TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Significant Progress Has Been Made in Implementing an Enterprise Risk Management Program

July 12, 2016

Reference Number: 2016-10-051

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

SIGNIFICANT PROGRESS HAS BEEN MADE IN IMPLEMENTING AN ENTERPRISE RISK MANAGEMENT PROGRAM

Highlights

Final Report issued on July 12, 2016

Highlights of Reference Number: 2016-10-051 to the Internal Revenue Service Chief Risk Officer.

IMPACT ON TAXPAYERS

As a result of concerns regarding the IRS's previous use of inappropriate criteria in reviewing of organizations applications for tax-exempt status, the Acting IRS Commissioner reported in June 2013 that a series of actions have been identified to improve performance and accountability within the IRS. These actions included implementing a formal Enterprise Risk Management program to better identify emerging risks and mitigate them before they impact performance. Effective risk management can help the IRS more effectively administer our nation's tax system.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the IRS's efforts to implement a comprehensive process for identifying and mitigating significant risks to effective tax administration.

WHAT TIGTA FOUND

The IRS has made significant progress in its efforts to implement an Enterprise Risk Management program to provide a structured framework for the identification and mitigation of significant organizational risks.

Steps already completed include appointing a Chief Risk Officer and establishing an embedded risk management structure within each of the IRS's four operating divisions and 20 functional offices. In addition, the IRS established a Risk Working Group (which includes representatives from the operating divisions and functional offices) and an Executive Risk Committee (comprised of IRS senior management) to facilitate collaboration on risk evaluation decisions.

In October 2014, the IRS completed an initial agency-wide risk assessment focused on using a high-level, top-down approach to identify and provide insight on enterprise risk areas. In December 2015, the IRS completed its second agency-wide risk assessment. The purpose of this assessment was to review risk areas across the organization in more depth, identify the top areas of risk impacting the IRS, and develop a coordinated agency-wide approach to addressing these risk areas. Based on this analysis, 12 top enterprise risk areas were identified. The IRS plans to complete another agency-wide risk assessment in Fiscal Year 2016.

Steps in process include integration with the IRS's strategic planning, budgeting, and internal controls processes and actively monitoring program performance. The IRS is also working to establish risk tolerance guidelines to assist in determining acceptable levels of risk associated with various IRS business decisions. Finally, the IRS is working to develop metrics, known as key risk indicators, to assist in signaling potential emerging risks.

WHAT TIGTA RECOMMENDED

TIGTA did not make any recommendations as a result of this review. However, key IRS officials reviewed this report prior to its issuance and agreed with the facts and conclusions presented.

.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

July 12, 2016

MEMORANDUM FOR CHIEF RISK OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Significant Progress Has Been Made in Implementing an Enterprise Risk Management Program (Audit # 201510009)

This report presents the results of our review on how Significant Progress Has Been Made in Implementing an Enterprise Risk Management Program. The overall objective of this review was to evaluate the Internal Revenue Service's (IRS's) efforts to implement a comprehensive process for identifying and mitigating significant risks to effective tax administration. This audit is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Achieving Program Efficiencies and Cost Savings.

The Treasury Inspector General for Tax Administration made no recommendations as a result of the work performed during this review. However, key IRS officials reviewed this report prior to its issuance and agreed with the facts and conclusions presented.

If you have any questions, please contact me or Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations).

Table of Contents

Abbreviations

COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
ERC	Executive Risk Committee
ERM	Enterprise Risk Management
FY	Fiscal Year
IRS	Internal Revenue Service
OMB	Office of Management and Budget
RWG	Risk Working Group
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) is a large and complex organization that faces significant ongoing risks in the delivery of its tax administration mission. The risks that the IRS faces are both external and internal. For example, the IRS faces risks in having to manage a growing workload with substantially fewer employees. Other risks include those related to recent extensive tax law changes, the growing impact of international tax law issues, increasing sophistication of efforts to evade tax compliance, and cyber threats to IRS taxpayer data.

The risks that the IRS faces are both external and internal. For example, the IRS faces risks associated with having to manage a growing workload with substantially fewer employees.

In May of 2013, the Treasury Inspector General for Tax Administration (TIGTA) reported that the IRS used inappropriate criteria that identified for review organizations applying for tax-exempt status based upon their names or policy positions instead of indications of potential political campaign intervention. Subsequently, in late May 2013, the President and the Secretary of the Treasury installed new leadership at the IRS and directed a number of actions, including comprehensive corrective actions to address the problems with the IRS's review of tax-exempt applications as well as an assessment to identify ways to improve IRS operations broadly.

