within their organizations.

Marine Corps Risk and Compliance. The effectiveness of the Marine Corps Managers' Internal Control Program contributes to its success at audit preparedness. The Program requires resources to be used in compliance with laws and regulations, and with minimal potential for waste, fraud, and mismanagement. Effective internal controls provide reasonable assurance that significant weaknesses in the design of program processes or inherent program weakness can be prevented or detected in a timely manner.

Naval Audit Service. Approximately 10 years ago, the Auditor General, Naval Audit Service, created the Internal Control, Contracting, and Investigative Audits Division. This team was established to blend the unique skills of the Naval Audit Service and Naval Criminal Investigative Service to deter, detect, and prevent fraud within the Department of the Navy. The Naval Audit Service devotes about 20 percent of its resources to support Naval Criminal Investigative Service Investigations annually.

The fraud risk assessment approach consists of brainstorming sessions and reviews of the internal control framework. Auditors identify internal control weaknesses to determine whether controls are in place to detect or prevent fraud. When a team's brainstorming session indicates that the potential for fraud is significant, they obtain additional technical guidance from the Assistant Auditor General, Internal Control, Contracting, and Investigative Support Audits Division. Auditors and

Executive Assistants are required to complete a Fraud Risk Assessment Checklist for all audits. This checklist is designed to ensure that auditors consider fraud risks and documented the results of their work during each engagement.

Naval Criminal Investigative Service. During FY 2011 and 2012, the Naval Criminal Investigative Service provided fraud awareness briefings to more than 42,000 individuals. Within the past year and a half, the organization developed its Text a Tip program. This program enables people to submit anonymous fraud tips through text messaging. Tipsters submit information to a service provider, which then forwards the text message to a Naval Criminal Investigative Service representative. The technology enables tipsters to communicate directly with the law enforcement agency, in real time, without revealing their identities. The entity's approach to assessing fraud risk is broadly based on information received from personnel at contiguous United States and overseas locations.

Naval Sea Systems Command. NAVSEA OIG's entity-wide fraud program is based on guidance developed by the ACFE. The integrated approach consists of policies, oversight, training, and execution. The following topics are emphasized in the NAVSEA OIG anti-fraud acquisition program:

- Code of Ethics
- Fraud Prevention Policies
- Communication and Training
- Fraud Risk Assessment
- Controls Monitoring
- Fraud Response Team

Representatives from the Contract Fraud Risk Assessment and Mitigation Branch facilitate fraud risk assessments at local commands. During the meetings, contract processes, internal control weaknesses, and fraud schemes are identified through discussions with process owners. The fraud risk assessments help to educate participants about fraud risk and increase their awareness of fraud. Reports documenting the identified vulnerabilities are sent to each command.

Navy Exchange Service Command. Within the past 4 years, the Office of Internal Audit has facilitated about 30 CSAs at contiguous United States and overseas locations. CSAs help to identify fraud risks, vulnerabilities, and opportunities to improve existing controls. During the assessments, the following goals are achieved:

- identify management's objectives,
- brainstorm risks to include discussions about what could go wrong,
- map processes and controls in place to reduce risks and identify gaps,
- assess risk,
- formulate risk rankings, and
- identify potential solutions to identified vulnerabilities.

The CSA process helps in mitigating the risk of potential fraud and educates employees about the importance of internal controls.

Navy Risk Management and Compliance Branch. As required by the DoD Managers' Internal Control Program, the Risk Management and Compliance Branch facilitates a fraud risk assessment of the Navy's Statement of Budgetary Resources. Participants consist of employees from diverse disciplines with a wide range of knowledge about Navy operations. A top-down approach, consisting of both qualitative and quantitative measures, is used to identify fraud vulnerabilities. Brainstorming sessions are conducted to discuss business operations, internal control vulnerabilities, and potential fraud schemes. A risk scoring model is used to evaluate the likelihood of potential fraud and develop approaches for internal control testing. The Risk and Compliance Branch conducts about 10 fraud risk briefings annually. Fraud briefings are tailored to address each business unit's unique fraud vulnerabilities. The Department of the Navy developed the Commander's Checklist for Audit Readiness to assist with educating employees about the importance of internal controls in mitigating fraud.

Department of the Air Force

Air Force Audit Agency. Air Force Audit Agency developed a 2-hour, internet-based fraud risk assessment training course. The course is accessible on Defense Connect Online.²⁹ The course includes information for auditors about requirements for conducting and documenting fraud risk assessments. Air Force Audit Agency also provides staff fraud training to include guidance on ways to support Air Force Office of Special Investigations during an investigation.

Air Force Office of Special Investigations. Air Force Office of Special Investigations completed an entity-wide threat assessment during 2013. A second assessment will be conducted during 2014. The purpose of the assessment was to provide senior management information about vulnerabilities and risks to the organization. Areas analyzed during the review were a 5-year trend analysis of fraud cases, identification of all program offices and their related products, consideration of schemes that could potentially threaten a program, and total expenditures for each program. In the future, other DoD organizations with differing areas of expertise will be invited to participate in the threat assessment. The organization is developing an on line fraud training course, which will be a mandatory requirement for all employees. Additionally, the Air Force Office of Special Investigations has historically conducted regional economic crime threat assessments, and has developed strong partnerships with both the Air Force acquisition community and legal community. The Air Force acquisition, legal, and law enforcement components have worked together to provide fraud training for acquisition officers.

At Joint Base Elmendorf, Richardson, Alaska, the Air Force Office of Special Investigations, implemented the Fraud Installation Working Group. Participating members include law enforcement representatives, Air Force Audit Agency, Air Force OIG, attorneys, nonappropriated fund accountants, contracting officials, and representatives from AAFES and the Defense Commissary Agency. The group holds quarterly meetings to discuss emerging fraud trends at contiguous United States and overseas locations. Brainstorming sessions are conducted to generate ideas about where and how fraud could occur at the Base. Similar working groups are also active at other locations within the United States and overseas locations that include Germany and the United Kingdom. A variety of subject matter experts are recruited to serve as members at each location to assist in preventing and detecting fraud throughout the Air Force.

²⁹ Defense Connect Online is a DoD collaborative tool that includes web conferencing, video application, and desktop sharing.

External Organizations

American Institute of Certified Public Accountants. The AICPA Internal Audit and Security Directorate completes an annual fraud risk assessment. Team members meet with high-level stakeholders and discuss their perceived risks and future trends. During the meetings, auditor's questions focus on the effectiveness of internal controls and the control environment to identify potential fraud risks. Interviewees are also asked to provide information about perceived fraud risks within other components. This information is then compared to the AICPA's strategic plan to identify situations when management's goals do not align with the organization's overall business objectives.

Association of American Medical Colleges. AAMC auditors use the annual entity-wide risk assessment as a method to teach employees about fraud and increase fraud awareness. The annual risk assessment includes both quantitative and qualitative assessments of fraud risks. During the quantitative assessment, business unit representatives are asked to consider whether fraud could occur within their areas. This approach helps to stimulate discussion and get employees thinking about fraud. Participants are also required to consider impact and opportunity when rating fraud risks. The qualitative component of the risk assessment consists of an on-line Risk Assessment Survey which is sent to all risk assessment participants. Survey participants are able to respond anonymously and report suspected fraud or fraud risks. The survey tool also provides information about internal control improvement opportunities within the organization.

Council of the Inspectors General on Integrity and Efficiency Training Institute. The CIGIE Training Institute provides specialized training to a cross-section of the OIG community and auditors, inspectors, criminal and administrative investigators, Hotline operators, attorneys, and others from CIGIE affiliated agencies. Several of the Training Institute's programs contain blocks of instruction specifically dedicated to procurement fraud, its anatomy, uniqueness, risk to the Government, and detection methods. The Training Institute also provides assistance at several Federal government seminars and conferences where procurement fraud and its risk are discussed.

Grant Thornton. The Grant Thornton approach for conducting fraud risk assessments consists of specific procedures such as:

- Conducting brainstorming sessions during audit planning to discuss ways in which fraud might occur. Participants vary depending on the

audit objectives and include experts in the areas of forensic auditing, information technology, economists, and actuaries.

- Asking management, those charged with governance, internal auditors, and others within the organization for information about potential fraud and fraud risks.
- Documenting an understanding of internal controls designed to prevent or detect fraud.
- Testing to include making relevant inquiries about management override of controls.

KPMG Forensic Practice. KPMG Forensic Practice developed “Fraud Risk Management, Developing Strategies for Prevention, Detection, and Response” as a guide for conducting organization-wide fraud risk assessments. KPMG includes forensic specialists on all Federal financial statement audit engagements. During organization risk assessments, clients are asked to provide information about perceived risks by answering the question; “What keeps you up at night?” For clients that have undergone prior audits, forensic reviews are tailored to include perceived fraud risks and past audit results. To ensure productive audit fraud brainstorming sessions, partners emphasize the importance of professional skepticism and require participation from an individual with fraud experience.

Smart Insights Group, LLC. The organization’s approach to fraud prevention and detection is summarized with the acronym EATting, which stands for Education, Awareness, Testing, and Training. During fraud training, scenarios are performed live by staff and participants are asked to describe the fraud indicators they observed. An end-to-end assessment of the procurement lifecycle is used to assess the risk of fraud. When evaluating the overall impact that fraud has within an organization, the following areas are considered:

- fraud scheme classification,
- fraudster profile,
- median loss to the business, and
- duration of scheme.

State of Florida, OIG. The Chief OIG used electronic polling software to determine the effectiveness of the state’s ethics program. The Florida State OIGs and Agency managers conducted an entity-wide risk assessment to determine the auditability of state programs. During the review, OIGs were paired with agency managers, based

on their subject matter expertise, to conduct brainstorming sessions about fraud risks. The teams considered the results of the ethics poll, past fraud findings, and prior investigations during the sessions. The entity-wide risk assessment identified high-risk programs and audit topics that would improve state agency operations.

State of North Dakota, Office of the State Auditor. Fraud risk assessments are conducted about every 2 years by 80 state agencies. The fraud risk assessment program is administrated by the State of North Dakota, Office of Management and Budget, and mandatory participation by each division and/or function is required. Participants include personnel from Finance and Accounting, Human Resources Management (payroll), Purchasing and Contracting, and Information Technology. The Office of the State Auditor reviews each assessment and makes recommendations for improvements, as needed. The assessments consist of a standardized fraud risk assessment template and questionnaires designed to evaluate an agency's control environment and computer security policies and procedures.

Texas Tech University System. Auditors at Texas Tech developed an organization-wide fraud risk assessment approach called the Perception-Based Approach for Assessing Fraud Risk. Auditors act as facilitators during each fraud risk assessment session. Experienced employees and subject matter experts at each campus are invited to participate and share their perceptions about fraud risks. Auditors develop a Glossary of Fraud Schemes based on the ACFE's Fraud Examiner's Manual. During the meetings, auditors explain each scheme to participants and describe how fraud could occur at their campus. Participants use electronic polling software to anonymously rank the fraud schemes using attributes such as materiality and likelihood. The auditors report the results of the assessments to Texas Tech management. Findings from the fraud risk assessments are used to develop fraud awareness training for employees.

