pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

System & Organization Controls (SOC) Reporting Procedure

ITP Number	Effective Date
OPD-BUS011B	January 27, 2020
Category	**Supersedes**
Business	--
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	January 2021

1. Purpose

Ensure the proper compliance, review, coordination, and recordkeeping of Systems and Organization Controls (SOC) reports received from Service Organizations as well as outline the responsibilities of stakeholders when evaluating the SOC reports and acting to address issues or exceptions noted in the SOC report.

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

Adverse Opinion - Is the most severe opinion that a Certified Public Accountant (CPA) firm can provide. Misleading or incomplete financial statements may lead auditors to give an Adverse Opinion. An Adverse Opinion in the context of a SOC report often means that the users cannot place any reliance on the Service Organization's system.

Assertions - A confident statement of fact or belief made by management regarding certain aspects of their business. Usually comprised of management's description of the system they are providing and how the system is designed and operating.

Complementary User Entity Controls ("CUEC") - Controls (for SOC 1 and SOC 2 reports) that management of the Service Organization assumes, in the design of the Service Organization's system, will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the Service Organization's system.

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

Cybersecurity Risk Management Program - Set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from security events that are not prevented.

Disclaimer Opinion - Is provided when auditors can't express an opinion. This typically occurs when a Service Organization does not provide the auditors with adequate information to render an opinion, in which the CPA firm may disclaim their opinion.

SOC Report Repository - Commonwealth internal and limited access repository for storing official SOC reports and all related correspondence.
https://itcentral.pa.gov/Pages/SOC_Reports.aspx

SOC 1 Type II Report - A report on 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 on a Service Organization 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 for Cybersecurity - A report on a Service Organization that focuses on controls within the Service Organization's Cybersecurity Risk Management Program and the suitability of the design of controls to meet cybersecurity objectives.

Standards for Attestation Engagements No. 18 (SSAE18) - An attestation standard whereby a Service Organization's auditor (i.e. CPA firm conducting the engagement) issues an opinion concerning a Service Organization's controls.

Service Organization - An entity that is external to the Commonwealth that provides services to the Commonwealth (also known as a user organization) that are part of the Commonwealth's information system.

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.

Qualified Opinions - An opinion given that either the internal controls were not designed or operating effectively for one or more control objectives included within a SOC 1 Type II Report or Trust Services Principle included within a SOC 2 Type II Report.

4. Procedural Overview

The SOC 1 and 2 reports review the specific controls implemented by a Service Organization, and through the tests and evaluations performed by the auditor provide transparency concerning the controls. The success or failure of these controls have a direct or indirect impact on the reputation, financial statements, and stability of the organization

that is the subject of the report(s). Agency staff that have responsibilities in supplier management related to financial and/or IT services and systems (i.e., contracts compliance, financial management, internal audit, IT service management and cybersecurity) have a vested interest in understanding the control structure of the Service Organization. Key elements for the protection of the system include granting authorized access (logical and physical) based on relevant needs, and preventing unauthorized access to the system, controls to prevent potential systems abuse as well as, alteration, destruction, and disclosure of information. It is important to determine whether the data hosted or processed at the Service Organization is secure and protected, and whether the Service Organization's system will be available for critical business operations.

An auditor's Qualified Opinions should be viewed by the appropriate stakeholders and in the context of the services that are provided to the user organization. The SOC reports provided by Service Organizations should be reviewed under a careful analysis to determine what risks are not mitigated due to control deficiencies. Qualified Opinions responses may require different actions. The Qualified Opinion may necessitate implementation of new controls. The Qualified Opinion may necessitate the user organization to find a new provider or Service Organization. The Qualified Opinion may not require any action. Context and risks of what can go wrong are the key considerations when evaluating a Qualified Opinion.

SOC for Cybersecurity examinations are designed to provide information to help users understand the Service Organization's management process for handling enterprise-wide cyber risks. Within the SOC for Cybersecurity, the Service Organization provides a narrative description of its current Cybersecurity Risk Management Program.

