



governmentattic.org

"Rummaging in the government's attic"

Description of document: Five (5) Treasury Inspector General for Tax Administration (TIGTA) Deputy Inspector General for Audit (DIGA) memoranda, 2016-2017

Requested date: 28-March-2017

Released date: 25-April-2017

Posted date: 19-February-2018

Source of document: Office of Chief Counsel Disclosure Branch
Treasury Inspector General for Tax Administration
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005
Fax: (202) 622-3339
Email: FOIA.Reading.Room@tigta.treas.gov

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

April 25, 2017

VIA E-MAIL

This is in response to your March 28, 2017 Freedom of Information Act (FOIA) request, seeking access to records maintained by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA Disclosure Branch received your e-mailed request on March 28, 2017.

Specifically, you requested a copy of the following Deputy Inspector General for Audit (DIGA) Memoranda:

DIGA Memo 17-002, Assessing the Reliability of Computer Processed Data.

DIGA Memo 17-003, Office of Audit Fiscal Year 2017 Performance and Workload Measures.

DIGA Memo 16-004, 2015 External Peer Review Results.

DIGA Memo 16-005, Revisions to Final Audit Report Disclosure Review Process.

DIGA Memo 16-006, Fiscal Year 2017 Planning Guidance.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

We have located sixty-seven (67) pages which are responsive to your request seeking copies of the above referenced Deputy Inspector General for Audit (DIGA) Numbered Memoranda. We are releasing fifty-six (56) pages in full and eleven (11) pages in part. A copy is enclosed. We are asserting FOIA subsections (b)(6), (b)(7)(C) and (b)(7)(E) as the justification for withholding.

FOIA subsection (b)(6) permits the withholding of records and information about individuals when disclosure of the information could result in a clearly unwarranted invasion of personal privacy. The withheld information consists of identifying information compiled with regard to individuals other than you. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. As a result, the privacy interests of the third parties outweigh the public's interest in having the information released.

FOIA subsection (b)(7)(C) permits an agency to withhold "information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy." The withheld information consists of identifying information compiled with regard to individuals other than you. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. The information was compiled for law enforcement purposes and the privacy interest of the third parties outweighs the public's interest in having the information released. As a result, this information has been withheld in response to your request.

FOIA subsection (b)(7)(E) permits an agency to withhold "records or information compiled for law enforcement purposes ... [that] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." The withheld information consists of techniques or guidelines not commonly known to the public and/or information that could lead to the circumvention of the law. As a result, this information has been withheld in response to your request.

We have enclosed an Information Sheet that explains the subsections cited above as well as your administrative appeal rights. If you file an appeal, your appeal must be in writing, signed by you, and postmarked or electronically transmitted within ninety (90) days from the date of this letter. You should address the envelope as follows:

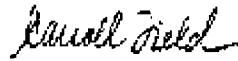
Freedom of Information Act Appeal
Treasury Inspector General for Tax Administration
Office of Chief Counsel
City Center Building
1401 H Street, NW, Suite 469
Washington, DC 20005

The cost incurred to process your FOIA request was less than \$25.00, the threshold set by Treasury's FOIA regulation, so no fees were assessed.

If you have any questions, please contact Carroll Field, Government Information Specialist, at (202) 927-7032 or Carroll.Field@tigta.treas.gov and refer to Disclosure File # 2017-FOI-00151.

You may contact our FOIA Public Liaison at (202) 622-4068 for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

Sincerely,



Carroll Field
(For) Amy P. Jones
Disclosure Officer and
FOIA Public Liaison

Enclosures



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

December 18, 2015

DIGA: 16-004

MEMORANDUM FOR ALL OFFICE OF AUDIT EMPLOYEES

A handwritten signature in black ink, appearing to read "Michael E. McKenney".

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: 2015 External Peer Review Results

The purpose of this memorandum is to communicate the results of the Department of Homeland Security (DHS) Office of Inspector General's (OIG) 2015 external peer review of the Office of Audit (OA). As part of the peer review process, organizations can receive a rating of *Pass*, *Pass with Deficiencies*, or *Fail*. I am pleased to share with you that the OA received a peer review rating of *Pass*. The DHS OIG's review confirmed that the OA's system of quality control has been suitably designed to provide the Treasury Inspector General for Tax Administration (TIGTA) with reasonable assurance that our organization is in conformance with applicable professional standards.

Although the OA received a *Pass* rating, the DHS OIG reported three findings in a Letter of Comment and provided suggestions to reemphasize compliance with *Government Auditing Standards* (GAS) and the OA's policies and procedures. The following paragraphs briefly summarize each finding along with the corresponding actions the OA will take to improve in these areas. I commend everyone for their efforts in helping the OA receive the *Pass* rating. However, I want to reemphasize that we all must remain diligent in ensuring sufficient audit evidence is obtained and that our indexing and referencing process is sufficient to support the audit findings in the report.

Findings and Actions

Finding 1: Continuing Professional Education – *Government Auditing Standards* (GAS), paragraph 3.76, requires auditors who perform work in accordance with generally accepted government auditing standards (GAGAS) to maintain professional competence through Continuing Professional Education (CPE).

The DHS OIG peer review team reviewed CPE records associated with audit staff who worked on a sample of 9 TIGTA audits and identified minor inaccuracies in TIGTA's CPE documentation for 3 of the 9 audits reviewed. Specifically, they found:

- (b)(6);(b)(7)(C) claimed an incorrect number of CPE credit for 1 allowable course; claimed CPE credit for 5 ineligible courses; and claimed duplicate CPE credits for 1 course.
- (b)(6);(b)(7)(C) claimed an incorrect number of governmental CPEs for 2 courses and was missing certificates for 2 different courses.
- (b)(6);(b)(7)(C) claimed CPE credit for 1 course in the incorrect year.
- (b)(6);(b)(7)(C) claimed duplicate CPE credits for 1 course.

Recommendation 1 – Provide refresher training that reminds staff to ensure CPE reports and records for auditors are accurate and sufficient documentation is available to substantiate the reported credits earned.

OA Action – The TIGTA was pleased to learn that all OA employees met their CPE requirements, and they agreed that (b)(6);(b)(7)(C) employees could have done a better job documenting their training. TIGTA will reemphasize the importance of ensuring CPE reports and records are accurate and sufficient documentation is available to substantiate the reported credits. TIGTA created a job aid to highlight to employees how to report CPE hours in their time reporting system and how to categorize the type of training received.

Finding 2: Indexing and Referencing Reports – The OA manual contains policies to ensure TIGTA audit reports are accurate and sufficient and appropriate evidence is available to support the findings and conclusions. However, the DHS OIG found:

- 2 of 9 reports reviewed had not indexed key facts to sufficient and appropriate evidence.
- 1 report was indexed to sufficient and appropriate evidence, but the indexing was confusing and could have been simplified.
- 2 reports contained errors which were not identified or corrected during the report indexing and referencing process.

Recommendation 2 – Provide refresher training on indexing and referencing to reemphasize the importance of ensuring all reported findings and conclusions are indexed and supported by sufficient and appropriate evidence and final reports are accurate.

OA Action – During Fiscal Year 2015, OA provided a training class to all employees that addressed indexing and referencing guidelines and processes. This occurred as a result of TIGTA's own internal peer reviews. Participants were provided the opportunity to conduct a case study aimed at completing a simulated referencing assignment along with follow-up discussions, including the types and sufficiency of evidence. Additionally, each Assistant Inspector General for Audit communicated

the importance of referencing to their staffs based on TIGTA's recent internal peer review recommendations. The Deputy Inspector General for Audit will reemphasize the importance of referencing and obtaining appropriate evidence when the results of the external peer review are shared with TIGTA employees.

Finding 3: Corroborating Evidence – *Government Auditing Standards* and the OA manual outline the importance of evaluating the objectivity, credibility, and reliability of testimonial evidence. The DHS OIG found that, in one audit, TIGTA did not corroborate testimonial evidence obtained from the IRS and used to develop a significant finding in the report.

Recommendation 3 – Develop internal training initiatives to remind auditors of the importance of obtaining corroborating evidence to support testimonial evidence

OA Action – As mentioned above, in Fiscal Year 2015, OA provided a training class to all its employees that addressed indexing and referencing to ensure sufficient audit evidence is obtained to support audit findings. The Deputy Inspector General for Audit will also reemphasize the importance of obtaining corroborating evidence to support testimonial evidence when the results of the external peer review are shared with employees. In addition, we will conduct a training course for all OA employees that will address evaluating the reliability of data used to support audit findings.

Attached are the final 2015 External Peer Review report and Letter of Comment. I encourage each employee to review these documents and incorporate the corrective actions in your current processes and audits. Additional guidance will be forthcoming.

Please contact Nancy LaManna, Acting Assistant Inspector General for Audit (Management Planning and Workforce Development), at (202) 622-3837 or Jeff Jones, Director, Office of Management and Policy, at (978) 684-9088 if you have any questions related to the 2015 External Peer Review or this memorandum.

Attachments


2015 Final DHS
Report.pdf


2015 Final DHS
LOC.pdf

**OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DEC 11 2015

The Honorable J. Russell George
Inspector General
Treasury Inspector General for Tax Administration
1401 H Street, NW
Washington, DC 20005

Dear Mr. George:

We have reviewed the system of quality control for the audit organization of Treasury Inspector General for Tax Administration (TIGTA) in effect for the year ended March 31, 2015. A system of quality control encompasses TIGTA's organizational structure and the policies adopted and procedures established to provide it with reasonable assurance of conforming with *Government Auditing Standards*¹. The elements of quality control are described in *Government Auditing Standards*. TIGTA is responsible for establishing and maintaining a system of quality control that is designed to provide TIGTA with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements in all material respects. Our responsibility is to express an opinion on the design of the system of quality control and TIGTA's compliance therewith based on our review.

Our review was conducted in accordance with *Government Auditing Standards* and the Council of the Inspectors General on Integrity and Efficiency *Guide for Conducting Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*. During our review, we interviewed TIGTA personnel and obtained an understanding of the nature of the TIGTA audit organization, and the design of TIGTA's system of quality control sufficient to assess the risks implicit in its audit function. Based on our assessments, we selected audits and administrative files to test for conformity with professional standards and compliance with TIGTA's system of quality control. The audits selected represented a reasonable cross-section of TIGTA's audit organization, with emphasis on higher-risk audits. Prior to concluding the peer review, we reassessed the adequacy of the scope of the peer review procedures and met with TIGTA management to discuss the results of our review. We believe that the procedures we performed provide a reasonable basis for our opinion.

¹ Issued by the Comptroller General, December 2011



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In performing our review, we obtained an understanding of the system of quality control for the TIGTA audit organization. In addition, we tested compliance with TIGTA's quality control policies and procedures to the extent we considered appropriate. These tests covered the application of TIGTA's policies and procedures on selected audits. Our review was based on selected tests; therefore, it would not necessarily detect all weaknesses in the system of quality control or all instances of noncompliance.

There are inherent limitations in the effectiveness of any system of quality control, and, therefore, noncompliance with the system of quality control may occur and not be detected. Projection of any evaluation of a system of quality control to future periods is subject to the risk that the system of quality control may become inadequate because of changes in conditions, or because the degree of compliance with the policies or procedures may deteriorate.

Enclosure 1 to this report identifies the TIGTA offices that we visited and audits that we reviewed.

In our opinion, the system of quality control for the audit organization of TIGTA in effect for the year ended March 31, 2015, has been suitably designed and complied with to provide TIGTA with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. Audit organizations can receive a rating of pass, pass with deficiencies, or fail. TIGTA has received an External Peer Review rating of **pass**. As is customary, we have issued a letter dated December 11, 2015 that sets forth findings that were not considered to be of sufficient significance to affect our opinion expressed in this report.

Sincerely,

A handwritten signature in black ink, appearing to read "John Roth", is positioned above the printed name.

