TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided

September 15, 2016

Reference Number: 2016-20-075

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

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.

HIGHLIGHTS

INFORMATION TECHNOLOGY: SHAREPOINT CONTROLS NEED IMPROVEMENT TO MITIGATE RISKS AND TO ENSURE THAT POSSIBLE DUPLICATE COSTS ARE AVOIDED

Highlights

Final Report issued on September 15, 2016

Highlights of Reference Number: 2016-20-075 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The IRS uses thousands of SharePoint® sites for collaboration, document management, records management, and enterprise content management. The implementation of operational and security controls for these sites is critical to the protection of sensitive IRS data.

WHY TIGTA DID THE AUDIT

The overall objective was to assess the IRS's implementation of SharePoint operational and security controls, including the SharePoint governance structure, policies and procedures, user access controls, protection of sensitive data, and the Information Technology Contingency Plan.

WHAT TIGTA FOUND

Improved risk management across the IRS SharePoint environment is needed to ensure that adequate operational and security controls are in place and functioning as intended to protect sensitive SharePoint sites and data. Operational controls are needed to ensure that SharePoint sites containing sensitive data are identified and have an approved Privacy and Civil Liberties Impact Assessment. Security controls are needed to ensure that a security assessment of the SharePoint product, sites, and data is completed; SharePoint site collection audit trails are enabled; quarterly reviews of users' accesses are performed; users' accounts and permissions are efficiently managed; security and content management policies are consistently enforced; and the Information Technology Contingency Plan and Business Impact Analysis are finalized.

The IRS has not evaluated and justified its SharePoint approach as a long-term solution within the Department of the Treasury's shared services strategy. As a result, the IRS may be incurring duplicate operational costs; operating in a less secure environment; and, in the event of a disruption, functioning in an environment in which SharePoint is not defined as a mission-critical system. The SharePoint Program Management Office allocated $5 million for operations and maintenance of the Fiscal Year 2016 IRS SharePoint program. However, sufficient cost information for SharePoint expenses across the IRS enterprise was not available to verify possible duplicate expenditures or potential net savings related to transitioning to the Treasury Enterprise Content Management environment.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer ensure that SharePoint sites are routinely scanned for sensitive data; privacy assessments are completed; a security assessment is completed for the SharePoint product, sites, and data; IRS business commissioners ensure that SharePoint site collection audit trails are enabled, quarterly security reviews are performed, access permissions are efficiently managed, and security policies are enforced; a contingency plan and a Business Impact Analysis are finalized; and a feasibility analysis of using the Treasury Enterprise Content Management environment is completed.

IRS management agreed with five of our 10 recommendations and partially agreed with the other five recommendations primarily because business unit commissioners have a shared responsibility for implementing SharePoint controls. The IRS has taken or plans to take corrective actions, including scanning sites for sensitive data, ensuring that privacy assessments are completed, ensuring that security controls are documented, issuing a memorandum to business unit commissioners on SharePoint responsibilities, and conducting a feasibility analysis.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 15, 2016

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided (Audit # 201520013)

This report presents the results of our review of the Internal Revenue Service's (IRS) implementation of SharePoint® operational and security controls, including user access privileges and protection of sensitive data on IRS SharePoint sites. This audit is included in our Fiscal Year 2016 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and IRS Employees.

Management's complete response to the draft report is included as Appendix VI**.**

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

EOps	Enterprise Operations
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
PCLIA	Privacy and Civil Liberties Impact Assessment
PGLD	Privacy, Governmental Liaison, and Disclosure
PII	Personally Identifiable Information
SA&A	Security Assessment and Authorization
SBU	Sensitive But Unclassified
TIGTA	Treasury Inspector General for Tax Administration

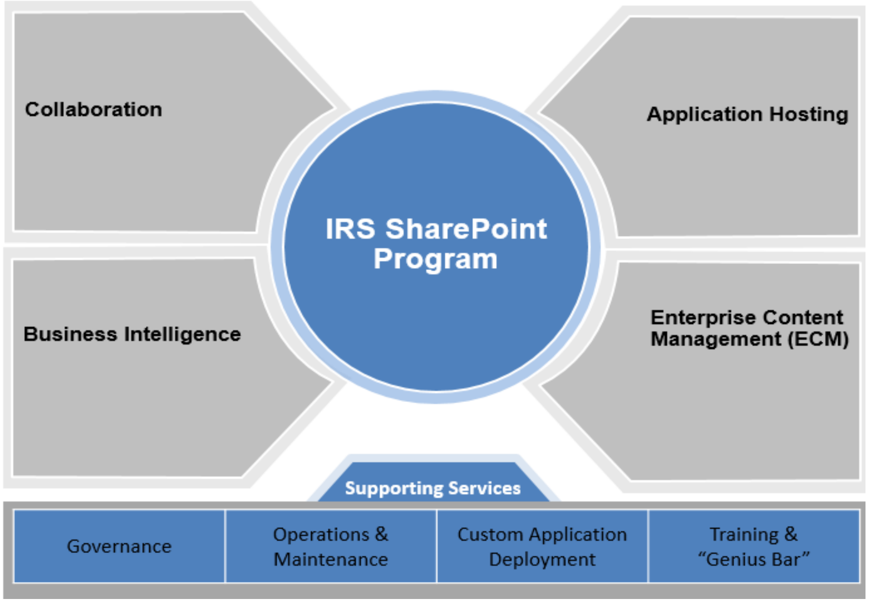
Background

SharePoint® is a Microsoft commercial off-the-shelf[1] product that supports collaboration, information dissemination through web portals, document management, records management, and application service delivery platforms. It also offers system integration, process integration, and workflow automation capabilities. It is a software platform that provides multiple methods to extend its capabilities via configuration, customization, and development.

IRS business units rely on the SharePoint platform primarily for collaboration, document management, records management, and enterprise content management.

Internal Revenue Service (IRS) business units rely on the SharePoint platform primarily for collaboration, document management, records management, and enterprise content management. Figure 1 presents the IRS Information Technology (IT)[2] organization's Enterprise Operations (EOps) SharePoint capabilities and services.

Figure 1: IRS SharePoint Capabilities and Services

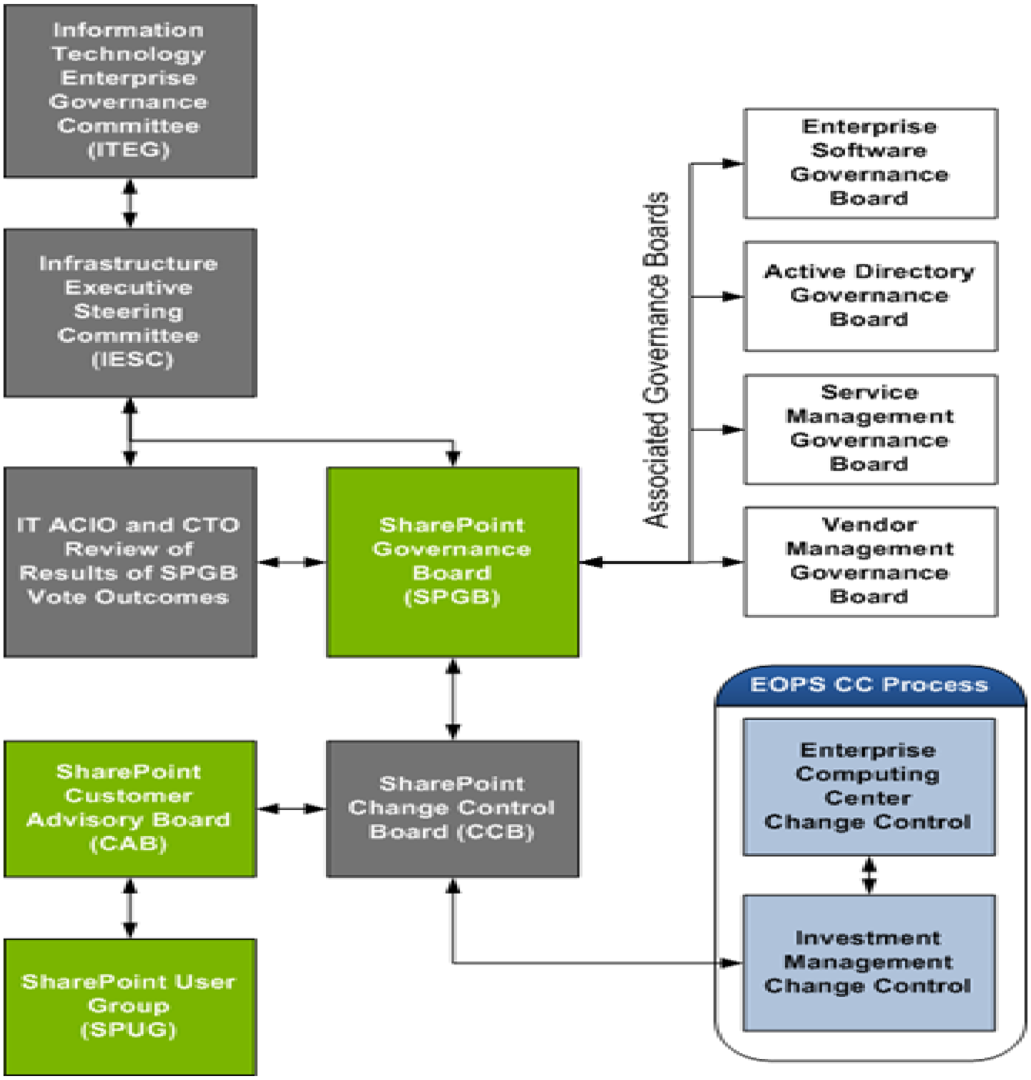


Source: IRS SharePoint Project Management Plan.

[1] See Appendix V for a glossary of terms.
[2] As of July 7, 2016, the IRS IT organization is now led by the Chief Information Officer instead of the Chief Technology Officer. Where possible, all references to the Chief Technology Officer have been revised to the Chief Information Officer.

The cornerstone of IRS SharePoint governance is the SharePoint Governance Board, which provides guiding principles for current and future direction. The SharePoint Governance Board includes business unit and Cybersecurity organization executives and other IRS IT organization stakeholders. The chair is the Director, EOps, Enterprise Technology Implementation. The SharePoint Governance Board coordinates with the existing EOps governance structures and escalates issues to the EOps Infrastructure Executive Steering Committee for dispute resolution. The SharePoint Customer Advisory Board and the SharePoint Users Group support the SharePoint Governance Board as depicted in Figure 2.

Figure 2: SharePoint Governance Structure


Information Technology Enterprise Governance Committee (ITEG)
Infrastructure Executive Steering Committee (IESC)
IT ACIO and CTO Review of Results of SPGB Vote Outcomes
SharePoint Governance Board (SPGB)
Associated Governance Boards
Enterprise Software Governance Board
Active Directory Governance Board
Service Management Governance Board
Vendor Management Governance Board
EOPS CC Process
Enterprise Computing Center Change Control
Investment Management Change Control
SharePoint Customer Advisory Board (CAB)
SharePoint Change Control Board (CCB)
SharePoint User Group (SPUG)

Source: IRS SharePoint Project Management Plan. ACIO – Associate Chief Information Officer, CC – Change Control, CTO – Chief Technology Officer.

