May 6, 2002

Audit Practices

Summary of Risk Assessment Methodologies
(D-2002-6-006)

Office of the Inspector General
of the Department of Defense

Quality *Integrity* *Accountability*

Additional Copies

To obtain additional copies of this report, visit the Inspector General of the Department of Defense, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AAA	Army Audit Agency
AFAA	Air Force Audit Agency
AICPA	American Institute of Certified Public Accountants
DCAA	Defense Contract Audit Agency
DFAS	Defense Finance and Accounting Service
GAO	General Accounting Office
IG	Inspector General
IIA	Institute of Internal Auditors
NAS	Naval Audit Service
OMB	Office of Management and Budget

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

May 6, 2002

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Report on Summary of Risk Assessment Methodologies
(Report No. D-2002-6-006)

We are providing this report for your information and use. This report contains no recommendations; therefore, written comments are not required.

We appreciate the courtesies extended to the staff. For additional information on this report, please contact Mr. Wayne C. Berry at (703) 604-8789 (DSN 664-8789) (wberry@dodig.osd.mil) or Mr. Edward A. Blair (216) 522-6091, extension 226 (DSN 580-6091) (eblair@dodig.osd.mil). See Appendix E for the report distribution. Team members are listed inside the back cover.

Patricia A. Brannin
Deputy Assistant Inspector General
for Audit Policy and Oversight

Special Notice

This report contains information and references about organizations outside the DoD. The information and references about these organizations do not in any way represent a recommendation or endorsement by the Inspector General of the Department of Defense.

DISTRIBUTION:
Director, Defense Commissary Agency
Internal Review Office
Director, Defense Contract Audit Agency
Director, Defense Contract Management Agency
Internal Review Office
Director, Defense Finance and Accounting Service
Director, Internal Review
Director, Defense Logistics Agency
Director, Internal Review
Director, Missile Defense Agency
Internal Review Office
Auditor General, Department of the Army
Auditor General, Department of the Navy
Auditor General, Department of the Air Force
Inspector General, Defense Information Systems Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office
Inspector General, National Security Agency
Inspector General, Special Operations Command
Chief, National Guard Bureau
Internal Review Office
Chief of Naval Education and Training
Headquarters, U.S. Marine Corps Nonappropriated Fund Audit Service
Director, Audits Division, Army and Air Force Exchange Service

Office of the Inspector General of the Department of Defense

Report No. D-2002-6-006 **May 6, 2002**
(Project No. D2001-OA-0122)

Summary of Risk Assessment Methodologies

Executive Summary

Introduction. This report provides the DoD audit community with information relating to risk assessment methodologies. The primary objective of an audit risk assessment is to provide its users with the assurance that audit resources are focused on those areas needing greatest attention and will provide the best value to the audit client. Audit risk assessments happen both on an overall (macro) and on a specific project (micro) level. DoD audit organizations rely on the results of risk assessment to help them manage the Department-wide audit resources of approximately 6,600 auditors. These auditors provide audit coverage for an organization that has an estimated annual budget of $329 billion in FY 2002. To accomplish their audit missions, auditors conduct risk assessments by following established standards, but also by developing additional procedures necessary for specific projects.

Government and professional organizations provide standards and guidance on the requirements for completing risk assessments. The General Accounting Office issues Government Auditing Standards, which prescribe standards of fieldwork for both financial and performance audits and require an assessment of control risk, internal or management controls, and adequate audit planning. The Office of Management and Budget provides risk assessment guidance in Circular No. A-123 "Management Accountability and Control" and in Circular No. A-133 "Audits of States, Local Governments, and Non-Profit Organizations." The American Institute of Certified Public Accountants Auditing Standards Board issues the Codification of Statements on Auditing Standards. The Statement on Auditing Standards requires adherence to the generally accepted auditing standards, which includes adequate planning and a sufficient understanding of internal controls for project planning under the Standards for Field Work.

Objectives. The objective of the review was to identify procedures for assessing risk when conducting DoD audits and to provide the DoD audit community with a resource of useful procedures. We included DoD audit activities and other government and private audit organization in our review.