John Roth
Inspector General

Enclosures



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ENCLOSURE 1

SCOPE AND METHODOLOGY

We tested compliance with TIGTA audit organization's system of quality control to the extent we considered appropriate. These tests included a review of 8 of 88 audit reports issued during the period April 1, 2014, through March 31, 2015. We also reviewed an audit report that had an internal quality control review completed by TIGTA. Lastly, we visited TIGTA offices located in Washington, DC and Denver, CO.

Selected Audit Reports Performed by TIGTA

Report No.	Report Date	Report Title
2014-10-073	09/29/2014	Controls Over Outside Employment Are Not Sufficient to Prevent or Detect Conflicts of Interest
2015-10-006	12/30/2014	Additional Consideration of Prior Conduct and Performance Issues Is Needed When Hiring Former Employees
2014-20-088	09/29/2014	The Information Reporting and Document Matching Case Management System Could Not Be Deployed
2014-23-072	09/29/2014	Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project
2014-30-067	09/26/2014	Additional Actions Are Needed to Ensure That Improper Fuel Tax Credit Claims Are Disallowed
2014-30-080	09/18/2014	Declining Resources Have Contributed to Unfavorable Trends in Several Key Automated Collection System Business Results
2014-40-058	09/03/2014	Processes Are Needed to More Effectively Address Potentially Erroneous Excess Social Security Tax Credit Claims
2014-40-093	09/29/2014	Existing Compliance Processes Will Not Reduce the Billions of Dollars in Improper Earned Income Tax Credit and Additional Child Tax Credit Payments
Audit Report Processed through TIGTA's Internal Quality Assurance Review		
2014-10-007	03/21/2014	The Awards Program Complied with Federal Regulations, but Some Employees with Tax and Conduct Issues Received Awards



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ENCLOSURE 2



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20000

December 7, 2015

The Honorable John Roth
Inspector General
Department of Homeland Security
245 Murray Lane, SW
Washington, D.C. 20528

Dear Mr. Roth:

Thank you for the opportunity to comment on your November 23, 2015 draft external peer review report of the Treasury Inspector General for Tax Administration. We are pleased to receive a peer review rating of pass. We appreciate the review team's periodic briefings on their review results and the opportunity to discuss our questions and perspective on their preliminary findings.

We are firmly committed to maintaining an effective system of quality controls and work continuously to improve our operations. We have provided a separate response to the findings and recommendations outlined in your Letter of Comment.

If you have any questions regarding the response, please contact Michael E. McKenney, Deputy Inspector General for Audit, at (202) 622-5816.

Sincerely,

J. Russell George
Inspector General



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

DECEMBER 11, 2015

The Honorable J. Russell George
Inspector General
Treasury Inspector General for Tax Administration
1401 H Street, NW
Washington, DC 20005

Dear Mr. George:

We have reviewed the system of quality control for the audit organization of Treasury Inspector General for Tax Administration (TIGTA) in effect for the year ended March 31, 2015, and have issued our report thereon dated December 11, 2015, in which TIGTA received a rating of *pass*. That report should be read in conjunction with the comments in this letter, which were considered in determining our opinion. The findings described below were not considered to be of sufficient significance to affect the opinion expressed in that report.

Finding 1. Continuing Professional Education

Government Auditing Standards (GAS), paragraph 3.76, requires auditors who perform work in accordance with generally accepted government auditing standards (GAGAS) to maintain professional competence through Continuing Professional Education (CPE). Audit organizations should maintain CPE records for an appropriate period of time to satisfy any legal or administrative requirements, including peer review.¹ We found inaccuracies in TIGTA's CPE documentation for 3 of 9 audits we reviewed. Specifically, the peer review team identified:

- (b)(6);(b)(7) claimed an incorrect number of CPE credit for 1 allowable course; claimed CPE credit for 5 ineligible courses; and claimed duplicate CPE credits for 1 course.
- (b)(6);(b)(7) claimed an incorrect number of governmental CPEs for 2 courses and was missing certificates for 2 different courses.

¹ *Guidance on GAGAS Requirements for Continuing Professional Education*, GAO-05-568G, April 2005, section 37



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- (b)(6);(b)(7)(C) claimed an incorrect number of governmental CPEs for 2 courses and was missing certificates for 2 different courses.
- (b)(6);(b)(7)(C) claimed CPE credit for 1 course in the incorrect year.
- (b)(6);(b)(7)(C) claimed duplicate CPE credits for 1 course.

Although the TIGTA employees selected for our review were compliant with GAGAS CPE requirements during the scope of this peer review, refresher training, which include accurate record-keeping and documentation retention, will ensure TIGTA continues to adhere to the GAGAS CPE requirements.

Recommendation 1 - The TIGTA should provide refresher training that reminds staff to ensure CPE reports and records for auditors are accurate and sufficient documentation is available to substantiate the reported credits earned.

Summary of Management's Comments: Concur.

The TIGTA was pleased to learn that all Office of Audit employees met their CPE requirements, and they agreed that [redacted] employees could have done a better job documenting their training. TIGTA will reemphasize the importance of ensuring CPE reports and records are accurate and sufficient documentation is available to substantiate the reported credits. TIGTA reported they created a job aid to highlight to their employees how to report CPE hours in their time reporting system and how to categorize the type of training received.

Finding 2. Indexing and Referencing

The TIGTA OIG *Operations Manual*, April 1, 2014, sections 90.6 and 90.7 *Indexing and Referencing of Office of Audit Documents* contains policies to ensure TIGTA audit reports are accurate and sufficient and appropriate evidence is available to support the findings and conclusions. However, we found that in 2 of the 9 reports, TIGTA had not indexed key facts to sufficient and appropriate evidence. We discussed our findings with the TIGTA audit team members who provided us additional indexes to audit work papers that fully supported the findings or conclusions in question. In another audit report, key facts were indexed to sufficient and appropriate evidence, but the indexing was circular and confusing. TIGTA's audit team agreed they could have indexed the audit better by simplifying the indexing.

Additionally, we identified errors in two final reports, which TIGTA did not identify nor correct during the report indexing and referencing process. These errors did not affect the overall conclusions of the audit reports.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 2 – The TIGTA should provide auditors refresher training on indexing and referencing to reemphasize the importance of ensuring all reported findings and conclusions are indexed and supported by sufficient and appropriate evidence and final reports are accurate.

Summary of Management's Comments: Concur.

During Fiscal Year 2015, the Office of Audit provided a training class to all employees that addressed indexing and referencing guidelines and processes. This occurred as a result of TIGTA's own internal peer reviews. Participants were provided the opportunity to conduct a case study aimed at completing a simulated referencing assignment along with follow-up discussions, including the types and sufficiency of evidence. Additionally, each Assistant Inspector General for Audit communicated the importance of referencing to their staffs based on TIGTA's recent internal peer review recommendations. The Deputy Inspector General for Audit will reemphasize the importance of referencing and obtaining appropriate evidence when he shares the results of this external peer review with TIGTA employees.

Finding 3. Corroborating Evidence

According to GAS, paragraph 6.62, testimonial evidence may be useful in corroborating documentary information. In addition, the *TIGTA Operations Manual*, April 1, 2014, sections 60.3.3, *Evaluating the Reliability of Computer-Processed Data*, describes policies on the strength and weaknesses of corroborating evidence. As such, auditors should evaluate the objectivity, credibility, and reliability of the testimonial evidence. We found in one audit, TIGTA did not corroborate testimonial evidence obtained from the IRS and used to develop a significant finding in the report.

Recommendation 3 – The TIGTA should develop internal training initiatives to remind auditors of the importance of obtaining corroborating evidence to support testimonial evidence.

Summary of Management's Comments: Concur.

As mentioned above, in Fiscal Year 2015, the Office of Audit provided a training class to all its employees that addressed indexing and referencing to ensure sufficient audit evidence is obtained to support audit findings. The Deputy Inspector General for Audit will also reemphasize the importance of obtaining corroborating evidence to support testimonial evidence when he shares the results of this external peer review with employees. In addition, TIGTA will

**OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

We have attached as Enclosure 1, the TIGTA response to our draft letter of comment. In this response, TIGTA agreed with the findings and reported they plan to have all corrective actions completed by July 31, 2016. We appreciate the professionalism, assistance, and cooperation from you and your staff during our review.

Sincerely,

A handwritten signature in black ink, appearing to read "John Roth", is positioned above the typed name.

John Roth
Inspector General

Enclosure



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

ENCLOSURE 1



INSPECTOR GENERAL
FOR THE
ADMINISTRATIVE

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

December 7, 2015

The Honorable John Roth
Inspector General
Department of Homeland Security
245 Murray Lane, SW.
Washington, D.C. 20528

Dear Mr. Roth:

Thank you for the opportunity to respond to your draft comment letter on the external peer review of the Treasury Inspector General for Tax Administration's Office of Audit, which was received by our office on November 23, 2015. We are pleased that your review confirmed that our system of quality control has been designed to meet the requirements of the quality control standards established by the Comptroller General of the United States and that our adherence to this system provides reasonable assurance of compliance with auditing standards, policies, and procedures.

The draft comment letter discusses three findings and recommendations related to documenting Continuing Profession Education; indexing and referencing of reports; and corroborating evidence used to develop report findings. Attached are our responses to your recommendations. We plan to have all corrective actions to address your recommendations completed by July 31, 2016.

We would like to thank your peer review team for their thorough review of our operations and the comments and suggestions contained in the draft comment letter.

Sincerely,

J. Russell George

J. Russell George
Inspector General



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

2

Recommendation 1 – The TIGTA should provide refresher training that reminds staff to ensure CPE reports and records for auditors are accurate and sufficient documentation is available to substantiate the reported credits earned.

Views of Responsible Official – The Office of Audit is pleased that the peer review team found that all of our employees met their CPE requirements, and we agree that employees could have done a better job documenting their training. We will reemphasize the importance of ensuring CPE reports and records are accurate and sufficient documentation is available to substantiate the reported credits. Specifically, a job aid has been created to highlight to our employees how to report CPE hours in our time reporting system and how to categorize the type of training received.

(b)(6);(b)(7)(C)

Recommendation 2 – The TIGTA should provide auditors refresher training on indexing and referencing to reemphasize the importance of ensuring all reported findings and conclusions are indexed and supported by sufficient and appropriate evidence and final reports are accurate.

Views of Responsible Official – The Office of Audit agrees with your observations that our audit reports were accurate and sufficient evidence supported the findings, but in certain reports indexing and referencing could have been improved. During our internal peer reviews, the Office of Audit recognized the need to improve its referencing. As a result, the Office of Audit provided a training class to all employees during Fiscal Year 2015 that addressed indexing and referencing guidelines and processes. During this class, the participants were provided the opportunity to conduct a case study aimed at completing a simulated referencing assignment along with follow-up discussions, including the types and sufficiency of evidence. Additionally, each Assistant Inspector General for Audit communicated the importance of referencing to their staffs based on our recent internal peer review recommendations. To further reiterate the importance of referencing and obtaining appropriate evidence, the Deputy Inspector General for Audit will reemphasize the topic when he shares the results of the external peer review with employees.

Recommendation 3 – The TIGTA should develop internal training initiatives to remind auditors of the importance of obtaining corroborating evidence to support testimonial evidence.

Views of Responsible Official – The Office of Audit agrees with your observation that the audit team did not corroborate certain testimonial evidence that was used in the one audit report. As mentioned above, the Office of Audit provided a training class in Fiscal Year 2015 to all employees that addressed indexing and referencing to ensure sufficient audit evidence is obtained to support audit findings. The Deputy Inspector General for



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

3

Audit will also reemphasize the importance of obtaining corroborating evidence to support testimonial evidence when he shares the results of the external peer review with employees. In addition, we will conduct a training course for all Office of Audit employees that will address evaluating the reliability of data used to support audit findings.