The EOps SharePoint Program Management Office provides operational oversight and governance of the SharePoint platform including infrastructure, support, and management. In addition, the SharePoint Program Management Office establishes management, technical, and operational standards; reviews policy impact on the use of SharePoint; recommends training; and supports configuration and customization of site solutions deployed on the SharePoint platform. The SharePoint Team maintains these practices and procedures on its SharePoint Central website, which is accessible to SharePoint users.

SharePoint site ownership is the responsibility of site collection owners within IRS business units. The site collection owners operate, manage, and maintain their SharePoint sites and are responsible for day-to-day site management, support, and compliance for user access, user permissions, content management, and audit trail management. End users within the business units are expected to work directly with their respective site collection owners to resolve questions and issues. Additionally, the SharePoint Program Management Office may require the site collection owners to participate in resolving support tickets.

The related mission of the Privacy, Government Liaison, and Disclosure (PGLD) Office is to preserve and enhance public confidence by advocating for the protection and proper use of identity information. Personally Identifiable Information (PII) and Sensitive But Unclassified (SBU) data can be stored within SharePoint, but special precautions must be taken, including having a Privacy and Civil Liberties Impact Assessment (PCLIA) approved by the PGLD Office. The PGLD Office has made available a SharePoint PCLIA template and corresponding policy to facilitate compliance. If PII or SBU content will be stored within a SharePoint site collection, the site collection should have an approved PCLIA before the owner or administrator submits the SharePoint site creation request to the SharePoint Program Management Office.

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, in the SharePoint Program Management Office during the period February through September 2015. 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 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

Our review found that IRS IT officials did not implement effective risk management processes to ensure that operational and security controls were in place and operating effectively to protect sensitive data maintained in the SharePoint environment. Operational controls failed to identify all SharePoint sites containing sensitive taxpayer data and ensure that PCLIAs were completed before the SharePoint sites were deployed. Cybersecurity officials did not complete a Security Assessment and Authorization (SA&A) for the SharePoint 2010 product, sites, and data. SharePoint site collection audit trails were not enabled and access permissions were not assigned according to established IRS guidelines. Across the IRS's sprawling SharePoint operational environment, site owners and administrators were not consistently maintaining approved user lists and performing quarterly security reviews, and operational controls did not ensure enterprise adherence to SharePoint security and content management policies. Further, an Information Technology Contingency Plan, including a Business Impact Analysis, was not in place to better ensure reliable and dependable SharePoint operations.

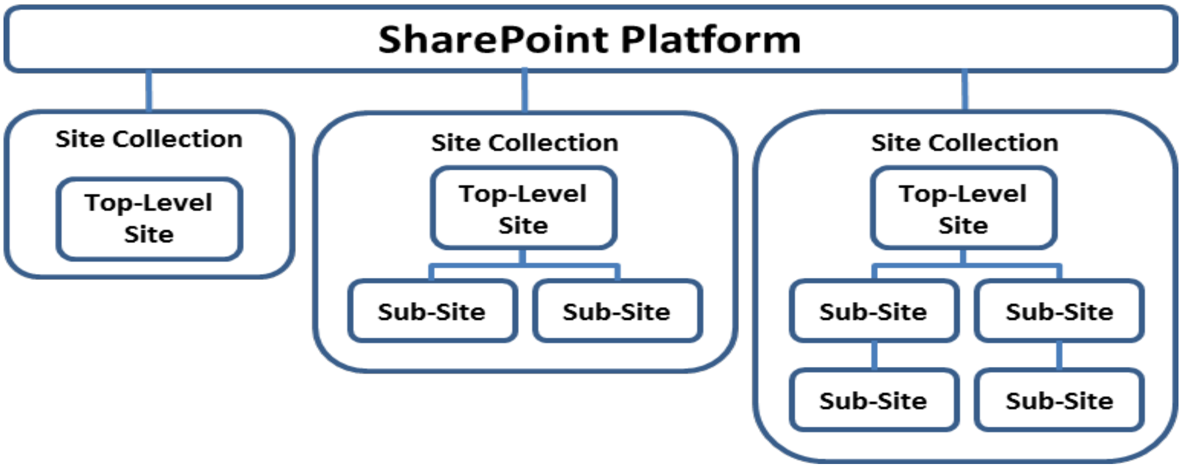
The IRS has not yet evaluated and justified its SharePoint strategy as a long-term solution within the Department of the Treasury's shared services strategy. For instance, IRS IT officials did not perform an assessment to determine whether using the Treasury Department's Enterprise Content Management environment for its SharePoint operations would be more effective or efficient. Our assessment of the IRS decision to not adopt the Treasury Department's shared service solution for SharePoint indicates that, by developing and maintaining its own SharePoint solution, the IRS may be incurring duplicate operational costs; operating in a less secure environment; and, in the event of a disruption, functioning in an environment in which SharePoint is not defined as a mission-critical system.

Improved Risk Management Across the SharePoint Environment Is Needed to Ensure That Effective Controls Protect Sensitive Sites and Data

IRS business units are increasingly relying on SharePoint sites for business processes and operations. At the time of our review, the SharePoint Program Management Office had completed its upgrade of Microsoft SharePoint 2003/2007 to SharePoint 2010. In April 2015, the IRS had approximately 16,218 SharePoint sites, 1,105 SharePoint site collections, 90,000 internal SharePoint users, 35 SharePoint licenses, and 91 primary SharePoint servers (27 for production, 14 for development, 13 for tests, 23 for disaster recovery, and 14 for utilities).

A SharePoint site collection is a grouping of one or more related SharePoint sites. Each site can contain subsites. Thus, a SharePoint site collection is a hierarchy of sites and subsites, as depicted in Figure 3.

Figure 3: Relationship of the SharePoint Platform to SharePoint Site Collections and SharePoint Sites



Source: *IRS EOps SharePoint Site Owner's Guide.*

IRS internal SharePoint users use the SharePoint sites for multiple purposes, including storing and sharing PII and SBU data. Examples of PII and SBU data on IRS SharePoint sites include:

- Social Security Numbers
- Names
- Addresses
- Cell phone numbers
- Standard Employee Identifiers
- E-mail addresses
- Passport numbers
- Financial account records
- Criminal records
- Dates of birth
- Employer Identification Numbers

The objectives of the IRS SharePoint program are to operate and maintain SharePoint across the enterprise, respond to and correct issues, and minimize disruptions to SharePoint users. We reviewed and tested operational and security controls within the SharePoint production environment, in which IRS SharePoint users access sites in real-time. Our review identified unmitigated risks within the following operational control conditions:

- Operational controls did not ensure that all sites with PII or SBU data were identified and supported by PCLIAs.
- The SA&A process was not completed for the SharePoint 2010 product, sites, and data.

- SharePoint site collection audit trails were not enabled to track user accesses and actions.
- SharePoint site collection owners and administrators were not maintaining approved user lists, performing quarterly reviews of accesses, or efficiently assigning users and permissions to groups.
- SharePoint governance roles and responsibilities did not ensure enterprise adherence to established SharePoint security and content management policies.
- An Information Technology Contingency Plan, including a Business Impact Analysis, was not in place to ensure the availability of SharePoint operations.

Operational controls did not ensure that all sites with PII or SBU data were identified and supported by PCLIAs

The IRS has established policies and procedures that are intended to ensure that a privacy risk management process is documented and implemented to assess the privacy risk to individuals that results from the collection, sharing, storing, transmitting, use, and disposal of PII or SBU data. A PCLIA must be conducted for information systems, programs, or other activities that pose a privacy risk.

In February 2013, the Treasury Inspector General for Tax Administration (TIGTA) reported on the effectiveness of the PCLIA process and stated that, "The IRS does not have adequate assurance that it is complying with the privacy provisions set forth by the Office of Management and Budget because PII could be stored on SharePoint sites for which a PCLIA has not been conducted."[3] In response to the report recommendations, the PGLD Office issued an interim guidance memorandum to IRS business unit executives on September 13, 2013, stating that the following actions were effective immediately:

- Internal collaborative application sites, *e.g.*, SharePoint, containing PII require a PCLIA at the site collection level.
- New SharePoint site collections with PII cannot be created without an approved PCLIA.
- Existing SharePoint site collections that transitioned to SharePoint 2010 and have PII are required to go through a SharePoint recertification.
- The PGLD Office of Privacy Compliance will monitor SharePoint site collections to ensure compliance with this policy and the use of PII as stated in the site collection's PCLIA.

[3] TIGTA, Ref. No. 2013-20-023, *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* p. 7 (Feb. 2013).

According to the *SharePoint Site Owner's Guide*,[4] for new SharePoint 2010 sites, IRS business units must submit a site request form to the SharePoint Program Management Office to create a SharePoint site. The IRS business unit requestor must disclose whether the site will contain PII or SBU data. The National Institute of Standards and Technology (NIST)[5] defines PII as any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name. The IRS defines SBU as any information that, if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Freedom of Information Act.[6] If the site will contain PII or SBU, the SharePoint Program Management Office refers the requester's form to the PGLD Office. The SharePoint Program Management Office supports the PGLD Office in implementing and ensuring that PCLIAs are completed for all SharePoint sites that are identified as containing PII or SBU data.

The PGLD Office has a three-year cycle for SharePoint recertification for sites that are identified as containing PII or SBU data. However, the EOps SharePoint Program Management Office recognizes that some of the existing SharePoint 2003/2007 sites that transitioned to SharePoint 2010 may not have gone through a SharePoint recertification and thus may be deployed without an approved PCLIA.

From the population of 1,303 IRS SharePoint sites created after September 13, 2014, we selected a judgmental sample[7] of 16 sites. A year earlier, on September 13, 2013, PGLD interim guidance stated that the Internal Revenue Manual (IRM) would be updated with privacy guidelines by September 13, 2014. We selected the sample after this date to allow PGLD officials a year to incorporate the privacy controls into the IRM. However, after selecting our sample, PGLD officials subsequently issued updated guidance stating that the IRM would not be updated until August 28, 2017. We selected a judgmental sample because our review was to evaluate whether controls were in place and working. We selected sample sites based on whether the site names indicated the potential for the presence of taxpayer information. Figure 4 provides the number of SharePoint sites sampled by business unit.

[4] IRS EOps organization, *SharePoint Site Owner's Guide* (Feb. 2015).
[5] NIST, Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[6] Internal Revenue Manual 10.8.1, *Information Technology Security, Policy, and Guidance* (July 2015). Freedom of Information Act, Pub. L. 104-231, 5 U.S.C. 552.
[7] A judgmental sample is a nonprobability sample, the results of which cannot be projected to the population.