Results. DoD audit organizations consider risk assessment results in assigning the audit resources to the functional areas identified as high risk. DoD audit organizations also respond to changing audit needs and changes in high-risk areas. The methodologies used by audit organizations varied from formal instructions for identifying high-risk areas to informal procedures such as documenting the result of an audit planning meeting with organizational managers. In each case, either through formal or informal methodologies, the objective was the same--to identify where audit resources can be used most effectively.

Some audit organizations have also developed or used standard risk assessment procedures for specific types of audits such as, information system audits, contract audits, and audits required under the Single Audit Act or the Chief Financial Officers Act. Many of these procedures are commercially available or available through the Internet. Other types of audits do not lend themselves to standard risk assessment methodologies. However, the concepts can often be tailored to these audits as well.

Table of Contents

Executive Summary i

Introduction

Background 1
Objectives 3

Results

Risk Assessment Methodologies 4

Appendixes

A. Project Process 12
B. Description of Risk Assessment Factors 13
C. Risk Assessment Resources and Contact Points 14
D. Example of Risk Assessment Tool 16
E. Report Distribution 17

Background

Significance of Risk Assessment Procedures in DoD Auditing. Risk assessment procedures are critical to DoD audit organizations in identifying and planning audit work that covers the varied and worldwide activities of the Department. Risk assessment procedures within DoD audit organizations with guidance provided by the General Accounting Office, the Office of Management and Budget, and other organizations, help provide audit focus and allow for proper planning. Risk assessments are essential to ensure that audit resources are effectively and efficiently used.

The DoD annual budget for FY 2002 is approximately $329 billion. DoD is the Nation's largest employer, with about 1.4 million active duty service members, 1.28 million volunteer guard and reserve members, and 672,000 civilian employees. The DoD also operates the largest acquisition system generating 15.8 million different acquisitions valued at more than $175 billion in FY 2001. The Department supports more than 600 fixed facilities worldwide including 250 major installations. DoD trains and equips the Armed Forces--the Army, Navy, and Air Force to perform warfighting, peacekeeping and humanitarian/disaster assistance tasks. Every year, DoD pays 5.5 million military and civilian members by issuing more than 135 million payroll payments valued at approximately $114 billion. Additionally, DoD disburses approximately $150 billion annually making more than 11.1 million contractor or vendor payments. This considerable activity requires an active role by the Department's audit organizations at all levels; however, to provide the audit support required for the activity, there are only about 6,600 auditors throughout the Department.

The Inspector General (IG) of the Department of Defense, with 525 auditors, serves as an independent and objective official in the Department of Defense who is responsible for conducting, supervising, monitoring, and initiating audits. Together with the Defense Contract Audit Agency (DCAA), the Army Audit Agency (AAA), the Naval Audit Service (NAS), and the Air Force Audit Agency (AFAA), we provide leadership and coordination and we recommend policies designed to promote economy, efficiency, and effectiveness in the administration of DoD programs and operations. We also seek to prevent and detect fraud and abuse in these programs. In addition, various Defense agencies and local commands have approximately 1,140 internal auditors to support their mission.

The DCAA with approximately 3,450 auditors is responsible for performing all contract audits for the Department of Defense and for providing accounting and financial advisory services regarding contracts to all DoD Components responsible for procurement and contract administration. DCAA provides audit cognizance for about 9,900 DoD contractors. In 2001, DCAA audited 8,874 pricing proposals with a total value of $123.5 billion and conducted other audits valued at $94.9 billion. DCAA provided net taxpayer savings of $3.2 billion.

The AAA, employing 541 auditors, provided audit coverage for an estimated $70.8 billion annual budget in FY 2001. The NAS with 259 auditors is responsible for internal audit of the $83 billion program of the Navy. The AFAA employing 713 auditors provides all levels of Air Force management with audit services valued at approximately $71.2 billion in FY 2001. However, over the last several years, DoD audit organizations have had significant reductions in staff. These reductions in staff require agencies to reassess priorities and determine where they can best use their valuable resources. Procedures used to address overall audit planning are referred to as macro risk assessments and they are designed to help audit organizations identify and reassess high-risk audit areas.

