MANUAL TRANSMITTAL

3.0.276

Department of the Treasury
Internal Revenue Service

DECEMBER 27, 2022

EFFECTIVE DATE

(12-27-2022)

PURPOSE

(1) This transmits revised IRM 3.0.276, *General, Scorecard Performance Measure Process - Security and Internal Control Review*.

MATERIAL CHANGES

(1) IRM 3.0.276.2.1 - Revised second bullet to add data-driven improvements - IPU issued 10-28-2020.

(2) IRM 3.0.276.2.4 - Revised to add first two bullets to the campus managers roles - IPU issued 10-28-2020.

(3) IRM 3.0.276.2.5 – (4) a) Added instructions to send the Custom Calendar Review Scheduler to SOI only if a weekend day is selected. Deleted (5) f and moved to new paragraph (6). Added new paragraph (6), clarified to complete Internal Control checklist and monthly Security Review, then prepare Campus Report - IPU issued 06-09-2020.

EFFECT ON OTHER DOCUMENTS

IRM 3.0.276 General, Scorecard Performance Measure Process - Security and Internal Control Review, dated May 29, 2019, and effective August 1, 2019, is superseded. The following IRM Procedural Updates (IPUs) have been incorporated into this IRM: 20U0679 issued 06-09-2020 and 20U1167 issued 10-28-2020.

AUDIENCE

These procedures apply to Submission Processing Headquarters; Program Management/Process Assurance Branch, Coordination & Quality Support Section, Accounting & Tax Payment Branch, Paper Processing Branch, Submission Processing Center(s) management and their designated representative.

James L. Fish
Director, Submission Processing
Wage & Investment Division

3.0.276
General, Scorecard Performance Measure Process - Security and Internal Control Review

Table of Contents

3.0.276.1 Program Scope and Objectives
3.0.276.1.1 Background
3.0.276.1.2 Authority
3.0.276.1.3 Responsibilities
3.0.276.1.4 Program Management and Review
3.0.276.1.5 Program Controls
3.0.276.1.6 Terms/Definitions/Acronyms
3.0.276.1.7 Related Resources
3.0.276.1.7.1 Protecting Taxpayer Data
3.0.276.2 Overview of Submission Processing Scorecard Measure Process - Security and Internal Control
3.0.276.2.1 Purpose of Submission Processing Scorecard Measure Process - Security and Internal Control
3.0.276.2.2 Use of Submission Processing Scorecard Measure Process - Security and Internal Control
3.0.276.2.2.1 Roles and Responsibilities in the Submission Processing Scorecard Measure Process - Security and Internal Control
3.0.276.2.2.2 W&I Submission Processing Headquarters Roles
3.0.276.2.3 Submission Processing Field Directors
3.0.276.2.4 Submission Processing P&A Chiefs, Operations Department, and Frontline Managers
3.0.276.2.5 Submission Processing Center Designated Reviewer(s)

3.0.276.1
(08-01-2019)
Program Scope and Objectives

(1) This IRM provides administrative instructions for the Internal Control, Security Review process at the Submission Processing Center(s).

(2) **Purpose:** Wage & Investment (W&I) is committed to an effective Internal Control performance measurement process to demonstrate the IRS commitment to high standards for safeguarding hard copy receipts and protecting taxpayer information.

(3) **Audience:** These procedures apply to Submission Processing (SP) Headquarter (HQ) branches, Coordination & Quality Support Section (CQS) within the Program Management/Process Assurance (PM) Branch, Accounting & Tax Payment (ATP), and Paper Processing Branch (PPB), and SP Center Management/Designated Reviewers.

(4) **Policy Owner:** The Director, Submission Processing oversees the policies in this IRM.

(5) **Program Owner:** Submission Processing, Program Management/Process Assurance Branch, Coordination & Quality Support Section (CQS).

(6) **Primary Stakeholders:** Submission Processing.