Figure 4: Number of SharePoint Sites Sampled Per Business Unit

Business Unit	Number of Sampled Sites
Information Technology organization	2 sites
Large Business and International Division	4 sites
Small Business/Self-Employed Division	5 sites
Wage and Investment Division	5 sites

Source: *IRS SharePoint documents provided by the SharePoint Program Management Office and TIGTA's sampled SharePoint sites.*

Our tests of these 16 sites found two documents that contained PII on one SharePoint site. The site administrator informed us that the particular site did not have an approved PCLIA and explained that he relied on the business unit staff to redact PII information before the files were added to the SharePoint site. However, in this instance, the PII information was not redacted before the documents were added to the SharePoint site.

Our review also noted that the IRS has not implemented a tool to automatically search its SharePoint websites and identify all sites containing PII and SBU data. In July 2010, the SharePoint Program Management Office began evaluating an automated tool for consideration within the IRS SharePoint environment. The tool's vendor states that the software product adds a layer of security at the content level to enforce data and web governance policies and improve collaboration while minimizing risk on a wide range of digital environments including SharePoint. However, the automated tool has not performed well during testing within the IRS SharePoint environment. The EOps SharePoint Program Management Office noted that there were multiple areas of concern with the tool, and the application of software patches did not resolve the problems. The tool's vendor is working with the IRS to attempt to address identified issues. In order to address the concerns, the SharePoint Program Management Office has begun considering an alternate tool.

Taking steps to adopt and fully implement an automated tool to periodically scan the IRS SharePoint site environment could help to better ensure that SharePoint site collections containing PII or SBU data have approved PCLIAs. When PCLIAs are not obtained, it increases the risk that confidential and sensitive information could be published on IRS SharePoint sites without the appropriate security access controls.

The SA&A process was not completed for the SharePoint 2010 product, sites, and data

The IRS requires that any implementation of a collaborative technology, such as SharePoint, is based on an assessment of risk with mitigation and assumption of risk by the appropriate authorizing official.[8] The risk assessment, performed as part of an SA&A, tests and evaluates the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Additional requirements of the security assessment include:

- Security Categorization – Federal Information Processing Standards Publication 199[9] requires the IRS to categorize information and information systems. The security categorization results and the supporting rationale should be documented in the security plan for the information system, and the security categorization decision must be reviewed and approved by the authorizing official. The security categories describe the potential adverse impacts to organizational operations, assets, and individuals if organizational information systems are compromised through a loss of confidentiality, integrity, or availability.
- System Security Plan – A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
- Security Control Assessment – The actual testing or evaluation of the security controls in an information system.

Our review found that an SA&A was not completed for the SharePoint 2010 product, sites, and data that reside on the SharePoint sites. IRS EOps officials advised that they performed a risk assessment of the SharePoint platform, which is documented in the General Support System 30 Security Change Assessment. Further, IRS EOps officials stated that the SharePoint application owners are responsible for their own security assessments over the SharePoint sites and data. However, IRS officials did not provide evidence that SharePoint was defined within the system boundaries of the General Support System 30 and that the risk assessment performed incorporated SharePoint sites and data. As such, IRS EOps officials have not determined the security risks and impact of adding the SharePoint technology to the IRS environment.

Cybersecurity officials stated that the SA&A was not completed because the related IRM is inaccurate. The IRM states: "The IRS has made a risk-based decision determining that internal collaborative application sites (*e.g.*, SharePoint, Centra) established and configured for basic file

[8] IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (July 2015).
[9] NIST, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

sharing and team collaboration will not require a security authorization." When TIGTA requested documentation of the risk-based decision, IRS security personnel provided the following response: "The reference in IRM 10.8.1 to a risk-based decision is inaccurate, and the language was inadvertently changed in the name of consistency. It should be noted that in IRM 10.8.1, we are trying to convey that the SharePoint technology, used for basic file sharing and collaboration, is an exception to the SA&A process."

In the absence of an SA&A on the SharePoint 2010 product, sites, and data, PII and SBU data may not be protected from unauthorized disclosure and inappropriate use. IRM 10.8.1 states that continuous monitoring and security assessments are interrelated. Information obtained during continuous monitoring and security assessments is used when making authorization decisions. According to NIST Special Publication 800-37,[10] a critical aspect of managing risk to information involves the continuous monitoring of the security controls employed within or inherited by the system. The objective of continuous monitoring is to determine if the set of deployed security controls continue to be effective over time in light of the changes that occur. Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A complete SA&A, including a risk assessment for SharePoint, would detail the security posture of important technical security controls such as access controls, identification and authentication, system and communications protection, and audit and accountability.

SharePoint site collection audit trails were not enabled to track user accesses and actions

Audit trails maintain a record of system activity, both by system and application processes and by user activity on systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications. IRS security standards state that the IRS shall create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. Audit trails for all IRS systems and applications shall capture, at a minimum, the following data for each auditable event:

- The date and time the event occurred.
- The unique identifier of the user or application initiating the event.
- The type of event.
- The subject of the event and the action taken on that subject.
- The success or failure of the event.

[10] NIST, Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Feb. 2010).

Best practices for SharePoint deployment also include monitoring site usage using audit trails, which would require SharePoint stakeholders to address key questions such as:

- Who is accessing the system and when?
- What sites are viewed?
- What files are viewed, modified, deleted, or checked out?
- What type of content is stored in the system?

We reviewed the status of audit trail controls for the SharePoint site collections. Site owners and administrators are responsible for enabling audit trails for their SharePoint site collections. During our review, we selected a judgmental sample of 16 SharePoint sites for detailed audit testing. While the SharePoint 2010 product is capable of capturing audit events for site collection audit settings, documents, items, lists, libraries, and sites, our tests found that site owners and administrators did not follow established policy and had not enabled audit trails for any of the 16 sites included in our sample. By not enabling audit trails for the site collections, site owners and administrators did not have the ability to collect, report, and analyze the usage and effectiveness of their sites. Figure 5 summarizes the results of our testing of audit trails for our 16 SharePoint sample sites.

SharePoint site collection owners and administrators were not maintaining approved user lists, performing quarterly reviews of accesses, or efficiently assigning users and permissions to groups

Within the scope of our review, we reviewed user and permission management for the SharePoint site collections, sites, and subsites. The relevant IRM states that site administrators must maintain an approved users list and perform quarterly reviews of accesses to ensure that only authorized users with a business need have access to the collaborative sites necessary to perform their job responsibilities.

We interviewed the site owners and administrators for the 16 sampled SharePoint sites to determine whether quarterly reviews of user accounts and permissions were performed. Our tests found that site owners and administrators for only two of the 16 sample sites were performing quarterly reviews. If quarterly reviews of accesses are not performed, it increases the risk that sensitive data in SharePoint sites could be subject to manipulation by unauthorized users.

The IRM states that site owners of internal collaborative sites shall decide what the users can do when accessing the collaborative sites by granting appropriate access. For efficiency of maintaining user permissions for a large user base, the *SharePoint Site Owner's Guide* cites the best practice of assigning users and permissions to groups. "When assigning permissions within SharePoint, it is recommended to grant access via groups. Assigning permissions to individual users is not recommended and can lead to problems managing access." Our sample tests found that six of the 16 SharePoint site collection owners were assigning permissions to individual users instead of assigning permissions to groups. While site owners and administrators were aware of the IRS guidance, they were not following the recommended practice of granting access to groups. Consistently assigning users and permissions to groups would help the IRS support manageability and allow site owners to efficiently review and maintain permissions across approximately 1,105 SharePoint site collections. Figure 5 summarizes the results of our testing of SharePoint sample sites, which shows whether quarterly reviews were performed and whether permissions were appropriately assigned to groups.

Figure 5: SharePoint Site Owners and Administrators Shared Responsibilities for SharePoint Site Collection Audit Trails, Quarterly Reviews, and Permission Management

SharePoint Site Owners' and Administrators' Duties	Results of Sample Sites Tested
Enable SharePoint site collection audit trails.	Audit trails were not enabled for any of the 16 sites.
Perform quarterly reviews of users' access to ensure that only authorized users with a business need have required access.	Quarterly reviews were performed for only two of the 16 sites.
Assign users and appropriate permissions to groups.	Users and appropriate permissions were assigned to groups for 10 of the 16 sites.

Source: *TIGTA summary test results for sample SharePoint sites.*

SharePoint governance roles and responsibilities did not ensure enterprise adherence to established SharePoint security and content management policies

The SharePoint 2010 product includes features that enable site owners to collect, report, and analyze the usage and effectiveness of their sites. Best practices for SharePoint deployment and governance published by ISACA® state that SharePoint implementations should be subject to regular monitoring and reporting based on criticality and sensitivity of data and adherence to management oversight requirements.[11] In addition, the IRS *SharePoint Site Owner's Guide* requires SharePoint site collection owners to monitor sites and ensure that the sites conform to acceptable practices. Site owners are encouraged to actively monitor their sites not only to identify and stop undesirable behavior and policy compliance issues but also to learn and understand how users are interacting with the sites.

[11] SharePoint Deployment and Governance Using CobiT 4.1: *A Practical Approach* (2010).

Our review of the established SharePoint governance structure and the underlying roles and responsibilities found that existing governance does not require regular monitoring and oversight of the approximately 1,105 SharePoint site collection owners and administrators. Monitoring and oversight is necessary to ensure that site collection owners and administrators are effectively complying with SharePoint security and content management policies and procedures. Our review of SharePoint site collection audit trails, quarterly reviews, and permissions management showed inconsistent enforcement of the governance policies and procedures. As a result, the IRS has little assurance that the approximately 16,218 SharePoint sites are secure, contain only authorized content, and are operating in accordance with established SharePoint enterprise policies and procedures.

An Information Technology Contingency Plan, including a Business Impact Analysis, was not in place to ensure the availability of SharePoint operations

The IRM states that the IRS shall develop a contingency plan for each information system that identifies essential mission and business functions.[12] The contingency plan should describe how these functions would be maintained in the event of a system disruption, compromise, or computing failure. The plan must also address full system restoration without deterioration of the security safeguards originally in the system.

The IRS SharePoint Information Technology Contingency Plan should identify the criticality of the SharePoint 2010 product, the SharePoint sites, and related data. EOps officials explained that they did not consider SharePoint as mission-critical because it does not process the production workload related to tax-processing applications. However, IRS officials in the Taxpayer Advocate Service advised us that they had key program functions residing in the IRS SharePoint environment. If IRS SharePoint operations were to fail, it could create serious issues for the Taxpayer Advocate Service program by not being considered mission-critical because would not be restored immediately. If there were a disaster that affected the computing operations, only mission-critical systems would have Service Level Agreements in place that would assure funding for immediate restoration of the system.