University System of Georgia, Board of Regents. The audit organization maintains a list of past frauds occurring at all University locations. When performing an audit in a related area, team members frequently duplicate past procedures to increase the likelihood of detecting fraud. Auditors that worked on prior fraud cases often participate in the current fraud risk assessment to promote transfer of talent among staff. Team members also consider the number and frequency of human resources complaints because they previously observed a high correlation between complaints and increased risk of fraud.

University of Georgia, Terry College of Business. The University partnered with the American Accounting Association and conducted extensive research to identify best practices for conducting auditor fraud brainstorming sessions. Studies showed that several factors enhanced the effectiveness of auditor brainstorming sessions such as whether the session was led by a partner or forensic specialist, the extent of discussions about how management might perpetrate fraud, and discussions about audit responses to fraud risk. Research revealed that the use of numeric risk rankings is more effective when compared to the frequently used risk rankings of high, medium, or low.³⁰

Yale New Haven Health System. Yale New Haven Health System outsourced its Internal Audit Function to Deloitte, LLP. The entity completes an annual entity-wide risk assessment, which includes an evaluation of fraud risk. Internal Audit also performs an annual risk assessment which includes interviews with executives to assess fraud risk. Based on the results of the interviews and identification of fraud risks, Internal Audit develops a survey. The survey is sent to all employees, and anonymous responses are permitted. Demographic queries such as department, supervisory or nonsupervisory employees, are documented to assist with analyzing responses. Follow-up interviews are then conducted, which focus on higher fraud risk areas and activities.

³⁰ American Accounting Association, "Auditors' Use of Brainstorming in the Consideration of Fraud: Reports from the Field," Joseph F. Brazel, North Carolina State University, Tina D. Carpenter, University of Georgia, J Gregory Jenkins, Virginia Polytechnic Institute and State University, 2010.

Appendix A

Scope and Methodology

This review was self-initiated. We conducted 100 interviews with subject matter experts, representing 45 organizations from the public and private sectors to identify approaches for assessing fraud risk, developing fraud awareness training programs, and obtaining information about fraud indicators and schemes. Subject matter experts included auditors, forensic auditors, investigators, attorneys, academics, and engineers. Interview question responses were evaluated to identify the most effective approaches for establishing fraud risk assessment programs and conducting fraud risk assessments for auditors. Additionally, we conducted background research to identify established approaches for both public and private sector organizations. The following organizations participated in the review:

Department of Defense

- Army and Air Force Exchange Service, Audit Division
- Defense Commissary Agency, OIG, Audit Division
- Defense Contract Management Agency, Contract Integrity Center
- Defense Contract Management Agency, Internal Review
- Defense Information Systems Agency, OIG, Audit
- Defense Information Systems Agency, OIG, Investigations
- Defense Logistics Agency, OIG, Audit Division
- Defense Logistics Agency, OIG, Investigations Division
- Defense Logistics Agency, Office of General Counsel
- DoD OIG, Office of the Deputy Inspector General for Audit
- DoD OIG, Office of the Deputy Inspector General for Policy and Oversight
- DoD OIG, Office of General Counsel
- DoD OIG, Defense Criminal Investigative Service
- Missile Defense Agency, Managers' Internal Control Program

- Missile Defense Agency, Internal Review
- Missile Defense Agency, Quality, Safety, and Mission Assurance
- National Geospatial Agency-Intelligence, OIG, Investigations
- Office of the Under Secretary of Defense, Comptroller, Financial Improvement and Audit Readiness
- Office of the Under Secretary of Defense, Acquisition, Technology, and Logistics, Defense Procurement and Acquisition Policy
- Tricare Management Activity, Program Integrity Office

Department of the Army

- Army Audit Agency
- Army Criminal Investigation Command

Department of the Navy

- Office of Inspector General Marine Corps
- Marine Corps Nonappropriated Funds Audit Service
- Marine Corps Risk and Compliance
- Naval Audit Service
- Naval Criminal Investigative Service
- Naval Sea Systems Command, Office of the Inspector General
- Navy Exchange Service Command, Office of Internal Audit
- Risk Management and Compliance Branch

Department of the Air Force

- Air Force Audit Agency
- Air Force Office of General Counsel
- Air Force Office of Special Investigations

Other Organizations

- American Institute of Certified Public Accountants
- Association of American Medical Colleges
- Council of the Inspectors General on Integrity and Efficiency, Training Institute
- Grant Thornton
- KPMG Forensic Practice
- Smart Insights Group, LLC
- State of Florida, OIG
- State of North Dakota, Office of the State Auditor
- Texas Tech University System
- University of Georgia, Board of Regents
- University of Georgia, Terry College of Business
- Yale New Haven Health System

Appendix B

Example Naval Audit Service Performance Audit Fraud Risk Policy

1. Areas Susceptible to Fraud

- a. GAGAS requires that in planning performance audits, auditors should assess risks of fraud occurring that are significant within the context of the audit objectives.
 - Audit team members should discuss, among the team, fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud.
 - Auditors should gather and assess information to identify risks of fraud that are significant within the scope of the audit objectives or that could affect the findings and conclusions. For example, auditors may obtain information through discussions with officials of the audited entity, or through other means to determine the susceptibility of the program to fraud, the status of internal controls the entity has established to detect and prevent fraud or the risk that officials of the audited entity could override internal controls. An attitude of professional skepticism in assessing these risks assists auditors in assessing which factors or risks could significantly affect the audit objectives.
 - When auditors identified factors or risks related to fraud that has occurred, or is likely to have occurred, that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud. Assessing the risk of fraud is an ongoing process throughout the audit and related not only to planning the audit but also to evaluating evidence obtained during the audit.

- When information comes to the auditors' attention that indicates that fraud significant within the context of the audit objectives may have occurred, auditors should extend the audit steps and procedures, as necessary, to determine whether fraud has likely occurred and if so, determine its effect on the audit findings. The audit managers should inform senior audit management of the potential fraud before extending their audit steps and procedures, and use their professional judgment in determining the nature and extent of additional audit steps and procedures to be performed. Each audit is unique, and any additional procedures performed should be determined on a case-by-case basis. As determined necessary, audit managers should also consider consulting with the agency Fraud Monitor for guidance.
 - If the fraud that may have occurred is not significant within the context of the audit objectives, the auditors should immediately make their chain of command aware of the potential fraud. Audit management will decide whether to address the potential fraud as part of the ongoing effort, or as a spin off audit effort by the same or another audit team. With senior audit management approval, a decision may be made to refer the matter to other parties with oversight responsibility or jurisdiction.
- b.** Auditors should never conclude that because an activity has good internal controls, it is unlikely that fraud exists. In any audited program, seemingly good internal controls can fail, (e.g., management and employees can inappropriately bypass or override internal controls, and a changing environment or collusion can cause internal controls to be ineffective in preventing fraud). Auditors need to consider in advance of site visits potential fraud schemes that could apply, and be aware of red flags that could be indicative that fraud may have occurred. Auditors must complete the Fraud Risk Matrix when performing their work.
- c.** When auditors identify factors or risks related to fraud that has occurred, or is likely to occur, that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud.

If subsequent to the completion of the fraud risk assessment, information comes to the auditors' attention that fraud may have occurred that is significant within the context of the audit objectives, auditors should extend the audit steps and procedures, as necessary, to determine whether the fraud has likely occurred, and if so, determine its effect on the audit findings.

- d. As part of the fraud risk assessment, the audit team should identify those aspects of the planned work that involve potential fraud that could significantly impact the results of the audit. The team **should prepare a work paper documenting the completion of the fraud risk assessment**, including the results of the fraud risk assessment, and the impact of fraud risks on the nature, timing, and extent of audit procedures.
- e. **Monitoring Fraud Risk Assessments.** In order to ensure documentation of compliance with GAGAS and agency standards for fraud risk assessments, Executive Assistants are required to monitor fraud risk assessments for each audit and work with auditors as needed to ensure that the audit team understands the requirements in the fraud risk assessment process.

(1) A Fraud Risk Assessment Checklist has been developed to ensure completeness and consistency for conducting fraud risk assessments. The checklist is to be completed by both the audit teams and the Executive Assistants.

- The audit team will complete the work paper reference column in order to assist Executive Assistants in their review of fraud risk assessments. Audit teams are encouraged to complete the checklist and send it to their Executive Assistant for review as early in the audit process as possible to avoid a delay in issuing the report.
- Executive Assistants will review the referenced documentation and place a checkmark in the appropriate column for each audit, verifying whether the referenced work paper documentation supports completion of the corresponding GAGAS requirement.

(2) Special Concerns for Surveys of Major Procurement and Contract Administration Functions

During the survey phase of major procurement and contract administration audits, auditors should determine the existence and consider the impact of audits issued by the Defense Contract Audit Agency. Such reports should be available at the command under review. If not, copies should be requested. Auditors should also determine during the survey phase whether any related contracts are administered by organizations other than the Department of the Navy, such as: Defense Contract Management Agency, Department of the Army, or Department of the Air Force.

Fraud Risk Assessment Checklist

Monitoring Fraud Risk Assessments

To ensure documentation of compliance with GAGAS and internal standards for fraud risk assessments, Executive Assistants, or other audit organization designees, are required to monitor the fraud risk assessment for each audit and work with auditors as needed to ensure that the audit team understands the requirements in the fraud risk assessment process. All Executive Assistants must complete the Fraud Risk Assessment Checklist for each audit and certify completion of this requirement on the Referencing Certification form. All questions are to be answered by going to source work papers (not summary work papers).

The first three items on the checklist are mandatory for every audit. The audit team should complete the Work Paper Reference column, and the reviewer must indicate "Yes" or "No" as applicable. The last two questions are applicable to the Executive Assistant only if fraud risk indicators were identified. If the team did not identify any fraud risk indicators, they should list "N/ A" in the Work Paper Reference column for those questions.

Questions that initially result in a "No" require the Project Manager to take appropriate action. If corrective action is taken by the Project Manager, the Executive Assistant should then change the "No" to "Yes." All unresolved issues must be elevated to the Assistant Auditor General.

Table B-1. Auditor Fraud Checklist

Question	Workpaper Reference	Yes	No
1. In planning the audit, did the audit team assess risks of fraud occurring that is significant within the context of the audit objectives? (GAGAS 6.30)			
2. Did the auditors document the discussion of fraud risks among the team members? (GAGAS 6.30)			
3. Did the team thoroughly document the fraud risk assessment, including audit procedures performed evidence obtained, and conclusions reached that support the auditors' conclusion on fraud risk? (GAGAS 6.79)			
4. If auditors identified factors or risks related to fraud that has occurred or likely to have occurred that they believe are significant within the context of the audit objectives, did the team design procedures to provide reasonable assurance of detecting fraud? (GAGAS 6.31)			
5. If there are indications that fraud that is significant within the context of the audit objectives may have occurred, did the auditor extend the audit steps and procedures to: (1) determine whether fraud has likely occurred, and (2) if so, determine its effect on the audit findings? (GAGAS 6.32)			

Note: Boxes Highlighted in Yellow Must be Completed

Example Draft and Final Report Cross-Referencing and Referencing Certification

Prior to release or issuance of the draft report, I completed the Fraud Risk Assessment Checklist to ensure the fraud risk assessment has been completed and that it contains documentation of compliance with GAGAS and agency policies and procedures.