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

February 9, 2016

DIGA: 16-005

MEMORANDUM FOR ALL OFFICE OF AUDIT EMPLOYEES

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Revisions to Final Audit Report Disclosure Review Process

The purpose of this memorandum is to advise you of changes to the final audit report disclosure checklist and to more clearly define the disclosure review process and respective responsibilities. The objective of these changes is to improve the clarity and consistency of the disclosure review procedures, thereby increasing the efficiency and timeliness of the overall process. These procedures are effective immediately for all new final audit reports submitted to the Office of Management and Policy (OMP) for review. Most notably, a revised Audit Report Disclosure Checklist has been developed, and reports with recommended redactions will now be submitted to OMP **after** the Deputy Inspector General for Audit (DIGA) has signed the final report. The revised disclosure checklist is attached and has been posted to the Templates section in Microsoft Office Word (*File/New/My Templates/Audit Forms*), in TeamMate, and in the Audit Templates and the Report Guidance sections on the Policy and Guidance page of the Office of Audit (OA) Community SharePoint site.

Revisions to the Disclosure Checklist

The Disclosure Checklist has been revised to show the redaction codes and associated disclosure questions/issues for consideration. The Checklist now shows all nine possible redaction codes that the OA uses when posting final reports to the Treasury Inspector General for Tax Administration (TIGTA) public website. The revised Checklist covers all of the disclosure questions that were included in the previous version of the Checklist dated October 2014. In addition, two previously unused redaction codes have been added: Redaction Code 6 (confidential informant) and Redaction Code 9 (national security information). Although these codes have not been previously used for our reports, we believe including them provides OA staff with a complete picture of all possible redaction areas that should be evaluated.

Further, the revised Checklist combines Redaction Codes 7 and 8, which were similar in nature and related to predecisional information. Therefore, the revised Checklist does

not show a Redaction Code 8. The redaction codes were not renumbered because we wanted to maintain consistency in the numbering of the redaction codes used in prior audit reports that are posted to our public website.

Following the redaction codes, pages 4 and 5 of the Checklist include additional "Other Redaction Considerations" questions. These questions address minimum necessary redactions, redaction consistency, identification of hypothetical cases described in reports, Internal Revenue Service (IRS) management's requests for redaction and OA's responsibilities for discussing these redactions with the IRS, and Sensitive But Unclassified (SBU) reports. SBU reports will now go through the disclosure process to facilitate the processing of any future Freedom of Information Act (FOIA) requests for the report, as well as other requests for disclosure of the report, such as requests by Congress.

Procedures and Responsibilities for Disclosure Review

The following sections describe the procedures and responsibilities for preparing final reports for Counsel's disclosure review, working with Counsel to resolve questions, and finalizing the redacted report that will be posted to TIGTA's public website.

1. If the audit team submits a final report that does not have recommended redactions:
 - a. The Assistant Inspector General for Audit (AIGA) submits the final report package for OMP review. The package consists of the final report, Outcome Measure Summary (OMS) document (if applicable), and the final report Audit Report Disclosure Checklist.
 - b. OMP processes the final report and submits the package to the DIGA for review and signature.
 - c. Following the DIGA's signature, OMP sends the final report and Audit Report Disclosure Checklist to Counsel for disclosure review. Note: This is the process currently followed for all reports.
2. If the audit team submits a final report with recommended redactions:
 - a. The AIGA submits the final report package for OMP review. The package consists of the final report and OMS document (if applicable).
 - b. OMP processes the final report and submits the package to the DIGA for review and signature.
 - c. Following the DIGA's signature, OMP will provide a copy of the final report to the AIGA, Director, and Audit Manager. The audit team will use the signed final report to highlight their suggested redactions. The AIGA should provide the redacted report, completed Audit Report Disclosure Checklist, and, if applicable, the IRS's request for redactions as soon as possible to OMP via the *TIGTA Audit Reports mailbox to ensure that Counsel's disclosure review can be timely initiated. Counsel has 10 business days to complete its disclosure review.

- d. Because the Office of Communications may use information in the Highlights page for media purposes, the Highlights page cannot include information that must be redacted for public release. The audit team must write the Highlights page making sure not to include information that cannot be publically released (e.g., return or return information protected under I.R.C. § 6103 and Privacy Act protected information).
- e. The audit team completes the Audit Report Disclosure Checklist to identify potential redactions, based on the information in the Audit Report and its sources, IRS management's request for redactions, and OMP's suggested redactions provided with the draft report quality assurance review. If the audit team is uncertain whether a particular statement should be redacted, the team should include a description of the uncertainty in the Checklist, rationale for making or not making the redaction, and ask Counsel for their guidance. The audit team should make sure that IRS requests for redactions be in writing, including if applicable, a description of the harm that would occur if the information was released. If the reason given for a redaction is possible circumvention of the law if the information is publically released, how the information could be used to circumvent the law would occur should be described. If OA plans to reject any IRS request for redaction, the audit team should notify the IRS, explain OA's rationale, and allow the IRS to further explain its position. If OA continues to believe the IRS requested redactions should not be made, then OA should inform the IRS of OA's plan to release the information. For the related Checklist question, the audit team should include in the comments section a discussion of OA's analysis for agreeing or disagreeing with the IRS redaction request and resolution of any disagreement, if any, following discussions with the IRS.
- f. The audit team should highlight the report where it determines redactions should be made, regardless of who recommended them. The audit team should highlight the pertinent portions of the audit report text or appendices, insert a comment referencing the redaction number from the Checklist to which the text relates, and describe the harm that OA believes would result if the information was disclosed. The recommended redactions should relate to one of the disclosure questions; *i.e.*, the cited reason should not simply state that OMP recommended or the IRS requested the redaction.
 - i. The highlighted final report should only show the redactions that the audit team is proposing.
 - ii. Provide descriptive reasons for the redactions. For example:
Descriptive: The report wording states that the IRS is not reviewing x, y, and z on the tax return. This could give unscrupulous individuals the specifics they need to file false information for those fields. Note: The first sentence is needed for the specifics, and the second sentence is needed to state how the fraud could be perpetrated.

Not Descriptive: This needs to be redacted because it can let unscrupulous individuals circumvent the tax system.

- iii. For Internal Revenue Code (I.R.C.) § 6103 information,¹ Counsel will contact the audit team if the report appears to contain return information that has not been highlighted for redaction. The audit team can clarify the reasoning by, stating, for example, whether the information raising concern is purely hypothetical,² stating the information is taken from the public court record in a tax administration proceeding,³ *etc.* If the audit team disagrees with Counsel on a Section 6103 information redaction, the audit team should elevate the disagreement to the Deputy Inspector General for Audit for final resolution.
- iv. For circumvention issues, the IRS and the OA are the factual experts, not Counsel. Potential for circumvention of agency regulations or statutes is based on judgment in connection with considered analysis of the facts, not law. As such, Counsel expects the audit team to make the determination on whether information in the report could cause circumvention.
- v. The audit team should only highlight for redaction the minimum information necessary to ensure the nature of the redaction cannot be understood when the report is released. Information that could be highlighted for redaction could be one number, one word, part of a sentence, or an entire paragraph.
- g. If redactions are needed in the IRS management response that is part of the final report, the audit team should use the "Review/New Comment" toolbar option to place a comment box on the page where the redaction is needed. When adding the comment, the audit team should identify the redaction code and then type into the comment box the **exact** wording that requires redaction. This is necessary because the management response is a picture and the wording in the response cannot be highlighted.
- h. The Disclosure Checklist will be signed and dated by the Audit Manager or Director who prepared the Checklist. In addition, the Checklist will identify a point of contact who Counsel should contact if they have any questions during the disclosure review.
- i. The AIGA submits to OMP the highlighted copy of the signed final report with recommended redactions, the completed Disclosure Checklist, and if applicable, IRS management's request for redactions.

¹ I.R.C. § 6103(a) mandates that returns and return information shall remain confidential unless disclosure is authorized by one of the exceptions to confidentiality.

² Hypothetical examples may be released in audit reports, but a hypothetical example must consist of a composite or fictional set of facts and circumstances not drawn from any specific taxpayer's case or situation. For example, using information taken from an actual taxpayer's case and changing names and other details such as dates, locations, dollar amounts, *etc.*, is not a hypothetical example for purposes of determining whether information is confidential return information.

³ Even though return information may appear in a court record, this does not necessarily mean that TIGTA may disclose this information in its audit reports. Only return information that has been made public in a **court proceeding pertaining to tax administration** may be disclosed.

5

- j. Following receipt of the field's highlighted redacted report and completed Disclosure Checklist (and if applicable, IRS management's request for redactions), OMP will send to Counsel for review the disclosure package, consisting of the DIGA signed/undated final report that is highlighted with the audit team's recommended redactions, the completed Audit Report Disclosure Checklist and, if applicable, IRS management's request for redactions.
3. Counsel's review of signed final report packages submitted by OMP:
- a. Counsel will perform a disclosure review of the DIGA's signed/undated final report using the audit team's completed Audit Report Disclosure Checklist and the audit team's recommended redactions.
 - b. If Counsel has questions, Counsel will e-mail the point of contact identified on the Audit Report Disclosure Checklist with a cc to the respective AIGA and OMP staff (John Anderson, Nancy Cassel, and LaVonne Hester-Smith), and the Office of Communications (Mark Anderson).
 - c. Counsel finalizes its review, based on decisions made with the OA, and annotates the final report with any questions or comments. Counsel e-mails the final report redactions (or clean version of the report if there are no redactions) to OMP (John Anderson, Nancy Cassel, and LaVonne Hester-Smith) and the Office of Communications (Mark Anderson), with a cc to the AIGA.
4. OMP prepares the final report for posting:
- a. OMP adds the redaction legend on the bottom of the report cover page, blocks out the information being redacted in the report, and adds the redaction number justifying the redaction.
 - b. OMP will convert the report to Adobe PDF for posting.

If you have any questions, please contact Jeff Jones, Director, Office of Management and Policy, at (978) 684-9088.



INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

March 25, 2016

DIGA: 16-006
MEMORANDUM FOR ALL OFFICE OF AUDIT EMPLOYEES

Michael E. McKenney

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Fiscal Year 2017 Planning Guidance

This memorandum provides guidance to the Office of Audit (OA) for the Fiscal Year (FY) 2017 Annual Audit Plan. Our FY 2017 planning process will provide the foundation of our audit coverage during the upcoming fiscal year. In FY 2017, we will continue to address the major management and performance challenges facing the Internal Revenue Service (IRS).

In FY 2016, as a supplement to the major management and performance challenges, the following emphasis areas were identified as being high risk and having a significant impact on tax administration:

- Authentication for Account Access
- Identity Theft Related Tax Fraud
- Affordable Care Act (ACA) Implementation and Administration
- International Tax Compliance

These continue to be significant areas of risk for consideration in planning for the upcoming fiscal year. Moreover, please consider whether any additional areas of emphasis are warranted.

OA Fraud Program

In addition to these emphasis areas, the OA will continue with its Fraud Program. The results continue to be encouraging; numerous referrals have been sent to the Office of Investigations. For FY 2017, each business unit is encouraged to be cognizant of potential fraudulent activity by IRS employees, contractors, vendors, and/or grantees during the risk assessment process. The Assistant Inspector Generals for Audit (AIGA) should plan to propose fraud-focused integrity projects for FY 2017 at the annual

planning meeting. The OA executive team will discuss the overall OA Fraud Program and make decisions on the long-term strategies and plans for the program, including the OA Fraud Board's coordination efforts with the Office of Investigations.

Audit Selection

Under the leadership of the AIGAs, each business unit will develop a program of suggested audits for the business unit. During the development of suggested audits, each business unit should continue to address the impact and oversight needs related to the ACA.

Additionally, consideration must be given to the potential for reportable audit outcomes during the planning process. The OA's planned performance measures categories for FY 2017 will be the same as in FY 2016, as outlined in Chapter 300, Section 90.26, of the Treasury Inspector General for Tax Administration (TIGTA) Operations Manual. For each suggested audit, business units should identify potential outcome measures based on the anticipated audit approach.

Further, staff responsible for planning should consider the performance measures and workload indicators in DIGA Memorandum 16-003 during their planning efforts. Chapter 300, Section 50, of the TIGTA Operations Manual contains guidance for the OA's strategic planning process, including risk assessments and outcome measures.

We have not received responses from the IRS or the Department of the Treasury regarding potential audit issues for FY 2017. If we receive a response, we will share it with the AIGAs and Directors and post it on the OA Community Page.