5. Prerequisites

Stakeholders required to review SOC reports should have knowledge of the following:

- SOC training and supplier management training
- Understanding of risk/impact assessments
- Knowledge of Service Organization contract owners and administrators
- Knowledge of Service Organizations that provided financial and/or information services to Commonwealth agencies and associated SOC reporting requirements
- Knowledge of the systems and/or services that are covered by the SOC report
- Knowledge of IT Points of Contact
- Understanding of financial and/or account controls for reviews/evaluations of SOC-1 reports
- Understanding of IT Controls for reviews/evaluations of SOC-2 reports or SOC -1 reports containing IT findings (i.e., administrative, physical and technical)
- Understanding NIST Critical Infrastructure Cybersecurity Framework for SOC for Cybersecurity reports
- Understanding ISO 270001/270002 for SOC for Cybersecurity reports

6. Procedures

Acronyms Table

Service Organization	SO
Contract Manager	CM
Office of Budget	OB
Information Technology program area	IT
Technology Business Office	TBO

6A.1 Procedural Tasks

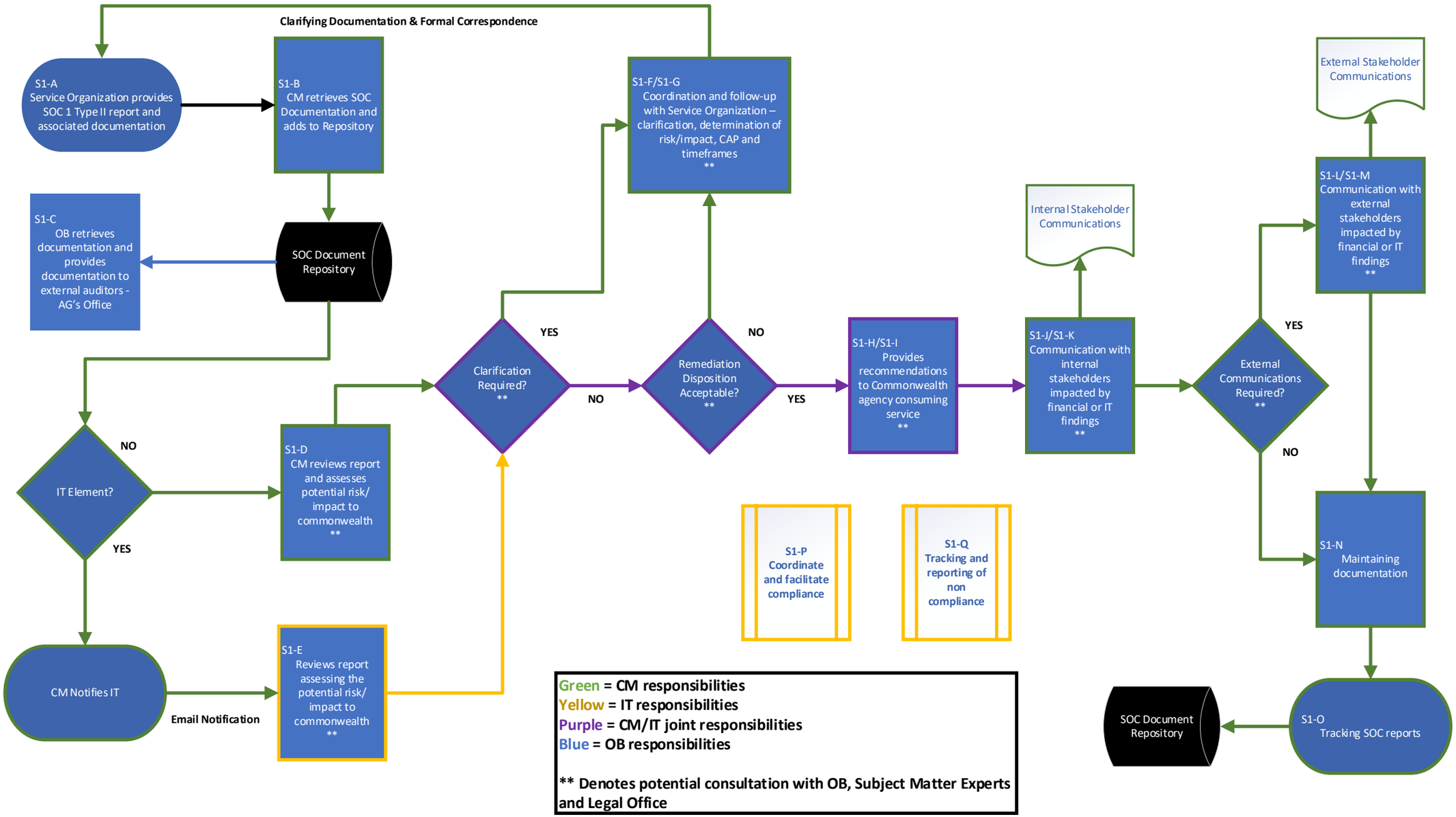
SOC 1-Type II Report

ID	Procedural Tasks Description	Owner
S1-A	Provide SOC 1-Type II Reports and associated description of systems and services (new & existing) to Contract Manager	SO
S1-B	Retrieves SOC 1-Type II documentation and adds to Repository	CM
S1-C	Provide SOC 1-Type II Reports and associated description of systems and services (new & existing) to Auditor General's Office for their review	OB
S1-D	SOC 1-Type II Report review and risk/impact evaluations (financial statement assertions, process control objectives, control deficiencies, disclosures, transaction flows, audit evidence, coverage period, service auditor's test of controls, Service Organization's corrective action plans, CUEC, carve-out reports, etc.)	CM