General Accounting Office Guidance. The General Accounting Office (GAO) issues Government Auditing Standards in what is commonly known as the Yellow Book. The Yellow Book prescribes standards of fieldwork for both financial and performance audits. These standards include the assessment of control risk and internal or management controls. These fieldwork standards relate to specific audits and require assessments of functional areas such as computerized information systems, safeguarding of assets, and the compliance with laws and regulations. Procedures used to address these standards are referred to as micro or specific audit risk assessment procedures.

Also, since 1990, the GAO has periodically reported on government operations that it identifies as high-risk. In January 2001, GAO identified Strategic Human Capital Management and Information Security as Government-wide high-risk areas. GAO also identified the following six high-risk areas specifically for DoD.

- Systems Modernization,
- Financial Management,
- Infrastructure Management,
- Inventory Management,
- Weapon Systems Acquisition, and
- Contract Management.

DoD audit organizations consider these high-risk areas for macro or overall audit planning and may include them as functional audit areas in an organizational audit or strategic plan.

Office of Management and Budget Guidance. The Office of Management and Budget (OMB) provides risk assessment guidance in the Circular No. A-123 “Management Accountability and Control” and in Circular No. A-133 “Audits of States, Local Governments, and Non-Profit Organizations.” OMB Circular A-123 requires agencies to develop strategic plans, set performance goals, and report annually on performance compared to

goals. Management controls are an integral part of the entire cycle of planning, budgeting, management, accounting, and auditing. Audit organizations can use these strategic plans and related management controls as a basis for audit planning. Auditors then provide information to management by conducting assessments of the management controls and making recommendations to assist in effectively meeting the plans and goals. OMB Circular A-133 sets forth standards for obtaining consistency and uniformity among Federal agencies for the audits of States, local governments, and non-profit organizations expending Federal awards. OMB Circular A-133 further provides audit requirements and the risk-based audit approach to determine which Federal programs are major programs.

Objectives

The objective of the review was to identify procedures for assessing risk when conducting DoD audits and to provide the DoD audit community with a resource of useful procedures. We focused on both overall audit planning procedures and specific risk assessment procedures used to address audit objectives. We included DoD audit activities and other government and private audit organizations in our review.

Risk Assessment Methodologies

Audit organizations, including DoD audit organizations, use different risk assessment methodologies when planning and conducting audits. These methodologies have either been self-developed or bought commercially. As a result, DoD audit organizations use a wide array of risk-based audit planning methodologies and risk assessment tools for conducting audits. There is not one method that would work for all audit activities. Instead, risk assessments must reflect the audit environment and activities audited.

Risk Assessments and Audit Planning

The DoD audit organizations and other governmental audit organizations use various formal and informal methods to assess risk during the audit planning phase. We defined formal risk assessment procedures as those procedures that are required by agency regulations or instructions. Informal risk procedures represent those procedures that, although not required, were developed and used by audit teams within the organization.

During audit planning, organizations consider several factors to help them identify auditable areas. These risk-based factors make it easier for agencies to identify areas needing greater audit attention. Table 1 below identifies some of the more common factors used to measure risk. The table also indicates where organizations use the corresponding risk factor to document the overall level of risk and allocate audit resources accordingly. A brief description of each factor is provided at Appendix B.

Table 1. Risk Factors Used by DoD Audit Organizations

Risk Assessment Factors	AAA	NAS	AFAA	DCAA	DFAS IR	IG DoD
Audit History/Prior Coverage	♦	♦	♦	♦	♦	♦
Degree of Decentralization					♦	
Dollar Value/Resources Used	♦	♦	♦	♦	♦	♦
Employee Competence					♦	
Employee Turnover/Growth	♦				♦	
Fraud, Waste & Abuse	♦	♦	♦	♦	♦	♦
Internal/Management Controls	♦	♦	♦	♦	♦	♦
Mission/Goals	♦	♦	♦			♦
Organizational Changes	♦		♦		♦	
Outside Concern/Sensitivity			♦			♦
Public Law	♦	♦	♦	♦		♦
Requested/Suggested Audits	♦	♦	♦	♦	♦	♦

KEY: AAA – Army Audit Agency, NAS – Naval Audit Service, AFAA – Air Force Audit Agency, DCAA – Defense Contract Audit Agency, DFAS-IR – Defense Finance and Accounting Service-Internal Review; IG DoD – Inspector General of the Department of Defense, Assistant IG for Auditing