(7) **Program Goals:** This information is used to provide instructions for administrative roles to complete the Scorecard Performance Measure Process - Security and Internal Control Reviews.

3.0.276.1.1
(08-01-2019)
Background

(1) The purpose of the Scorecard Performance Measure Process - Security and Internal Control Reviews is to measure that each SP Center maintains an appropriate level of Security and Internal Control in the review components reviewed.

3.0.276.1.2
(08-01-2019)
Authority

(1) The following provides authority for the instructions in this IRM to be performed, IRM 1.4.2, *Monitoring and Improving Internal Control*.

3.0.276.1.3
(08-01-2019)
Responsibilities

(1) The Director, Submission Processing is the executive responsible for the Scorecard Performance Measure Process - Security and Internal Control.

(2) Program Management/Process Assurance Branch (PM), Coordination & Quality Support Section (CQS) has oversight for the Scorecard Performance Process - Security and Internal Control which includes coordinating, maintaining, and distributing updates to documents annually, monthly or as needed to internal and external customers.

(3) The CQS manager ensures the IRM is timely submitted to Publishing each year.

(4) The Accounting & Tax Payment (ATP) Branch IRM Author(s) will coordinate with CQS any IRM updates that impact the Scorecard Performance Measure Process - Security and Internal Controls.

(5) The Paper Processing Branch (PPB) IRM Author(s) will coordinate with CQS any IRM updates that impact the Scorecard Performance Measure Process - Security and Internal Controls.

(6) Statistics of Income (SOI) has oversight for maintaining the document titled, "Appendix 1 - Summary of Scoring Rules", the Custom Calendar Review Scheduler, the Data Collection Instrument and related instructions.

(7) Each SP Center Field Director, Operation, Department, and Frontline managers must maintain the integrity and quality of the Scorecard Performance Process - Security and Internal Controls.

(8) The SP Center Management or SP Center Designated Reviewer(s) have oversight to perform a monthly unbiased, consistent, and accurate review of Security and Internal Control Reviews.

3.0.276.1.4
(08-01-2019)
Program Management and Review

(1) **Program Reports** W&I is dedicated to a proactive approach of reviewing operations and evaluating controls that are in place. A responsibility of the Federal Government is to ensure management controls are in place and working as intended. W&I is committed to an effective internal control performance measurement process.

(2) **Program Effectiveness** SP established a review process to evaluate the success of maintaining an appropriate level of security and internal controls based on consistent review criteria and methodology for gathering reliable data and results. Organizational reviews are extremely important to the IRS and can result in saved resources, enhanced mission accomplishments, and more effective responses to issues identified by the Government Accountability Office (GAO) and the Treasury Inspector General for Tax Administration (TIGTA).

3.0.276.1.5
(08-01-2019)
Program Controls

(1) Goals, measures and operating guidelines are listed in the yearly Scoring Methodology.

(2) Each SP Center will conduct a monthly review of each Review Component and Internal Control Checklist as part of the Scorecard Performance Measure Process - Security and Internal Control Review.

3.0.276.1.6
(08-01-2019)
Terms/Definitions/ Acronyms

(1) In this IRM section is a list of common terms used throughout this IRM.

Defined Terms

Term	Definition
Appendix 1 - Scoring Rules	SOI created document for the Security Review that identifies **"met"** or **"not met"** checkpoints (CP) for each Review Component that is part of the Scoring Methodology.