S1-E	SOC 1-Type II Report review and risk/impact evaluation with general computer control objectives and/or IT findings (IT audit evidence, IT control deficiencies, coverage period, service auditor's test of IT controls, Service Organization's corrective action plans, CUEC, carve-out reports, etc.)	IT
S1-F	Coordination and follow-up communications with Service Organization regarding SOC 1-Type II report financial/accounting findings: clarification and determination of financial risks/impacts to the Commonwealth and associated corrective action plans and timeframes	CM
S1-G	Coordination and follow-up communications with Service Organization regarding SOC 1-Type II IT findings clarification and determination of IT risks/impacts to the Commonwealth and associated corrective action plans and timeframes	CM
S1-H	Provide recommendations to Commonwealth agency consuming the service regarding the Service Organization's SOC 1-Type II Report findings regarding the suitability of the design and operating effectiveness of financial/accounting controls, corrective action plans, and remediation/resolution timeframes	CM
S1-I	Provide recommendations to Commonwealth agency consuming the service regarding the Service Organizations SOC 1-Type II Report findings regarding the suitability of the design and operating effectiveness of IT controls, corrective action plans, and remediation/resolution timeframes	IT
S1-J	Need to know communications to key internal stakeholders impacted by financial/accounting findings via appropriate channels, protocols, and governance (business/program areas, legal office, contract officer(s) and administrator, DGS, OB, etc.)	CM