Signature:

Executive Assistant, or

Other Organization Designee Signature:

Performance Audit Tool: Fraud Risk Matrix – Considering Whether Fraud is Significant to Performance Audit Objectives

The team should answer the following questions as part of their consideration of the risks due to fraud that could significantly affect their audit objectives and the results of their audit. When responding to the questions below, consider that some activities are more susceptible to fraud than others. For example, if the

audit objective focuses on the authorized use of purchase cards, fraud could be significant to the audit objectives if the program lacked adequate internal controls over the possession and use of purchase cards.

Table B-2. Auditor Fraud Risk Matrix

Consideration of Risk Due to Fraud	If “Y(es),” the risk of fraud is relevant and potentially significant to the audit objectives
1. In the team’s judgment, was the program or activity covered by the audit objectives susceptible to a significant risk of fraud from: • Misappropriation or misuse of program assets; or • Misstatement or misrepresentation of program information or results in order to obtain or continue receiving government funding or benefits?	
2. Did the team identify conditions, such as the following, that might indicate a heightened risk of fraud? • The entity’s financial stability, viability, or budget is threatened by economic, programmatic, or entity operating conditions; • The nature of the audited entity’s operations provided opportunities to engage in fraud; • Poorly designed internal controls that provide the opportunity for fraud to occur and not be identified by existing management and oversight processes; • Weak management that fails to enforce existing internal controls or provide adequate oversight over the control process; • Inadequate separation of duties, especially those that relate to controlling and safeguarding resources; • Inadequate monitoring by management for compliance with policies, laws, and regulations; • The organizational structure is unstable or unnecessarily complex; • Transactions that are out of the ordinary and are not satisfactorily explained, such as unexplained adjustments in performance or financial information; • Repeated use of sole-source contracting; • Instances when employees of the audited entity refused to take vacations or accept promotions; • Lack of communication and/or support for ethical standards by management; • Management has a willingness to accept unusually high levels of risk in making significant decisions; • A history of impropriety, such as previous issues with fraud, waste, abuse, or questionable practices, or past audits or Investigations with findings of questionable or criminal activity; • Operating policies and procedures have not been developed or are outdated; • Key documentation is lacking, altered, does not exist, or there are unexplained delays in providing information;	

Consideration of Risk Due to Fraud	If “Y(es),” the risk of fraud is relevant and potentially significant to the audit objectives
• Lack of asset accountability or safeguarding procedures; • Improper payments; • False or misleading information; • A pattern of large procurements in any budget line with remaining funds at year end, in order to “use up all of the funds available”; or • Unusual patterns and trends in contracting, procurement, acquisition, and other activities of the entity or program under audit.	
3. Had the team identified indications of potential fraud in areas that fall outside the audit objectives that could have a significant impact on program or function operations or reputation? (Use the same indicators discussed in question 2 in making this assessment.)	
4. Had the team identified strong indications that potential fraud occurred, regardless of significance to the audit objectives, that could pose a reputation risk to the Department of the Navy if exposed to the public?	

Procedures for Coordinating with Other Organizations

The audit team should determine whether the OIG for the activity being audited has identified through investigations or other means any questionable or criminal activity in the program that is significant to the audit objectives and whether there have been any Hotline or other complaints related to the audit objective. This may be accomplished through inquiry and/or a review of any applicable Hotline complaints, published investigation reports, or other written documents. The audit team should coordinate with their chain of command to determine if they have received copies of any Hotline complaints or referrals that are significant either to the audit objectives or that identify potential fraud, and are outside the potential objectives. Auditors must include a slide in the 90-day survey briefing for senior audit management that discusses the results of the fraud risk assessment.

Actions Required if There Are Indications of Fraud

If the auditors answered “Yes” to question 1, 2, 3, or 4 in Table B-2, or if the auditors identified other indications of fraud during coordination with the activity OIG, Fraud Monitor, or any other individual they should inform senior audit management. The Fraud Monitor will be available (as requested) to meet with the Project Manager and/or Audit Director to discuss any potential fraud issues.

Additional Audit Program Requirements

When the auditors identified factors or risks related to fraud that has occurred, or is likely to have occurred, that they believe are significant within the context of the audit objectives, they should design procedures to provide reasonable assurance of detecting such fraud. If subsequent to the completion of the fraud risk assessment, information comes to the auditors' attention that fraud may have occurred that is significant within the context of the audit objectives, the auditors should extend the audit steps and procedures, as necessary, to determine whether the fraud has likely occurred, and if so, determine its effect on the audit findings.

Documenting the Impact of Fraud on Audit Planning

As part of the fraud risk assessment, the audit team should identify those aspects of the planned work that involve potential fraud that could significantly impact the results of the audit. The team should prepare a work paper documenting the completion of the fraud risk assessment, including the results of the fraud risk assessment, and the impact of fraud risks on the nature, timing, and extent of audit procedures.

Appendix C

Example Naval Audit Service Fraud Risk Assessment Work Paper

Work Paper Title: Planning

Step Title: Fraud Risk Assessment

Prepared By: Auditor, Date

Reviewed By: Audit Manager, Date

Purpose: Discuss with audit team members, and the auditee, potential fraud risks, considering fraud factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud;

- Gather and assess information necessary to identify fraud risks that are within the scope of the audit objectives, or could affect the results of their audit.
- Complete the Fraud Risk Matrix and the Fraud Assessment Checklist and attach to this audit step.

Criteria: GAGAS December 2011 Revision, paragraph 6.30, states that in planning audits, auditors should consider risks due to fraud that could significantly affect their audit objectives and the results of their audit.

Source: Audit Program (Additional detail should be provided for source as deemed appropriate for conducting the fraud risk assessment.)

Audit Personnel: List engagement personnel

Scope/Methodology: The team discussed the Fraud Risk Matrix and the environment with the auditee to determine if the potential for fraud existed and to ensure that the audit objectives captured any areas of risk.

Results: After discussing considerations outlined in the Fraud Risk Matrix, the team determined that the potential risk of fraud for the auditee is significant to the audit objectives. Box 1 of the Fraud Risk Matrix states, "In the team's judgment, is the program or activity covered by the audit objectives susceptible to a

significant risk of fraud from, 1) misappropriation or misuse of program assets; or 2) misstatement or misrepresentation of program information or results in order to obtain or continue receiving government funding or benefits.” The audit team felt that the auditee was susceptible to both of these risks based on information obtained thus far. The information obtained showed that the organization received money through multiple funding streams. To date, the organization was not able to present team members with an acceptable audit trail and supporting documentation regarding how the funds were received and disbursed.

Box 2 of the Fraud Risk Matrix states, “Did the team identify conditions, such as the following, that might indicate a heightened risk of fraud?” Below are some of the main points team members discussed regarding fraud risks:

- “The nature of the audited entity’s operations provides opportunities to engage in fraud.” The audit team felt that this was a fraud risk because the organization’s mission requires employees to travel extensively. During some of the preliminary analysis, the audit team noticed that the internal controls over the travel process may be weak (missing receipts, lack of proper scrutiny, and excess expenses claimed). Therefore, we believe the extensive travel paired with the weak internal controls provide an opportunity for fraud to occur.
- “The organizational structure is unstable or unnecessarily complex.” The positions at the audited entity are constantly changing. The audit team was told by employees of the auditee that they are unsure of their position titles because the organizational structure has frequently changed. The audit team noted that some employees’ titles differ from what is listed on their position descriptions and the job functions they are performing.
- “A history of impropriety, such as previous issues with fraud, waste, abuse, or questionable practices, or past audits or investigations with findings of questionable or criminal activity.” The audit team obtained two investigations that were conducted at the organization, one completed in 2000 and the other in 2011; both of these investigations contained similar findings. The investigations mentioned the possibility of inappropriate use of funds, i.e. funds not being used for their intended purpose. The investigations also mentioned possible

abuse of travel within the organization. Although we have not proven any of the accusations detailed in the investigation at this time, we believe that the potential risk of fraud was higher, based on the results of the prior investigations.

- “Operating policies and procedures have not been developed or are outdated.” The audit team reviewed the hiring practices of the organization. The review disclosed that the auditee was lacking policies or procedures related to hiring new employees. As a result, we feel that the lack of official guidance provides opportunities to circumvent Federal hiring laws and regulations.
- “Improper Payments.” The audit team has documented several instances of excessive mileage claimed on traveler’s vouchers. The excess mileage was sometimes double what it should have been, resulting in over payments to the travelers. The audit team also encountered questionable items on traveler’s vouchers that did not contain receipts or supporting documentation, i.e. cancelled airfare claimed on a voucher.
- “False or misleading information.” The audit team interviewed the Travel Manager and were told that there are no Self-Approving Officials. Upon further investigation, the team identified one traveler (the Travel Manager) listed in DTS as a Self-Approving Official.
- Box 3 of the Fraud Risk Matrix stated, “Has the team identify indications of potential fraud in areas that fall outside the audit objectives that could have a significant impact on program or function operations or reputation?” The audit team answered no to this question. However, we identified high-risk areas that fall outside the audit objectives that could have a significant impact on the program, function, operations, and reputation. Our opinion is based on a procurement audit that is currently being performed by another Federal audit organization (in response to the 2011 investigation). Additionally, the auditee employs a large number of contractors, in comparison to the number of Government employees. This situation could potentially lead to contractors performing inherently governmental tasks.

Fraud – Results:

Box 4 of the Fraud Risk Matrix stated, “Has the team identify strong indications that potential fraud actually occurred, regardless of significance to the audit objectives, that could pose a reputation risk to the Department of the Navy if exposed to the public?” The audit team answered yes to this question based on our analysis of travel vouchers. We observed excess mileage claims, missing receipts for airfare and lodging, and one voucher that claimed reimbursement for a cancelled airfare ticket.

The Fraud Risk Matrix includes a requirement for auditors to coordinate with their chain of command to determine if there were any Hotline complaints or referrals that are significant either to the audit objectives or that identify potential fraud that were outside the objectives. The Fraud Risk Matrix stated that the Fraud Risk Monitor would be available (as requested) to meet with audit management to discuss any potential fraud issues. Based on the audit team’s assessment of the Fraud Risk Matrix, we determined that a meeting should be requested with the Fraud Monitor.

The team also completed the fraud assessment checklist and referenced the applicable work papers.

Conclusion:

The audit team developed audit objectives to detect fraud and reduce fraud risk based on the results of the Fraud Risk Matrix.

Appendix D

Example DoD OIG, Fraud Interview Questionnaire – Financial Statement Audit

AICPA, Statement on Auditing Standards 99, Consideration of Fraud in a Financial Statement Audit Interview Questionnaire
Interviewee:
Interviewee Title:
External Audit Organization Interviewers:
OIG representative(s):
Date of interview:

I. Business Risks Faced

1. Without regard to fraud and abuse, what are the key business risks that you face in carrying out your office's responsibilities?
2. Did these business risks affect other offices outside your span of control?
3. What have you done to address these business risks as it relates to instituting/strengthening internal controls and revising processes?