Term	Definition
Campus Report	Monthly roll-up report of the Internal Control Checklist which includes action(s) to prevent future vulnerabilities for: • Manual Refunds • Form 809, Receipt for Payment of Taxes (for cash received in the mail) • Field Office Payment Processing ***Note:*** No scoring methodology applies to the Campus Report .
Checkpoint (CP)	Individual review points that make up a Review Component as part of the Security Review.
Custom Calendar Review Scheduler	Monthly tool that randomly selects days of review for each Review Component as part of the Security Review, which includes option(s) to customize days, swing/night shifts, and weekends.
Data Collection Instrument (DCI)	The Security Review is to capture data related to each Review Component and their corresponding CP. The DCI is generally programmed to create a score of **"met"** or **"not met "** for each CP. ***Note:*** Not Applicable, **"NA",** may be used for some CP(s). The Center will provide an explanation on the additional comments tab on the corresponding DCI to substantiate the **"NA"** for the corresponding CP(s).
Internal Control Checklist	Monthly unmeasured review (yes/no questions) of vulnerabilities identified by HQ, GAO, TIGTA for: • Manual Refunds • Form 809, Receipt for Payment of Taxes (for cash received in the mail) • Field Office Payment Processing ***Note:*** No scoring methodology applies to the Internal Control Checklist. These vulnerabilities may change from year to year as items are identified.
Finding	Term used on the Campus Report. A finding is a **"not met"** CP on the Security Review DCIs.

Term	Definition
Review Component	Topic that identifies area(s) to be reviewed as part of the Security Review. The review components include: • Candling • Courier • Discovered Cash Inside of Receipt & Control (R&C) • Discovered Remittances, Cash or Items of Value Outside of R&C • Overstamping • Physical Security • Remittance Security
Scorecard	Is created monthly by SOI. The scorecard is a monthly summary of the Security Review and includes **"met"** and **"not met "** Review Components. The Scorecard includes a monthly numeric **"score"** for the month. The numeric score breakdown can be located on the, Scoring Methodology.
Scoring Methodology	Breakdown of the Security Review, Appendix 1 - Scoring Rules, of each checkpoint that receives a score of **"met"** and **"not met"** and are reviewed as part of the Review Components.
Scorecard Performance Measure Process - Security and Internal Control	SP organization review process to measure our success of maintaining an appropriate level of security and internal controls based on consistent review criteria and methodology for gathering reliable data and results.
Security Review	Measured review which includes seven Review Components.
Special Scoring Caveat	The document titled, Appendix 1 - Scoring Rules states, if a checkpoint received a **"not met"** in consecutive months, then the tolerance of one checkpoint rated **"not met"** is revoked and the SP Center will receive a **"not met"** for the month. **Note:** The Special Scoring Caveat applies to the following Review Components: Candling, Overstamping, and Physical Security.
Vulnerability	Term used on the Campus Report which identifies a topic coded as **"no"** on the Internal Control review.

Acronyms

ATP	Accounting & Tax Payment Branch
CP	Checkpoint
CQS	Coordination & Quality Support Section
GAO	Government Accountability Office
HQ	Headquarters
PM	Program Management/Process Assurance Branch
PPB	Paper Processing Branch
R&C	Receipt & Control
SOI	Statistics of Income
TIGTA	Treasury Inspector General for Tax Administration

3.0.276.1.7
(08-01-2019)
Related Resources

(1) **IRM Deviation Statement:** IRM Deviations must be submitted in writing following instructions from IRM 1.11.2.2, IRM Standards, and elevated through appropriate channels for executive approval. No deviations can begin until reviewed by the Program Owner and approved by the Policy Owner (Executive Level).

(2) The following IRMs outline the tasks related to a review component and/or vulnerability topic:

a. Candling, Overstamping, and Remittance Security -IRM 3.10.72 , *Campus Mail and Work Control, Receiving, Extracting, and Sorting*
b. Courier - IRM 3.8.45, *Deposit Activity, Manual Deposit Process*
c. Discovered Cash Outside/Inside of Receipt & Control - IRM 3.8.46, *Deposit Activity, Discovered Remittance*
d. Physical Security - IRM 10.2.11, *Security, Privacy, and Assurance, Physical Security Program, Basic Security Concepts*
e. Forms 809 for cash received in the mail and Field Office Payment Processing - IRM 3.8.47, *Manual Deposit for Field Office Payment Processing*
f. Manual Refunds - IRM 3.17.79, *Accounting & Data Control, Accounting Refund Transactions*

(3) There are multiple documents related to the Security and Internal Control Review process. Contact the PM CQS HQ Analyst to request documents needed to complete these reviews.