Risk Assessments

Planning efforts for FY 2017 should start with risk assessments in accordance with Chapter 300 of the TIGTA Operations Manual. Chapter 300 includes a description of the key factors to be considered when preparing a risk assessment. Risk factors are the criteria used to identify the relative significance of and likelihood that conditions or events may occur that could adversely affect an organization. Risk assessments will ultimately lead to the suggested audits.

Attached is an Excel workbook that should be used to document the risk assessment process and to satisfy external peer review requirements.



The AIGAs should identify the high-risk audits from the risk assessment that they would complete if additional resources were available. The information will be discussed at the annual planning meeting held by the OA executive team and will be consolidated by

Management Planning and Workforce Development (MPW) staff for budget planning purposes.

Audit Justifications

Audit justifications should be prepared for all audits, including carryover audits and those that would be added to the Annual Audit Plan if additional resources were available. Integrity project justifications should be prepared for all potential projects each business unit is considering for FY 2017. Attached below are the templates for the FY 2017 Audit Justification and FY 2017 Integrity Project Justification. MPW will complete the planning spreadsheets again this year, so it is important that all the information requested on the Audit Justification template is completed. Complete Audit Justifications will streamline the process and save time when the planning spreadsheets are sent to the business units for review and revision before the Annual Audit Plan is developed.



FY 2017 Audit
Justification.docx



FY 2017 Integrity
Project Justification.docx

Data Needs

For FY 2017, the OA will again catalog its data needs for the suggested audits identified by the business units. Attached is a spreadsheet each business unit should complete to identify the various data needed to complete specific audits. The purpose of identifying the data needs is to ensure that the Strategic Data Services Division has sufficient resources available to access IRS data and files needed by auditors to carry out audit objectives. It is important to include as much information on the spreadsheet about the data that is needed and, if possible, when the data will be needed in order to complete the audit timely. Please provide as much information on the spreadsheet as possible. If Modernized Tax Return Database (MTRDB) or Information Returns Master File (IRMF) data will be needed, please specify the documented code or form number that will be requested. Each business unit should e-mail its completed spreadsheets to Debra.Kisler@tigta.treas.gov by August 12, 2015.



FY 2017 Data
Needs.xlsx

OA Executive Planning Meeting

During July 12-13, 2016, the OA executives will meet to finalize the selection of audits for the FY 2017 Annual Audit Plan. The meeting will be held at TIGTA Headquarters. An agenda will be sent out at a later date. In order for MPW to prepare for the meeting,

business units should provide electronic copies of all Audit Justifications and Integrity Project Justifications to Debra.Kisler@tigta.treas.gov by July 7, 2016.

After the OA Executive Planning Meeting, MPW will distribute Excel workbooks that will capture the information submitted on the audit justifications to each business unit for review and revisions. The information on the spreadsheets will be used to compile the Annual Audit Plan.

If you have any questions on this guidance, please contact Jeff Jones, Director, Office of Management and Policy at (978) 684-9088.

FY 2013 Objectives**Business Unit Title (e.g., Compliance and Enforcement)**

Determine if the

Major and non-major projects

Private Debt Collection

XXX

YYY

etc.

Follow-up on Significant Recommendations

AAA

BBB

CCC

etc.

Other High Risk, High Impact Areas

DDD

EEE

FFF

GGG

Efficient Use of Funds

Risk Rankings and definitions from Chapter 300, Section 50 TIGTA Operations Manual	
Risk Factor Ranking	Definition
(Before Weighting)	
10	Extreme Risk
7 to 9	High Risk
4 to 6	Moderate Risk
1 to 3	Low Risk
0	No Risk

Stakeholder Concerns: Internal Revenue Service, IRS Oversight Board, Congress, Department of the Treasury, Government Accountability Office. (Weight = 1.6)

Business Unit Methodology		Business Unit Methodology is determined by each respective business unit. The descriptions here are examples for consideration.
Description	Score	
The auditable area was mentioned in the latest Taxpayer Advocate's yearly report, the latest IRS Oversight Board yearly report, a GAO report within the last year, TIGTA's FY 2008 and 2009 testimony, TIGTA reported as an IRS Management Challenge, IRS Highest Priority Initiatives, or was provided as an audit suggestion as part of the FY 2010 risk assessment.	10	
The auditable area did not score a "10"; however, it involves an area designated high risk by the GAO and the IRS	9	
The auditable area is a major program.	8	
The auditable area involves a non-major program.	4-6	
The auditable area involves a minor program.	1-3	

Size of Program: Budget, revenue impacted. (Weight = 1.4)

Business Unit Methodology	
Description	Score
	10
	6
	5
	4
	3

	2
--	---

Financial/Regulatory: Privacy, security/Federal Information Security Management Act, disclosure, Government Performance and Results Act, Federal Financial Management Improvement Act. (Weight = 1.4)

Business Unit Methodology

Description	Score
	10
	7
	0

Taxpayer Impact: Taxpayer burden, customer service, customer satisfaction, taxpayer entitlements, taxpayer relations, taxpayer rights. (Weight = 1.4)

Business Unit Methodology

Description	Score
The auditable area has a direct impact on a large amount of taxpayers	10
The auditable area has a direct impact on a smaller subset of taxpayers	8
The auditable area indirectly impacts taxpayers	4-6
The auditable area does not have any impact on taxpayers	0

Change Management: New programs, tax law changes, organizational changes, reengineering efforts, information technology/modernization. (Weight = 1.3)

Business Unit Methodology

Description	Score
	8-10
	5-7
	2-4
	0

Strategy and Planning: Strategic Plans, Annual Plans, goals, performance measures. (Weight = 1.1)

Business Unit Methodology

Description	Score
	10
	7
	0

Internal Control Assessment: Prior audit findings, last audit coverage, integrity issues. (Weight = .9)

Business Unit Methodology

Description	Score
The auditable area has been mentioned in any of the previous 4 Semiannual Reports to Congress	10
The auditable area has not been mentioned in any of the previous 4 Semiannual Reports to Congress; however, it is directly mentioned in a TIGTA/GAO finding	7
The auditable area has not been mentioned in any of the previous 4 Semiannual Reports to Congress and it is indirectly mentioned in a TIGTA/GAO finding	3
The auditable area has not been mentioned as part of a TIGTA/GAO finding	0

Data Analysis: Trends and performance measures. (Weight = .9)

Business Unit Methodology

Description	Score
Results from the Business Performance Review over the last year show a decrease from a green rating to a red rating	10
Results from the Business Performance Review over the last year show a constant red rating	9
Results from the Business Performance Review over the last year show a decrease from a green rating to a yellow rating or a yellow rating to a red rating	7
Results from the Business Performance Review over the last year show a constant yellow rating	5

Results from the Business Performance Review over the last year show a constant green rating, the project is new, or the auditable area is not a project and therefore does not lend itself to trending and performance measures	0
--	---

3/29/2017

FY 2017 Risk Assessment
Risk Rankings by Total Score

Rank	Source	Auditable Area	Stakeholder Concerns	Size of Program	Financial/Regulatory	Taxpayer Impact	Change Mgmt.	Strategy and Planning	Fraud Waste/Internal Control	Data Analysis	Total Score	Comments	Potential Outcome Measure	Potential Audit Objective
		Assessment Weights	1.6	1.4	1.4	1.4	1.3	1.0	1.0	0.9	100.0			

Proposed FY 2017 Audits

**Fiscal Year 2017 Planning
Potential Audits for Other TIGTA Business Units**

Project	Business Unit	Comments

Fiscal Year 2017 Audit Justification

Management Challenge	[Enter the title of one (or more) of the major management challenge areas] Please enter the primary MMC first
IRS Functional Area	[Enter IRS functional area]
Title	
Audit Objective	
Justification/ Reason for Initiation AND Impact on Tax Administration	
Source	[e.g., Mandatory, Risk Assessment, Stakeholder Request (add which stakeholder), etc. You can indicate more than one source, if applicable.]
Carryover	[Yes or No – Will the audit still be in process at the end of FY 2014 (final report has not been issued as of September 30, 2014)? If this is a carryover, please indicate the current audit number].
Ranking Score	
Emphasis Area?	[Yes or No – Add the title of the applicable emphasis area]
Follow-up Audit?	[Yes or No – Indicate Yes if the audit will plan to follow up on prior recommendations, even if that is only one of the objectives for the audit and the audit title does not contain "Follow Up."]
Outcome Measures	

Note: This information above should be provided in one-page.

**Fiscal Year 2017
Audit Justification**

Director

Start Quarter

Report Quarter

Staff Days-total

**Staff Days – FY
2015**

Fiscal Year 2017 Integrity Project Justification

Management Challenge Integrity Project

Functional Area {enter IRS functional area}

Title

Audit Objective

**Justification/
Reason for Initiation**

AND

**Impact on Tax
Administration**

Source

Carryover

Ranking Score

Cross-Cutting?

Follow-up Audit?

Outcome Measures

Fiscal Year 2017 Audit Project Related Data and Other Resource Needs

Business Unit/Director	
Audit Title/Topic	
Expected Start Quarter	
IRS Systems and/or Data Files Needed to Conduct Review (spell out the acronyms when possible)	
Past Issues Requesting Access to These Systems and/or Obtaining These Files	
Timeframe for Data Needs (e.g., 3 years, 1 year, cycles needed, etc)	
Is Information Contained on DCW? If so, what specific files will you be working with?	
Has anyone had access to this data or system in prior reviews? If so, direct access or was a download of the data received?	



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

October 17, 2016

DIGA: 17-002

MEMORANDUM FOR ALL OFFICE OF AUDIT EMPLOYEES

A handwritten signature in black ink, appearing to read "Michael E. McKenney".

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Assessing the Reliability of Computer-Processed Data

The purpose of this memorandum is to communicate the policy for assessing the reliability of computer-processed data and to introduce a new Data Reliability Assessment (DRA) form and guidance for completing a DRA. This policy and use of the revised DRA form are effective immediately.

Many Office of Audit (OA) reviews involve the extraction, analysis, and testing of computer-processed data in order to meet one or more objectives. Auditors should be aware of the potential risks associated with computer-processed data. Auditors who use these data to support findings must assure that the data are reliable. In this context, data reliability means that data are reasonably **complete** and **accurate**,¹ meet the intended purposes, and are not subject to inappropriate alteration. Auditors are not expected to ensure that all possible errors are detected, but that the data are sufficient and appropriate for their specified purpose. The auditor's judgment in relying on system controls, selecting data testing methods, and determining the extent of data testing is critical to ensuring the integrity of the Treasury Inspector General for Tax Administration's audit products.

¹ In the context of data reliability, **completeness** refers to the extent that all relevant data records are present and that the fields in each record are populated appropriately. **Accuracy** refers to the extent that recorded data reflect the actual underlying information.

2

The audit team should assess data reliability if the data to be analyzed are intended to support audit results, findings, conclusions, or recommendations. Some data used only as background information, such as data requested from a source and used in a table, may not require an assessment. A determination of the best approach to satisfy Generally Accepted Government Auditing Standards (GAGAS) requirements will be made on an audit-by-audit basis. The results and basis for assessing the reliability of computer-processed data must be documented in the workpapers and the audit report.

When an assessment is required, the audit team will include general steps in the Audit Plan to assess the reliability of computer-processed data. When completing the assessment, the audit team should perform those tests considered necessary to support an opinion on the data reliability and to accomplish the overall objectives of the audit. Depending on the purpose for which the data will be used, not every step will be applicable or necessary for all data sources. The framework for the DRA process includes:

- Plan the assessment by reviewing information from the agency, Government Accountability Office (GAO), and other sources (e.g., existing reports, data dictionaries, etc.) to determine if the data are appropriate.
- Conduct the data assessment with an appropriate mix of work. This includes, but is not limited to: reviewing existing information, interviewing knowledgeable agency officials, tracing samples, electronic testing, and reviewing selected system controls.
- Make the final data reliability determination. If enough information was obtained for a determination, determine if the data is sufficiently reliable, not sufficiently reliable, or undetermined reliability for the purposes of the audit. If not enough information was obtained, request more information. If the reliability of the data is undetermined, the report should make the limitations of the data clear so incorrect or unintentional conclusions will not be drawn from the data. For example, the report should indicate how the use of the data could lead to an incorrect or unintentional message.