A key component of the Information Technology Contingency Plan is a Business Impact Analysis, which is used to determine recovery priorities in the event of a significant disruption to SharePoint computing resources. Because the IRS wanted the Information Technology Contingency Plan to reflect its current disaster recovery technology, in February 2015, the SharePoint Program Management Office paused its work on the SharePoint 2010 Information Technology Contingency Plan while it began to design and implement a warm disaster recovery capability.[13] Without an approved plan and a related Business Impact Analysis to determine the criticality of business processes, analyze resource requirements, and identify recovery priorities,

[12] IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (July 2015).
[13] Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.

the IRS may not timely recover the SharePoint environment and restore services if a disruption to IRS computing resources occurs.

Recommendations

The Chief Information Officer should:

Recommendation 1: Ensure that an automated tool is identified, deployed, and routinely executed to identify SharePoint sites containing PII or SBU data.

> **Management's Response:** The IRS agreed with this recommendation. The IRS ensured that an automated tool was identified, deployed, and executed to identify SharePoint sites containing PII or SBU data.

Recommendation 2: Ensure that SharePoint site collections containing PII or SBU data have approved PCLIAs.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will ensure that SharePoint site collections containing PII or SBU data have approved PCLIAs.

Recommendation 3: Ensure that an SA&A considers the SharePoint product, sites, and data within the appropriate authorization boundary and assesses key security controls.

> **Management's Response:** The IRS partially agreed with this recommendation. The IRS will ensure that the SharePoint product is clearly identified and applicable security controls are documented within the authorization boundary in which it resides.
>
> **Office of Audit Comment:** The IRS partially agreed with this recommendation because an SA&A is performed on a General Support System, not on the individual systems or applications that are within the General Support System boundary. However, we believe the IRS SA&A of the related General Support System should also include a risk assessment and testing of the SharePoint application-specific controls because these controls are necessary to protect SharePoint sites with PII and SBU data from unauthorized disclosure and inappropriate use.

Recommendation 4: Coordinate with the respective business unit commissioners to ensure that the SharePoint site collection owners and administrators enable audit trails of key user activities on their sites and that they review audit trails on a regular basis.

> **Management's Response:** The IRS partially agreed with this recommendation. The IRS will ensure that audit trails are enabled to capture all key user activities on all SharePoint sites. The IRS will also issue a memo to all business unit commissioners to remind them of the IRM requirements that site collection owners and administrators review audit trails on a regular basis.

Office of Audit Comment: The IRS partially agreed with this recommendation because business unit commissioners have a shared responsibility for implementing SharePoint controls. We believe the IRS's corrective actions appear responsive to the recommendation.

Recommendation 5: Coordinate with the respective business unit commissioners to ensure that SharePoint site owners and administrators perform quarterly reviews of user accesses in order to ensure that only authorized users with a business need have access to perform their assigned responsibilities.

Management's Response: The IRS partially agreed with this recommendation. The IRS will issue a memo to all business commissioners to remind them of the IRM requirement that SharePoint site owners and administrators perform quarterly reviews of users' accesses so that only authorized users with a business need have access to perform their assigned responsibilities.

Office of Audit Comment: The IRS partially agreed with this recommendation because business unit commissioners have a shared responsibility for implementing SharePoint controls. We believe the IRS's corrective action appears responsive to the recommendation.

Recommendation 6: Coordinate with the respective business unit commissioners to ensure that the SharePoint site owners and administrators efficiently manage user permissions by consistently assigning users and appropriate permissions to groups.

Management's Response: The IRS partially agreed with this recommendation. The IRS will ensure that training is available for SharePoint site owners and administrators on efficient management of user permissions. The IRS will also provide information on best practices for efficient management of user permissions to SharePoint site owners and administrators so they can consistently and appropriately assign user permissions.

Office of Audit Comment: The IRS partially agreed with this recommendation because business unit commissioners have a shared responsibility for implementing SharePoint controls. We believe the IRS's corrective actions appear responsive to the recommendation.

Recommendation 7: Coordinate with the respective business unit commissioners to ensure that the SharePoint governance structure is enhanced to provide enterprise adherence to SharePoint security and content management policies.

Management's Response: The IRS agreed with this recommendation. The IRS will ensure coordination with the respective business commissioners SharePoint Governance Board representatives so the SharePoint governance structure, where needed, is enhanced to provide enterprise adherence to SharePoint security and content management policies.

Recommendation 8: Ensure that the draft SharePoint Information Technology Contingency Plan, including a Business Impact Analysis, is finalized and approved by management.

> **Management's Response:** The IRS agreed with this recommendation. The draft SharePoint Information Technology Contingency Plan is being updated to reflect the current environment and will be submitted for review to finalize the document.

The SharePoint Approach Should Be Evaluated and Justified As a Long-Term Solution Within the Treasury Department's Shared Services Strategy

The IRS Enterprise Life Cycle[14] recognizes that governance is a critical component of the software development framework. The primary objective of IRS governance is to ensure that assigned investment, program, and project objectives are met; risks are managed appropriately; and enterprise expenditures are fiscally sound. The governance process applies to all information technology assets, including information technology and security projects, programs, systems, and components. Each IRS governance board is required to ensure adherence to the Enterprise Life Cycle methodology and framework principles and IRS security requirements.

The Enterprise Life Cycle is a software development framework used by IRS projects to ensure consistency and compliance with Government and industry best practices. The Enterprise Life Cycle framework is the workflow that projects follow to move an information technology solution from concept to production while making sure that the projects comply with IRS guidelines and are compatible with the overall goals of the IRS. The Enterprise Life Cycle also states that projects which are part of the current production environment may undergo a combination of maintenance and new development. The classification of these projects, new development or maintenance, depends on the extent of the changes to the solution. In addition, the Enterprise Life Cycle requires that business cases should include a well-reasoned argument to convince the stakeholders of the benefits of an information technology investment while educating them about the changes, costs, and risks that will be part of the effort.

The IRM requires that an SA&A be performed on IRS systems and applications as part of the security authorization process.[15] The SA&A includes a System Security Plan that identifies and evaluates the status of security controls and a Security Control Assessment that tests the security controls. The IRM further requires that the implementation of collaborative technology and systems, such as SharePoint, be based on an assessment of risk with mitigation and assumption of risk by the appropriate authorizing official.

In May 2010, the Treasury Department's Assistant Secretary for Management and Chief Financial Officer issued a policy memorandum to bureau and departmental office heads

[14] IRM 2.16.1.1, *Enterprise Life Cycle Guidance* (May 2014).
[15] IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (July 2015).

announcing that the Treasury Department is focused on increasing the efficiencies of departmental operations and will soon begin leveraging the Enterprise Content Management program to provide the strategy, management discipline, architectural framework, and technology to meet this goal. Enterprise Content Management is a set of web-based tools to electronically capture, store, search, analyze, collaborate, share, and manage documents. At its core, Enterprise Content Management uses SharePoint, which is an online platform for inter-office collaboration and centralization. In May 2010, all Treasury Department offices were required to be governed by the Enterprise Content Management Executive Steering Committee for information technology systems and services associated with the Freedom of Information Act; eDiscovery; correspondence tracking; collaborative document review; evidence management; case management; and paper reduction through digitization, accessibility, and storage of information in a centralized records repository.

In June 2011, the Treasury Department's Deputy Assistant Secretary and Chief Information Officer issued a memorandum to all Treasury Department bureaus mandating the establishment of two-way trust between each bureau and the Treasury Enterprise Content Management environment by July 29, 2011. According to the Treasury Department's Fiscal Year 2014 Interagency Agreement with the IRS, the Shared Services Division within the Treasury Department provides shared services on a centralized basis, where they can be administered more advantageously and economically. The Treasury Department's Enterprise Content Management environment was initially developed with department-wide systems and capital investment program funds. The environment was developed with the understanding that ongoing operations and maintenance costs would be shared by Treasury Department bureaus. Interagency agreements exist between the Treasury Department and its bureaus by which each bureau pays shared costs for about 20 shared services, such as Clearance Tracker for documents needing the signature of the Secretary of the Treasury, Apportionment Tracker for budgeting, and the Treasury Federal Information Security Modernization Act[16] System. The amount of the shared cost is based on usage and the number of bureau full-time equivalents.

From Fiscal Year 2013 to Fiscal Year 2015, the IRS paid the Treasury Department approximately $7.9 million for the use of the Treasury Enterprise Content Management environment. IRS payments were made using IRS funds in the Treasury Franchise Fund as part of the Enterprise Content Management Program. During the same period, IRS IT officials expended approximately $15 million to operate and maintain the IRS SharePoint environment.[17] For Fiscal Year 2016, Treasury Enterprise Content Management officials estimated that the IRS mandatory annual payment would be $3.6 million, while IRS IT officials estimated it would spend $5 million to operate and maintain the IRS SharePoint environment.[18]

[16] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073.
[17] Our analysis did not include the costs incurred by IRS business units for administering SharePoint sites.
[18] The dollar amounts were provided by the SharePoint Program Management Office and the Treasury Enterprise Content Management Office, and the auditors did not verify the completeness or accuracy of the data provided.

Following the June 2011 Treasury Department mandate, IRS IT management officials did not fully comply with the Enterprise Life Cycle and information technology security IRM requirements. In particular, IRS IT management officials did not: 1) perform an SA&A of the IRS SharePoint product, sites, and data to identify and evaluate the security controls; 2) complete an assessment to identify risks and mitigation actions; and 3) conduct a feasibility analysis regarding use of the Treasury Enterprise Content Management environment, including an assessment of costs and benefits. While key events are included in the body of the report, Appendix IV provides a timeline and supporting details of events for the Treasury Enterprise Content Management and the IRS SharePoint environments.

The Treasury SharePoint application is categorized as mission-critical and, as such, funding to support the immediate restoration of SharePoint services if there were a disaster would be made available. In contrast, since the IRS SharePoint solution is not considered mission-critical, funding has not been secured to support the immediate restoration of SharePoint if needed. In 2014, the IRS Taxpayer Advocate Service sought approval to move its SharePoint sites and data to the Treasury Enterprise Content Management environment. The request, based on a need to approach SharePoint as a mission-critical platform, addressed the Taxpayer Advocate Service's concerns about lack of funding for the IRS's SharePoint environment. However, the IRS Chief Information Officer did not approve this request and subsequently directed that all IRS business units residing on the Enterprise Content Management environment return to the IRS SharePoint environment. According to the December 15, 2014, SharePoint Governance Board minutes, the Chief Information Officer expressed concerns regarding network security, safeguarding of taxpayer data, and compliance with IRS policies. During the review, we shared our assessment with IRS SharePoint and Cybersecurity officials regarding the need to identify and document specific security concerns or other reasons for the decision to prevent IRS business units from using the Treasury Enterprise Content Management environment.