II. Fraud Awareness

1. How long have you been in this position?
2. How long have you been with the organization?
3. Do you have any knowledge of any fraud that has been perpetrated, or any alleged or suspected fraud perpetrated against the organization?
4. Do you have any knowledge of allegations or actual fraudulent reporting, that is to say, knowledge that raw data or reports are being or have been manipulated to present reported results which differ from the actual results?
5. Do you have any knowledge of misstated balances that were knowingly reported at the end of a period, hoping that those balances would correct themselves in the subsequent reporting period?

6. Do you have any knowledge of allegations or actual misappropriation of assets by individuals at the organization, or knowledge of individuals inappropriately incurring obligations for which the entity will be responsible for settling?
7. Do you have any knowledge of anyone within the organization's management team overriding or subverting internal controls, or concerns of any potential opportunities for such overrides to be perpetrated?
8. Are you aware of any pressures or incentives at any level of management that might contribute to fraudulent activities?
9. Are your annual performance ratings tied to any benchmarks for financial performance and/or reporting metrics?
10. Do you perceive the risks of fraud to exist within your office, and what controls did you rely upon to mitigate the risks of fraud?
11. Do you feel that agency management was honest and forthright, and do you feel comfortable approaching management if you had any issues or concerns?
12. Do you feel that agency management and staff receive the proper training and supervision to perform their duties?
13. If you were to become aware of, or suspect, an act of fraud or other illegal activity, what steps would you take to address it, and who would you notify?
14. Are you aware of any additional offices for which a risk of fraud may be more likely to exist than others, or are of specific concern to you? .
15. Do you believe that there are any members of internal or external senior management who are unfit to perform their assigned duties, or should not hold a position of authority?

III. Conclusion

Given what we have discussed today, is there anything else that you would like to bring to our attention?

Appendix E

Example IIA, AICPA, ACFE, Fraud Risk Assessment Framework

Table E is for illustrative purposes and focuses solely on potential revenue recognition risks within financial reporting.³¹ A full fraud risk assessment would consider fraudulent financial reporting in other areas relevant to the organization, such as accounts subject to estimation, related-party transactions, and inventory accounting. In addition, the risk of misappropriation of assets, corruption, and other misconduct would be assessed in the same manner.

Table E. Example Financial Reporting Fraud Risk Assessment

Identified Fraud Risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing Anti-fraud Controls (5)	Controls Effectiveness Assessment (6)	Residual Risks (7)	Fraud Risk Response (8)
Financial Reporting Revenue recognition Backdating agreements	Reasonably possible	Material	Sales personnel	Controlled contract administration system	Tested by IA	N/A	Periodic testing by IA
Holding books open	Reasonably possible	Material	Accounting	1. Standard monthly close process 2. Reconciliation of invoice register to general ledger 3. Established procedures for shipping, invoicing, and revenue recognition 4. Established process for consolidation	1. Tested by IA 2. Tested by management 3. Tested by IA 4. Tested by IA	Risk of management override	Testing of late journal entries Cut off testing by IA

³¹ IIA, AICPA, ACFE, "Managing the Business Risk of Fraud: A Practical Guide," not dated.

Identified Fraud Risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing Anti-fraud Controls (5)	Controls Effectiveness Assessment (6)	Residual Risks (7)	Fraud Risk Response (8)
Late shipments	Reasonably possible	Significant	Shipping dept.	1. Integrated shipping system, linked to invoicing and sales register 2. Daily reconciliation of shipping log to invoice register 3. Required management approval of manual invoices	1. Test by IA 2. Tested by management 3. Tested by IA	Risk of management override	Cut off testing by IA
Side letters/ agreements	Probable	Material	Sales personnel	1. Annual training of sales and finance personnel on revenue recognition practices 2. Quarterly signed attestation of sales personnel concerning extra contractual agreements 3. Internal audit confirming with customers that there are no other agreements, written or oral, that would modify the terms of the written agreement	1. Tested by management 2. Tested by management	Risk of override	Disaggregated analysis of sales, sales returns, and adjustments by salesperson
Inappropriate journal entries	Reasonably possible	Material	Accounting & Finance	1. Established process for consolidation 2. Established, systematic access controls to the general ledger 3. Standard monthly and quarterly journal entry log maintained. Review process in place for standard entries, and nonstandard entries subject to two levels of review	1. Tested by IA 2. Tested by IA 3. Tested by management	1. Risk of override 2. N/A 3. N/A	Data mining of journal entry population by IA for: • Unusual Debit/Credit combinations • Late entries to accounts subject to estimation
Roundtrip transactions	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
Manipulation of bill and hold arrangements	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A

Identified Fraud Risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing Anti-fraud Controls (5)	Controls Effectiveness Assessment (6)	Residual Risks (7)	Fraud Risk Response (8)
Early delivery of product	Reasonably possible	Significant	Sales and shipping	Systematic matching of sales order to shipping documentation; exception reports generated	Tested by management	Adequately mitigated by control	N/A
Partial shipments	Reasonably possible	Significant	Sales and Shipping	1. Systematic shipping documents manually checked against every shipment. 2. Systematic matching of sales order to shipping documentation; exception reports generated. 3. Customer approval of partial shipment required prior to revenue recognition	Tested by management	Adequately mitigated by control	N/A
Additional revenue risks				Systematic shipping documents manually checked against every shipment			

- (1) **Identified Fraud Risks and Schemes:** This column should include a full list of the potential fraud risks and schemes that may face the organization. This list will be different for different organizations and should be based on industry research, interviews of employees and other stakeholders, brainstorming sessions, and activity on the whistleblower hotline.
- (2) **Likelihood of Occurrence:** To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the organization establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.
- (3) **Significance to the Organization:** Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to an organization. For example, certain fraud risks may only pose an immaterial direct financial risk to the organization, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the organization. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.

- (4) **People and/or Department Subject to the Risk:** As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the organization are subject to the risk. This knowledge will assist the organization in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.
- (5) **Existing Anti-fraud Internal Controls:** Map pre-existing controls to the relevant fraud risks identified. This activity occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the organization to assess identified fraud risks on an inherent basis, without consideration of internal controls.
- (6) **Assessment of Internal Controls Effectiveness:** The organization should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks. Companies subject to the provisions of The U.S. Sarbanes-Oxley Act of 2002 Section 404, will have a process such as this in place. Organizations not subject to Sarbanes-Oxley should consider what review and monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.
- (7) **Residual Risks:** After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including properly designed controls are not in place to address certain fraud risks or controls identified are not operating effectively. These residual risks should be evaluated by the organization during the development of the fraud risk response.
- (8) **Fraud Risk Response:** Residual risks should be evaluated by the organization and fraud risk responses should be designed to address remaining risk. The fraud risk response could be one. or a combination of implementing additional controls, designing proactive fraud auditing techniques, and/or reducing the risk by exiting the activity.

Appendix F

Example Smart Insights Group, LLC, Internal Control Evaluation Questionnaire

Question Title	Description	Points	Score	Comments/Notes
Oversight	To what extent has the overall agency established a process and resources responsible for the identification and oversight of fraud risks?	0-20	20	DoD Instruction, XYZ, directed all business units to establish safeguards to prevent, detect, and report fraud at all Medical Treatment Facilities.
Ownership	To what extent has the agency created ownership of fraud risks by assigning a member of its senior management team with responsibility for: 1. Managing fraud risks within the organization; and 2. Communicating to agency personnel about the topic of fraud and their responsibilities for reporting incidents?	0-20	20	All senior officers were required to develop and maintain effective internal controls across their areas of responsibility. Each senior officer was required to document their anti-fraud efforts to include: • Designation of an Anti-Fraud Program Manager. • A high level statement outlining the responsibility of all personnel to monitor against fraud and prevent fraud. • The process for monitoring, reporting, and investigating fraud, with clearly defined roles and responsibilities. • Appropriate anti-fraud training. • Process to promote fraud awareness among staff and outside parties (including vendors, patients, etc.). • Identification of available remedial actions when fraud occurs (e.g., criminal, civil, and administrative penalties.) • Regular and active involvement of senior leadership on fraud issues and corrective actions.

Question Title	Description	Points	Score	Comments/Notes
Assessment	To what extent has the agency implemented an ongoing process to identify and evaluate changing fraud risks?	0-20	20	Periodically, but at a minimum, annually, each business unit must assess and document fraud risks. The assessment must address the following topics: • Overall incentives, opportunities, and pressures to commit fraud. • Programs where ineffective or nonexistent internal controls create opportunities for fraud. • Likelihood and impact of fraud within those programs. • A final report, summarizing the assessment results and planned corrective actions, must be sent to senior leadership prior to December 31. Information for the assessment can come from: • OIG Inspections and Hotline reports. • Managers' Internal Control Program and other internal reviews. • External audits, reports, and studies. • Management observations and judgment.
Risk Management Policy	To what extent has the agency implemented a fraud policy? The policy should identify the individual/team, within the agency, that will be responsible for managing fraud risks, and the associated activities to be undertaken to manage the fraud risks.	0-30	30	DoD Instruction, XYZ, established the organization's fraud policy. This policy outlined the responsibilities of employees regarding the organization's fraud program to include military and civilian personnel. Anti-Fraud Program Manager, General Counsel, Comptrollers, Contracting Officers.
Anti-Fraud Controls	To what extent has the agency implemented process level controls and/or activities that are designed to prevent, deter and/or detect the fraud risks identified through the agencies risk assessment?	0-20	10	The organization identified preventive and detective controls as part of the annual fraud risk assessment. However, the organization would benefit by implementing additional detective controls.
Process Re-engineering	To what extent has the agency implemented measures to eliminate or reduce, through process re-engineering, the fraud risks identified through the agencies risk assessment?	0-20	0	The organization did not consider process re-engineering as an approach to address fraud risks.

Question Title	Description	Points	Score	Comments/Notes
Workplace Culture	Preventing major frauds requires a strong emphasis on creating a workplace environment that promotes ethical behavior, deters wrongdoing, and encourages all employees to communicate any known or suspected wrongdoing to the appropriate person. To what extent has the organization implemented a process to promote ethical behavior, deter wrongdoing and facilitate two-way communication on ethical issues?			
	Is there an identified Senior Member of the management team that has been singularly tasked with the responsibility for ensuring the agency's processes promote ethical behavior, deter wrongdoing and report matters of misconduct in a timely manner (i.e., a designated Ethics Officer)?	0-10	5	Yes, the organization is required to have an Anti-Fraud Program Manager. However, because of the size of the program and increased fraud risks, the duties should be shared with another employee.
	A code of conduct for employees, which gives clear guidance as to what behavior is permitted/prohibited. The code of conduct should identify how employees: 1. Seek additional advice when faced with uncertain ethical dilemma; 2. Communicate concerns about known or potential wrongdoing.	0-10	10	The organization does have a code of conduct and also requires annual ethics training. Information about communicating potential wrongdoing is documented in DoD Instruction, XYZ.
	Regular fraud training is available for all new hires as well as all on-board FTEs and contractors.	0-10	3	Annual fraud training is required for all employees, to including contracting officers. However, current training has not been updated within the past five years and contractors are not required to participate in the training.
	Multiple communication methods are available to employees, contractors, and vendors to seek advice prior to making difficult ethical decisions and to express concern about known potential wrongdoing. - Agency communication methods should include an ethics/compliance hotline or e-mail address that is actively monitored by ethics or compliance personnel. - Provision should be made to enable communications to be made anonymously. - Emphasis should also be placed upon the Whistleblower provisions, which are intended to protect individuals from retribution.	0-10	4	The organization maintained fully staffed and experienced Hotline personnel at various contiguous United States locations. Anonymous reporting is allowed. Awareness of Whistleblower protections could be improved when the annual fraud training is updated.