Generally, a DRA is performed as early as possible in the audit. Examining the information early is necessary to help the team determine whether the data would be appropriate for addressing the objectives in the first place. The process is likely to differ from one audit to another. However, it should include sufficient work to allow the auditor to have a good understanding of how the data were collected, the systems they were extracted from, and the process and system controls related to the key data elements for the engagement.

To document the analysis performed to assess the reliability of computer-processed data, the audit team should complete the DRA. One DRA should be completed for

3

each analysis performed and should include summary information for all data sources used.

During the DRA process, the auditor or analyst may identify issues that result in limitations to the data and/or expected analysis to be performed. Any issues or impediments identified should be documented in the DRA. Further, if data is determined to be unreliable or to have undetermined reliability, the audit team should discuss with TIGTA management the best approach of how to proceed. Attached are the revised DRA form and guidance for how to complete a DRA. The DRA template can be found in the Audit Forms tab in the Templates section of Microsoft Word and in the Templates section in TeamMate.

Completed DRA forms should be maintained in your TeamMate workpapers and should also be submitted to the ***TIGTA Audit PGP1** e-mail address for retention in the Integrity Data System (IDS).

If you have any questions about this policy please contact Nancy LaManna, Acting Assistant Inspector General for Audit (Management Planning and Workforce Development) or Erika Axelson, Director, Applied Research and Technology.

Attachments



Data Reliability
Assessment Form.doc



TIGTA OA Data
Analysis Guide-Assess

Record of Data Reliability Assessment

Government Auditing Standards require auditors to assess the sufficiency and appropriateness of computer-processed information. Assessing and reporting on the reliability of computer-processed data is significant to an audit team's findings, conclusions, and recommendations. Data reliability means that data are reasonably complete and accurate, meet the intended purposes, and are not subject to inappropriate alteration.

If an audit team deems a data reliability assessment is needed, this Record of Data Reliability Assessment (DRA) should be used to document the steps completed by the audit team to assess the reliability of the audit data, identify any limitations, and make a final determination of the overall reliability. One DRA should be completed for each analysis performed. If multiple data sources are assessed, **each** assessment should be summarized on this DRA.

Audit Number	Audit Title	
Director	Audit Manager	
Prepared by		
Date Prepared		

The Computer Matching and Privacy Protection Act (CMPPA) (5 USC 552(a)(8)) establishes reporting requirements regarding Computer Matching Agreements (CMA). TIGTA maintains a CMA with the IRS and is required to report all CMA-related computer matches for which it has been either the source agency or recipient agency. This only includes data matches where the primary purpose of the match would impact Federal benefits (i.e., the primary purpose is to find wrongdoing by IRS employees). Data matches performed where the primary purpose is program-related (i.e., to identify issues/control weakness of IRS operations or programs) are not applicable. Therefore, it is expected the majority of computer matches performed by OA would not be reported for the CMA. Coordination with Counsel Office to determine whether the Computer Matching and Privacy Protection Act provisions are applicable before proceeding with the project may be necessary.

Data Source #1
Name:
Description:
Time period covered:

Data from this source are expected to be used in the final report in the following manner:

- ☐ Sole support for findings, conclusions, or recommendations
- ☐ One of multiple sources of evidence to support the findings, conclusions, or recommendations
- ☐ Contextual or background information that is expected to materially affect the report's findings, conclusions, or recommendations

Indicate which of the following steps were completed during the reliability assessment from this data source.
Detailed documentation for each step should be included on the following pages

- ☐ Review of related documentation
- ☐ Interviews with knowledgeable agency officials
- ☐ Review of related internal controls
- ☐ Traced selection or random sample to or from source (e.g., IDRS, AIMS Table 37)
- ☐ Electronic or manual data testing for missing data, outliers, or obvious errors
- ☐ Other (explain):

NOTE: Not every item/step below will be applicable or necessary for all data sources. Please complete the items below, when appropriate.

Describe from where/how the data was obtained.

Briefly describe/list the data fields assessed from this data source (e.g., TIN, MFT, date). Only data fields used in the analysis and results need to be assessed.

TM link to data request with extract criteria:

TM link to Information Services Data Delivery and Validation form received from SDS or to IRS Data Delivery and Validation form:

If this data has been used in the past, describe (or provide TM links to) reliability results that are applicable to the current reliability assessment for the audit purpose. Include links to relevant prior reports or data reliability assessments.

Describe (or provide TM links to) any results from a review of related documentation that pertains to the reliability of the data being assessed (e.g., data dictionaries, data book, internal IRS system documents).

Describe (or provide TM links to) any results of interviews or other correspondence with agency officials related to the reliability of the data being assessed. Include information on any testing/validation performed by the agency and their confidence with the data.

Describe (or provide TM links to) any review of related internal controls that could affect the reliability of the data.

Describe (or provide TM links to) any results from a traced selection or random sample of records to or from the source (e.g., IDRS, AIMS Table 37).

Describe (and/or provide TM links to) results from applicable electronic data testing on key fields.

TM Link

Test

- ☐ All fields requested were received

Comments:

- ☐ Record count equals what was expected/documented

Comments:

- ☐ Missing records/missing or obviously invalid values

Comments:

- ☐ Erroneous duplicates

Comments:

- ☐ Range

- ☐ Do values fall within specified limits?
- ☐ Do values include the FULL RANGE expected?
- ☐ Do values for date fields fall within the expected/requested timeframe?
- ☐ Do values for date fields include the FULL RANGE of the requested timeframe?
- ☐ Are there negative numbers when there shouldn't be?
- ☐ Are there values of zero when there shouldn't be?

Comments on Range:

- ☐ Frequencies

- ☐ Does the frequency make sense logically given the auditor's knowledge?
- ☐ Are there an excessive number of missing/blank or obviously invalid values for a field?
- ☐ Are there an excessive number of zero values for a field?
- ☐ Are there duplicate values for a field when there should not be?

-
-
-
-
- ☐ Are there values of a field that do not correspond with the documented possible values (i.e., invalid values)?
- ☐ Are there values of a field that were expected but did not appear in the frequency counts?

Comments on Frequencies:

☐ Outliers

-
-
-
-
- ☐ Does the maximum value of a field seem reasonable?
- ☐ Are there an excessive number of extremely large values for a field?
- ☐ Does the minimum value seem reasonable?
- ☐ Are there an excessive number of extremely small values for a field?

Comments on Outliers:

☐ Other

-
-
-
-
- ☐ When applicable, does the record layout of the imported data equal the official record layout provided/received?
- ☐ Do the average values of the data elements seem reasonable?
- ☐ Are there "impossible" values for combinations of fields (crosstabs)?
- ☐ If there should be sequenced values, are there gaps/missing records?
- ☐ Other. Please describe below.

Comments on Other:

Describe (or provide TM links to) other information that could affect the reliability of the data.

Describe (or provide TM links to) any limitations identified that may affect the overall reliability of the data.

Considering the results from all steps completed, indicate which of the following best describes the overall conclusion on the reliability of the data:

- ☐ All data elements assessed are sufficiently reliable for the purpose of this audit (the limitations, if any, are described above)
 - ☐ Some data elements assessed are sufficiently reliable and the limitations, if any, are described above. Those data elements that are not sufficiently reliable are excluded from this audit
 - ☐ No data elements are sufficiently reliable for the purpose of this audit, and they are excluded from this audit
 - ☐ Undetermined reliability; limitations and their effect are described above
 - ☐ Other (e.g., primary objective was to assess the reliability of a system or part of a system) (explain):
-

NOTE: Please add additional pages if more than one data source was used for this audit.

Assessing the Reliability of Computer-Processed Data

Many Office of Audit (OA) reviews involve the extraction, analysis, and testing of computer-processed data in order to meet one or more objectives. Auditors should be aware of the potential risks associated with computer-processed data. Auditors who use these data to support findings must assure that the data are reliable. In this context, data reliability means that data are reasonably **complete** and **accurate**, meet the intended purposes, and are not subject to inappropriate alteration. Auditors are not expected to ensure that all possible errors are detected, but that the data are sufficient and appropriate for their specified purpose. The auditor's judgment in relying on system controls, selecting data testing methods, and determining the extent of data testing is critical to ensuring the integrity of TIGTA's audit products.

The audit team should assess data reliability if the data to be analyzed are intended to support audit results, findings, conclusions, or recommendations. Some data used only as background information, such as data requested from a source and used in a table, may not require an assessment. A determination of the best approach to satisfy Generally Accepted Government Auditing Standards (GAGAS) requirements will be made on an audit-by-audit basis. The results and basis for assessing the reliability of computer-processed data must be documented in the workpapers and the audit report.

When a data reliability assessment is required, the audit team will include general steps in the Audit Plan to assess the reliability of computer-processed data. When completing the assessment, the audit team should perform those tests considered necessary to support an opinion on the data reliability and to accomplish the overall objectives of the audit. Depending on the purpose for which the data will be used, not every step will be applicable or necessary for all data sources. The framework for the data reliability assessment process includes:

- Plan the assessment by reviewing information from the agency, Government Accountability Office (GAO), and other sources (e.g., existing reports, data dictionaries, etc.) to determine if the data are appropriate.
- Conduct the data assessment with appropriate mix of work. This includes, but is not limited to: reviewing existing information, interviewing knowledgeable agency officials, tracing samples, electronic testing, and reviewing selected system controls.
- Make the final data reliability determination. If enough information was obtained for a determination, determine if the data is sufficiently reliable, not sufficiently reliable, or undetermined reliability for the purposes of the audit. If not enough information was obtained, request more information. If the reliability of the data is undetermined, the report should make the limitations of the data clear so incorrect or unintentional conclusions will not be drawn from the data. For example, the report should indicate how

¹ In the context of data reliability, **completeness** refers to the extent that all relevant data records are present and that the fields in each record are populated appropriately. **Accuracy** refers to the extent that recorded data reflect the actual underlying information.

Assessing the Reliability of Computer-Processed Data

the use of the data could lead to an incorrect or unintentional message.

Computer-processed data includes data obtained from many different sources. It may be data entered into a computer system or resulting from computer processing. Examples include:

- Data extracts from databases or data warehouses (e.g., DCW, CDW)
- Data maintained in Excel, Access, or similar products
- Data extracts from enterprise software applications (e.g., SAAS, ANMF)
- Public use data that is accessible through an application other than the original source (e.g., datasets from www.data.gov)
- Data collected from forms and surveys on web portals
- Data summarized in a report or copied from a table
- Data provided by other Federal Agencies

Data may be obtained from DCW, SDS, IRS, or external entities.

Complete the Record of Data Reliability Assessment

Generally, a data reliability assessment is performed as early as possible in the audit. Examining the information early is necessary to help the team determine whether the data would be appropriate for addressing the objectives in the first place. The process is likely to differ from one audit to another. However, it should include sufficient work to allow the auditor to have a good understanding of how the data were collected, the systems they were extracted from, and the process and system controls related to the key data elements for the engagement.

To document the analysis performed to assess the reliability of computer-processed data, the audit team should complete the Data Reliability Assessment (DRA). One DRA should be completed for each analysis performed and should include summary information for all data sources used.

During the DRA process, the auditor or analyst may identify issues that result in limitations to the data and/or expected analysis to be performed. Any issues or impediments identified should be documented in the DRA. Further, if data is determined to be unreliable or to have undetermined reliability, the audit team should discuss with management the best approach of how to proceed.