3.0.276.1.7.1
(08-01-2019)
Protecting Taxpayer Data

(1) While conducting internal control activities employees are responsible to safeguard documents with Sensitive but Unclassified (SBU) data (including Personally Identifiable Information (PII) and tax information). The obligation to protect taxpayer privacy and to safeguard the information taxpayers entrust to us is a fundamental part of the IRS Mission. Taxpayers have the right to expect that the information they provide will be safeguarded and used only per the law. Protecting taxpayer data is the responsibility of all IRS employees and IRS contractors (including contractors, subcontractors, non-IRS-procured contractors, vendors, and outsourcing providers).

(2) To implement the requirements of the Taxpayer Browsing Protection Act, the IRS created the willful unauthorized access (UNAX), attempted access or inspection of taxpayer records, (UNAX) program. Willful unauthorized access or inspection of taxpayer records is a crime, punishable upon conviction, by fines, imprisonment, and termination of employment. Taxpayer records include hard copies and electronic formats of returns and return information. Unauthorized access or inspection is looking or accessing tax records that are not necessary to complete official IRS duties as assigned by management.

(3) The public expects that IRS records are available where and when they are needed, by whom they are needed, for only as long as they are needed, in order to conduct business, adequately document IRS activities, and protect the interests of the federal government and American taxpayer. All IRS records are required under the Federal Records Act to be efficiently managed until final disposition.

(4) Adhere to current policy to dispose of all taxpayer information that must be discarded in a classified waste receptacle according to the work type. Proper disposition of taxpayer information will prevent unauthorized disclosure of confidential information and the unlawful/unauthorized destruction of records. For additional information refer to IRM 10.5.1, *Privacy and Information Protection, Privacy Policy.*

(5) Do not use taxpayer information to post as a visual aid, etc. Notify management immediately when these items are identified within the workplace. If in doubt about the validity of the posted information, discuss the issue with your supervisor.

(6) Direct any other problems concerning disclosure matters (Privacy Act, Freedom of Information Act, IRC 6103) to Disclosure. See the *Contact Disclosure* web page for contact information.

(7) Any employee who has knowledge of an actual or suspected **willful** unauthorized access (UNAX) violation, must immediately contact the local Inspector General Special Agent, or call the Treasury Inspector General for Tax Administration (TIGTA) Hotline at 1–800–366–4484.

(8) All IRS employees are required to report the loss or theft of an IRS Information Technology (IT) asset, or an asset in the Bring Your Own Device program, or hardcopy record or document containing SBU data, including PII and tax information, or the inadvertent unauthorized disclosure of SBU data, including PII and tax information, whether it be electronically, verbally or in hardcopy form, within one hour. The timely reporting of all inadvertent unauthorized disclosures of SBU data, including PII and tax information, and all losses or thefts of SBU/PII and IT assets and BYOD assets is critical for quickly initiating any needed investigation or recovery of information. A prompt report decreases the

possibility that the information will be compromised and used to perpetrate identity theft or other forms of harm. See IRM 10.5.4.3, **Reporting Losses, Theft and Disclosures,** and the **Data Protection** page in the *Disclosure and Privacy Knowledge Base Site*.

(9) For additional information regarding willful unauthorized access (UNAX), refer to IRM 10.5.5, *Security, Privacy and Assurance, Privacy and Information Protection* or Inspection of Taxpayer Records (UNAX) Program or the Supplemental Guide for IRS' Awareness Briefing on Unauthorized Access-UNAX for additional information, or contact the Privacy, Governmental Liaison and Disclosure UNAX Program Office via email at *UNAX. The UNAX website is as at the following email address UNAX Web page.

3.0.276.2
(08-01-2019)
Overview of Submission Processing Scorecard Measure Process - Security and Internal Control

(1) This section is designed to provide procedures for SP Center reviews for Security Review and Internal Control Checklist.