Our assessment of the IRS's decision to not adopt the Treasury Department's shared service solution indicates that, by developing and maintaining its own SharePoint solution, the IRS may be incurring duplicate operational costs; operating in a less secure environment; and, in the event of a disruption, functioning in an environment in which SharePoint is not defined as a mission-critical system. Further, we found that the IRS solution did not provide a comparable level of operational capabilities related to security and disaster recovery as shown below. Figure 6 provides an overview of the size, security, and mission-critical attributes of the Treasury Enterprise Content Management solution verses the IRS SharePoint environment.

Figure 6: Key Attributes of the Treasury Enterprise Content Management and IRS SharePoint Environments As of December 9, 2014

Metric	Treasury	IRS
Sites	12,883	15,096
Site Collections	1,137	1,073
Database Size	1.1 Terabyte	3.09 Terabyte
Full-Time Equivalents	Federal: 12 Contractor: 20	Federal: 5 Contractor: 15
Security Assessment and Authorization	High	None
Disaster Recovery Prioritization	Mission-Critical	Not Mission-Critical

Source: Documentation provided by the IRS SharePoint Program Management Office.

Our review of the IRS SharePoint environment found that the IRS may be purchasing products and services that are already available in the Treasury Enterprise Content Management environment. We interviewed IRS IT officials to identify potential duplicate expenditures for the products and services that were available in the Treasury Enterprise Content Management environment, including SharePoint and automated tool licenses, help desk services, vendor contracts, and records management capabilities. IRS officials acknowledged that a thorough analysis of expenditures has not been completed and that taking this step would help to validate current assertions about SharePoint expenditures. The SharePoint Program Management Office allocated $5 million for operations and maintenance of the Fiscal Year 2016 IRS SharePoint program. However, sufficient cost information for SharePoint expenses across the IRS enterprise was not available to verify possible duplicate expenditures or potential net savings related to transitioning to the Treasury Enterprise Content Management environment.

Recommendations

The Chief Information Officer should:

Recommendation 9: Ensure that a feasibility analysis is conducted regarding use of the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.

> **Management's Response:** The IRS agreed with this recommendation. A feasibility analysis will be conducted regarding utilizing the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.

Recommendation 10: Ensure that the IRS's decision regarding use of the Treasury Enterprise Content Management environment is based on the conclusions of the above feasibility analysis.

> **Management's Response:** The IRS partially agreed with this recommendation. The IRS will include the results of the feasibility analysis, outlined in Recommendation 9, as one of the factors in the decision to use the Treasury Enterprise Content Management environment.
>
> **Office of Audit Comment:** The IRS partially agreed with this recommendation because the decision regarding whether to use the Treasury Enterprise Content Management environment will involve the results of the feasibility analysis as well as other factors, such as the perspectives of the business unit officials. We believe the IRS's corrective action appears responsive to the recommendation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to assess the IRS's implementation of SharePoint® operational and security controls, including user access privileges and protection of sensitive data on IRS SharePoint sites. To accomplish our objective, we:

I. Determined whether IRS SharePoint operations include a sufficient governance structure to guide necessary policies and procedures for administrators and owners with day-to-day operations of the SharePoint environment.

A. Interviewed EOps management officials responsible for managing the SharePoint infrastructure environment.

1. Identified and evaluated the responsibilities of management officials and staff in the EOps organization's SharePoint Program Management Office.
2. Identified and evaluated SharePoint roles and responsibilities for the business unit site collection[1] administrators and site collection owners.
3. Identified and evaluated the responsibilities of established SharePoint Governance Boards, including the decisions affecting the migration of the IRS SharePoint sites to the Treasury Enterprise Content Management environment.
4. Reviewed and evaluated the SharePoint policies for governance of the SharePoint environment, including the *SharePoint Site Owner's Guide*, Change Management, Site Collection Requests, and Site Deletion Requests.
5. Identified and evaluated activities to implement improvements to the SharePoint operational control environment (*i.e.*, corrective actions to prior TIGTA audit report findings[2] and implementation of an automated tool).

B. Interviewed management officials in the PGLD Office to determine their roles in controlling data that reside in the SharePoint environment, including PII and SBU data.

1. Reviewed and evaluated PGLD Office responsibilities in monitoring SharePoint sites that contain PII and SBU data.

[1] See Appendix V for a glossary of terms.
[2] TIGTA, Ref. No. 2013-20-023, *Improvements Are Needed to Ensure the Effectiveness of the Privacy Impact Assessment Process* p. 7 (Feb. 2013).

2. Reviewed and evaluated PGLD Office policies and procedures to monitor PII and SBU data on SharePoint sites.

II. Determined whether adequate SharePoint security controls are documented, approved, and implemented in the SharePoint environment.

A. Reviewed and evaluated security guidelines for the SharePoint environment, including IRM 10.8.1[3] and NIST Special Publication 800-53.[4]

B. Determined if applicable guidelines (IRM 10.8.1, NIST Special Publication 800-53, and Federal Information Processing Standards 199)[5] require an SA&A and classification (*i.e.*, low, moderate, or high) of SharePoint if it will contain PII or SBU data. We discussed with EOps and Cybersecurity officials their rationale for not performing an SA&A of SharePoint. We determined if an assessment of potential risks was performed. We evaluated the IRS justification.

C. Reviewed and evaluated configuration policy settings to determine how SharePoint users are being identified and authenticated.

D. Reviewed and evaluated how SharePoint groups and permissions are established and managed for users and administrators.

E. Reviewed and evaluated monitoring and audit trails that were in place for SharePoint.

F. Discussed with IRS personnel which IRS systems had permissions to view or edit PII or SBU data.

G. Determined the population of IRS SharePoint sites established after September 13, 2014,[6] selected a judgmental sample[7] of those IRS SharePoint sites, determined if the sites contained PII or SBU, and determined whether those sites had a PCLIA.

We coordinated our sampling approach with the TIGTA contract statistician, who assisted in selecting the judgmental sampling methodology and reviewed and approved the sampling plan. From the population of 1,303 IRS SharePoint sites created after September 13, 2014, we selected a judgmental sample of 16 sites. We selected the 16 SharePoint sites based primarily on whether the site names indicated the potential for the presence of taxpayer information.

[3] IRM 10.8.1, *Information Technology Security, Policy, and Guidance* (July 2015).
[4] NIST, Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).
[5] NIST, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).
[6] This is the date that the Privacy Office guidance regarding controls over the development of PCLIAs was to be incorporated into IRM 10.5.1, *Privacy, Information Protection, and Data Security*.
[7] A judgmental sample is a nonprobability sample, the results of which cannot be projected to the population.

1. Determined if the sampled sites contained PII or SBU.
2. If the sampled sites contained PII or SBU data, determined if a PCLIA existed at the site collection level.

III. Determined whether a SharePoint Information Technology Contingency Plan was developed in accordance with established security guidelines.

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: the SharePoint governance structure and decisions, including SharePoint operational policies and procedures; implementation of adequate security and privacy risk mitigation practices; and the SharePoint Information Technology Contingency Plan. We evaluated these controls by conducting interviews with management, reviewing and analyzing evidence of compliance with SharePoint guidelines, determining if management followed required security guidelines when developing and deploying the SharePoint environment, and selecting and testing a judgmental sample of SharePoint sites' security controls.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn A. McGowan, Director
Carol L. Taylor, Audit Manager
Wallace C. Sims, Lead Auditor
Mildred Rita Woody, Senior Auditor
Felicia A. Heard, Information Technology Specialist

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
National Taxpayer Advocate
Commissioner, Large Business and International Division
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Strategy and Planning
Director, Office of Audit Coordination

Appendix IV

Timeline of Events for the Treasury Enterprise Content Management and IRS SharePoint Environments

Year	Agency	Event
2010	IRS	IRS personnel were on the Treasury Executive Steering Committee and actively participated in establishing the Treasury Enterprise Content Management governance structure.
2010	Treasury	The Treasury Department Assistant Secretary for Management and Chief Financial Officer issued a policy memorandum to bureau and departmental office heads announcing that the Treasury Department is focused on increasing the efficiencies of departmental operations and will soon begin leveraging the Enterprise Content Management program to provide the strategy, management discipline, architectural framework, and technology to meet this goal.
2010	Treasury	The Treasury Department Assistant Secretary for Management announced the formation of an Enterprise Content Management Executive Steering Committee to identify which existing and prospective information technology investments would participate in the Enterprise Content Management program and manage implementation.
2010	Treasury	All Treasury Department offices were required to be governed by the Enterprise Content Management Executive Steering Committee for information technology systems and services associated with the Freedom of Information Act; eDiscovery; correspondence tracking; collaborative document review; evidence management; case management; and paper reduction through digitization, accessibility, and storage of information in a centralized records repository. Enterprise Content Management is a set of web-based tools to electronically capture, store, search, analyze, collaborate, share, and manage documents. At its core, Enterprise Content Management uses SharePoint, which is an online platform for inter-office collaboration and centralization.

Year	Agency	Event
2011	Treasury	The Federal Information Processing Standards 199 security categorization for the Treasury Enterprise Content Management environment is as follows: **Security Category** **Rating** Confidentiality High Integrity High Availability Moderate Overall High
2011	Treasury	The Treasury Department Deputy Assistant Secretary for Information Systems and Chief Information Officer issued a memorandum to all bureau Chief Information Officers mandating establishment of a two-way trust between each bureau and the Treasury Enterprise Content Management environment by July 29, 2011. The Enterprise Content Management environment provides a collaborative workspace and a consistent development platform from which applications can be built throughout the Treasury Department and, correspondingly, decreases duplication of effort across the Treasury Department.
2012	IRS	IRS staff began to use the Treasury Enterprise Content Management environment for their SharePoint sites or applications: • goFOIA: Freedom of Information Act requests and dispositions. • Clearance Tracker: Items requiring the Secretary of the Treasury's signature.
2012	IRS	IRS Cybersecurity established a one-way trust with the Treasury Enterprise Content Management environment based on an Interconnection Security Agreement.
2013	IRS	Additional IRS staff began to use the Treasury Enterprise Content Management environment for their SharePoint sites or applications: • eCase Suspension and Debarment: Treasury-wide legal actions for those suspected of defrauding the Government. • EEO eComplaints: Treasury-wide equal opportunity case management. • Franchise Fund: All franchise fund budget and Interagency Agreements, including the IRS Interagency Agreement, are managed though this system. • eCase: Case management system for major IRS tax cases. • Enterprise Content Management Business Intelligence: Used by the IRS Vendor Management team.

Year	Agency	Event
2014	IRS	Additional IRS staff began to use the Treasury Enterprise Content Management environment for their SharePoint sites or applications: • Integrated Apportionment Tracker: Treasury-wide budget management system. • TFIMS: Treasury-wide Federal Information Security Modernization Act Information Management System. • Telework: IRS Telework application.
2014	IRS	Taxpayer Advocate Service officials asked IRS IT officials to migrate their SharePoint sites and data to the Treasury Enterprise Content Management environment because of a need to be on a mission-critical platform and concerns about lack of funding and information technology support of the IRS SharePoint environment.
2014	IRS	The IRS Chief Information Officer did not allow Taxpayer Advocate Service officials to migrate to the Treasury Enterprise Content Management environment and directed all business units currently on the Treasury Enterprise Content Management environment to return to the IRS SharePoint environment.