Perform Electronic Testing on Key Fields

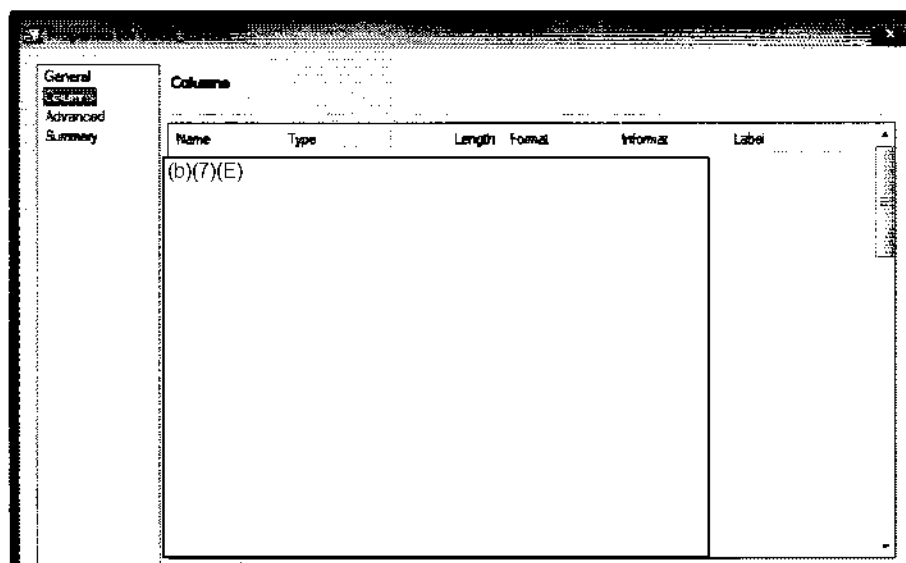
A major part of assessing the reliability of computer-processed data includes electronic testing of the data. Electronic testing need only be completed on the fields used in the analysis and should ensure that the data elements are complete, accurate, and reasonable for the purposes used in the audit. It is most effective when performed on a detail level data rather than summary level. The DRA includes many of the tests that should be considered.

Assessing the Reliability of Computer-Processed Data

The following discussion includes some, but not all, of the techniques that might be performed during electronic testing. There is some overlap and some SAS techniques may satisfy more than one type of electronic test.

Data Completeness

When computer-processed data is used to support audit findings, conclusions, or recommendations, **audit teams are responsible for confirming that the data is complete.** There are several simple steps that can be performed when assessing the completeness of the data. First, the auditor can check to confirm that the dataset contains all the data fields requested (e.g., from a DCW query, in a Form 7550, or in a formal request to IRS). In SAS this can be accomplished by inspecting the results from SAS column names and comparing them to the data fields requested in a Form 7550 or the formal request sent directly to the agency. To view details on columns in SAS EG, right click on the SAS dataset, select "Properties", then select "Columns". This technique is useful to confirm that the record layout of the dataset matches the specifications of the data fields that were requested.



Additionally, the auditor or analyst should confirm that the actual record count of the data received and assessed equals what is expected. If the actual record count does not agree with the expected record count, there are several possible explanations for the discrepancy. How the auditor or analyst handles the discrepancy should depend on the source. Sources of discrepancies could include:

- There was an error when data was created/output (e.g., an oversight was made when the file was created by IRS, the logic in the DCW query was flawed, etc.)
- There was an error made during the process in which the data was input in SAS
- There was a typo/error in the documentation and the record count is different than originally indicated

Assessing the Reliability of Computer-Processed Data

It is important to note that the auditor or analyst should not assume data pulled from DCW or received from SDS has every record needed. DCW validates record counts against IRS source systems to ensure they extracted all records. However, the source data may not contain the records needed. For example, Masterfile tables on the DCW do not contain all tax modules. Tax modules drop to different retention levels when those modules are full paid or meet other conditions

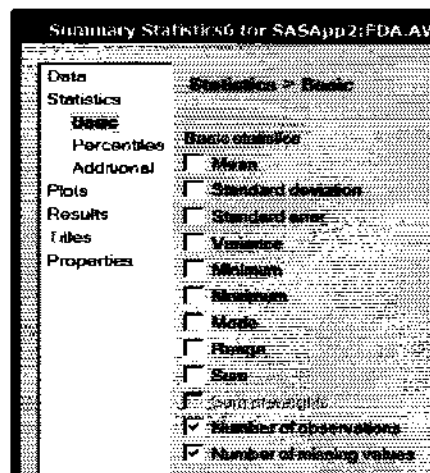
Missing or Obviously Invalid Values

SAS generally has two types of data—character and numeric. Date and date/time fields are considered numeric in SAS. When using the defaults, SAS represents missing values for character fields with a blank. Missing values for numeric fields are represented with a period (.).

Generally speaking, a small number of missing/blank or obviously invalid values in a field is acceptable. If a large number occurs (e.g., more than 5% of the records), it could be an indication that there is something wrong with the data. In some circumstances, it may mean the data should be re-extracted. The audit team should discuss if the large number of missing/blank or obviously invalid values could affect (i.e., limit) the results of the analysis or be an impediment in any way and it should be documented in the DRA.

There are a number of different ways to determine if fields contain missing values. To identify missing data in a field using SAS EG, you can query your dataset and apply a filter on the field(s) using the operator “Is Missing”.

Another SAS EG technique is to perform the Task “Describe”, then select “Summary Statistics”. In the option Statistics, Basic (see below) select the options “Number of missing values”. Additionally selecting the “Number of observations” can provide a nice basis to determine the percent of missing values for a field. This technique is useful to determine the number of missing values for a list of fields simultaneously.



To determine if any records are missing in a sequence (e.g., a gap analysis) the SAS function MONOTONIC() function can be extremely useful. The

Assessing the Reliability of Computer-Processed Data

function allows the user to identify gaps in a dataset for a field with assigned sequential numbers (e.g., case numbers, invoice numbers). For example, to determine if cases are missing from a dataset which uses sequential case numbering, first ensure the dataset is sorted in ascending order by the case number column. Next, within Query Builder, create a Computed Column using the MONOTONIC function and run the Query Builder.

Enter an expression:

monotonic()

Create an additional, new query to compare the assigned case numbers to the MONOTONIC case numbers by creating another Computed Column and subtracting the MONOTONIC case number from the assigned case number. A gap is identified each time the difference between the assigned case number and the Monotonic case number increases. The example below indicates case number 221 was missing from the assigned case numbers because its value went from 0 to 1. Subsequently, the next identified assigned case number missing was 1282, because "Diff Row Calc" went from 1 to 2.

	ca_y	AssignedCaseNumber	MONOTONIC	DiffRowCalc
220	2014			0
221	2014	(b)(7)(E)		(b)(7)(E)
222	2014		222	1
223	2014		223	1

	ca_y	AssignedCaseNumber	MONOTONIC	DiffRowCalc
1280	2014		(b)	1
1281	2014	(b)(7)(E)	(7)((b)(7)(E)
1282	2014		1282	2
1283	2014		1283	2

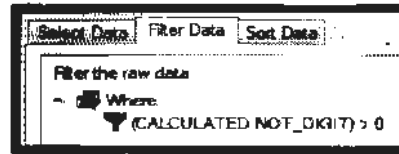
There are also a number of methods to determine if there are obviously invalid values for a field(s). For example, to determine if a field contains characters that are not numerals, the SAS function NOTDIGIT is applied. The function searches a character string for any character that is not a digit and returns the first position at which that character is found. Within Query Builder, create a Computed Column using the appropriate NOTDIGIT function syntax [i.e., NOTDIGIT(data element)]

Enter an expression:

(b)(7)(E)

Once the Computed Column is created, filter the raw data where the NOTDIGIT value is greater than zero. This filter is necessary because all valid TINs should have a NOTDIGIT value equal to zero.

Assessing the Reliability of Computer-Processed Data



The output dataset will therefore identify TINs that have invalid characters. When using NOTDIGIT to identify invalid TINs, the length of the TIN field should already be nine characters. Otherwise, false positives may be identified since extra spaces (including leading and trailing spaces) are also treated as characters that are not digits. Example output where the NOTDIGIT function is greater than zero is:

	TIN	NOT_DIGIT
1	(b)(7)(E)	
2		
3		

Erroneous Duplicates

A duplication of records sometimes occurs in datasets. In many circumstances duplicate records are expected and acceptable. It should be determined if there are erroneous duplicates that may be an impediment to the analysis and/or affect the reliability of the data and it should be documented in the DRA. For example, in some instances, a taxpayer files their tax returns in one cycle and it is re-sequenced and filed in a later cycle. This causes two entries for this taxpayer with the same DLN but with different filing cycles. These duplicate records need to be identified before data is analyzed.

It should be noted that in some cases—especially extracts of a larger database, two or more records may appear to be duplicates. In actuality, there may be a separate field that was not obtained which differs for the two records. Additionally, in some circumstances, users may inadvertently introduce duplicates during the analysis. For example, if only a portion of the closed Audit Information Management System (AIMS) record is used rather than the entire AIMS record, it can appear that the AIMS dataset may have duplicate records. This can occur when taxpayers make multiple assessments in a fiscal year on the same tax year, but the assessment and disposal information are stripped off by the user during a query. The circumstance of “false duplicates” should be considered and it should be evaluated if additional data is required for the analysis and/or if it should be treated as a duplicate.

The audit team should discuss if it is believed there is an excessive number of erroneous duplicates in the data, what the repercussions to the analysis might be, and if any actions should be taken. It should also be documented in the DRA.

Using SAS, the user can remove duplicate records but should never do so blindly. Further, removing records from a dataset should always be documented, including the reason for removal. Duplicates can also be

Assessing the Reliability of Computer-Processed Data

identified and kept as a separate dataset for later review.

One of these SAS EG techniques is applying the SAS function COUNT * Aggregate. This function returns the number of records in a table without any duplicate elimination. Within Query Builder, create a Computed Column using the appropriate COUNT * Aggregate function syntax [i.e., COUNT(*)].

Once the Computed Column containing the COUNT * Aggregate function is created, confirm that it is included in the output data containing the records that you want to count. In the example below, a record is comprised of

(b)(7)(E)

(b)(7)(E)

Select Data	Filter Data	Sort Data	
Column Name	Source Column	Summary	Details
(b)(7)(E)			COUNT(*)

The output dataset will result in a table containing no duplicate records. However, the Computed Column will identify the number of times each record appeared in the original dataset. As shown in the example below, the records in the first and second rows appeared multiple times in the original dataset. Information about the number of duplicate records from the original table and the specific records that were duplicated may identify additional findings and areas for further investigation.

(b)(7)(E)	COUNT
	3
	2
	1
	1

Range Tests During electronic testing, range tests should be performed on key fields. Questions to evaluate for the data include:

- Do values fall within specified limits?
Checks should be made to see if all values are within the specified or expected range.

For example, suppose a request was made to extract data for taxpayers with Federal withholdings between \$10,000 and \$50,000. When the data is received, the user should test the data

Assessing the Reliability of Computer-Processed Data

for this criterion. If there are values outside less than \$10,000 or more than \$50,000, then there is likely an issue with the extract that should be addressed.

- Do values include the FULL RANGE expected?
Checks should be made to see if the values of the data span the full spectrum of what was expected.

For example, if data on closed cases is requested from the Automated Underreporter (AUR) Program, and prior meetings with IRS officials have identified that the AUR Program completes cases on three tax years concurrently, does the data include cases from three tax years?

- Do values for date fields fall within the expected/requested timeframe?

For example, if Fiscal Year 2015 data is requested, was data for Calendar Year 2015 received (i.e., are there values that are not inside the date range from October 1, 2014 to September 30, 2015)?

- Do values for date fields include the FULL RANGE of the requested timeframe?

For example, if for three fiscal years was requested, was one or more quarter inadvertently left out?

- Are there negative numbers when there shouldn't be?
When combining more than one dataset, how a negative value is represented is very important.

For example, if a debit is represented in one dataset as a negative value but not in another, combining the two and summing the fields can lead to erroneous results.

- Are there values of zero when there shouldn't be?
Values of 0 should be examined closely. Sometimes a value of 0 is, in actuality, representative of a missing value. In other situations, the user may be expecting all dollar values to be positive, but some values of 0 were inadvertently included.