Documentation indicated that the risk assessment factors are frequently used; however, where we did not indicate use by a specific organization does not mean the organization does not consider these factors. The purpose of the table is to illustrate that macro risk assessment procedures are varied and should be designed to meet the needs of the audit organization. Certainly, many more factors exist that can affect an organization's audit resources. Audit organizations can use these commonly known factors, but they must also anticipate future events to properly plan for high-risk audit issues. It is important for an audit organization to have established macro risk assessment procedures to assist them in allocating audit resources. The following discussion provides information and examples about risk assessment methodologies used by audit organizations.

Army Audit Agency. The AAA assesses risks and reviews internal controls as part of most audit projects. Risk assessment methods are usually incorporated into the overall audit planning function. AAA uses many informal risk assessment methods to identify high-risk audit areas. For example, AAA managers would consider a significant reduction in staffing in a particular area as a high-risk indicator and plan audit coverage accordingly. The AAA relies on its senior audit managers to assess functional areas and determine the high-risk areas needing audit coverage. Therefore, AAA managers rate known risk factors associated with particular issues to accomplish macro audit planning.

Naval Audit Service. The NAS has also used various risk assessment methods and selected risk factors to help develop an overall audit plan. Recently, the NAS has reorganized its functional audit areas and is currently working to develop a framework for determining the allocation of audit resources to the highest risk areas. The NAS has contracted with KPMG, LLP to conduct a macro risk assessment project. The risk assessment project will identify and prioritize auditable entities within the Navy.

Air Force Audit Agency. The AFAA has developed and incorporated formal audit risk assessment procedures into their audit instructions. The instructions include planning documents with risk criteria sections used in planning audit projects. The planning document outlines the procedures to be followed that would rate the audit risk by assigning a score to critical factors. Some critical factors rated by AFAA include dollar value or resources used, the effectiveness of internal or management controls, audits suggested or requested by management, the level of concern or sensitivity outside the organization, audits required by public law, and recent significant organizational changes. AFAA uses this formal audit planning document and risk assessment to help determine their audit plan.

Defense Contract Audit Agency. The Defense Contract Audit Agency (DCAA) uses a formal risk assessment method to rank and determine programs requiring audit coverage. DCAA has developed and established many risk assessment worksheets for use during audit planning. The worksheets were developed to assess risk and document the results relating to a specific type of DCAA audit. The worksheets were also designed to address the risk assessment requirements outlined in the DCAA Contract Audit Manual. For example, at

major contractors, those with more than $80 million in auditable costs, DCAA uses separate audit assignments to review and evaluate each significant contractor accounting and management system and their related controls. The resulting control risk assessments are documented using the DCAA Internal Controls Audit Planning Summary process, which provides a summary of control risk assessments on the 10 major business areas. Other auditors can use the Internal Controls Audit Planning Summary process to understand the level of risk associated with the contractor's accounting and management systems as it relates to the individual audit assignments they are working on. DCAA auditors use the information obtained and the risk assessed to determine the extent of transaction testing.

In an effort to address its audit backlog with decreased staff levels, DCAA developed a sampling initiative for audits of incurred cost contracts with an annual maximum dollar volume of $10 million. DCAA believed that the backlog of incurred cost audits represented a significant risk to the organization's mission, so they developed an audit-sampling plan to help reduce this risk. DCAA analyzes the contractor to determine questioned costs, audit leads, risk identified by the contracting officer, and audit experience with the contractor. If the analysis determines that none of these factors are currently present at the contractor, the contractor is rated as low risk and will be audited in a 3-year cycle. However, if these factors are present, the contractor will receive a high-risk rating and will be audited yearly.

Although the risk assessment procedures used by DCAA are specific to the types of audits they conduct, they provide good examples of how audit organizations would benefit from developing and establishing guides or pro-forma documents to help ensure that risk factors are adequately assessed.

Defense Finance and Accounting Service (DFAS) Internal Review. DFAS Internal Review uses a formalized risk assessment method in selecting areas for inclusion in their audit plan. The assessment is designed to measure the overall risk of one functional area as it relates to other functional areas. The risk factors in the assessment methodology include: performance achievement, financial perspective, personnel issues, system problems, and control environment. Based on the assessment, functional areas are categorized as high, moderate, or low risk. The rating represents the criticality or impact of the functional unit to the overall DFAS mission.