On June 24, 2013, the Acting Commissioner of the IRS issued a report, *Charting a Path Forward at the IRS: Initial Assessment and Plan of Action*. This report included a review of IRS operations and risks and identified a series of actions intended to improve performance and accountability by ensuring that critical program or operational risks are identified early, raised to the right decision-makers in the organization, and are timely shared with external stakeholders. These actions include implementing a formal Enterprise Risk Management (ERM) program to better identify emerging risks and mitigate them before they impact performance. Effective risk management can help the IRS more effectively administer our Nation's tax system. The purpose of the IRS's ERM program is to provide a structured framework for the identification and mitigation of significant risks before they impact performance.

ERM is an emerging discipline that implements across the organization a process designed to identify potential events that may affect the organization and to manage risk to provide reasonable assurance regarding the achievement of objectives.[1] A fundamental concept of ERM is that it considers activities at all levels of the organization and identifies entity-wide risks. This

[1] The Association for Federal Enterprise Risk Management defines ERM as a discipline that addresses the full spectrum of an organization's risk, including challenges and opportunities, and integrates them into an enterprise-wide, strategically aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals, and objectives.

structure is supported in some organizations, especially those that are larger and more complex, by a dedicated executive and staff specifically responsible for organizational risk management.

The IRS's Fiscal Year[2] (FY) 2014–2017 Strategic Plan delineates the primary objective for the ERM program: *To implement and maintain a robust ERM program that identifies emerging risks and mitigates them before they impact performance*. Strategies specified by the plan in support of this objective include:

- Create governance structures, policies, procedures, and training to serve as the framework for the enhanced risk management program.
- Enhance the flow of communication between all layers of management to ensure that emerging risks are properly elevated through the management chain.
- Establish routine reporting procedures to external stakeholders on operational risks.

Direction regarding ERM practices has been developed by a number of private and Government organizations and continues to be expanded. For example, in September 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[3] developed the *Enterprise Risk Management – Integrated Framework* to assist management in improving their organizations' ERM. The COSO framework describes risk management as "a process applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." According to the COSO, a proactive approach to risk management is necessary and includes processes and activities that are intertwined within an organization's core activities so that risk management is performed on an ongoing, consistent basis by employees throughout the organization. The IRS's ERM program uses the COSO framework as the model for its design. In May 2013, the COSO updated its Internal Control Integrated Framework to include 17 principles of internal control, four of which apply to risk management.

The Government Accountability Office also addresses risk management principles in its *Standards for Internal Control in the Federal Government* (Green Book).[4] Specifically, in its September 2014 revision, the Government Accountability Office adopted the same 17 underlying principles from the COSO May 2013 update.

Although the Office of Management and Budget (OMB) currently does not specifically require Federal agencies to implement a formal ERM function, it does expect agencies to manage risks

[2] A fiscal year is any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins October 1 and ends on September 30.
[3] The COSO is a voluntary private-sector organization dedicated to providing frameworks and guidance to executive management and governance entities on enterprise risk management, internal control, and fraud deterrence.
[4] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

to their mission, goals, and objectives. In addition, the Government Performance and Results Act of 1993[5] requires Federal agencies to develop strategic plans with long term goals, performance plans with annual goals and measures, and performance reports on prior year performance. A strategic plan defines the agency mission, long-term goals, strategies planned, and approaches it will use to monitor its progress in addressing specific needs, challenges, and opportunities related to its mission. Because the strategic plan focuses on long-term objectives, it is important that agencies consider risks and how risks change over time during formulation of the plan. Considering risk management in the early stages of the strategic planning process will ensure that the agency's management of risk is appropriately aligned with the organization's overall mission, objectives, and priorities. Federal agencies also should maintain a robust set of measures to track performance.

OMB Circular A-123[6] specifically addresses the management of internal controls and associated risks over the key areas of Operations, Reporting, and Compliance. ERM, by contrast, is a strategic business discipline that addresses the full spectrum of an agency's risk. The OMB is also considering significant expansion of the scope of Circular A-123. This expansion, as envisioned, would include guidelines regarding both agency strategic risk management and governance.

This review is a follow-up to a previous TIGTA audit,[7] which reported (in September 2011) that improvements were needed in the IRS's existing risk management processes. Specifically, TIGTA found that the efficiency of the IRS's efforts to identify and address organizational risks could be improved by developing a more structured approach supported by formal guidelines. TIGTA also reported that the sharing of identified risks needed to be improved and a review of the process the IRS uses to identify organizational risks should be completed. At that time, the IRS declined to implement TIGTA's recommendations regarding implementing a more structured approach to risk management and improving the sharing of information on corporate risk.