Question Title	Description	Points	Score	Comments/Notes
Workplace Culture (cont'd)	Monitoring of compliance with the code of conduct and participation in required training (i.e. requiring an annual employee attestation of understanding, compliance and completion of training and auditing of such attestations to confirm their completeness and accuracy)	0-10	4	The organization has yet to implement a process that ensures that all employees completed annual fraud training. The current process requires a self-certification without documentation (i.e. Certificate of Training, etc.)
Proactive Detection Methods	To what extent has the agency established a process to proactively detect incidents of potential fraud • Develop and perform fraud detection tests? • Implement embedded transaction 'flags' (manual or automated) to target suspicious transactions or activity.	0-20	10	The organization performs manual fraud detection tests quarterly. However, there are no automated transaction flags to detect suspicious transactions or activities.

Excerpts from Department of the Navy Bureau of Medicine and Surgery Instruction 5370.4, April 1, 2010

From: Chief, Bureau of Medicine and Surgery

Subject: NAVY MEDICINE ANTI-FRAUD PROGRAM

1. **Purpose.** To direct Navy Medicine commands to establish safeguards to prevent, detect, and report fraud. This instruction documents existing anti-fraud efforts and initiates new and enhanced efforts to implement fraud programs at Navy Medicine Medical Treatment Facilities.
2. **Applicability.** Applies to all Navy Medicine commands.
3. **Background.**
 - a. Fraud is any willful means of taking or attempting to take unfair advantage of the government, including but not limited to:
 - (1) The offer, payment, or acceptance of bribes or gratuities.
 - (2) Making of false statements, submission of false claims, or use of false weights or measures.
 - (3) Evasion or corruption of inspectors and other officials.

- (4) Deceit by suppression of the truth or misrepresentation of a material fact.
 - (5) Adulteration or substitution of material.
 - (6) Falsification of records or accounts.
 - (7) Arrangements for secret profits, kickbacks, or commissions.
 - (8) Cases of conflict of interest, criminal irregularities, and unauthorized disclosure of official information connected with acquisition and disposal matters.
 - (9) Conspiracy to use any of these devices.
 - b. Navy Medicine is susceptible to fraud committed by government personnel (civilian and military), contractors, vendors, patients, or other outside parties.
4. **Policy.** Fraud directly threatens our core mission of providing high-quality, economical health care to eligible beneficiaries. As such, all personnel within Navy Medicine must maintain constant vigilance to identify and report suspected fraud. Commanders, commanding officers, and officers in charge must establish a tone across their area of responsibility that fraud, regardless of magnitude, will not be tolerated. Accordingly, each command in Navy Medicine must develop an anti-fraud program that includes the following elements:
- a. **Fraud Risk Management Program.** Each command must formally document its anti-fraud assets and efforts, including
 - (1) A high-level command statement outlining the responsibility of all personnel to monitor against and prevent fraud (e.g., code of conduct, command policy, commander's note).
 - (2) The process for monitoring, reporting, and investigating fraud, with clearly defined roles and responsibilities.
 - (3) An anti-fraud program manager, appointed by the commander.

- (4) Appropriate anti-fraud training.
- (5) Processes to promote fraud awareness among staff and outside parties (including vendors, patients, etc.).
- (6) Identification of available remedial actions when fraud occurs (e.g., criminal, civil and administrative penalties).
- (7) Regular and active involvement of command senior leadership, including the Executive Steering Committee on fraud issues and corrective actions.

b. **Periodic Fraud Risk Assessment.** A command's mission, size, complexity, organizational structure, and resources help determine its vulnerability to fraud. These factors differ at each command and vary over time. Periodically, but at least annually, each Navy Medicine command must assess and document its own fraud risk. Assessing fraud risk allows commands to focus internal control efforts where the likelihood and/or impact of fraud is greatest. Since prevention of fraud is one of the key objectives of internal controls, the fraud risk assessment should be a subset of a comprehensive internal control risk assessment.

(1) **Information for this assessment can come from:**

- (a) OIG inspections and Hotline reports.
- (b) Managers' Internal Control Program assessments.
- (c) Command Evaluation Program and other internal reviews.
- (d) External audits, reports, and studies.
- (e) Commanders and/or management observations and judgment.

(2) **The assessment should identify the:**

- (a) Overall incentives, opportunities, and pressures to commit fraud.
 - (b) Programs where ineffective or nonexistent internal controls create opportunities for fraud.
 - (c) Likelihood and impact of fraud within those programs.
- c. **Prevention Techniques.** An effective system of internal controls is the best means to prevent fraud. Although fraud of any magnitude negatively impacts mission accomplishment, each command must determine an acceptable level of risk and develop internal controls accordingly. Preventative controls must be focused on areas where the likelihood and/or impact of fraud are the highest. Preventative controls can include policies, procedures, training, and communication.
- d. **Detection Techniques.** For certain types of fraud, it is more effective to detect and address fraud after it occurs rather than trying to prevent it before it occurs. Detective controls are most effective for areas where the likelihood of fraud is low but potential impact is severe. They can also help assess the effectiveness of preventative controls. Detective controls are often clandestine in nature, to ensure they are not easily circumvented.
 - (1) Examples of detective controls include:
 - (a) Unannounced inventory inspections.
 - (b) Reconciling accounting transactions with supporting documentation at random intervals.
 - (c) Ad hoc audits and analyses.
 - (d) Data mining.
 - (e) Automated system flags (e.g., disbursements over a certain dollar amount, excessive number of purchase card transactions to a single vendor).

- (2) Potential fraud may also be detected during the course of internal reviews (including the command evaluation program) and external audits (e.g., OIG inspections, Naval Audit Service audits).

e. Reporting, Investigative, and Corrective Action Process

- (1) Navy Medicine personnel will report all suspected fraud for further analysis and investigation. If there is any doubt on whether or not something constitutes fraud, the incident should be reported.

5. Responsibilities

a. Commanders will:

- (1) Formally establish and document a culture across their area of responsibility that fosters constant vigilance against fraud, protects those who report fraud, and demands appropriate corrective action when fraud occurs.
- (2) Implement a system of effective internal controls to detect and prevent fraud across the programs with the highest level of risk.
- (3) Ensure full cooperation with all fraud Investigations.
- (4) Develop a comprehensive remedies plan, with appropriate corrective and disciplinary action, for all substantive fraud cases within their area of responsibility.
- (5) Review substantive cases of fraud for systemic internal control deficiencies and report, as appropriate, in the annual Managers' Internal Control Program, Statement of Assurance.
- (6) Appoint an Anti-Fraud Program Manager, from within the command's OIG staff, to advise the command on anti-fraud matters.
- (7) Ensure personnel complete mandatory annual anti-fraud training.
- (8) Ensure full compliance with this instruction within their area of responsibility.

- b. **All Navy Medicine Personnel (military and civilian) will:**
 - (1) Exercise due diligence in monitoring for fraud.
 - (2) Report suspected fraud per this instruction.
 - (3) Complete mandatory annual anti-fraud training.
- c. **The Anti-Fraud Program Manager will:**
 - (1) Serve as senior advisor to management on fraud issues.
 - (2) Develop and implement initiatives to promote awareness across the AOR of means to detect, prevent, and report fraud.
 - (3) Provide periodic updates to the Executive Steering Committee (or equivalent) on fraud issues within the area of responsibility.
 - (4) Provide anti-fraud course content requirements for inclusion in the contracting office representative training course.
 - (5) Develop anti-fraud training for all Navy Medicine personnel. Anti-fraud training should include, at a minimum:
 - (a) Legal definition of fraud.
 - (b) Areas of greatest fraud vulnerability within Navy Medicine.
 - (c) Responsibility of all personnel to monitor for and report suspected fraud.
 - (d) Signs of fraud.
 - (e) Ways to detect and prevent fraud.
 - (f) Ways to report suspected fraud.
 - (g) Potential criminal, civil, and administrative consequences of fraud.

Appendix G

Example Grant Thornton Client Report and Heat Map

Confidential

Date

Client Name

Re: Fraud Risk Assessment Preliminary Report

Dear (Auditee Name),

At your request, we have performed certain procedures under your direction to assess fraud risk. This report concludes Phase I of our work as described in our engagement letter dated XX. On (date) we visited the organization to interview select personnel and gather documentation. We describe below the procedures performed, our findings, and recommendations for additional steps.

Procedures Performed

This engagement was designed to include the following four distinct phases:

- I. Overall risk assessment/project organization
- II. Assess existing compliance systems, practices and procedures
- III. Develop findings and recommendations
- IV. Prepare report with recommendations

In this phase, Phase I, we performed an overall assessment of your current anti-fraud and governance policies and procedures. The objective of this phase was to obtain enough of an understanding of the control structure and potential risks at the organization to allow us to finalize the scope for the remainder of the project.

The primary procedures performed during the risk assessment included:

1. Review of the current code of conduct and anti-fraud policies and procedures.

2. Review of relevant background information including prior internal audit reports, employee handbooks, and various policies and procedures.
3. Interviews with select personnel, including:
 - i. Controller
 - ii. Business Administrator
 - iii. Human Resources Manager
 - iv. Information Technology Manager
4. Identified high-risk areas.

Findings and Observations

Based on the procedures listed above, as well as discussions with personnel, we identified the following observations and recommendations:

1. Department X currently does not have formal anti-fraud policies and procedures. The organization should document and implement fraud specific policies and procedures that describe fraudulent conduct, punishment for engaging in fraudulent conduct, and procedures to report the fraudulent conduct. These policies should be disseminated to all employees through e-mail communications, training programs, or other intercompany communication methods.
2. Organization policies state that complaints can be made anonymously, but it does not provide instructions on how to make an anonymous complaint. A “hotline” does not exist. Clarifying the policy and implementing an anonymous whistleblower hotline would provide a channel for employees to anonymously voice concerns regarding irregularities in the company’s accounting methods, internal controls, or auditing matters, without fear of repercussions from individuals within the organization.
3. Controls over the set up and maintenance of vendors are lacking. Vendors are added on an ad hoc basis without conducting background checks, or vendor due diligence. Implementing a vendor approval process, including using background checks and vendor due diligence to screen vendors will reduce the risk that unauthorized vendors are added to

the system. In addition, to prevent the appearance of favoritism or conflict of interest, vendors should be periodically rotated, where it makes business sense.