- Security Review **(measured)** which includes the following review components:
  Candling
  Courier
  Discovered Cash Inside of R&C
  Discovered Remittances, Cash or Items of value outside of R&C
  Overstamping
  Physical Security
  Remittance Security
- Internal Control Checklist **(unmeasured)** which includes the following identified vulnerabilities:
  Forms 809 for Cash Refund in the Mail
  Field Office Payment Processing
  Manual Refund

3.0.276.2.1
(10-28-2020)
Purpose of Submission Processing Scorecard Measure Process - Security and Internal Control

(1) The purpose of the SP Scorecard Measure Process - Security and Internal Control is to:

- Provide a positive control environment
- Identify potential risk area(s) and make data-driven improvements
- Ensure adequate and effective controls are in place
- Report results of reviews to the next level management
- Ensure reports are accurate and complete
- Provide adequate resources to correct identified problems
- Implement corrective actions timely
- Validate outcomes

3.0.276.2.2
(08-01-2019)
Use of Submission Processing Scorecard Measure Process - Security and Internal Control

(1) Results of SP Scorecard Measure Process - Security and Internal Control reviews may not be used as the basis of evaluative recordation for bargaining employees.

3.0.276.2.2.1
(08-01-2019)
Roles and Responsibilities in the Submission Processing Scorecard Measure Process - Security and Internal Control

(1) The success of the SP Scorecard Measure Process - Security and Internal Control reviews depends on the participation of all the following:

- Wage and Investment, Submission Processing Headquarters staff
- Submission Processing Field Directors
- Submission Processing P&A Chiefs, Operation, Department and Frontline Managers
- Submission Processing Centers Designated Reviewer(s)

3.0.276.2.2.2
(08-01-2019)
W&I Submission Processing Headquarters Roles

(1) **HQ PM CQS** is the owner of the Security and Internal Control Review process. The responsibilities include but are not limited to:

a. Serving as a liaison between ATP Branch, PPB, SOI and the SP Centers.
b. Coordinating with SOI to update DCIs and instructions as well as monthly Scorecard results.
c. Distributing the monthly Scorecard to each SP Center.
d. Verifing that SP Centers have provided corrective actions for "**not met**" review components.
e. Providing SP Centers feedback for incomplete, unclear, and late documents.
f. Maintaining the Security Review SharePoint Site and providing access to the SharePoint site.
g. Distributing, updating, and coordinating, annual and ongoing updated documents related to the Security and Internal Control Review process and documents, which include:

- Appendix 1 - Summary of Scoring Rules
- Campus Report
- Custom Calendar Review Scheduler
- DCI and Instructions
- File Naming Scheme
- Internal Control Checklist
- Scoring Methodology

(2) **HQ ATP** Branch is the owner of the IRM Procedures listed below. The responsibilities include but are not limited to:

a. Notify HQ PMPA CQS of any yearly IRM updates that impacts Security and Internal Control Review process.
b. Provide timely feedback on Security and Internal Control Review documents and process.
c. Maintain current and accurate documents which include DCI and Internal Control Checklist:

- IRM 3.8.45, **Deposit Activity, Manual Deposit Process**
- IRM 3.8.46, **Deposit Activity, Discovered Remittance**
- IRM 3.8.47, **Manual Deposit for Field Office Payment Processing**
- IRM 3.17.79, **Accounting & Data Control, Accounting Refund Transactions**

(3) **HQ PPB** is the owner of the IRM procedures listed below. The responsibilities include but are not limited to:

a. Notify HQ PMPA CQS of any yearly IRM updates that impact the Security and Internal Control Review process.

b. Provide timely feedback on Security and Internal Control Review documents and process.
c. Maintain current and accurate documents which include DCI:

- IRM 3.10.72, **Campus Mail and Work Control, Receiving, Extracting, and Sorting**

(4) **HQ SOI** is the owner and will maintain the documents related to:

