

Information Technology Policy

System & Organization Controls (SOC) Correspondence Procedure

Number OPD-SEC040C	Effective Date January 27, 2020
Category Security	Supersedes OPD-BUS011C
Contact RA-ITCentral@pa.gov	Scheduled Review January 2024

1. Purpose

Ensure proper compliance, coordination and recordkeeping of Systems and Organization Controls (SOC) reports received from [Service Organizations](#) by requiring consistent and uniform communications by the responsible stakeholders.

2. Scope

This procedure applies to all departments, offices, boards, commissions, and councils under the Governor’s jurisdiction (hereinafter referred to as “agencies”). Agencies not under the Governor’s jurisdiction that utilize Commonwealth IT resources are strongly encouraged to use this as a guide to establish their own procedures.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Responsibilities

[Contract Managers](#) have overall responsibility for communication in a variety of appropriate means with the Service Organization as well as internal and external stakeholders impacted by the findings of the SOC reports. Contract Managers are required to save all SOC reports from the Service Organization, associated documentation, and [Formal Communications](#) in the designated folders in the [SOC Report Repository](#).

After receiving notification from the Contract Manager, IT is responsible for reviewing SOC reports that contain an IT element. IT is responsible for assisting the Contract Manager in the drafting of communications to the Service Organization for clarification, [Corrective Action Plans](#), internal and external stakeholder

communications and recommendations to agencies consuming the services described in the SOC reports.

Legal is responsible for assisting the Contract Manager in the drafting of communications to the Service Organization for clarification, Corrective Action Plans, internal and external stakeholder communications and recommendations to agencies consuming the services described in the SOC reports, if necessary.

4. Procedural Overview

The SOC reports identifies specific controls implemented by a Service Organization. Agency staff that have responsibilities in supplier management related to financial and/or IT services and systems have a vested interest in understanding the appropriate tasks and responses to these SOC reports.

The communication matrix listed in this document provides the format, frequency, purpose, and distribution of the communication between the Contract Manager and the Service Organization or Stakeholders.

The communication task description table in this document provides the flow of steps to be taken from receipt of the SOC reports to the external communication with stakeholders and outlines the owners of those tasks.

Communication Matrix

Communication Name	Purpose	Frequency	Format	Owner	Recipients	Consulted (if applicable)	SOC Report Repository
Acknowledgement of Receipt	Acknowledge receipt of SOC report and associated documentation	After receipt of SOC report email from SO	Email	CM & IT	Service Organization, SOC RA, and CM	IT and Legal	No
IT Review Communication	Sends communication to IT that a SOC report, which contains an IT element, is in the SOC Report Repository for their review	After determining if a SOC report contains an IT element	Email	CM	IT	IT and Legal	Yes
Acknowledgement of Review	IT acknowledgement of review of SOC report (with IT findings) and associated documentation	After receipt of SOC report email from CM	Internal Memo	IT	CM	CM and Legal	Yes
Clarification Request	Request for clarification of the SOC report and associated documentation	As needed	Form Letter	CM	Service Organization and SOC RA	IT and Legal	Yes
Corrective Action Plan Request	CAP which includes identifying the non-conformities, requirements and expectations and timeframes	As needed	Template	CM	Service Organization and SOC RA	IT and Legal	Yes
External Stakeholder Communication	Communication sent to external stakeholders impacted by findings from the SOC report	As needed	Form Letter	CM	Stakeholders and SOC RA	IT and Legal	Yes
Internal Stakeholder Communication	Communication sent to internal stakeholders impacted by findings from the SOC report	As needed	Internal Memo	CM	Stakeholders and SOC RA	IT and Legal	Yes
Memorandum of Record	A formal record of a conversation or meeting	As needed	Template	CM	Stakeholders and SOC RA	IT and Legal	Yes
Recommendation	Recommendation to Commonwealth agencies consuming the service described in the SOC report	After SOC report has been reviewed	Internal Memo	CM	Stakeholders and SOC RA	IT and Legal	Yes
SOC for Cybersecurity Request	Request for SO to send a SOC for Cybersecurity report	As needed	Form Letter	CM	Service Organization and SOC RA	IT and Legal	Yes

Table of Abbreviations

CM	Contract Manager
OB	Office of Budget
IT	Respective Chief Information Officer, Chief Technology Officer, Chief Information Security Officer
SO	Service Organization

Communication Tasks Description	Owner
Request to Service Organization for SOC for Cybersecurity report and carbon copy Resource Account.	CM
Service Organization provides SOC reports and associated documentation to Contract Manager and carbon copy Resource Account.	SO
Retrieves SOC documentation and adds to SOC Report Repository.	CM
Provides acknowledgement of receipt of SOC report and associated documentation to Service Organization.	CM
SOC report review and risk/impact evaluations.	CM
If there is an IT element, Contract Manager sends communication to appropriate IT stakeholder and carbon copy Resource Account.	CM
IT provides acknowledgement to the CM regarding their review of the SOC report and associated documentation, outlining concerns or recommendations based on their risk impact analysis.	IT
Coordination and follow-up with Service Organization for clarification of findings and/or proposed corrective actions.	CM
Coordinate internally with business and/or IT stakeholders to review findings, CAPs, resolution timeframes, assessing the risks/impacts and creating necessary communications and carbon copy Resource Account.	CM
Provides SOC reports, associated descriptions of systems and services and associated documentation to Auditor General’s Office for their review from SOC Report Repository.	OB
Recommendation provided to Commonwealth agencies consuming the service and carbon copy Resource Account.	CM
Communication sent to internal stakeholders impacted by the findings of the SOC report and carbon copy Resource Account.	CM
Communication sent to external stakeholders impacted by the findings of the SOC report and carbon copy Resource Account.	CM

5. Resources

6.1 SOC Report Repository

The SOC Report Repository is the centralized location for SOC reports and all Formal Communication to ensure the appropriate personnel are evaluating and acting to address issues or exceptions noted in the report. It is the Contract Managers responsibility to save SOC reports, associated documentation, and all Formal Communication in the repository.

The repository is organized by:

- Delivery Group
- Agency
- Service Organization
- Contract #
- Fiscal Year
- SOC report

6.2 SOC Resource Account

The [SOC Resource Account \(RA-OASOCReports@pa.gov\)](mailto:RA-OASOCReports@pa.gov) allows OA/OIT the ability to facilitate compliance with IT Policies and procedures and to update those IT Policies and procedures to align with changes to contract and supplier management procurement and legal guidelines, audits, standards, and industry best practices.

6. Authority

[Executive Order 2016-06](#) Enterprise Information Technology Governance

7. Publication Version Control

It is the [Authorized User's](#) responsibility to ensure they have the latest version of this publication, which appears on <https://itcentral.pa.gov> for Commonwealth personnel and on the Office of Administration public portal: <http://www.oa.pa.gov/Policies/Pages/default.aspx>. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

This chart contains a history of this publication's revisions.

Version	Date	Purpose of Revision
Original	01/27/2020	Base Document
Revision	11/10/2021	Changed OPD Number from BUS011 to SEC040 Changed Category from Business to Security Added Subservice Organizations to the document Moved OBs Task
Revision	01/06/2022	Removed Subservice Organization from the Purpose, Responsibilities, Procedural Overview and Communication Tasks
Revision	01/30/2023	No Changes – Updates to OPD-SEC040A only