Inspector General of the Department of Defense, Assistant Inspector General for Auditing. The IG DoD plans audits and evaluations based on planning research efforts and audits required by law or requested by the Congress. Audit planning must respond to management needs and provide balanced coverage for the Department. Therefore, the IG DoD relies on its senior managers to ensure that a sufficient level of research is conducted within their assigned functional area to identify audit needs. Senior managers should:

- maintain an inventory of significant auditable entities for their functional area,

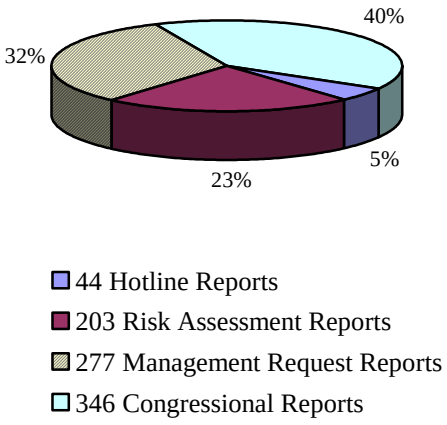
- coordinate with applicable DoD-wide planning groups,

- coordinate with DoD managers to obtain their ideas and priorities, and

- coordinate with GAO counterparts.

Where law, regulation, or congressional direction does not mandate the audit topics, the IG develops its audit plan relying on risk assessment results and in consultation with DoD managers when possible. The projects are coordinated in the joint audit planning groups that address coverage in each major functional area. The functional areas included Acquisition Management, Contract Management, Finance and Accounting, and Readiness and Logistics Support. Table 2 provides an overview of IG DoD audit workload by source for FYs 1998 through 2001. Table 2 indicates that 23 percent of our workload is self-generated based on risk assessments. With only about 23 percent of our audit staff resources available, we must use risk assessment procedures to identify those projects having the highest risk in order to ensure that we are providing effective audit coverage to areas not already mandated.

Table 2. Inspector General of the Department of Defense, Audit Reports by Source FY 1998-FY 2002



In an effort to keep the Congress informed of issues affecting the Department, the IG DoD identifies and periodically reports the DoD top 10 management challenges. Inspectors General at other executive departments also gather similar information for the Congress and senior management. These high-risk areas are then also used as a basis for assigning audit resources. The IG DoD reported these issues in its semiannual report, which is available at www.dodig.osd.mil.

Other Audit Organizations. The State of Ohio Auditor’s Office relies on standard audit steps to assess risk and generally performs audits based on requirements such as OMB Circular A-133 or other statutory requirements. Therefore, the State of Ohio Auditor's Office has found it useful to develop and

establish questionnaires and standard forms for use by its auditors to assess risk and determine audit coverage. Many of the tools used by the State of Ohio Auditor's Office are available via the Internet. The Inspector General,

Department of Health and Human Services, Office of Audit Services also has standard working paper forms that specifically address risk analysis. The Office of Audit Services at the Department of Health and Human Services makes their standard working papers available through the Internet.

Commercially Available Risk Assessment Programs. In recent years there has been an increase in the number of software programs developed to assist audit organizations in assessing risk. Public accounting firms and several other commercial organizations market risk assessment software programs that help audit organizations gather information and identify potential high-risk audit areas. Some software programs include:*

- Audit Leverage by IAD Solutions,
- Auditor Assistant by Norstan Consulting,
- Auto Audit by Paisley Consulting Inc., and
- Teammate (TeamRisk) by PriceWaterhouseCoopers.

These software programs provide organizations with an opportunity to perform risk assessments using automated software that will also support the entire audit lifecycle such as project management, automated work paper files, audit followup, and other functions. The software provides an organization with the overall framework for completing risk assessments while allowing the software programs to be modified to meet specific needs of the organization. It is important to note that this software may be especially helpful to organizations that do not have established risk assessment procedures or are currently reorganizing their audit functions to meet a change in mission. Specific details on how the software programs operate should be requested from the developer. We did not attempt to evaluate the effectiveness of these software programs. We are only providing this as information on resources available for organizations that are seeking commercially available programs to improve their audit risk assessment processes and procedures.