- Appendix 1 - Summary of Scoring Rules
- Custom Calendar Review Scheduler
- Data Capturing Instrument and Instructions

3.0.276.2.3
(08-01-2019)
Submission Processing Field Directors

(1) The SP Field Director at each SP Center must review the monthly Campus Report. Once review has been completed for accuracy and completeness the SP Field Directory will sign and date in the appropriate fields. Review the following field(s):

- **Repeat Findings/Vulnerabilities:** are Findings (Security Review) **"not met"** and/or Vulnerabilities (Internal Control Review coded as "no"). This includes ANY findings UNRESOLVED (corrective action has not corrected the Finding/Vulnerability) from a PRIOR period (month) or identified in one of the past three monthly reviews.
- **New Findings/Vulnerabilities:** Provide details of the New Findings (Security Review "not met") and/or Vulnerabilities (Internal Control Review coded as "no").
  This includes Findings/Vulnerabilities not identified in one of the past three monthly reviews.
- **Closed Findings/Vulnerabilities:** Provide details of the Closed Findings (Security Review "not met") and/or Vulnerabilities (Internal Control Review coded as "no").
  This includes Repeat or New Findings/Vulnerabilities from ALL prior Monthly reviews.

(2) The Campus Report MUST be signed and dated by those who conducted the review.

(3) If the SP Field Director has a designated actor who is authorized to sign on their behalf, include "acting" behind their name.

(4) The SP Field Director will return the signed and dated document to the SP Center's Designated Reviewer before the sixth day of the following month or the next business day.

(5) The SP Field Director will select an employee(s) of their choosing as the Designated Reviewer(s) who will have oversight of the Security and Internal Control Review.

3.0.276.2.4
(10-28-2020)
Submission Processing P&A Chiefs, Operations Department, and Frontline Managers

(1) SP P&A Chiefs, Operations, Department and Frontline Managers with oversight of these reviews must:

- Communicate the purpose of the review.
- Encourage employees and reviewers to partner to identify risks and improvements.

- Identify and recommend potential new processes and procedural changes that will improve work processes for any identified findings/ vulnerabilities. Procedural changes should be submitted via Servicewide Electronic Research Program (SERP) to the appropriate IRM analyst.
- Ensure feasible recommendations are presented to enhance procedural, policy, and system work practices.
- Elevate improvement process recommendations to those with oversight of the Security and Internal Control Reviews at the SP Center.
- Attend and assist with training on improvement methods.
- Ensure appropriate recommendations are implemented in a timely manner.
- Identify and communicate IRM procedures impacting the Security and Internal Control Review process to those with oversight of the Security and Internal Control Reviews at the SP Centers.
- Communicate Findings/Vulnerabilities identified on the Campus Report and monthly Scorecard in monthly meetings with the SP Field Director or their designated actor.
- Provide support to the SP Centers Designated Reviewer.
- Identify ways to timely and effectively communicate IRM updates to employees.

3.0.276.2.5
(12-27-2022)
Submission Processing Center Designated Reviewer(s)

(1) The Designated Reviewer(s) responsibilities include:

- Complete a monthly Security and Internal Control Review.
- Perform an unbiased, consistent, and accurate review of work.
- Code the appropriate **"met"** or **"not met"** (Security Review) and/or **"yes/no"** (Internal Control Review) of any processes not following IRM guidelines.
- Review IRM updates applicable to topics being reviewed.
- Provide timely documents to PMPA CQS.
- Communicate any IRM discrepancies or area's of concern with the PMPA CQS analyst when identified.
- Refer to the Security Review SharePoint site for all documents.

  Note: If access to the SharePoint site is needed, contact the PM CQS Analyst.

- Reviewers will document unauthorized disclosure in the comments section of the DCI using the keyword **"FLASH"** and advise the Operation that they must report the incident per IRM 3.0.276.1.7.1, *Protecting Taxpayer Data*. All **"FLASH"** related findings MUST be recorded on the monthly campus report.