4. Department X should establish a standard vendor contract that includes a right to audit clause. Large vendors that transact frequently with the Department X should be required to execute the standard vendor contract.
5. Department X does not monitor external employment of its employees. Based on our discussions, we learned that some employees may have additional external employment. To preclude potential conflicts of interest, Department X should require employees to complete a disclosure document that includes external employment and business ownership. This document should be reviewed to identify potential conflicts of interest and the information should be kept in a log by Human Resources.
6. During the course of our interviews, we were informed that several managers and officers were not completely familiar with the contents of the employee handbook. To effectively manage and monitor employee performance, managers and officers should be aware of the standards that apply to employees.
7. The organization does not have a formal training program. It is recommended that the organization implement formal training for all employees. Areas that should be addressed include: new hire training, periodic training for managers and officers on the employee handbook, and specific training covering ethics and anti-fraud policies of the entity. Employees should be required to sign a document acknowledging participation in such training. This helps create awareness and responsibility throughout the organization.
8. Employees are not required to take vacations. It would be advisable to implement a mechanism to monitor vacation balances of key employees and encourage employees who have accrued maximum allowed vacation days to take vacations. Many internal frauds require manual intervention, and are, therefore, discovered when the perpetrator is absent from their duties for a period of time. The enforcement of mandatory vacations can reduce the risk that frauds are not detected.

9. During the course of our interviews, we inquired about previous instances of fraud. Three of the interviewees stated that they could recall only one instance of fraud. Each cited an incident that was different from that cited by the other interviewees. As such, we were made aware of three separate incidents of fraud that had occurred over the last three to five years. We also learned that a consolidated fraud incident list is not maintained. Maintaining a list of fraud incidents can serve as an educational tool to increase awareness and improve controls within the organization.
10. Department X receives checks and cash by mail. Mail is sorted and employees believed by mail room personnel to contain checks and/or cash are delivered to the finance department. This mail sorting function is not supervised. A surveillance camera to monitor activity in the mailroom can reduce the risk of theft of funds received by mail. Rotating personnel performing the mail sorting function could limit the risk of checks or cash being intercepted prior to delivery to the finance department.
11. We were informed that employees perceived differences in perquisites between officers and non-officer employees. For example, an officer may be permitted to bring a child into the office during the work day, while this is prohibited for non-officer employees. The differences perceived by employees could negatively impact employee morale.
12. The controller is the lone approver for user rights within the accounting software. This would potentially allow the controller to request a change to his rights to circumvent current controls within the finance function. At a minimum, the Business Administrator should review and approve requests for changes to the controller's access rights. This would allow the controller to continue to review and approve changes to the accounting staff's rights.
13. Computers do not automatically lock users out after a period of inactivity and screensavers are not password protected. This would allow a passerby to access an individual's computer and potentially access sensitive information or circumvent internal controls within the finance function.
14. Currently, the system allows multiple simultaneous log-ins using the same user identification and password. The organization should implement a procedure that would prohibit use of a user identification to log in simultaneously on multiple computers.

15. Computers are not currently encrypted. It was mentioned during our interviews, that the organization would be implementing encryption on the computers within Finance, Human Resources, and Information Technology Management. However, as it currently stands, the lack of encryption potentially exposes sensitive organizational data if the computers were stolen.
16. Although the capability exists to monitor failed access attempts, the Information Technology Department does not currently monitor the log. Periodic monitoring would help to detect hackers attempting to gain access to sensitive data.

Proposed Phase II Tasks

As indicated in our proposal, we have used results and findings of the Phase I assessment as the basis to design Phase II of the project. We have identified areas where we believe it would be beneficial to conduct additional procedures. We propose performing the following more detailed procedures:

1. *Vendor and payment procedures.* Grant Thornton can perform an in-depth analysis of vendors and payments including:
 - a. Analysis of vendor maintenance procedures.
 - b. Vendor master file and employee master file matching,
 - c. Vendor master file analysis (same/similar addresses, PO Boxes, no addresses).
 - d. Vendor usage by department.
 - e. Vendor usage by type of expense.
 - f. Above average payments to a vendor.
 - g. Above average voided vouchers per vendor.
 - h. Duplicate payment testing.
 - i. Accounts payable credits and voided voucher matching.
 - j. Vendor selection approval and bid review process.

2. *Cash and check receipting procedures.* Grant Thornton can perform a thorough walk-through of the cash and check receipting procedures to determine proper controls surrounding the process from the moment a check/cash enters the facility to its deposit in the bank and recording of the receipt in the accounting books. This review will also include testing controls around petty cash, wire transfers and payroll.
3. *Vacation activity.* Grant Thornton can conduct a historical review of vacation activity of key employees to determine if any employees have not taken vacation days.
4. *Policies and procedures.* Grant Thornton can perform tests in certain areas to ascertain whether practice conforms to written policies and procedures. Examples of areas we could examine include:
 - a. Investment monitoring – perform a basic review of the investment policy to verify management of investment accounts conform to stated investment policy. We understand the last in-depth external analysis of investment policy compliance was performed in 2007.
 - b. Hiring/termination of employees – verify that Human Resources conducts background checks prior to making an offer of employment to new hires. Verify that Human Resources follows the steps outlined in the terminations/resignations policies and procedures.
 - c. Information Technology – verify compliance with policies and procedures providing access to key systems and programs by testing selected authorization documentation. Key systems and programs would include: (Insert Names).
 - d. Finance and accounting – verify that proper invoice approval is obtained from department heads prior to payment.

Restrictions of this Report

This preliminary report is prepared solely for the internal use of the organization. Our services were provided in accordance with the statement of standards for consulting services promulgated by the AICPA and, accordingly, did not constitute a rendering by Grant Thornton LLP or its partners or staff of any legal advice, nor do they include the compilation, review, or audit of financial statements. Grant Thornton makes no representations regarding questions of legal sufficiency. We performed the procedures within the agreed upon scope. Had we performed other procedures, we may have identified other information that would have been included in this report. If additional information that may change our findings is found, we reserve the right to supplement this report accordingly.

We appreciate the opportunity to serve you in this matter. If we could assist you by explaining our work in more detail, please do not hesitate to contact us.

Sincerely,

Name/Title

TABLE G. Example Grant Thornton Client Heat Map

Entity/ Unit/ Region	Structure Risk Factors						Alignment to Headquarters Factors					Audit					Total Risk Score
	"Local Accounting System Fully Integrated"	Accounting Function Co-Located within geography	Revenue and Balance Sheet Balances Typically Above Materiality	Local Operations Solely a Support Function	% of Revenue Generated by Third Party Business Development in FY 2011 – Three Quarters	Structure Score	Prior Investigation Conducted	Number of Ethics Line Reports for FY	Years of Service – Finance Manager	Years of Service – Country Manager	Fraud & Corruption Score	Fiscal Year of Last External Audit Visit	Entity Below Scoping Threshold for External Audit (20%)	Fiscal Year of Last Internal Audit Visit	Entity Below Scoping Threshold for Internal Audit (10%)	Audit Structure Score	
[Insert Relevant Entity]	Yes	Yes	Yes	No	4%	3	Yes	3	2.33	2.25	-2	2011	No	2011	No	4	1.7
[Insert Relevant Entity]	Yes	Yes	Yes	No	0%	3	No	0	9.58	0	2	2011	Yes	2011	Yes	0	1.7
[Insert Relevant Entity]	Yes	Yes	Yes	No	4%	3	No	0	3	1.5	2	2010	Yes	2010	Yes	0	1.7
[Insert Relevant Entity]	Yes	Yes	Yes	No	2%	3	Yes	0	6.25	1.42	0	2011	Yes	2011	Yes	0	1.0
[Insert Relevant Entity]	Yes	Yes	Yes	No	0%	3	No	0	1.42	1.25	2	2009	Yes	2009	Yes	0	1.7

The following weights were used to develop the Heat Map's weights: Structure Risk Factors 33%, Alignment to Headquarters Factors 33%, Audit 33%.

Appendix H

Example NAVSEA, Office of the Inspector General, Contract Fraud Risk Assessment and Mitigation Branch, Organization Fraud Risk Assessment Report

Risk Area

Contract Fraud Risk Assessment

Prepared by

Contract Fraud Risk Mitigation (C-FRAM) Team

Risk Concern

Command's (CMD's) efforts to mitigate the risk of contract fraud, waste, abuse, and mismanagement.

Methodology

Our objective is to assess the CMD's tone from the top, internal controls, and ongoing monitoring efforts related to mitigating the risk of contract fraud, waste, abuse, and mismanagement. At the CMD, the C-FRAM Team met with CMD Contract Department leadership and discussed management's tone from the top regarding fraud, waste and abuse. The C-FRAM team also conducted a COR focus group and randomly selected 2, out of 13, CORs for further interviews. The team interviewed these CORs and examined their COR files to assess the methods the CORs used to detect and deter fraud, waste, abuse, and mismanagement. The team also conducted a focus group with the contracting officers. Our findings are described in detail below.

Tone from the Top

A positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Several key factors affect the control environment. One factor is the integrity and ethical values maintained and demonstrated by management and staff. Agency management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's

ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate.³²

During the COR focus groups and follow-up interviews the team inquired whether the CORs were familiar with the CMD's code of ethics. The CORs stated that they all took the annual ethics training in the Total Workforce Management System (TWMS). The CORs also stated that they received quality support from the command counsel. The CORs also stated that the CMD's code of ethics was not discussed on a regular and recurring basis and most could not remember the last time the Commanding Officer expressed his opinion on the subject. The CORs also stated they discussed some questionable ethical situations with their department heads. The Commanding Officer acknowledged that in a command of roughly 11,000 people, reaching the staff a challenge.

NAVSEA Instruction (NAVSEAINST) 4200.17E, "Contracting Officer's Representative," May 13, 2013, pg. 9, para b (2) states "The COR Supervisor is required to provide oversight and monitor the performance of the CORs duties and responsibilities as well as seek performance feedback from the respective contracting officers. The COR supervisors shall ensure that adequate time and resources are available for performance of the COR responsibilities. The COR supervisor MUST establish a performance objective for the employee reflecting the COR's assigned duties. The COR Supervisor shall include a separate critical performance element, either on single contract or multiple contracts, reflecting COR duties assigned."

During the COR focus group, several focus group members stated they were overwhelmed and rarely had time to complete their COR responsibilities. The C-FRAM Team requested copies of each CORs' performance objectives. Of the three performance objectives reviewed, none had a separate performance element reflecting COR duties assigned. Failing to ensure COR performance plans include a separate critical element describing COR responsibilities, increases the risk that this important oversight function will be undervalued and underperformed, and violates NAVSEAINST 4200.17E, "Contracting Officer's Representative," May 13, 2013

³² GAO, Standards for Internal Control in the Federal Government, GAO/AIMD-00-21.3.1 (November 1999: Washington D.C.), pg. 8.

The C-FRAM Team was informed that Code 400 annually assesses COR files. These assessments take place between April and June. COR supervisors provide performance feedback in either March or October, depending on the CORs' pay plan. Therefore, the official performance feedback provided to CORs is on a 3-month to 11-month lapse from the time of performance.

Conclusion

The team assessed CMD's tone from the top as marginally ineffective. A majority of the focus group members could not recall the last time the Commanding Officer discussed ethical behavior nor could they state the Commanding Officer's opinion on fraud, waste, abuse, and mismanagement. Further, failing to ensure that employees are properly rated on their oversight functions, such as COR responsibilities, indicates that this function is not valued by management. These factors, taken as a whole, imply a negative tone from the top on oversight.

Control Activities

Cost mischarging is a fraud scheme in which a contractor intentionally submits false or inflated invoices to the government. Cost mischarging is differentiated from erroneous billing by the fact that inappropriate charges for cost mischarging are intentional. Proper cost monitoring and COR surveillance mitigates both the risk of cost mischarging and erroneous billing.