S1-K	Need to know communications to key internal stakeholders impacted by SOC 1-Type II IT findings via appropriate channels, protocols, and governance (business/program areas, legal office, contract officer(s) and administrator, DC CIO, DC ISO, DGS, OB, OA/OIT, etc.)	CM
S1-L	Need to know communications to key external stakeholders impacted by financial/accounting findings via appropriate channels, protocols, and governance (business partners, service consumers, employees, citizens, service provider, independent auditors, etc.)	CM
S1-M	Need to know communications to key external stakeholders impacted by SOC 1-Type II IT findings via appropriate channels, protocols, and governance (business partners, service consumers, employees, citizens, service provider, independent auditors, etc.)	CM
S1-N	Maintaining documents and associated internal and external correspondence associated with SOC 1-Type II reports in compliance with records retention policy	CM
S1-O	Track reports	CM
S1-P	Facilitating compliance with IT Policies and procedures. Coordinating with stakeholders in establishing and implementing corrective actions for noncompliance incidents. Updating IT Policies and procedures to align with changes to contract and supplier management procurement and legal guidelines, audits, standards and industry best practices	TBO
S1-Q	Tracking and reporting incidents of noncompliance and resolution outcomes	TBO

6A.2 Workflow

SOC 1 Type II Report



6A.3 RACI

SOC 1-Type II Report

Procedural Task ID	Service Organization (SO)	Contract Manager (CM)	OA/OIT TBO	OA/OIT ISO	OA/OIT CTO	OA/OIT CIO	Legal	OB – Comptroller Audit Bureau
S1-A	A/R	I						I
S1-B		A/R						
S1-C								A/R
S1-D		A/R					C	C
S1-E		C	I	A/R	C	I	C	I
S1-F		A/R		C		C	C	C
S1-G		A/R	I	C	C	C	C	I
S1-H		A/R		I		I		C
S1-I			I	A/R	C	I		I
S1-J		A/R		C		C	C	I
S1-K		A/R	I	C	C	C	C	I
S1-L		A/R		I		I	C	I
S1-M		A/R	I	C	C	C	C	I
S1-N		A/R						
S1-O		A/R						
S1-P			A/R					
S1-Q			A/R					

6B.1 Procedural Tasks

Acronyms Table

Service Organization	SO
Contract Manager	CM
Office of Budget	OB
Information Technology program area	IT
Technology Business Office	TBO