Summary. The risk assessment resources available to auditors are numerous. Many organizations have been conducting risk assessment procedures using similar methods for years. However, their procedures may not be formally documented as a risk assessment procedure. When the audit requirements of an organization are similar or mandated by statute, it is beneficial to develop and maintain a library of risk assessment documents or tools to be used for audit planning and during future audits. The above information and examples are just a few of the methods used by audit organizations. Of course, there are many other organizations with established formal methods. Appendix C provides a listing of

*Reference to the listed software and the software development companies does not represent a recommendation or endorsement by the Inspector General of the Department of Defense.

some available resources where auditors can research current trends and issues relating to risk assessment methodologies and links to access their web site.

Risk Assessments Tools for Audit Projects

Micro or specific audit risk assessments occur during actual audit projects. An audit team is responsible for developing audit steps that will identify the high-risk areas specific to the objectives and goals of the particular audit project. Generally audit organizations develop assessment tools to assist the audit teams in determining the overall level of risk associated with the audit. The assessment tools address the objective of the audit and help to identify high-risk issues within a defined area or function. By determining the levels of risk associated with a particular audit, the audit manager is able to allocate sufficient resources to the high-risk areas.

Risk assessment tools can be simple worksheets developed to rank internal controls or they can be complex computer software programs that identify vulnerabilities within a computer system or network. In either case, the assessment is a planned review of some portion or segment of the overall audit objective. It is important that risk assessments specific to the audit objective be completed during the survey phase and again, if necessary, early during the audit phase. The results of the risk assessment will then allow the auditors to focus on the areas needing the most attention.

Many micro risk assessment procedures or tools are developed while completing audits that are similar in nature. For example, the American Institute of Certified Public Accountants (AICPA) has guides available to help auditors in specific industries such as gambling, utilities, or health care. Companies have developed system or network scanning software that can be commercially purchased and used by information system auditors. The following discussion provides some examples of the tools developed during audits that assist auditors in assessing high-risk areas on specific projects.

Professional Organizations. The AICPA and the Institute of Internal Auditors (IIA) provide many useful tools to help auditors conduct risk-based audit procedures and apply risk assessment methods during actual audit projects. The AICPA provides guides related to specific industries, as previously discussed. For example, the AICPA resource online library contains auditing literature on standards, technical practice aids, reporting trends, and guidance. The library contains current audit risk alerts for specific industries and organizations. The IIA also makes resources available online. The IIA provides guidance by issuing practice advisories or guidelines. There are specific practice advisories addressing risk assessment engagement planning, guides to help link the audit plan to identified risks and exposures, and information about the internal audit's role in the risk management process. These products are available online through AICPA and IIA membership subscriptions.

General Accounting Office. The GAO provides audit organizations with useful audit planning information by issuing periodic executive guidance. For example, in a May 1998 executive guide "Information Security Management:

Learning From Leading Organizations," and its November 1999 supplement, the GAO discusses risk assessments and risk management. In its guidance, GAO provides the basic elements generally included in all risk assessments. GAO points out how it is necessary for organizations to reassess the controls that were implemented to mitigate perceived risks that have changed over time. In their November 1999 supplemental guidance, GAO provided a Risk Assessment Matrix and a Risk Assessment Table that were developed as useful tools to help the auditor assess information system risk. The risk assessment matrix was developed for use during information security audits. Appendix D is a copy of the matrix, which provides examples of the areas of vulnerability and the associated risk of loss. The matrix is another example of how organizations would benefit from tools that assist audit teams in assessing risks associated within similar types of audits.

Army Audit Agency. AAA developed risk assessment worksheets for computer system and installation management audit projects. For example, a scorecard assessment was developed to help auditors identify the technical, resource, and time risks associated with computer systems that would impact the Army's mission during the audits of year 2000 systems. For the installation management functional area, an assessment worksheet was developed that identifies high-risk activities based on financial results reported by golf courses operated by the Army. By ranking the reported financial results, the audit team identified golf courses that may potentially have a higher level of risk of internal control problems or other management issues.