NAVSEA Office of the Inspector General reviewed the CMD's service contracting process, to include Professional Support³³ and Multi-Ship / Multi-Option (MSMO) contract processes. CMD contracting staff and Shipbuilding Specialists stated that the bulk of CMD's contracting is done via MSMO contracts. MSMO contracts use an incentive fee to ensure taxpayers receive good value for dollars allocated to the contract. The incentive fee awards the contractor for completing work under the agreed estimate of costs. For the incentive fee methodology to work properly, the government must ensure the contractor does not over-inflate its estimates. Over-inflated contractor estimates increase NAVSEA's risk of cost mischarging schemes and erroneous billings.

³³ CMD's support service contracts are under other CMD's warrant.

During our review, the C-FRAM Team discussed the CMD's processes for ensuring that proper work estimates are provided in a timely manner. The members of the contract specialist/officer focus group unanimously stated that the Independent Government Estimates (IGE) were unusable because they lacked any detail or substantiation. The Technical Assessment Review (TAR) Team echoed these concerns and stated that the IGE is sometimes numbers without any explanation. Further, the TAR Team stated that the Fleet would frequently either change or add new work at the last minute, which gives the TAR group insufficient time to ensure that the contractor estimate is not over-inflated and is otherwise accurate. For example, one contractor Variance Analysis Worksheet explained a 75 hour underrun by stating "Resources allocated for the beginning of the job overestimated the level of effort required based upon historical risk analysis. Based on current work progress, expect full utilization of remaining resources to provide oversight as work pace increases." The Worksheet went on to explain "Resource loading in the schedule will be adjusted to reflect where level of effort will be needed." So, the contractor overestimated the number of hours needed to do the job, and the government did not catch the overestimation.

Another Variance Analysis Worksheet explained a 35% variance with the following:

"Reasons for schedule variance are as follows:

- Work stopped while the contractor considered subcontracting this work item out. When work resumed by the contractor, a Quality Control inspection of the door found a failed chalk test, and work was stopped again.
- Unplanned costs for repairing the door and frame of about 200 hours are starting to impact the estimate at completion cost.
- Slow and poor workmanship has impacted the hours of this work item."

Yet another Variance Analysis Report explained a 305.11% variance, totaling 1,481.5 additional hours. Of the 1,481.5 hours, approximately 500 hours were due to "The Contractor Shipyards welder and shipfitter inefficiencies." These Variance Analysis Worksheets indicate the contractor cost control incentives built into this contract are not working. Further, the vague and non-descriptive explanations limit the government's ability to improve its estimation process; or identify potential fraud, waste, abuse, and mismanagement.

Conclusion

The team assessed the CMD's fraud, waste, abuse, and mismanagement control activities as ineffective. By failing to ensure the contractor has not overinflated its estimates and that the contractor provided detailed explanations for cost variances, the CMD increased NAVSEA's risk of cost mischarging, fraud, waste, abuse, and mismanagement.

Monitoring

Internal control should generally be designed to ensure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties.³⁴

During our contracting specialist/officer focus group, the C-FRAM Team was informed that the number one factor affecting their ability to ensure good value for the taxpayer dollar was the fact that the work packages continued to change throughout the contract negotiation process. According to the Joint Fleet Forces Maintenance (JFFM) Schedule, changes are supposed to stop at a certain date to give the TAR group sufficient time to analyze the requirements and to give the contracting specialist/officer sufficient time to properly negotiate with the contractor. But according to the focus group members this schedule is not being respected. During the meeting, the C-FRAM Team requested data supporting these claims. Further, the C-FRAM Team interviewed the TAR group and the Contract Department management asking about metrics on these claims. We were informed that no such metrics exist.

The CMD uses several other contracting commands to obtain services and materials. During the review the C-FRAM Team was informed that the CMD Contracting Department has little to no visibility over the money put on these contracts and the work performed by these contractors. As these contracts are not let on a NAVSEA warrant, they are not the CMD Contracting Department's responsibility. However, if the CMD does not have an internal control to ensure a Statement of Work (SOW) to SOW comparison, then the CMD is at risk for contract-shop

³⁴ GAO, Standards for Internal Control in the Federal Government, GAO/AIMD-00-21.3.1 (November 1999: Washington D.C.), pg 20.

shopping,³⁵ duplicative services fraud schemes,³⁶ and waste. The CMD does not have regular and recurring command metrics on CMD funds transferred to other commands for contractual services. The C-FRAM Team asked the CMD Finance Department about funds going to other contracting shops, specifically, the CMD Contracting Department. The CMD Finance Department provided a “50/50” report that listed, amongst other things, amounts obligated by the Contracting Department to other commercial shipyards.

During our focus groups and follow-up interviews, the team noted the CMD COR workload was unevenly distributed, especially, at another detachment. The vast majority of the CORs we interviewed at the CMD Headquarters were COR on one or two contracts; however, the CORs at CMD detachments were COR on up to eight contracts. Most concerning was an individual that was COR on seven cost-plus type contracts and one fixed price contract. This same individual was also the project manager on multiple availabilities. We followed up with the COR Certification Manager (CCM) to determine the root cause of the uneven distribution in workload. The CCM stated (1) that he was new to the seat and working to get a previously semi-dormant program back up to full speed; and (2) there are limited CORs available at the detachments.

Conclusion

The team assessed the CMD’s monitoring efforts as marginally ineffective. The CMD’s ineffective distribution of COR workload, increases the risk these oversight functions will not be performed and increases the risk of fraud, waste, abuse, and mismanagement.

Recommendations

To address our finding that the CMD could improve its tone from the top, the team recommends that the CMD:

1. Develop a means to communicate the Commanding Officer’s message on fraud, waste, abuse, and mismanagement to CMD contract oversight personnel, which includes but is not limited to, CORs, contract specialists, and contracting officers.

³⁵ Other contract CMDs do not require the stringent COR oversight described under NAVSEAINST 4200.17, “Contracting Officer’s Representative,” May 13, 2013

³⁶ A duplicative services fraud scheme occurs when an individual contracts with the first contractor to actually do the work and then contracts with a second contractor that bills the government for the same work. The individual then receives some kickback from the second contractor.

To address our finding that the CMD failed to follow NAVSEAINST 4200.17E, “Contracting Officer’s Representative,” May 13, 2013, the CMD is required to:

2. Ensure that all CORs have separate performance objectives describing their COR responsibilities.

To address our finding that the CMD’s internal controls were ineffective, the team recommends that the CMD:

3. Ensure that IGEs contain sufficient detail to give contracting officers and specialists the information they need to effectively negotiate with the contractor; and
4. Develop a means to get meaningful explanations for contractor cost variances.

To address our finding that the CMD could improve its methods for monitoring internal controls, the team recommends the CMD:

5. Develop metrics that track (1) the timeliness of work changes on scheduled availabilities; and (2) the true cost of those changes, which includes but is not limited to, dollars spent on planning work that is descoped and price differences for new work added late in the process;
6. Develop a process that ensures the CMD Contracting Department is given a “right of first refusal” for all contracts funded by the CMD; and
7. Evenly distribute COR workload at the CMD and all detachments.

C-FRAM’s assessment of the organization’s tone at the top, control activities and ongoing monitoring efforts related to mitigating the risk of contract fraud, waste, abuse, and mismanagement are illustrated in Table H. Ratings of ineffective or effective are applied to summarize the review results.

Table H. C-FRAM’s Assessment of the Reviewed Organization

	Ineffective				Effective
Tone from the Top		✓			
Control Activities	✓				
Monitoring		✓			

Appendix I

Procurement Fraud Personality Risk Profiles

Similar to the Fraud Triangle model, specific personality risk profiles³⁷ were developed to describe procurement fraudsters. These six personality risk profiles can be placed into three categories: the Procurement Fraudsters, the Procurement Abusers, and Procurement Non-Compliance Employees. Each one of the six personalities created a different risk or vulnerability to organizations. The six personality risk profiles are:

- Situational Fraudster
- Deviant Fraudster
- Business Abuser
- Multi-Interest Abuser
- Well-Intentioned Noncompliance Employee
- Disengaged Noncompliance Employee

While the Fraudsters and Abusers of the procurement process create a direct financial loss, or damage the organization's reputation, or cause media embarrassment, the Noncompliance employees create unnecessary exposure to fraud, litigation, and wasted resources and funds. However, the most concerning is that the Noncompliance employees open the door and create new opportunities for fraudsters, which is why the vulnerabilities they create need to be taken seriously.

Situational Fraudster

The Situational Fraudster is very similar to the traditional fraudster. This employee appears to be frustrated at work; has rationalized their right to an illegal enrichment; and perpetrates the fraud scheme when the right occasion occurs, usually because of weak internal controls. When the Situational Fraudster is caught, other employees are not surprised that the individual was involved in the fraud.

³⁷ Tom Caulfield, Executive Director, CIGIE, Training Institute, "Procurement Integrity's Integrated Controls vs. the Fraudster," May 2013, to be published at a future date.

Deviant Fraudster

The Deviant Fraudster is the most serious threat to the organization because they cause the most damage. They are always proactive in their search for opportunities to commit fraud; possibly perceived as one of the company's hardest workers or best contractors; and carry the "veil of trust" from others within the organization. This employee has a strong group of advocates who deny assertions that the fraudster is involved with any wrongdoing. The Deviant Fraudster, when internal to an organization, was also the employee that took only a few days of leave each year and seems to have their hand in every process within their business unit. This person is sometimes described as a "wheeler-dealer."

When comparing the Situational Fraudster and the Deviant Fraudster, the Situational Fraudster is far more prevalent in any contract, but the losses are much less; normally under a hundred thousand dollars. However, if the Deviant Fraudster successfully bribes an official to allow fraudulent billing submissions with a promise of kickbacks, or a contractor implements a fraudulent cost accounting scheme, the losses could be in the millions of dollars.

Business Abuser

Most published articles or classes on procurement fraud discuss the Situational or Deviant Fraudsters, however, additional vulnerabilities are created by other personality types. For example, the Business Abuser is the person that committed an inappropriate act that on its face seems to benefit the organization and not themselves. However, in reality, the Business Abuser commits the fraud to increase their standing within the organization, as someone that could continuously increase business and generate revenues. In general, this employee is looking to enhance their financial position in yearly bonuses, awards, or incentive pay.

The Business Abuser may inappropriately shift cost between contracts to make their unit appear better managed than it really is; or will bypass required quality control steps to ensure more timely or early deliverables. The Business Abuser is found in organizations with unrealistic operational demands perceived by the workforce, or when product delivery is emphasized above everything. The employee rationalizes their inappropriate actions as entitlement because it is linked to mission success. This individual places a great deal of difficulty for prosecution as the fraud investigator has to demonstrate with sufficient evidence that the fraud was done knowingly, and to receive monetary compensation in the future.