This review was performed at the IRS National Headquarters in Washington, D.C., in the offices of the Chief Risk Officer (CRO), Appeals Division in Dallas, Texas; Information Technology Division in Washington, D.C.; Wage and Investment Division in Atlanta, Georgia and the Small Business/Self-Employed Division in Lanham, Maryland during the period August 2015 through February 2016. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and

[5] Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (codified as amended in scattered sections of 5 U.S.C., 31 U.S.C., and 39 U.S.C. (2013)).
[6] Office of Management and Budget, OMB Circular No. A-123 (Revised), *Management's Responsibility for Internal Control*, (Dec. 2004).
[7] TIGTA, Ref. No. 2011-10-096, *Risk Management Efforts Could Be Improved With Clearly Defined Procedures and Expanded Information Sharing* (Sept. 2011).

conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Significant Progress Has Been Made in Implementing a Structured Framework for the Identification and Mitigation of Significant Organizational Risks

The IRS has made significant progress in its efforts to implement an ERM program to provide a structured framework for the identification and mitigation of significant organizational risks. Steps already completed include appointing a CRO and establishing an embedded risk management structure within each of the IRS's four operating divisions and 20 functional offices. Risk assessment procedures were also developed and training was provided to staff responsible for performing risk assessment activities. In addition, the IRS established a Risk Working Group (RWG), which includes representatives from the IRS's operating divisions and functional offices, and an Executive Risk Committee (ERC), comprised of IRS senior management, to facilitate collaboration on enterprise risk decisions. The RWG generally meets monthly, and the ERC generally meets quarterly.

In October 2014, the IRS completed an initial agency-wide risk assessment focused on using a high-level, top-down approach to identify and provide insight on enterprise risk areas. As a result of this assessment, management identified 15 high-level enterprise risk categories. The IRS termed this review "a risk temperature check," and its purpose was to establish a baseline of agency risk.

In December 2015, the IRS completed its second agency-wide risk assessment. The purpose of this assessment was to review risk areas across the organization in more depth, identify the top areas of risk impacting the IRS, and develop a coordinated approach to addressing these risk areas. The first step in this process was the completion of separate risk assessments by the IRS's operating divisions and functional offices of the risks to their specific mission, goals, and objectives. These assessments were documented using a standard methodology developed by the CRO. As a result of these assessments, a total of 343 individual risks were identified across the IRS. These 343 risks were then analyzed to identify common categories and causes. Based on this analysis, 29 total risk areas were identified, of which 12 were prioritized as the top enterprise risk areas. The top 12 risk areas were further consolidated to identify six risk focus areas. The FY 2015 top 12 enterprise risks and top six risk focus areas identified by the IRS are summarized in Figure 1 below.

Figure 1: FY 2015 Top Six Risk Focus Areas and 12 Enterprise Risk Areas

Top Six Risk Focus Areas	Top 12 Enterprise Risk Areas
Budget	1. Budget Limitations and Complexity
Cybersecurity	2. Cumulative Risk – unknown impact of accumulated risks accepted over time
	3. Complexity of Cyber Threats
Authentication/Authorization	4. Authentication/Authorization – challenges increase opportunities for refund fraud and identify theft
	5. Digital Service – online system security
Integrated Strategy and Objectives	6. Integrated Strategic Objectives – development of a comprehensive approach
Operational Effectiveness and Efficiency	7. Internal Controls – insufficient emphasis
	8. Policies and Procedures – voluminous and outdated
	9. Taxpayer Accounts – inaccurate information
	10. Workarounds – overreliance on short term fixes
Workforce	11. Employee Engagement and Morale – risks resulting from increased workload with fewer resources 12. Specialized Expertise and Capacity – ability to address emerging issues

Source: ERM Program - ERC Briefing December 8, 2015.

A key element in the IRS's approach in identifying the top 12 risk areas and six risk focus areas was a focus on determining risk categories and common root causes that applied to multiple individual risks so that a more comprehensive approach could be used in identifying actions to address the risks. The IRS's ERM program approach relies on the responsible operating division or functional office to assess individual risks to specific IRS programs.

Our review indicated that all 343 risks identified were considered and reviewed as part of the FY 2015 agency-wide risk assessment and that this process was adequately documented. The

top 12 risk areas and six risk focus areas developed were also reviewed and approved by the ERC. Finally, the summary results of this assessment were reported to the Department of the Treasury, Office of the Assistant Secretary for Management, in January 2016.

To address the top 12 risk areas and six risk focus areas, the IRS identified 42 mitigation actions. Input from operating division and functional office stakeholders were solicited during this process. The 42 mitigation actions were approved by the ERC, and a responsible executive for each mitigation action was designated. Procedures were then developed and approved by the ERC requiring that progress on completion of the 42 actions be monitored quarterly by the applicable Deputy Commissioner. The IRS plans to complete another agency-wide risk assessment in FY 2016.