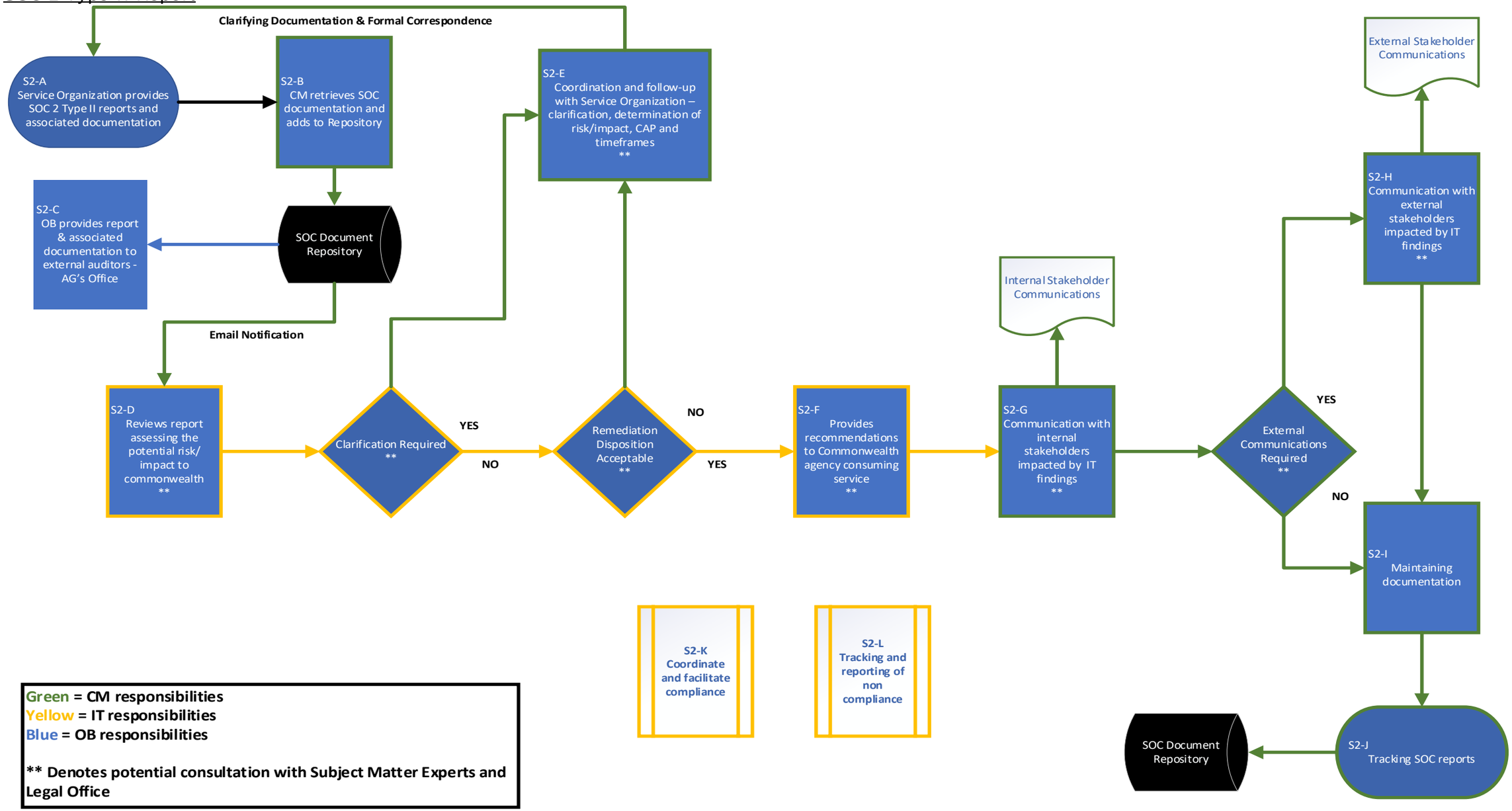
SOC 2-Type II Report

ID	Procedural Tasks Description	Owner
S2-A	Provide SOC 2-Type II Reports and associated description of systems and services (new & existing) to Contract Manager	SO
S2-B	Retrieves SOC 2-Type II documentation and adds to Repository	CM
S2-C	Provide SOC 2-Type II Reports and associated description of systems and services (new & existing) to Auditor General's Office for their review	OB
S2-D	SOC 2-Type II Report review and risk/impact evaluations (IT audit evidence, IT control deficiencies, coverage period, service auditor's test of IT controls relevant to security, availability, process integrity, confidentiality, or privacy, Service Organization's corrective actions, CUEC, carve-out reports, etc.)	IT
S2-E	Coordination and follow-up communications with Service Organization regarding SOC 2-Type II IT findings clarification and determination of IT risks/impacts to the Commonwealth and associated corrective action plans and timeframes	CM
S2-F	Provide recommendations to Commonwealth agency consuming the service regarding Service Organization's SOC 2-Type II IT findings regarding the suitability of the design and operating effectiveness of IT controls relevant to security, availability, process integrity, confidentiality, or privacy, corrective action plans, and remediation/resolution timeframes	IT
S2-G	Need to know communications to key internal stakeholders impacted by SOC 2-Type II IT findings via appropriate channels, protocols, and governance (business/program areas, legal office, contract officer(s) and administrator, DC CIO, DC ISO, DGS, OB, OA/OIT, etc.)	CM
S2-H	Need to know communications to key external stakeholders impacted by SOC 2-Type II IT findings via appropriate channels, protocols, and governance (business partners, service consumers, employees, citizens, service provider, independent auditors, etc.)	CM
S2-I	Maintaining documents and associated internal and external correspondence associated with SOC 2-Type II Reports in compliance with records retention policy	CM
S2-J	Track reports	CM
S2-K	Facilitating compliance with IT Policies and procedures. Coordinating with stakeholders in establishing and implementing corrective actions for noncompliance incidents. Updating IT Policies and procedures to align with changes to contracts and supplier management procurement and legal guidelines, audits, standards and industry best practices	TBO