Source: Treasury Department and IRS documents.

Appendix V

Glossary of Terms

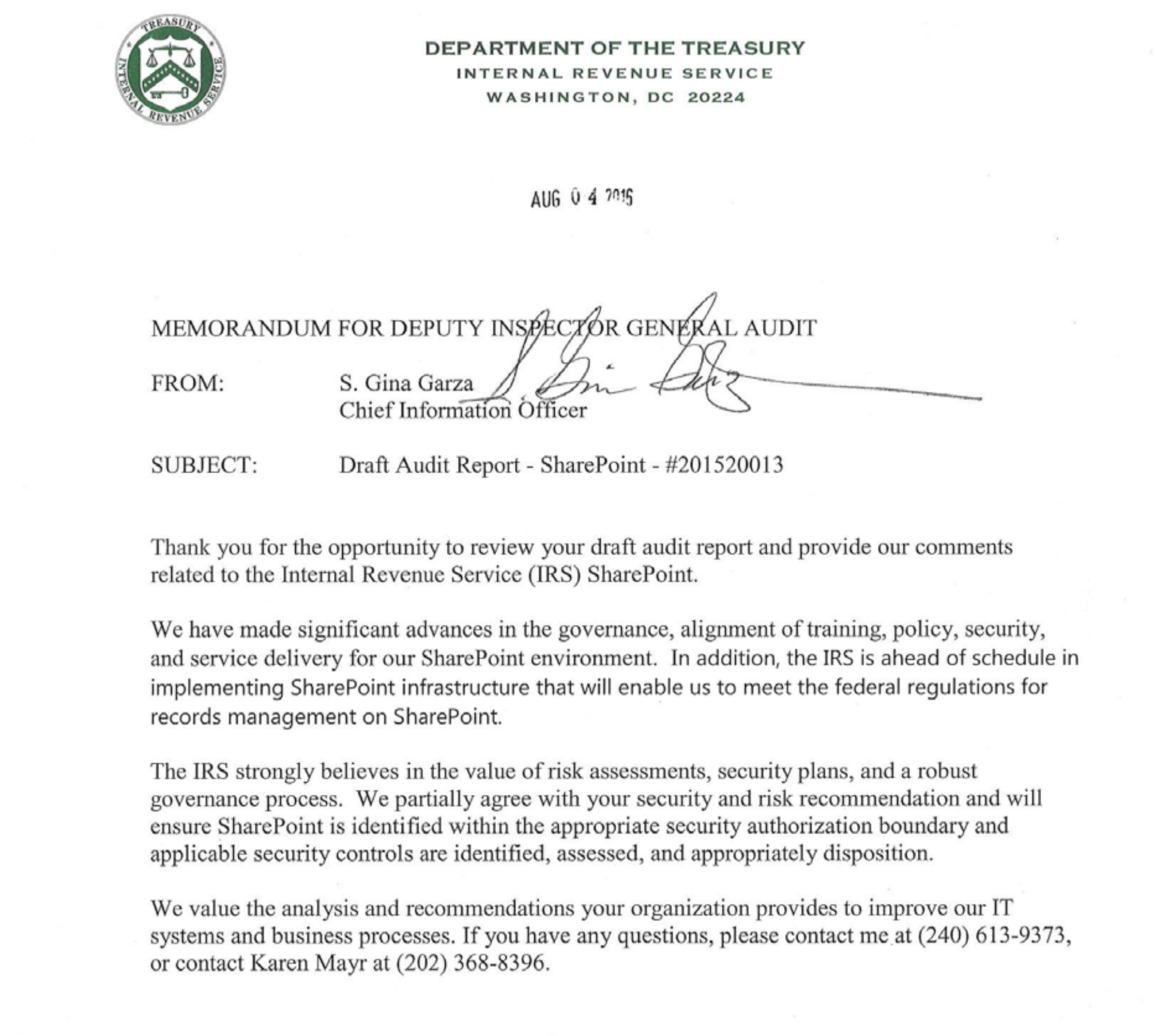
Term	Definition
Audit Trail	Maintains a record of system activity, both by system and application processes and by user activity on systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
Availability	Ensuring timely and reliable access to and use of information.
Best Practice	A technique or methodology that, through experience and research, has proven to reliably lead to a desired result.
Business Impact Analysis	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Commercial Off-the-Shelf	Prepackaged, vendor-supplied software that will be used with little or no modification to provide all or part of the solution.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including a means for protecting personal privacy and proprietary information.
Enterprise Life Cycle	Establishes a set of repeatable processes and a system of reviews, checkpoints, and milestones that reduce the risks of system development and ensure alignment with the overall business strategy.
Federal Information Processing Standards 199	Standards for categorizing information and information systems; establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems.
Information System Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Integrity	Guarding against improper information modification or destruction; includes ensuring information nonrepudiation and authenticity.
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.

Term	Definition
Privacy and Civil Liberties Impact Assessment	An analysis of how information in an identifiable form is collected, stored, protected, shared, and managed. The process also provides a means to assure compliance with all applicable laws and regulations governing taxpayer and employee privacy.
Production Environment	The location where the real-time staging of programs that run an organization are executed; this includes the personnel, processes, data, hardware, and software needed to perform day-to-day operations.
Risk Assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of an information system.
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in Federal Information Processing Standards 199 for non–national security systems.
Security Controls	The management, operational, and technical controls (prescribed for an information system) to protect the confidentiality, integrity, and availability of the system and its information.
Sensitive But Unclassified	Refers to any information that, if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest, the conduct of Federal programs (including IRS operations), or the privacy to which individuals are entitled under the Freedom of Information Act (5 U.S.C. 552).
Site Collections	A site collection is a logical container for grouping sites and allows hierarchical arrangement of sites within it. A site collection has exactly one default top-level site and may have many subsites. By default, all sites of a site collection share navigation, security, permissions, templates, and content types.
Sites	A site allows the IRS to organize and store all content in SharePoint; the content can be lists, libraries (document, picture, report, and form), web pages, or sites. Further, a site can have subsites in its hierarchy.
Standard Employee Identifier	The standard identifier for any user of an IRS system. A randomly generated five-character designation.
System Security Plan	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Taxpayer Advocate Service	An independent organization within the IRS to help taxpayers resolve problems with the IRS and recommend changes that will prevent the problems.

Term	Definition
Technical Controls	Security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of a system.
Web Application	In the SharePoint hierarchy, a web application is the top tier. It is an Internet Information Services website that is specifically configured to run as a SharePoint site and contains at least one or more site collections.

Appendix VI

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

AUG 0 4 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL AUDIT

FROM: S. Gina Garza
Chief Information Officer

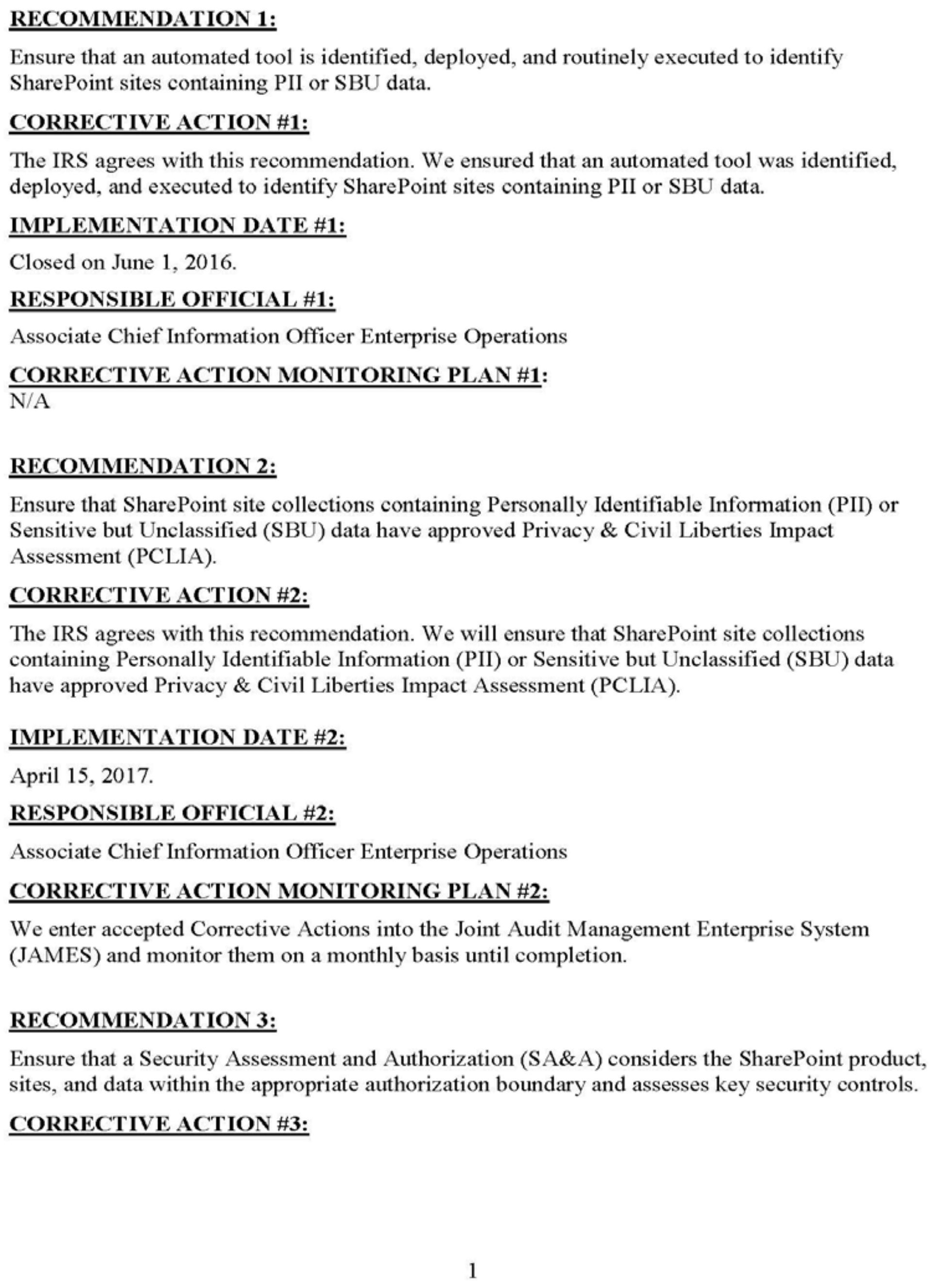
SUBJECT: Draft Audit Report - SharePoint - #201520013

Thank you for the opportunity to review your draft audit report and provide our comments related to the Internal Revenue Service (IRS) SharePoint.