Air Force Audit Agency. AFAA sought commercially developed software programs to help them assess network security and reliability at Air Force bases. These audits used scanning software to test base network security and make recommendations to commanders. AFAA also developed standard work paper guides to complete audit requirements of the Air Force Working Capital Fund financial statement audits. These guides provided audit teams with an established form of required steps or procedures necessary to complete their assigned audit area. Whether developed in-house or sought commercially, audit organizations would benefit from establishing a library of risk assessment tools for use by audit teams that conduct routine or similar audits.

Conclusion

To accomplish their audit mission, DoD audit organizations must conduct risk assessments by following standards issued by GAO, OMB, and other professional auditing organizations. These standards require assessment of control risk, internal controls, and adequate planning. However, audit organizations also need to develop additional procedures for specific projects. Auditors conduct risk assessments almost daily as a normal aspect of the their job. When auditors exercise judgment, an important part of auditing, they are conducting "mini" risk assessments to reach a decision. Auditors weigh known factors and use past experiences to decide a particular issue. The issue may be as different as what audit site to visit or the size of an audit sample. Auditors have many formal and informal resources available to them to help accomplish risk assessments. Audit organizations would benefit from the establishment of proven methods that assist audit managers in aligning resources to the high-risk areas. Additionally, audit

teams would equally benefit from documenting and maintaining proven procedures that can be easily modified to assess risks associated with specific projects. Worksheets, matrixes, guides, or other assessment tools should be developed, archived, and shared by audit agencies for specific functional areas or audit projects. By making available these proven tools, an organization will help to ensure that the audit team is adequately assessing the project's risk areas and focusing on the high-risk areas instead of the low-risk areas.

Appendix A. Project Process

Scope and Methodology. The project objective was to provide the DoD audit community with information relating to risk assessment methodologies and identify procedures and useful resources. We gathered data from the DoD Service audit agencies, the Defense Contract Audit Agency, the General Accounting Office, and other organizations. Additional research was conducted through the Internet accessing professional accounting and auditing organizations. We did not attempt to review the adequacy of risk assessment procedures at the organizations we contacted. We collected overall and specific audit planning methods that organizations have developed and found to be useful.

Contacts During the Project. We visited or contacted DoD audit organizations, other Federal audit organizations, and state and local audit organizations. Further details are available upon request.

Appendix B. Description of Risk Assessment Factors

Audit History/Prior Coverage. No audit history, the length of time between audits, the results of prior audits, and the management actions taken are all risk indicators that should be measured to decide the level of risk associated with the project.

Degree of Decentralization. The degree of management or functional decentralization will increase the risk factor rating. For example, if a disbursing function takes place at many locations, the level of risk is higher than that of a centrally controlled disbursing function.

Dollar Value/ Resources Used. The dollar value, volume of transactions, number of employees involved, asset values, or use of resources will affect the risk rating.

Employee Competence. An assessment of the matching of employee's knowledge, skills, and abilities to the requirements for job performance will affect the level of risk associated with a project.

Employee Turnover/Growth. High employee turnover or a large increase or decrease in the number of employees in an area may indicate potential problems and, therefore, affect the risk rating.

Fraud, Waste and Abuse. The vulnerability of the audit subject to fraud, waste, and abuse. For example, those activities having assets that could be easily converted to cash or personal use would receive a high-risk rating.

Internal/Management Controls. The project entity's management self-evaluation affects the risk rating. Also, past experience on management control programs of the subject and at the potential project entity will impact the risk rating. Limited or no controls will be rated as high risk, adequate controls or no past experience will be rated as medium risk, and significant controls will be rated as low risk.

Mission/Goals. Audit projects that directly affect an organization's ability to complete its mission or accomplish its goals, such as weapon system performance, would be rated as high risk. Projects that indirectly affect the mission or goals, such as computer or communication networks, would be rated as medium risk. Projects that have no direct affect, such as billeting or club operations would be rated as low risk.

Organizational Changes. Changes in an entity's mission, structure, staffing levels, or financial results are all indications that may affect rating level.

Outside Concern/Sensitivity. The sensitivity of the project to outside criticism or adverse public opinion increases the risk factor rating. For example, environmental safety is of great concern to communities around military installations.