  Note: DO NOT save any SP Centers information to the SharePoint Site. Save the document to the SP Centers designated file before inputting data to the document.

(2) **Time Reporting:** Designated Reviewers completing the Security and Internal Control Review will use time code 990-80101 to report their time.

(3) **Monthly Security and Internal Control Review Due Date:**

- The Security and Internal Control Review documents are due to PMPA CQS by the sixth day of the following month. If the sixth falls on a weekend the due date is the next business day.

Note: If an extension is needed contact the PMPA CQS analyst before the due date.

- The monthly Security and Internal Control Reviews **"MUST"** be completed during the current month.

(4) **Complete the following steps as part of the monthly Security Review Process:**

a. Complete the Custom Calendar Review Scheduler for the Security Review to randomly select days of review for each Review Component which includes option(s) to customize day, swing/night shifts, and weekends. The Custom Calendar Review Scheduler **"MUST"** be provided to SOI, ONLY if a weekend day is selected, and PMPA CQS the week prior to the start of the month.

Note: This tool is not used for the Internal Control Review

b. Complete review on the days designated by the Custom Calendar Review Scheduler.

Note: If review cannot be completed on the day selected by the Custom Calendar Review Scheduler do **"NOT "**skip the review. Select another day that the review can be completed and input a comment in the DCI. Do NOT re-run the Custom Calendar Review Scheduler.

c. Review each CP in the Review Component(s) for the corresponding DCI.

Note: The CP being reviewed relates to the IRM procedures. Use the corresponding DCI instructions available on the Security Review SharePoint Site to complete the DCI fields.

d. If a **"not met"** is identified on the DCI the reviewer must document the corrective action on one of the following area(s); the DCI main tab, additional comments tab, or the CP tab.

(5) **Complete the following steps as part of the monthly Internal Control Review Process:**

a. Complete the Internal Control Review using the Internal Control Checklist document.
b. Select a day to conduct the review.
c. Complete heading information which includes: Campus Reviewed, Month of Review and Year, and Name of Reviewer(s).
d. Select as appropriate, **"yes/no"**.

Note: A **"yes"** response indicates compliance. A **"no"** response indicates a deficiency, which **"MUST"** be addressed on the Monthly Campus Report.

e. If **"no"** was selected, a deficiency was identified and the reviewer **"MUST"** input a brief comment of what occurred to receive the **"no"** rating.

Note: Do not include PII when leaving a narrative.

(6) **After the Internal Control Checklist and the Security Reviews have been completed for the month, prepare the Campus Report with any Findings/ Vulnerabilities.**

- Repeat Findings **"(not met)"** - which includes ANY findings UNRESOLVED (corrective action has not corrected the Finding/Vulnerability) from PRIOR period (month) or identified in one of the past three monthly reviews.
- New Findings **"not met"**- provide details of the New Findings **"not met"**, which includes Findings not identified in one of the past three monthly reviews.
- Closed Findings **"not met"** - provide details of the Closed Findings **"not met"**, which includes Repeat or New Findings from ALL prior monthly reviews.

  Note: The closed findings will include **"not met"** for the current fiscal year (October - September).

- Reviewers **MUST** sign and date the Campus Report.
- Reviewers **MUST** secure SP Field Director's signature and date. If the SP Field Director has a designated actor who is authorized to sign on their behalf, include "acting" behind their name.

(7) **Documenting complete Monthly Security and Internal Control Review:**

- No later than the sixth day of the following month, email the corresponding documents for the Security and Internal Control Review to the appropriate PMPA CQS Analyst with oversight of the Security Reviews.

  Note: The PMPA CQS Analyst with oversight to Security Reviews can be located on the SP website, *Headquarter Directories, Program Management/Process Assurance, Coordination & Quality Support Section*.

(8) **Retention Standard** SP HQ and the SP Center may destroy these documents after five years if no further corrective acton is needed; however, longer retention is authorized if required by the business unit, per the *General Records Schedule 5.7 Item 020.*