We have made significant advances in the governance, alignment of training, policy, security, and service delivery for our SharePoint environment. In addition, the IRS is ahead of schedule in implementing SharePoint infrastructure that will enable us to meet the federal regulations for records management on SharePoint.

The IRS strongly believes in the value of risk assessments, security plans, and a robust governance process. We partially agree with your security and risk recommendation and will ensure SharePoint is identified within the appropriate security authorization boundary and applicable security controls are identified, assessed, and appropriately disposition.

We value the analysis and recommendations your organization provides to improve our IT systems and business processes. If you have any questions, please contact me at (240) 613-9373, or contact Karen Mayr at (202) 368-8396.



RECOMMENDATION 1:

Ensure that an automated tool is identified, deployed, and routinely executed to identify SharePoint sites containing PII or SBU data.

CORRECTIVE ACTION #1:

The IRS agrees with this recommendation. We ensured that an automated tool was identified, deployed, and executed to identify SharePoint sites containing PII or SBU data.

IMPLEMENTATION DATE #1:

Closed on June 1, 2016.

RESPONSIBLE OFFICIAL #1:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #1:

N/A

RECOMMENDATION 2:

Ensure that SharePoint site collections containing Personally Identifiable Information (PII) or Sensitive but Unclassified (SBU) data have approved Privacy & Civil Liberties Impact Assessment (PCLIA).

CORRECTIVE ACTION #2:

The IRS agrees with this recommendation. We will ensure that SharePoint site collections containing Personally Identifiable Information (PII) or Sensitive but Unclassified (SBU) data have approved Privacy & Civil Liberties Impact Assessment (PCLIA).

IMPLEMENTATION DATE #2:

April 15, 2017.

RESPONSIBLE OFFICIAL #2:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #2:

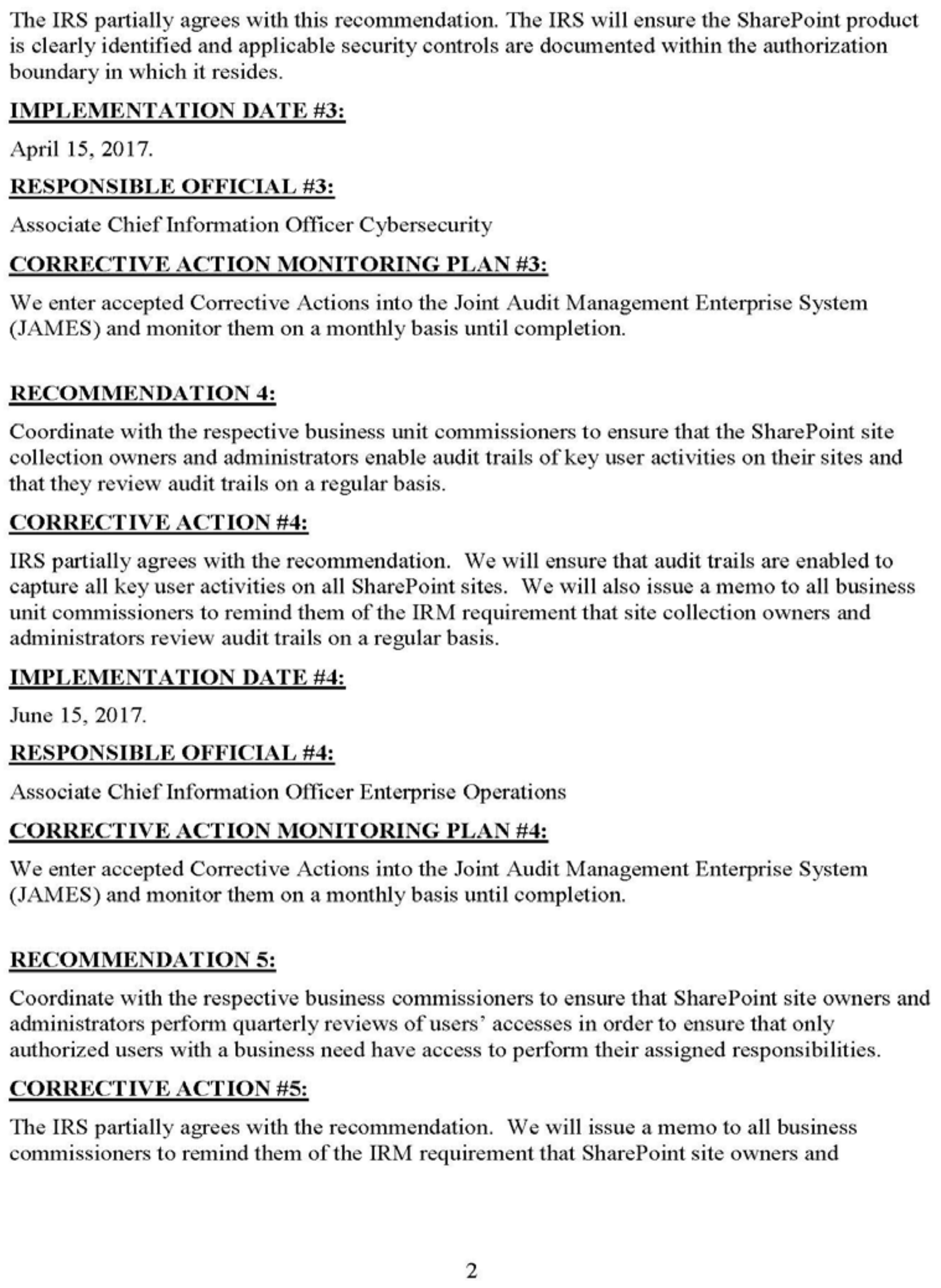
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 3:

Ensure that a Security Assessment and Authorization (SA&A) considers the SharePoint product, sites, and data within the appropriate authorization boundary and assesses key security controls.

CORRECTIVE ACTION #3:

1



The IRS partially agrees with this recommendation. The IRS will ensure the SharePoint product is clearly identified and applicable security controls are documented within the authorization boundary in which it resides.

IMPLEMENTATION DATE #3:

April 15, 2017.

RESPONSIBLE OFFICIAL #3:

Associate Chief Information Officer Cybersecurity

CORRECTIVE ACTION MONITORING PLAN #3:

We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 4:

Coordinate with the respective business unit commissioners to ensure that the SharePoint site collection owners and administrators enable audit trails of key user activities on their sites and that they review audit trails on a regular basis.

CORRECTIVE ACTION #4:

IRS partially agrees with the recommendation. We will ensure that audit trails are enabled to capture all key user activities on all SharePoint sites. We will also issue a memo to all business unit commissioners to remind them of the IRM requirement that site collection owners and administrators review audit trails on a regular basis.

IMPLEMENTATION DATE #4:

June 15, 2017.

RESPONSIBLE OFFICIAL #4:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #4:

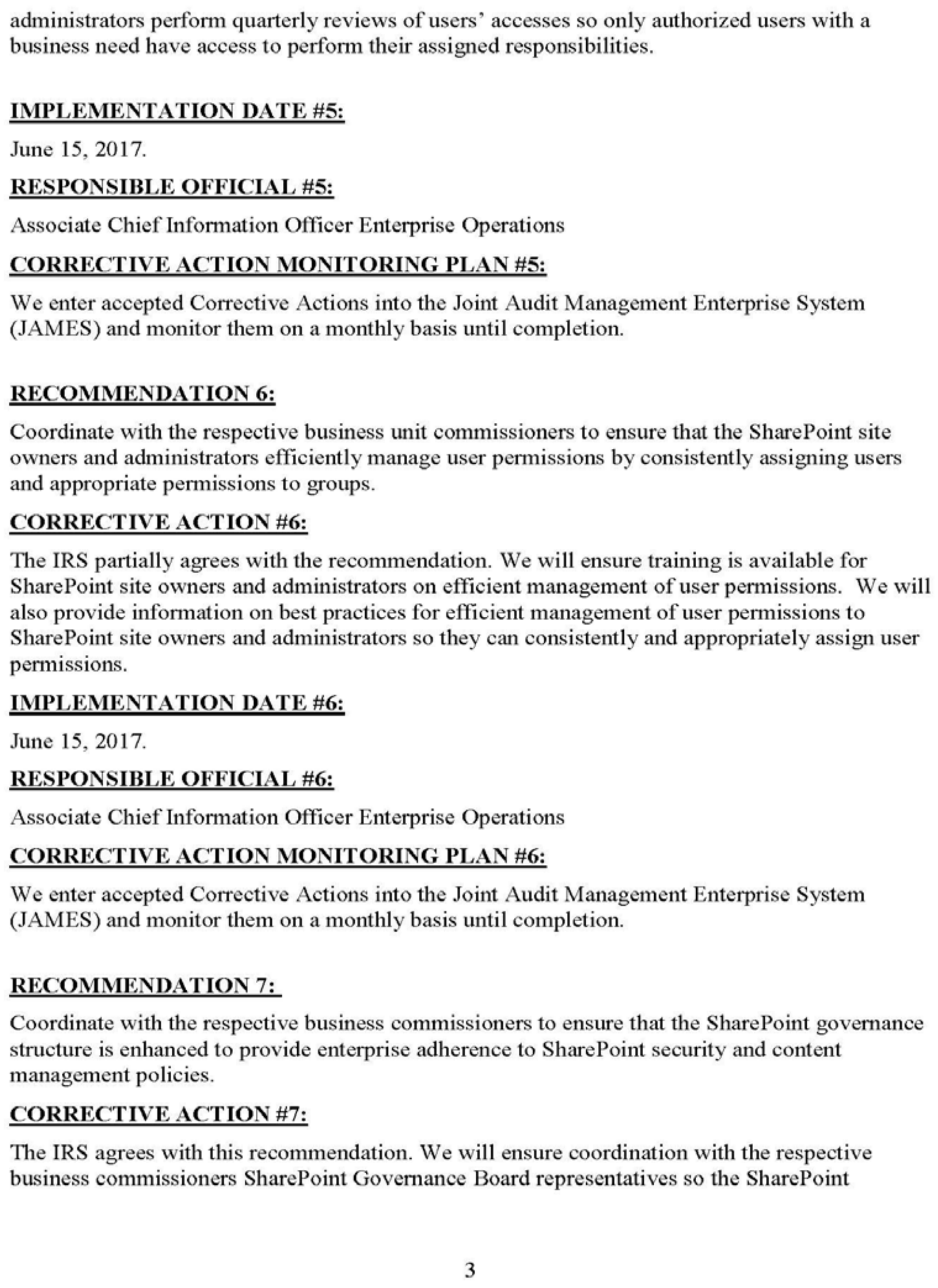
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 5:

Coordinate with the respective business commissioners to ensure that SharePoint site owners and administrators perform quarterly reviews of users' accesses in order to ensure that only authorized users with a business need have access to perform their assigned responsibilities.