S2-L	Tracking and reporting incidents of noncompliance and resolution outcomes	TBO

6B.2 Workflow

SOC 2 Type II Report



6B.3 RACI

SOC 2 Type II Report

Procedural Task ID	Service Organization (SO)	Contract Manager (CM)	OA/OIT TBO	OA/OIT ISO	OA/OIT CTO	OA/OIT CIO	Legal	OB – Comptroller Audit Bureau
S2-A	A/R	I						I
S2-B		A/R	I	I	I	I		
S2-C								A/R
S2-D		C	I	A/R	C	I	C	I
S2-E		A/R	I	C	C	C	C	I
S2-F			I	A/R	R	I		I
S2-G		A/R	I	C	C	C	C	I
S2-H		A/R	I	C	C	C	C	I
S2-I		A/R						
S2-J		A/R						
S2-K			A/R					
S2-L			A/R					

6C.1 Procedural Tasks

Acronyms Table

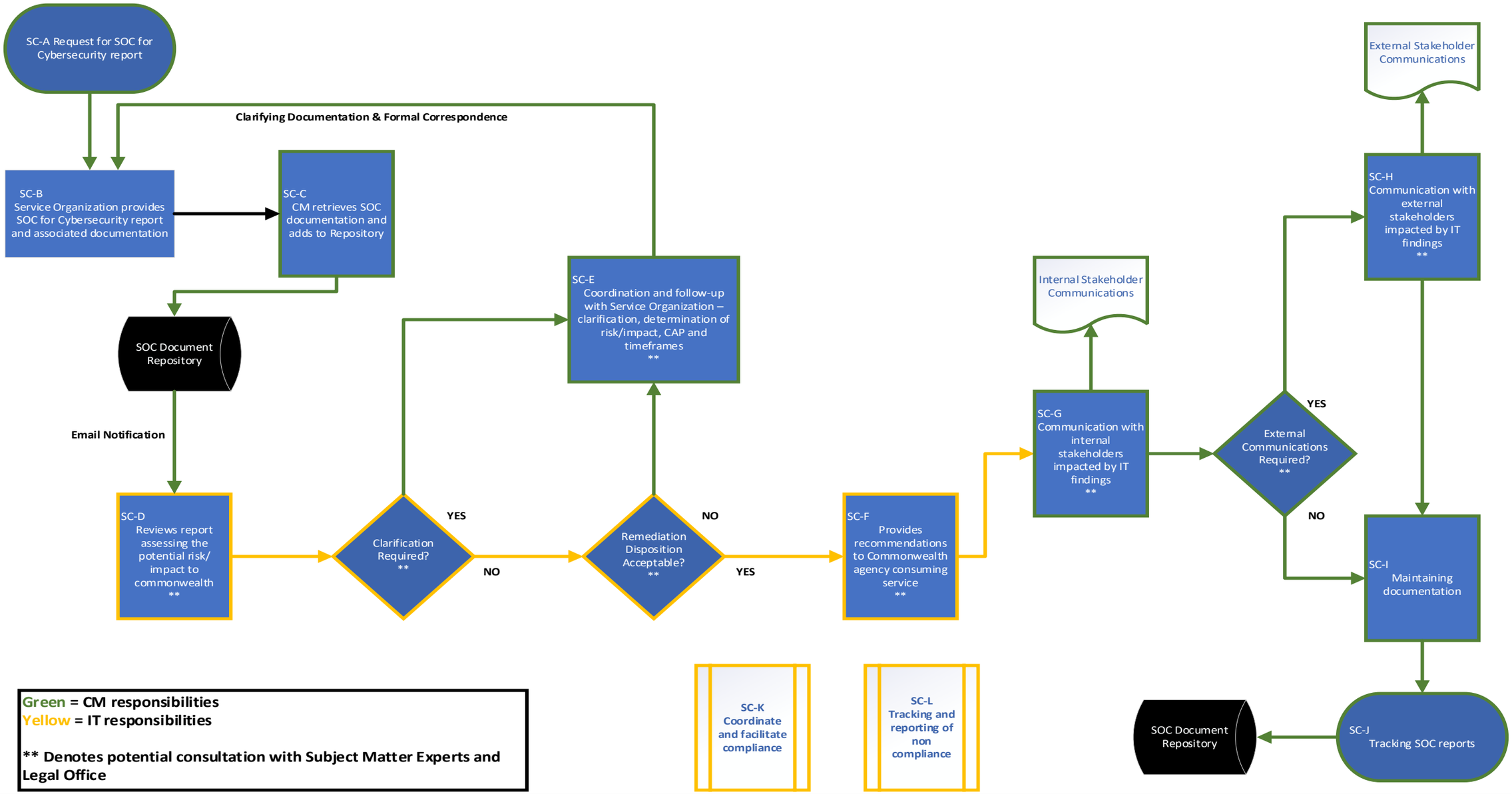
Service Organization	SO
Contract Manager	CM
Office of Budget	OB
Information Technology program area	IT
Technology Business Office	TBO