Steps still in process in the implementation of the ERM program include continuing to provide risk management training to all employees; integrating ERM with the IRS's strategic planning, budgeting, and internal controls processes; and actively monitoring ERM program performance, including performing reviews of the risk management activities of its embedded risk management structure. Further, the IRS is also working to establish risk tolerance guidelines to assist in determining acceptable levels of risk associated with various IRS business decisions.

Finally, the IRS plans to develop metrics, known as key risk indicators, to assist in signaling emerging risks. A basic example of a key risk indicator would be the volume of taxpayer examinations that are appealed and subsequently conceded by the IRS Appeals function. If, for example, there is a high volume of conceded examination cases involving the same issue, the IRS may need to provide clearer guidance and training regarding the issue. The key risk indicator in this case, the volume of conceded cases, allows the IRS to quickly identify and address a risk before the volume of conceded cases becomes unmanageable.

At the time of our audit field work, overall progress in developing a comprehensive set of key risk indicators across the IRS had been limited, and the CRO was still in the process of developing a strategy and detailed timeline to guide this effort. Preliminary steps included the development of guidance by the CRO in November 2014 on developing key risk indicators. The purpose of this guidance is to provide an understanding of the use and design of key risk indicators. The CRO also provided training to the operating division and functional office risk coordinators in March 2015 regarding the identification of key risk indicators.

Key performance indicators are generally focused on historical performance and therefore provide insight about a risk that has already occurred, while key risk indicators are designed to provide timely indicators of emerging risks. Key risk indicators may signal that a mitigation action needs to be taken or changed and also allow for comparisons across time. In developing key risk indicators, to improve an ERM process, management may consider identifying and analyzing risk metrics already developed and obtaining input from subject matter experts responsible for managing organizational units and processes.

This review focused on evaluating IRS's progress in implementing an ERM program. TIGTA did not make any recommendations.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the IRS's efforts to implement a comprehensive process for identifying and mitigating significant risks to effective tax administration. To accomplish our objective, we:

I. Determined whether the IRS has established adequate controls over the implementation and operation of its ERM program.

A. Obtained and reviewed industry best practices and Government criteria, including the Government Accountability Office "Green Book," [1] OMB Circular A-123, and COSO *Enterprise Risk Management – Integrated Framework* related to implementing an ERM program.

B. Reviewed short-term and long-term implementation plans developed by the IRS to guide planning and implementation efforts for the ERM program, including any training planned.

C. Analyzed policies and procedures developed by the ERM program office, including the program charter and governance structure.

D. Interviewed the CRO and selected ERM liaisons (in two randomly selected operating divisions and two randomly selected functional offices) to obtain their understanding of the overall ERM process, including the roles and responsibilities.

E. Reviewed the results of the IRS's initial FY 2014 risk temperature check process.

II. Assessed the methodology used by the ERM program in identifying and mitigating significant risks to effective tax administration.

A. Reviewed the process developed to support the ongoing identification and evaluation of entity-level risks.

1. Evaluated the ERM risk tracking methodology (ERC level) and determined whether it contained sufficient information to effectively track and manage entity-level risk areas.

2. Identified the top risk areas as of December 30, 2015, and assessed the source of the risk areas. The IRS identified 12 top enterprise risk areas for FY 2015.

[1] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

3. Ascertained whether the top 12 risk areas identified met the criteria for classification as entity-level risks developed by the IRS.
4. Assessed documentation of the actions taken by the IRS to address each of the top 12 risk areas, including mitigation methods and status.
5. Reviewed documentation of decisions reached by the ERC regarding risk accountability for risk mitigation activities for each of the top 12 risk areas.

B. Evaluated executive oversight of entity-level risks and risk mitigation activities.

1. Reviewed ERC and RWG meeting minutes for the period October 2014 through February 2016.
2. Interviewed selected RWG members (ERM liaisons from the two randomly selected operating divisions and two randomly selected functional offices) regarding the methodology used to identify and elevate risks having entity-level impact and obtained any concerns regarding this process.
3. Evaluated the process used by the ERC to establish the entity-level overall risk tolerance (risk appetite).
4. Analyzed reporting procedures to external stakeholders of significant emerging risks.

C. Reviewed the implementation and overall results of the FY 2015 annual agency-wide risk assessment.

D. Interviewed ERM liaisons for the two randomly selected operating divisions and two randomly selected functional offices regarding implementation of the FY 2015 annual agency-wide risk assessment.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRS policies and procedures for implementing an enterprise risk management program, including conducting annual risk assessments and monitoring mitigation action plans. We evaluated these procedures by interviewing the CRO and selected enterprise risk personnel, analyzing enterprise management procedures, and reviewing the FY 2015 enterprise risk assessment and supporting documentation.

Appendix II

Major Contributors to This Report

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)
Alicia Mrozowski, Director
Anthony Choma, Audit Manager
Angela Garner, Lead Auditor
Paige Krivda, Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Director, Office of Audit Coordination