Multi-Interest Abuser

The Multi-Interest Abuser is the person that manipulates the procurement process to advance their own interests and the interests of another person. This is not done to obtain any financial advantage, but instead to help a friend secure a contract, or to ensure that an award goes to a desired contractor, or to help family members. The Multi-Interest Abuser is the person who drafted contract specifications for a specific contractor; or who embellished the need for a sole source justification to avoid the competitive process; or who slanted technical specifications to a specific bidder. The Multi-Interest Abuser is not motivated by any direct financial compensation, but raises significant risk to an organization in contract protests or in potential payment of higher costs because the competitive process is circumvented. Clearly, if the inappropriate actions of this person were motivated for personal financial gain, this person would be categorized as a Procurement Fraudster and not an abuser.

The next two personality risk profiles are rarely talked about during fraud courses, but present a risk to the organization that is harder to identify than the Fraudster or Abuser. These last two risk profiles fall into the category of the Procurement Noncompliance Employees.

Well-Intentioned Noncompliance Employee

The Well-Intentioned Noncompliance Employee believes that their deviation from the procurement process does not harm the organization. As a matter of fact, they sometimes believe they are helping the organization in obtaining greater efficiency or obtaining better services. The self-described well-intentioned non-compliance employee is normally an employee who has been with the organization for several years and has a good working knowledge of procurement processes or requirements and therefore knows how to advance their idea of efficiency. This is the employee who will not identify to the procurement division the true scope of a requirement to ensure the contract remains under a particular dollar threshold thereby allowing the award to be expedited (split purchase). This is also the employee who knows what key descriptions in an organizational purchasing document to use, or not to use, to avoid any additional procurement steps. This Well-Intentioned Noncompliance employee is found in organizations that allow low-dollar purchases without approval from an independent department or the purchasing department, or, organizations with limited checking on compliance with their procurement processes. This person's actions, similar to the Multi-Interest Abuser, raises the risk of contract protests, or in potentially paying

higher than needed cost for items due to the absence of a fair and open competitive process.

Disengaged Noncompliance Employee

The Disengaged Noncompliance Employee is the one who puts little or minimal effort into a specific procurement step. This person will not verify a contractor's bond, or not examine a contractor's past performance record, or not confirm a contractor's deliverable prior to approving payment. The actions, or lack of actions, by the disengaged person is the byproduct of a disgruntled or dissatisfied employee.

Case study examples of a DoD Multi-Interest Abuser and Situational Fraudster are discussed in Figures I-1 and I-2.

Figure I-1. Contracting Scheme

The DoD Multi-Interest Abuser

Service Member Contracting Scheme

Case Facts – A service member misused their position as Chief Contracting Officer at an overseas location. The individual steered military contracts to a company owned by their family. In one scheme, the family business received over \$30,000 in a prearranged contract to purchase military equipment. Over time, the family's profits exceeded 3 million dollars.

A plea agreement revealed that the service member exploited a partnership with a contractor by guiding work to their company. As part of the arrangement, the contracting company steered significant portions of certain contracts to the family operated business. Because of their position, the service member was the only family member that was knowledgeable about government contracting processes, which government contracts were likely to be awarded to a competitor, and which government contracts were previously awarded to competing businesses.

Outcome – The service member was charged with conflict of interest and sentenced to 30 months in prison for public bribery. In exchange for his guilty plea, the family members were not prosecuted.

Figure I-2. Civilian Bribery Scheme

The DoD Situational Fraudster

Former DoD Civilian Sentenced for Bribery

Case Facts – A DoD civilian was responsible for placing orders with local vendors for industrial supplies and cleaning agents. They initially accepted gifts such as college basketball tickets and video game systems in exchange for placing orders through a local vendor. Within six months, the employee increased orders of cleaning supplies by approximately \$30,000. The unnecessary increases were made so the local vendor would contribute to their son's baseball team.

Next, the employee and the vendor agreed to formalize their arrangement. The pair agreed that the employee would receive a cash payment equal to 2.25% of the total amount of any order placed with the vendor. During a two week period, eight separate orders were placed totaling over \$280,000. In exchange for placing these orders, the vendor paid the employee \$6,800. However, the employee was greedy and complained that they were owed over \$7,000 based upon the agreed rate of 2.25%.

This arrangement continued for over a year. Over time, the employee inflated numerous orders and, in exchange, was paid over \$34,000 in gifts and cash from the local vendor.

Outcome – The employee was sentenced to 30 months in prison for public bribery.

Appendix J

Organization Tool for Evaluating Fraud Control Program

Organizations are encouraged to use the checklist³⁸ below as a tool for evaluating the effectiveness of their fraud control program. The checklist is intended for illustrative purposes only. DoD organizations are encouraged to modify the checklist to suit their mission, size, complexity, and maturity of their fraud control program.

Fraud Control Governance Arrangements

1. Does the entity have an effective and articulated fraud control framework in place?
2. Does the entity have a central point of contact for fraud control within the entity?
3. Does the Audit Committee have a role in overseeing the development and implementation of the fraud risk assessment and fraud control plan?
4. Is information on the entity's values and code of conduct easily accessible to employees and included as part of its induction processes?
5. Does the entity have a conflict of interest policy and is this easily accessible and understood by employees?

Fraud Prevention

6. Has the entity undertaken a comprehensive fraud risk assessment in the previous two years, or following any significant change to the entity if earlier?
7. In identifying the fraud risks, does the entity consider: the entity's role, size and function; any change in structure or function; external and internal fraud; new and emerging fraud risks; and the broader organizational risks?
8. Has a fraud control plan been developed to minimize the impact and likelihood of identified risks?

³⁸ Australian National Audit Office, "Fraud Control in Australian Government Entities," Better Practice Guide, March 2011.

9. Has a fraud policy been issued by the Chief Executive Officer outlining the entity's position on fraud?
10. Do agreements with non-government service providers consider the applicable elements of the organization's Code of Conduct?
11. Does the entity ensure that adequate employment screening procedures are implemented?
12. Does the entity take steps to ensure the bona fides of new suppliers and customers and periodically confirm these?
13. Does the entity ensure that adequate fraud awareness activities and training are conducted within the organization? This should also include external parties such as suppliers and customers.
14. Does the entity have a formal process in place for communicating the outcomes of completed fraud investigations? Internal audit department to tailor and target fraud awareness activity and information.

Fraud Detection

15. Does the entity have a range of internal and external reporting mechanisms in place for parties to report suspected unethical behavior (including fraud)?
16. Are the entity's reporting mechanisms easily accessible by internal and external parties?
17. Does the entity use internal audit to actively review its detective control environment?
18. Does the entity provide sufficient information to enable employees to recognize the possible 'red flags' or early warning signs of fraud activity?
19. Does the entity require active fraud detection measures such as data mining or 'hot spot analysis'??

Monitoring, Evaluating and Reporting

20. Are there effective reporting channels (internal and external) in place to ensure all reported instances of fraud are adequately monitored?
21. Do the monitoring systems ensure appropriate accountability for fraud control?

22. Is there a quality assurance review system in place to help identify problems in all aspects of fraud control and its operations?
23. Following an instance of fraud, does the entity review the work processes subject to the fraud to determine whether changes were required to existing processes, including processes relating to fraud risk assessment and fraud prevention?

Appendix K

Suggested Reading

- AICPA, “Management Override of Internal Controls”, January 2005
<http://www.aicpa.org/catalogs/masterpage/Search.aspx?S=management+override+of+internal+controls>
- Australian National Audit Office, “Fraud Control in Australian Government Entities, Better Practice Guide”, March 2011
<http://www.anao.gov.au/Publications/Better-Practice-Guides/2010-2011/Fraud-Control-in-Australian-Government-Entities>
- American Accounting Association, “Auditors’ Use of Brainstorming in the Consideration of Fraud: Reports from the Field,” Joseph F. Brazel, North Carolina State University, Tina D. Carpenter, University of Georgia, J Gregory Jenkins, Virginia Polytechnic Institute and State University, 2010
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=965453
- Chartered Institute of Management Accountants, “Fraud risk management, A guide to good practice,” January 2009
<http://www.cimaglobal.com/Thought-leadership/Research-topics/Governance/Fraud-risk-management-a-guide-to-good-practice/>
- Department of the Navy, Bureau of Medicine and Surgery, “Navy Medicine Anti-Fraud Program, Instruction 5370.4,” April 1, 2010
<http://www.med.navy.mil/directives/Pages/BUMEDInstructions.aspx>
- Grant Thornton, “Managing fraud risk: The audit committee perspective,” not dated.
<http://www.grantthornton.com/issues/library/articles/audit/2012/Audit-2013-06-Managing-fraud-risk-2012.aspx>
- IIA, AICPA, ACFE, “Managing the Business Risk of Fraud: A Practical Guide,” not dated.
<http://www.acfe.com/resource-library.aspx>
- Independent Commission Against Corruption’s publication titled “Fighting Fraud, Guidelines for State and Local Governments,” November 2002

<http://www.cmc.qld.gov.au/topics/misconduct/misconduct-prevention/major-risk-areas/fraud-and-corruption>

- KPMG Forensic Practice, “Fraud Risk Management, Developing Strategies for Prevention, Detection, and Response,” 2006

[http://www.informationweek.com/whitepaper/Business Intelligence/wp902902?articleID=902902](http://www.informationweek.com/whitepaper/Business%20Intelligence/wp902902?articleID=902902)

- Pricewaterhouse Coopers, “How principles-based risk assessment enables organizations to take the right risks,” 2008

<http://www.pwc.com/us/en/issues/enterprise-risk-management/publications/guide-to-risk-assessment-risk-management-from-pwc.jhtml>

- United Kingdom, Department of Finance and Personnel, “Anti-Fraud Policy Response Plan,” April 2011

<http://www.dfpni.gov.uk/search.lsim?sb=0&qt=drug&sr=80&ha=dfp-cms&cs=iso-8859-1&mt=1&nh=10&sc=&sm=0>

- DoD OIG, Fraud Investigative Resources

www.dodig.mil/resources/fraud/index.html

This online tool contains the following information: fraud scenarios and indicators, GAGAS requirements for auditors, fraud knowledge tests, and links to additional fraud resources.

Acronyms and Abbreviations

AAA	Army Audit Agency
AAFES	Army and Air Force Exchange Service, Audit Division
AAMC	Association of American Medical Colleges
ACFE	Association of Certified Fraud Examiners
AICPA	American Institute of Certified Public Accountants
C-FRAM NAVSEA OIG	Contract Fraud Risk Assessment and Mitigation Branch, Naval Sea Systems Command, Office of the Inspector General
CIGIE	Council of the Inspectors General on Integrity and Efficiency, Training Institute
CMD	Command
COR	Contracting Officer Representative
CSA	Control Self-Assessment
DoD EA	DoD Education Activity
DTS	Defense Travel System
FA	Family Assistance
GAGAS	generally accepted government auditing standards
Grant Thornton, LLP	Grant Thornton
IA	Internal Audit
IIA	Institute of Internal Auditors
OIG	Office of Inspector General
MCNAFAS	Marine Corps Nonappropriated Funds Audit Service
NAVSEA	Naval Sea Systems Command
NEXCOM	Navy Exchange Service Command
Texas Tech	Texas Tech University System
USDA	US Department of Agriculture

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

Monthly Update

dodigconnect-request@listserve.com

Reports Mailing List

dodig_report@listserve.com

Twitter

twitter.com/DoD_IG

DoD Hotline

dodig.mil/hotline



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