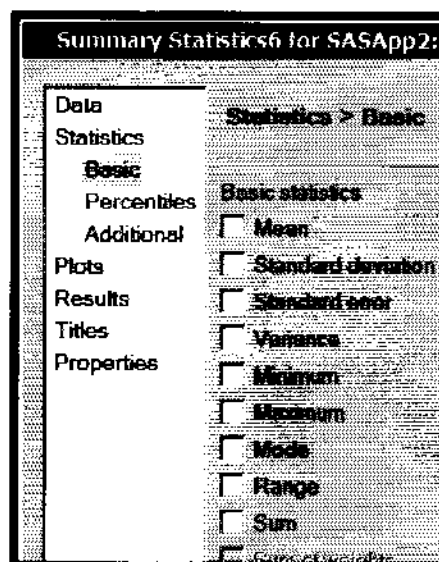
- Are values missing a decimal point—i.e., do the data contain an implied decimal point?
Sometimes data extracts are missing decimal points and/or the decimal is implied. In these situations the amounts are overstated since the true values are the amounts divided by 100. Auditors should check totals with IDRS to ensure amounts are accurately represented.

Any issues that would affect or be an impediment to the analysis for the audit should be discussed among the audit team and decisions should be made of how it is best to proceed. It should also be documented in the DRA.

Using SAS EG to perform a range test is very simple and can be performed

Assessing the Reliability of Computer-Processed Data

by multiple techniques. A user can use Query Builder and create field(s) containing the Minimum and Maximum Value for a field(s). Additionally, a user can perform the Task "Describe", then select "Summary Statistics". In the option Statistics, Basic (see below) select the Basic Statistics options of interest (e.g., Minimum, Maximum, Range).



Frequency Tests

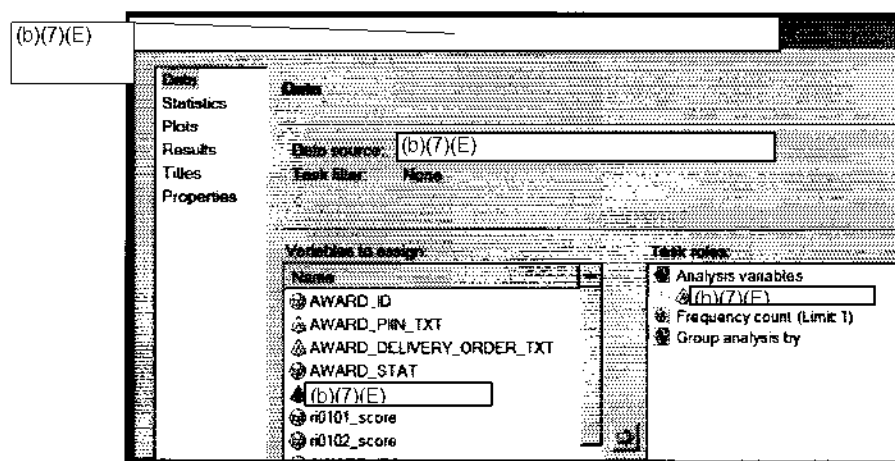
During electronic testing, frequency tests should be performed on key fields. Questions to evaluate for the data are found below. Techniques used to answer some of these questions overlap with other tests performed, depending on the order of the electronic testing.

- Does the frequency make sense logically given the auditor's knowledge? In general, does the frequency of occurrences meet expected outcomes in planning? Are there an excessive number of missing/blank values for a field?
Generally speaking, a small number of missing/blank or obviously invalid values in a field is acceptable. If a large number occurs (e.g., more than 5% of the records), it could be an indication that there is something wrong with the data. In some circumstances, it may mean the data should be re-extracted. The audit team should discuss if the large number of missing/blank or obviously invalid values could affect (i.e., limit) the results of the analysis or be an impediment in any way and it should be documented in the DRA.
- Are there an excessive number of zero values for a field?
Similar to the issue with missing/blank or obviously invalid values, a large number of zero values for a field should be discussed among the audit team. If a large number occurs (e.g., more than 5% of the records), it could be an indication that there is something wrong with the data. In some circumstances, it may mean the data should be re-pulled. The audit team should discuss if the large number of zero values could affect (i.e., limit) the results of the analysis or be an impediment in any way and it should be documented in the DRA.

Assessing the Reliability of Computer-Processed Data

- Are there duplicate values for a field when there should not be? For example, in many cases a field such as invoice number should have a unique value for all records. Issues identified during testing for duplicate values should be addressed and handled similarly to duplicate records.
- Are there values of a field that do not correspond with the documented possible values (i.e., invalid values)? Are there Null values, *, or other special characters or values that are not expected? For example, suppose a data dictionary indicates the possible values of a particular field are X, Y, and Z. If the data received have values of E, F, X, Y, and Z, it could be an indicator that the extract was not received as expected or that further research on the field/data needs to be done.
- Are there values of a field that were expected but did not appear in the frequency counts? For example, suppose an extract of records should include records from Tax Years 2014 and 2015. If the extract only contains records from Tax Year 2014, the Tax Year 2015 records may have inadvertently been left off the extract.

There are multiple techniques that use SAS EG to perform a frequency test. For performing a frequency test on data elements that have a **limited number** of possible values (e.g. Tax Year, State, Activity Code) the “One Way Frequency” tool can be used. To do this, the user selects the Task “Describe” and then “One Way Frequencies”. For the option “Data” in the leftmost window (see below) the user selects the fields of interest by dragging the field name from the “Variables to assign” window to the “Analysis variables” in the “Task roles” window.



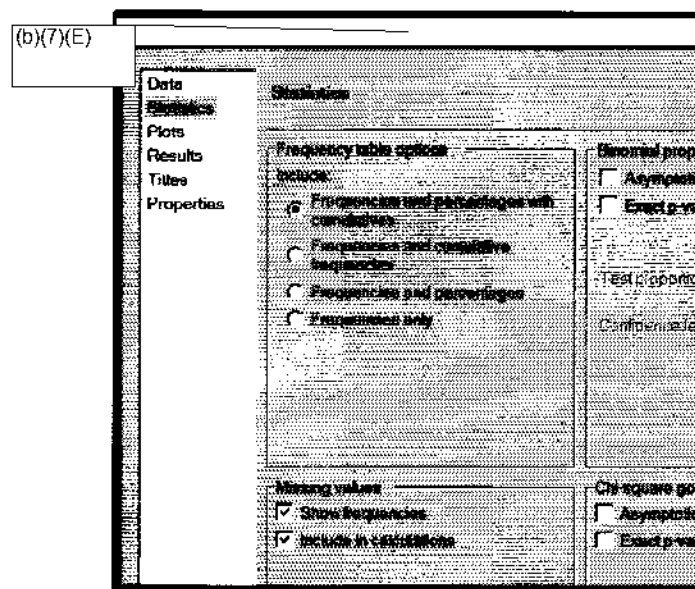
Next, the user defines what information to display in the output. For the option “Statistics” in the leftmost window (see below) the user selects the options to display by clicking a radial button under “Frequency table options include.”

Please note that when performing a frequency count, consideration should be given to how to treat missing values

Assessing the Reliability of Computer-Processed Data

and whether or not they should be included in the calculations of frequencies. For example, suppose a dataset has 4 records with a field containing the values A, B, C, and <missing>. When calculating the frequencies, should the frequency of A, B, and C be 33.3%, 33.3% and 33.3% or should you include missing values and have A, B, C, and <missing> as 25%, 25%, 25%, and 25%?

Continuing with the previous technique, the options can be chosen by the user checking the applicable box for the options listed under “Missing values.”



To perform a frequency test on data elements that have numerous possible values (e.g. (b)(7)(E) etc), the SAS function COUNT * Aggregate should be used. Similar to how we previously used this function to identify duplicate records, it can also be used to perform frequency counts on individual data elements. Within Query Builder, create a Computed Column using the appropriate COUNT * Aggregate function syntax.



Once the Computed Column containing the COUNT * Aggregate function is created, confirm that it is included in the output data set of the data element that you want to count. In the example below, a frequency count is being performed on the TIN.

Assessing the Reliability of Computer-Processed Data

Column Name	Source Column	Summary	Details
(b)(7)(E)			COUNT(*)

To ensure that the output dataset is sorted in descending order by frequency count, the user should sort by the computed column containing the Count * Aggregate function.

Column Name	Source Column	Sort Direction
COUNT	Computed	Descending

The output dataset will result in a table that identifies the number of times each appeared in the source dataset. As shown in the example below, this also includes missing values.

(b)(7)(E)

(b)(7)(E)	COUNT
	5
	4
	3
	2
	2

Outlier Tests

During electronic testing tests for outliers should be performed on key fields. In some cases, extreme values in numeric data variables may indicate invalid data. Questions to evaluate for outliers are found below. Techniques used to answer some of these questions overlap with other tests performed, depending on the order of the electronic testing.

- Does the maximum value of a field seem reasonable?
- Are there an excessive number of extremely large values for a field? Sometimes the maximum value for a field is reasonable, but the number of large values is not.

For example, in one situation it was determined that there were an excessive number of large values for a dollar amount field. The audit team found that the AIMS files on DCW showed 648 closed Estate Tax audits in FY 2013 where the Gross Estate Amount exceeded \$1 Billion. It seemed very unlikely that 648 Billionaires died during that period. The team used (b)(7)(E) (b)(7)(E) to compare to AIMS and determined that the field in AIMS (b)(7)(E)

- Does the minimum value seem reasonable?
- Are there an excessive number of extremely small values for a field? Sometimes the minimum value for a field is reasonable, hut the

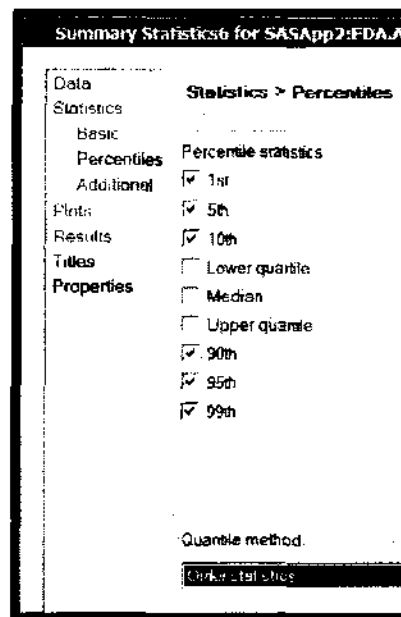
Assessing the Reliability of Computer-Processed Data

number of small values is not.

Extreme values can be identified by running simple queries, filters, tasks, and/or sorts in SAS EG.

Sorting the file and manually reviewing the first entry and last entry to ensure they are within the required range is one way to check the data. However, **for large datasets** (i.e. greater than 10 fields and over 100,000 records) **sorting should be avoided if possible**. If a sort is required and the file has a large number of fields, it would be best from a system resource standpoint to extract the data into a limited dataset and only sort on the fields needed. Sorting large datasets can take a lot of DCW system resources and space. When sorting, the dataset can grow three to six times its size as the system builds the sorted file.

To determine how many large or small values exist, one can evaluate the percentiles. One technique using SAS EG is to perform the Task "Describe", then select "Summary Statistics". In the option Statistics, Percentiles (see below) select the Percentile Statistics options of interest for small values and/or large values (e.g., the 1st, 5th, 10th and/or the 90th, 95th, 99th percentile options). If the percentile values seem reasonable, then an excessive number of small or large values is not an adverse issue.



Other Tests During electronic testing tests there are a number of miscellaneous questions which might be addressed:

- When applicable, does the record layout of the imported data equal the official record layout provided/received?
- Do the average values of the data elements seem reasonable?

Assessing the Reliability of Computer-Processed Data

- Are there ‘impossible’ values for combinations of fields (crosstabs)?
- If there should be sequenced values, are there gaps/missing records?
- Are there data elements with indications of potential truncation issues? (e.g. email addresses with missing and/or incomplete domains, incomplete phone numbers)

Other Steps in the Data Reliability Process

In addition to electronic testing, there are other steps in the data reliability assessment process that should be performed. The process is likely to differ from one audit to another. However, it should include sufficient work to allow the auditor to have a good understanding of how the data were collected, the systems they were extracted from, and the process and system controls related to the key data elements for the audit. Deciding which steps to take is iterative. Most often the auditor may start with the relatively simple steps of reviewing existing information and basic testing. The outcome of these steps may lead to other steps in order to gather enough information. The mix of steps taken depends on any potential weaknesses identified and circumstances specific to the audit, such as the importance of the data to the audit and corroborating evidence. Focus should be placed on the aspects of the data that pose the greatest potential risk for the audit.