CORRECTIVE ACTION #5:

The IRS partially agrees with the recommendation. We will issue a memo to all business commissioners to remind them of the IRM requirement that SharePoint site owners and



administrators perform quarterly reviews of users' accesses so only authorized users with a business need have access to perform their assigned responsibilities.

IMPLEMENTATION DATE #5:

June 15, 2017.

RESPONSIBLE OFFICIAL #5:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #5:

We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 6:

Coordinate with the respective business unit commissioners to ensure that the SharePoint site owners and administrators efficiently manage user permissions by consistently assigning users and appropriate permissions to groups.

CORRECTIVE ACTION #6:

The IRS partially agrees with the recommendation. We will ensure training is available for SharePoint site owners and administrators on efficient management of user permissions. We will also provide information on best practices for efficient management of user permissions to SharePoint site owners and administrators so they can consistently and appropriately assign user permissions.

IMPLEMENTATION DATE #6:

June 15, 2017.

RESPONSIBLE OFFICIAL #6:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #6:

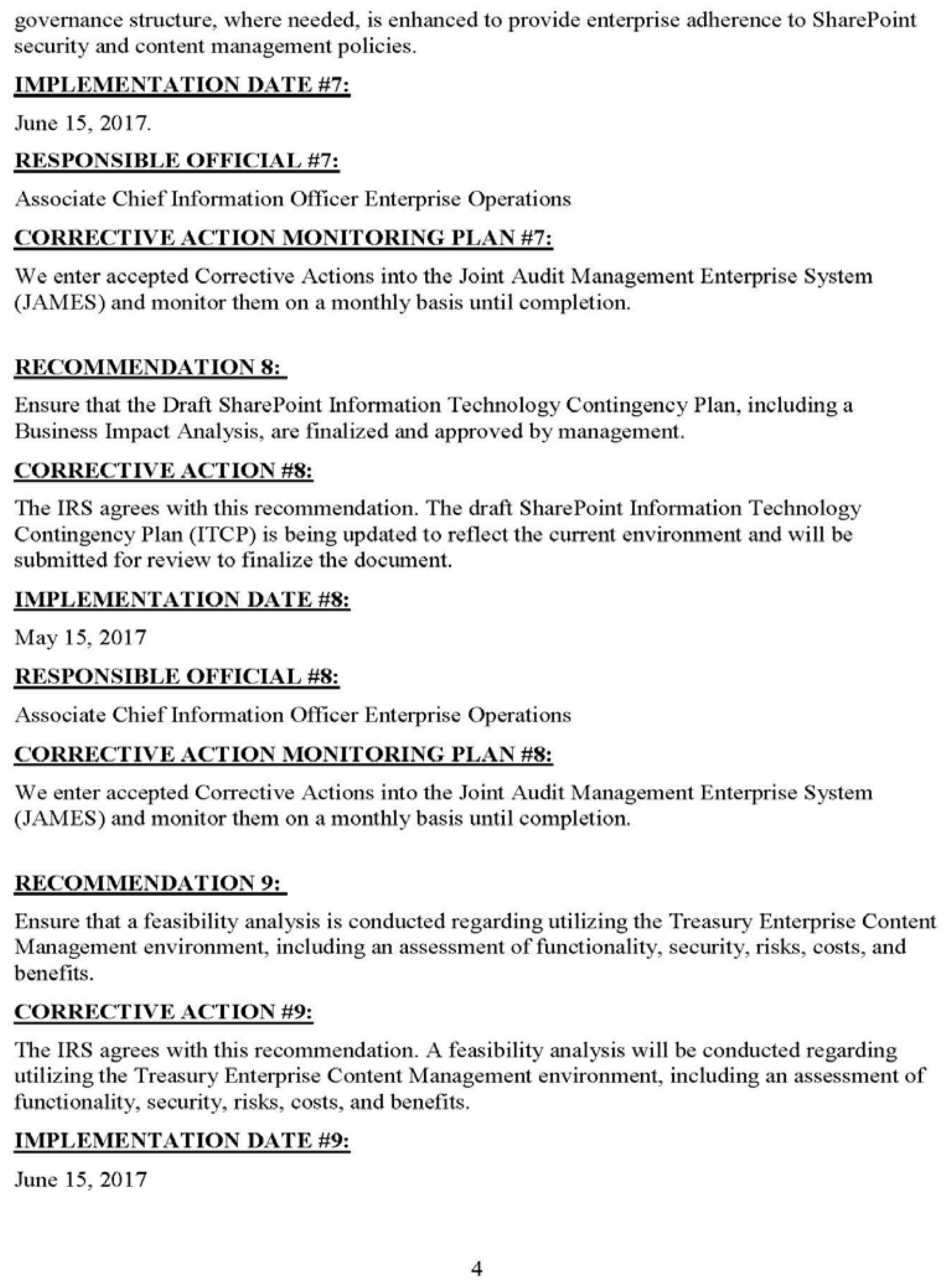
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 7:

Coordinate with the respective business commissioners to ensure that the SharePoint governance structure is enhanced to provide enterprise adherence to SharePoint security and content management policies.

CORRECTIVE ACTION #7:

The IRS agrees with this recommendation. We will ensure coordination with the respective business commissioners SharePoint Governance Board representatives so the SharePoint



governance structure, where needed, is enhanced to provide enterprise adherence to SharePoint security and content management policies.

IMPLEMENTATION DATE #7:

June 15, 2017.

RESPONSIBLE OFFICIAL #7:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #7:

We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 8:

Ensure that the Draft SharePoint Information Technology Contingency Plan, including a Business Impact Analysis, are finalized and approved by management.

CORRECTIVE ACTION #8:

The IRS agrees with this recommendation. The draft SharePoint Information Technology Contingency Plan (ITCP) is being updated to reflect the current environment and will be submitted for review to finalize the document.

IMPLEMENTATION DATE #8:

May 15, 2017

RESPONSIBLE OFFICIAL #8:

Associate Chief Information Officer Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN #8:

We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 9:

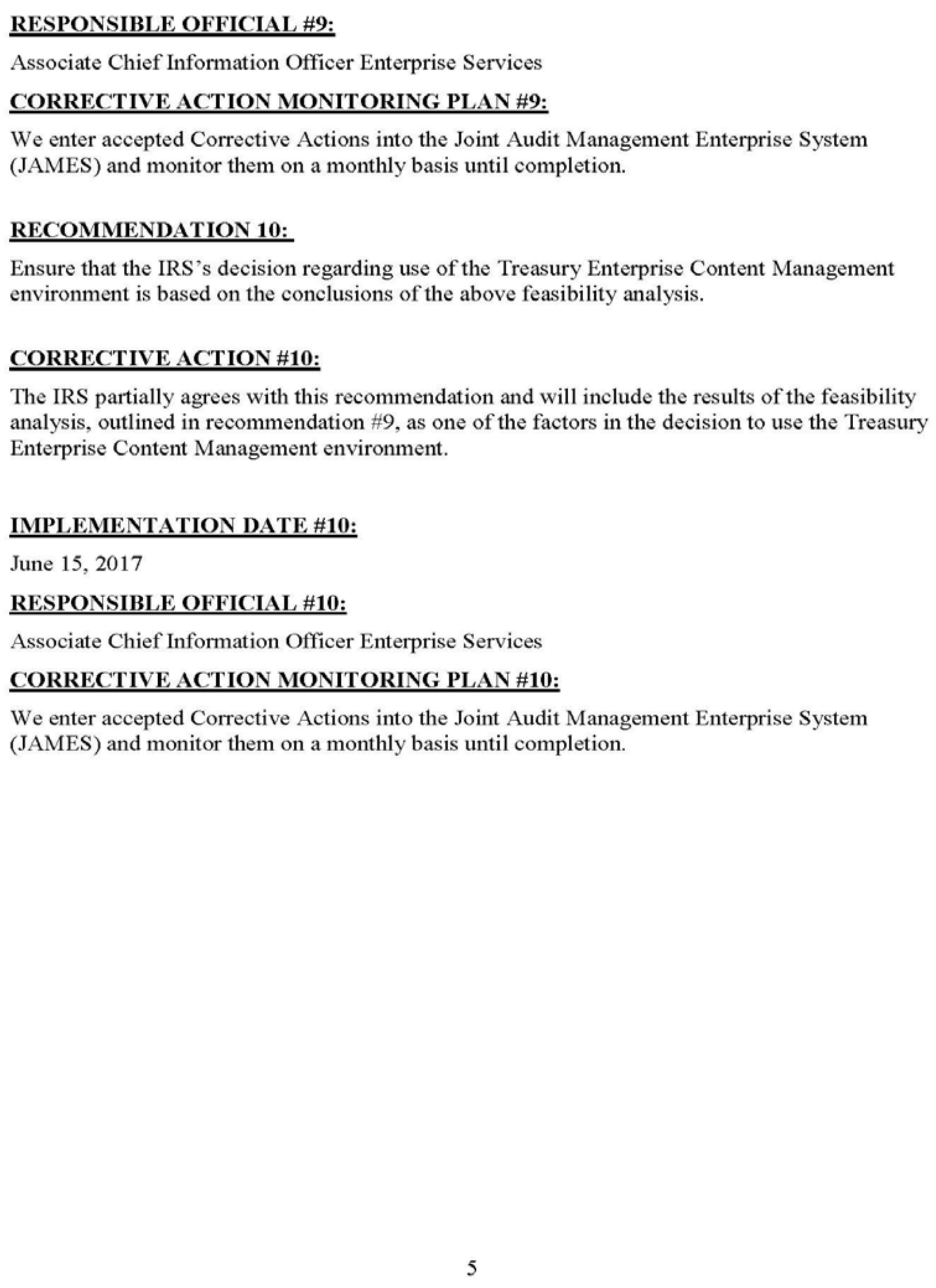
Ensure that a feasibility analysis is conducted regarding utilizing the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.

CORRECTIVE ACTION #9:

The IRS agrees with this recommendation. A feasibility analysis will be conducted regarding utilizing the Treasury Enterprise Content Management environment, including an assessment of functionality, security, risks, costs, and benefits.

IMPLEMENTATION DATE #9:

June 15, 2017



RESPONSIBLE OFFICIAL #9:

Associate Chief Information Officer Enterprise Services

CORRECTIVE ACTION MONITORING PLAN #9:

We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION 10:

Ensure that the IRS's decision regarding use of the Treasury Enterprise Content Management environment is based on the conclusions of the above feasibility analysis.

CORRECTIVE ACTION #10:

The IRS partially agrees with this recommendation and will include the results of the feasibility analysis, outlined in recommendation #9, as one of the factors in the decision to use the Treasury Enterprise Content Management environment.

IMPLEMENTATION DATE #10:

June 15, 2017

RESPONSIBLE OFFICIAL #10:

Associate Chief Information Officer Enterprise Services

CORRECTIVE ACTION MONITORING PLAN #10:

We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.