SOC for Cybersecurity

ID	Procedural Tasks Description	Responsible
SC-A	Request for SOC for Cybersecurity report	CM
SC-B	Provide SOC for Cybersecurity, description of Cybersecurity Risk Management Program (new & existing) to Contract Manager	SO
SC-C	Retrieves SOC documentation and adds to Repository	CM
SC-D	SOC for Cybersecurity review (Cybersecurity Risk Management Program effectiveness of controls relevant to Security, Availability, and Confidentiality and suitability of design)	IT
SC-E	Coordination and follow-up communications with Service Organization regarding SOC for Cybersecurity examination for clarification and determination of risks/impacts to the Commonwealth	CM
SC-F	Provide recommendations to Commonwealth agency consuming the services regarding the Service Organization's SOC for Cybersecurity examination	IT
SC-G	Need to know communications to key internal stakeholders impacted by SOC for Cybersecurity findings via appropriate channels, protocols, and governance (business/program areas, legal office, contract officer(s) and administrator, DC CIO, DC ISO, DGS, OB, OA/OIT, etc.)	CM
SC-H	Need to know communications to key external stakeholders impacted by SOC for Cybersecurity findings via appropriate channels, protocols, and governance (business partners, service consumers, employees, citizens, service provider, independent auditors, etc.)	CM
SC-I	Maintaining documents and associated internal and external correspondence associated with SOC for Cybersecurity in compliance with records retention policy	CM
SC-J	Track reports	CM
SC-K	Facilitating compliance with IT Policies and procedures. Coordinating with stakeholders in establishing and implementing corrective actions for noncompliance incidents. Updating IT Policies and procedures to align with changes to the contracts and supplier management procurement and legal guidelines, audits, standards and industry best practices	TBO
SC-L	Tracking and reporting incidents of noncompliance and resolution outcomes	TBO

6C.2 Workflow

SOC for Cybersecurity



6C.3 RACI

SOC for Cybersecurity

Procedural Task ID	Service Organization (SO)	Contract Manager (CM)	OA/OIT TBO	OA/OIT ISO	OA/OIT CTO	OA/OIT CIO	Legal	OB – Comptroller Audit Bureau
SC-A		A/R	I	C	C	C	C	
SC-B	A/R	I						
SC-C		A/R	I	I	I	I		I
SC-D		C	I	A/R	C	C	C	I
SC-E		A/R	I	C	C	C	C	I
SC-F			I	A/R	R	I		I
SC-G		A/R	I	C	C	C	C	I
SC-H		A/R	I	C	C	C	C	I
SC-I		A/R						
SC-J		A/R						
SC-K			A/R					
SC-L			A/R					

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