Review Related Documents

A review of existing information helps the auditor determine what is already known about the data and the computer processing. The related information collected can indicate both the accuracy and completeness of the entry and processing of the data, as well as how data integrity is maintained. Sources for related information include the TIGTA, IRS, GAO, and others.

The first source of relevant information is TIGTA. There may be existing reports available and applicable. In addition to reports, there may be useful information collected from previously conducted data reliability assessments to inform the current assessment. The fact that an assessment already exists might be helpful but may not be sufficient for the current audit.

In addition to TIGTA, the IRS may have documents or information on system controls, data testing, user manuals, data dictionaries, or data quality assurance program manuals. There may also be GAO reports with relevant information.

Interview Agency Officials

The auditor should consider interviewing individuals with detailed knowledge about the data and the system that produces the data—either TIGTA or IRS personnel. The questions should focus on accuracy, completeness, internal controls, and leverage existing information, if available.

Assessing the Reliability of Computer-Processed Data

Potential reliability issues with the data can be identified in the initial steps of the assessment from interview questions, before further assessment work is performed. Interviewing agency officials early in the process about how appropriate the data are for the audit objections can help in making decisions as further work to assess the reliability of the data is planned. Agency officials are often aware of evaluations of their computer data or systems and usually can direct the auditor to them. However, keep in mind that information from agency officials may be biased.

Some example questions to ask include:

- Are there any known limitations on the data?
- How are data collected?
- What practices and controls, such as edit checks, help to ensure that data are entered and maintained accurately?
- Are there any controls separate from the system helping to ensure data quality?
- Do data owners or a contractor implement quality control practices, such as data verification to source documents?
- Are there any other concerns about the quality of the data?

Review Related Internal Controls

It is possible that if internal controls are inadequate it could directly affect the reliability of related data. To address issues in system controls the audit team might choose to

- Examine how data are controlled when entered into the system
- Examine controls relating to access to the system
- Explore if system disruptions have affected data integrity, especially completeness
- Evaluate controls that most directly affect the data, usually:
 - General controls (logical access and control of changes to the data)
 - Application controls (ensure that data are accurate and complete)

Trace Selection of Records to Source

In most circumstances a subset or sample of data should be traced to or from source records. In most cases a small judgmental sample of subset of the data records (at least 10) should be verified for accuracy against an appropriate system (e.g., IDRS) to ensure that the data meets the purposes of the audit tests. For example, if the review involves a refund on a tax return, IDRS can be used to confirm whether the refund was actually issued.

Make the Reliability Determination

There are many factors to consider when deciding whether the data is sufficiently reliable for the audit purpose. The primary factors to consider include the expected importance of the data to the final product, the

Assessing the Reliability of Computer-Processed Data

strength or weakness of any corroborating evidence, and the anticipated level of risk in using the data.

Before making a decision about the reliability of the data, consider the results of all the steps taken to conduct the assessment. Appropriately document and review the results before entering into the decision-making phase of the assessment because these results will, in whole or in part, provide the evidence that support the conclusion. After weighing all the factors, the audit team should come to an agreement on the assessment of the reliability of the data for the purposes of the audit.

The assessment should generally result in one of the following decisions:

- The data are sufficiently reliable for the audit purpose
- The data are not sufficiently reliable for the audit purpose
- The data has undetermined reliability for the audit purpose

When the assessment provides assurance that the data are reasonably complete and accurate and therefore sufficiently for the audit purpose, the data should be used and the auditor should disclose and document the work completed to assess the data's reliability, along with any limitations of the data.

The assessment should result in a decision that the data are not sufficiently reliable when the results indicate that the data are unacceptably incomplete and/or inaccurate and could possibly lead to an incorrect message. In that circumstance the audit team should not use the data for the assessed audit purpose and the team should explore other options, including modifying the engagement question or approach or seeking other sources of data. In some cases, the results should be reported or explored further in another audit. It is important to note, that data can be determined to be unreliable for one purpose but reliable for a different purpose.

Data can be considered of undetermined reliability when the work has provided too little information to judge reliability, there is limited access or no access to information about the data source, or there is a wide range of data that may be impossible to examine. In those cases, the auditor should consider whether using the data will result in an inaccurate or misleading message. If so, the data should not be used for the audit purpose unless circumstances force the use. In that case, all limitations and how the limitations affect the interpretation of the data should be clearly documented.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

**INSPECTOR GENERAL
 for TAX
 ADMINISTRATION**

October 18, 2016

DIGA: 17-003
MEMORANDUM FOR ALL OFFICE OF AUDIT EMPLOYEES

Michael E. McKenney

FROM: Michael E. McKenney
 Deputy Inspector General for Audit

SUBJECT: Office of Audit Fiscal Year 2017 Performance and Workload Measures

Fiscal Year 2016 was another productive year for the Office of Audit (OA). We issued 107 audit reports and other products that included potential financial benefits of more than \$14.5 billion and affected more than 1.1 million taxpayer accounts. In terms of our total financial outcomes, we exceeded our goal by more than \$13.3 billion. We also identified reportable outcome measures in 49 percent of our reports versus 41 percent in FY 2015. In addition, we exceeded our goal for the number of final reports/other products issued by six and exceeded our FY 2015 total by 11. I would like to thank each of you for your contributions in helping us accomplish these results.

For FY 2017, we will continue to identify opportunities for the IRS to improve the administration of the Nation's tax laws and achieve program efficiencies and cost savings. Besides maintaining the emphasis on the impact of our audit reports, we will also focus on improving other aspects of our operational performance. One area we continue to emphasize is the issuance of our reports proportionally throughout the year. We issued approximately 47 percent of our reports and other products in the last quarter of the year compared to 42 percent in FY 2015.

The OA-wide FY 2017 report, outcome measure, workload measure, and other goals are summarized on the following pages.

Goals for FY 2017

Report and Outcome Measures		2017 Goal
Final Reports Issued		101
Total Financial Benefits		\$1.256 billion
• Total Cost Savings	\$125 million	
• Increased Revenue/Revenue Protection	\$940 million	
• Taxpayer Rights and Entitlements	\$169 million	
• Inefficient Use of Resources	\$22 million	
Percentage of Final Reports With Quantifiable Outcomes		35%
Percentage of Final Reports With Cost Savings		10%
Taxpayer Accounts Impacted		3.60 million
Workload Measures		2017 Goal
Average Staff Days to Issue Final Audit Report		350
Average Calendar Days to Issue Final Audit Report		325
Percentage of Audits Meeting Planned Staff Days		70%
Other		2017 Goal
Percentage of Past Recommendations Implemented (look back four years to identify percentage of recommendations completed)		85%
Percentage of New Audit Products Issued With Recommendations		70%
Percentage of Audit Products Delivered When Promised to Stakeholders (met planned draft due dates)		68%

- **Report Goal:**

Final Reports Issued (includes congressional testimonies, integrity projects, and other products) – 2017 Goal = 101: The FY 2016 goal was also 101 reports.

- **Outcome Measure Goals:**

Financial Benefits – 2017 Goal = \$1.256 billion: This goal consists of:

- \$125 million in *Cost Savings*.
- \$940 million in *Increased Revenue and/or Revenue Protection*.
- \$169 million in *Taxpayer Rights and Entitlements*.
- \$22 million in *Inefficient Use of Resources*.

This goal is consistent with our FY 2016 goal. In FY 2016, we reported more than \$14.5 billion in financial benefits. After considering results from FYs 2012 through 2016, the OA-wide goals were determined to be reasonable and achievable targets.

In FY 2017, our goal is to issue 35 percent of all final reports with quantifiable outcomes, with 10 percent of the reports with cost savings. This goal remains the same as our FY 2016 goal. In FY 2016, 49 percent of our non-DCAA reports contained quantifiable outcomes, and 4 percent had cost savings.

Taxpayer Accounts Impacted – 2017 Goal = 3.6 million: This goal consists of the following components: *Taxpayer Rights and Entitlements, Taxpayer Burden, Taxpayer Privacy and Security, Increased Revenue and/or Revenue Protection, and Protection of Resources and/or Reliability of Information.*

The 3.6 million goal is consistent with our FY 2016 goal. In FY 2016, our reports cumulatively impacted more than 1.1 million taxpayer accounts. While we have established business unit goals related to the overall 3.6 million goal, we have not established any specific goals either OA-wide or for the business units for any of the five components. Similar to the financial benefits goal, the components of Taxpayer Accounts Impacted varied significantly by year and business unit; therefore, we established business unit goals for only the overall 3.6 million goal.

- **Workload Measure Goals**

Staff Days – 2017 Goal = Average of 350 Days: This goal remains the same as our FY 2016 goal. Our actual result for FY 2016 showed we averaged 306 staff days per audit.

Calendar Days – 2017 Goal = Average of 325 Days: This goal remains the same as our FY 2016 goal. Our actual result for FY 2016 showed we averaged 344 calendar days per audit.

Percentage of Audits Meeting Planned Staff Days – 2017 Goal = 70%: This goal remains the same as our FY 2016 goal. Our actual result for FY 2016 showed we met our planned staff days 77 percent of the time.

- **Other Goals**

Many of the benefits that result from our work cannot be measured in dollars. To form a broader picture of OA accomplishments and our impact on tax administration, we implemented additional measures in FY 2007 to assess our performance.

Percentage of Past Recommendations Implemented – 2017 Goal = 85%: Another way to measure our effect on improving the Internal Revenue Service's (IRS) accountability, operations, and services is by tracking the percentage of recommendations we made four years ago that have since been implemented. The goal for FY 2017 remains the same as our FY 2016 goal. For FY 2016, the actual result for this measure was 97 percent. Because the IRS needs time to act on recommendations, we will assess recommendations implemented after four years.

This is the point at which we believe that if a recommendation has not yet been implemented, it is not likely to be.

Percentage of New Audit Products Issued With Recommendations –

2017 Goal = 70%: In FY 2007, we began tracking the percentage of new products with recommendations because we wanted to encourage staff to develop recommendations that, when implemented by the IRS, will produce financial and other benefits for tax administration. For FY 2016, the actual result for this measure was 83 percent. By establishing a goal of 70 percent for FY 2017 (unchanged from our FY 2016 goal), we recognize that our products do not always include recommendations and that the IRS, Congress, and other stakeholders also find informational reports useful. Our informational reports have the same analytical rigor and meet the same quality standards as those with recommendations and, similarly, can help to bring about significant financial and other benefits. Therefore, this measure allows us ample leeway to respond to requests that result in reports without recommendations.

Percentage of Audit Products Delivered When Promised to Stakeholders –

2017 Goal = 68%: This goal measures the timely delivery of our audit products, as calculated by audits meeting the planned draft report date. Draft reports provide IRS management with the formal results and recommendations of our audits, so we will use the draft report as our measurement of audit products delivered to stakeholders. The goal for FY 2017 remains the same as our FY 2016 goal. In FY 2016, we delivered our audit products when promised 75 percent of the time.

Impact of Measurement Changes

The FY 2017 report, outcome measure, workload measure, and other goals will help us assess the value and impact of our work. Through these measures, we plan to have a positive impact on the IRS, other stakeholders, and the Treasury Inspector General for Tax Administration, as follows:

- External Impact.
 - Identify financial benefits.
 - Affect taxpayer accounts.
 - Improve IRS programs and operations.
 - Increase the use and awareness of TIGTA and its products.
- Internal Impact.
 - Improve the timeliness, efficiency, and effectiveness of our efforts.
 - Recognize the realized results of our efforts.
 - Increase our own strategic and corporate planning efforts.

If you have any questions, please contact Jeff Jones, Director, Office of Management and Policy, at (781) 254-1830.