pennsylvania
OFFICE OF ADMINISTRATION

# Information Technology Policy

## *System & Organization Controls (SOC) Correspondence Procedure*

| **ITP Number**<br>OPD-BUS011C | **Effective Date**<br>January 27, 2020 |
|---|---|
| **Category**<br>Business | **Supersedes**<br>-- |
| **Contact**<br>RA-ITCentral@pa.gov | **Scheduled Review**<br>January 2021 |

## 1. Purpose

The purpose of the SOC Correspondence Procedure is to 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, boards, commissions and councils under the Governor's jurisdiction. 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.

## 3. Definitions

**Contract Manager (CM) -** Individual responsible for managing the day-to-day activities of a contract post award.

**Corrective Action Plan (CAP)** - A detailed plan outlining a set of actions identified to remedy an unsatisfactory performance. A CAP includes time limits and goals.

**Formal Communication** - Communication in which the exchange of information is systematic, timely and done through the pre-defined channels. The communication conforms to established rules, standards and processes. Formal communication includes but is not limited to request for clarification, corrective action plan, request for SOC reports and recommendations to Commonwealth agencies.

**SOC 1 Type II Report** - A report on controls at a Service Organization relevant to internal controls over financial transactions and reporting. The report focuses on the suitability of the design and operating effectiveness of the controls to achieve objectives throughout a specific reporting period.

**SOC 2 Type II Report** - A report that focuses specifically on IT controls of a system as they relate to relevant Trust Service Principles. The report, based upon and inclusive of auditors' opinions, indicates whether controls placed in operation were suitably designed to meet or exceed the criteria of each relevant Trust Service Principle and whether those controls operated effectively for the reporting period.

**SOC 3 Type II Report** - A version of the SOC 2 Type II Report that omits detailed test results and is intended for general public distribution. SOC 3 report is required during the RFP technical evaluation to provide assurances on the internal controls over financial reporting or IT controls relevant to the Trust Service Principles or cybersecurity risk management.

**SOC for Cybersecurity -** A report that focuses on controls within a Service Organization Cybersecurity Risk Management Program and the suitability of the design of controls to meet cybersecurity objectives.

**SOC report repository –** A repository that hosts relevant artifacts to be utilized by authorized Commonwealth employees' task with managing SOC reports and official correspondence relating to the SOC reports.

**SOC resource account (SOC RA)** - The resource account allows OA/OIT to view incoming SOC report emails to monitor for IT elements and verify the Contract Manager is forwarding on to the appropriate IT group for review.

**Service Organization (SO) -** An external party engaged to perform operational processes for the Commonwealth, such as, but not limited to, accounting and payroll processing, security services or health care claims processing.

**Trust Service Principles**

- *Security* - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information.
- *Availability* – Information and systems are available for operation and used as committed or agreed.
- *Processing Integrity* – Systems processing is complete, valid, accurate, timely, and authorized.
- *Confidentiality* – Information designated as confidential is protected as committed or agreed.
- *Privacy* – Personal information is collected, used, retained, disclosed, and disposed in conformity with the commitments in the privacy notice.

## 4. 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, associated documentation and formal communications in the designated folders in the SOC report repository.

IT is responsible for reviewing SOC reports that contain an IT element. They are responsible for assisting the Contract Manager in the drafting of communication 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 communication 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.

## 5. Procedural Overview

The SOC reports review 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 |
| **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 & 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 |

| 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 |
| Provides SOC reports and associated documentation to Auditor General's Office for their review from SOC Report Repository | OB |
| SOC report review and risk/impact evaluations | CM |
| If there is an IT element, Contract Manager sends 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 |
| 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 |

## 6. Resources

**6.1 SOC Report Repository** (https://itcentral.pa.gov/Pages/SOC_Reports.aspx (*Limited Access*)) 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** (RA-OASOCReports@pa.gov) allows OA/OIT to view incoming SOC reports and verify the appropriate IT stakeholders review and provide communication support to the Contract Managers when responding to the Service Organizations. The resource account will also allow IT to track SOC reports to verify the Service Organization is sending the reports in a timely manner. It is the Contract Managers responsibility to carbon copy the SOC Resource Account on all formal communication.

## 7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

## 8. Publication Version Control

It is the 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.

| Version | Date | Purpose of Revision | Redline Link |
|---|---|---|---|
| Original | 01/27/2020 | Base Document | N/A |