Public Law. Projects required by public law will automatically be rated as high risk.

Requested/Suggested Audits. An audit requested or suggested by Congress or senior management will normally receive a high-risk rating.

Appendix C. Risk Assessment Resources and Contact Points

The inclusion of an organization does not represent an IG DoD recommendation, endorsement, or agreement with the information offered by the organization. The following list of resources is provided for information purposes only.

Organization Name	Description of Resource	Resource Web site At
Air Force Audit Agency	Web site providing information and guidance on the audit process	www.afaa.hq.af.mil
American Institute of Certified Public Accountants	Professional organization web site providing accounting and auditing guidance and products	www.aicpa.org or www.cpa2biz.com
Army Audit Agency	Web site providing information and guidance on the audit process	www.hqda.army.mil/AAA WEB
Defense Contract Audit Agency	Web site providing general audit guidance and information on the audit process	www.dcaa.mil
General Accounting Office	Governmental guidance and related resources	www.gao.gov
Institute of Internal Auditors	Professional organization providing auditing and consulting guidance and products	www.theiia.org
Naval Audit Service	Web site providing information and guidance on the audit process	www.hq.navy.mil/Naval Audit
Office of Audit Services, Inspector General, Department of Health and Human Services	Governmental agency web site providing tools for conducting audits and preparing reports	www.oig.hhs.gov

Office of Management and Budget	Governmental guidance and related resources	www.whitehouse.gov/omb
State of Ohio Auditor's Office	State governmental agency providing audit information for state and local government audits	www.auditor.state.oh.us

Additional Contact Points

The following contact points are provided for organizations that would like to obtain additional risk assessment procedures information.

Defense Contract Audit Agency
Headquarters, Policy and Plans
Quality Assurance Division
(703) 767-2250
dcaa-pqa@dcaa.mil

Naval Audit Service
Environmental Risk Assessment
Joan Hughes
(202) 433-5551
Hughes.Joan@hq.navy.mil

Acquisition and Logistics Risk Assessment
Randy Exley
(202) 433-6260
Exley.Randy@hq.navy.mil

Macro Risk Assessment
Vinnie D'Orazio
(202) 433-6874
Dorazio.Vinnie@hq.navy.mil

Appendix D. Example of Risk Assessment Tool

The GAO developed this risk assessment matrix for information security audits. It provides a good example of a tool that can be used on similar audits or modified as needed.

Table 1: Risk Assessment Matrix

Areas of vulnerability and possible effects of damage	Risk of monetary loss			Risk of productivity loss			Risk of loss of customer confidence		
	H	M	L	H	M	L	H	M	L
Personnel									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Facilities and equipment									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Applications									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Communications									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									
Software and operating systems									
Unauthorized disclosure, modification, or destruction of information									
Inadvertent modification or destruction of information									
Nondelivery or misdelivery of service									
Denial or degradation of service									

36 GAO/AIMD-00-33 Information Security Risk Assessment

Appendix E. Report Distribution

Department of the Army

Auditor General, Department of the Army
Chief, National Guard Bureau
  Internal Review Office

Department of the Navy

Auditor General, Department of the Navy
Chief of Naval Education and Training
  Command Evaluation Officer
Headquarters, U. S. Marine Corps, Nonappropriated Fund Audit Service
Director, Office of Internal Audit, Navy Exchange Service Command

Department of the Air Force

Auditor General, Department of the Air Force

Defense Agencies

Director, Defense Commissary Agency
  Internal Review Office
Director, Defense Contract Audit Agency
Director, Defense Contract Management Agency
  Internal Review Office
Director, Defense Finance and Accounting Service
Director, Defense Logistics Agency
  Internal Review Office
Director, Missile Defense Agency
  Internal Review Office
Inspector General, Defense Information Systems Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office
Inspector General, National Security Agency
Inspector General, Special Operations Command

Other Defense Agencies

Director, Audits Division, Army and Air Force Exchange Service

Team Members

The Deputy Assistant Inspector General for Audit Policy and Oversight, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General of the Department of Defense, who contributed to the report, are listed below.

Patricia A. Brannin
Wayne C. Berry
Edward A. Blair
Krista S. Gordon