Information Technology Policy

System & Organization Controls (SOC) Reporting Procedure

Number
OPD-SEC040B

Effective Date
January 27, 2020

Category
Security

Supersedes
OPD-BUS011B

Contact
RA-ITCentral@pa.gov

Scheduled Review
July 2024

1. Purpose

The purpose of this document is to ensure the proper compliance, review, coordination, and recordkeeping of System 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. Procedural Overview

The SOC 1 and 2 reports review the specific controls implemented by a Service Organization and its Subservice Organizations, 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 Service 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 audits, 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 Commonwealth, 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 Commonwealth 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 and Subservice Organization's management process for handling enterprise-wide cyber risks. Within the SOC for Cybersecurity, the Service Organization provide a narrative description of its current Cybersecurity Risk Management Program.

3. 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;
- Knowledge of any relevant Subservice Organizations as they relate to the Service Organization and the services being provided;
- 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 of NIST Critical Infrastructure Cybersecurity Framework for SOC for Cybersecurity reports; and
- Understanding of ISO 270001/270002 for SOC for Cybersecurity reports.

4. Reporting Procedures

4.1 SOC 1-Type 2 Reports

A. Procedural Tasks

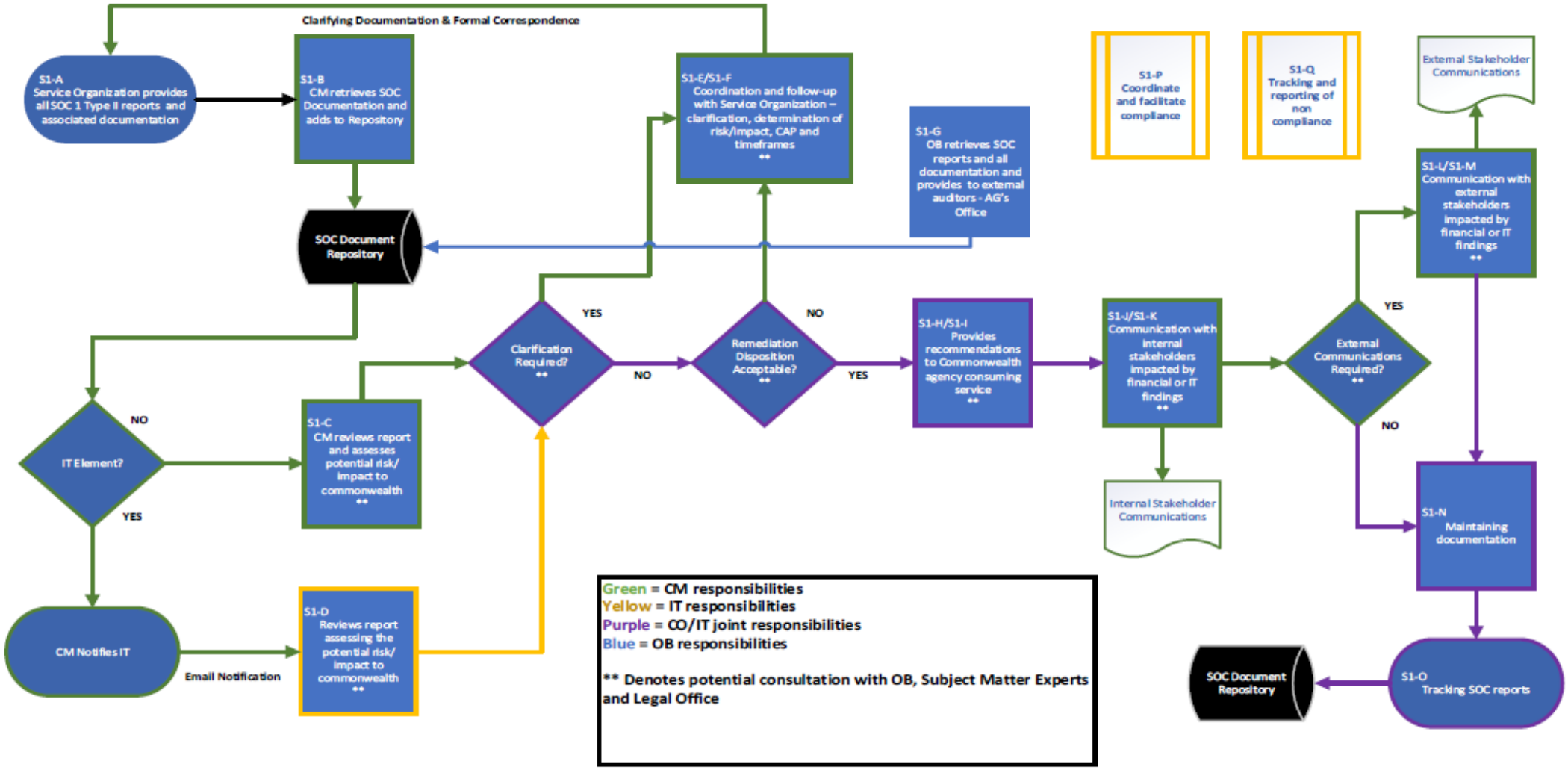
Acronyms Table

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

ID	Procedural Tasks Description	Owner
S1-A	Provides all SOC 1-Type 2 Reports and associated description of their systems and services (new & existing) and all associated documentation (cover letter, Service Organization's attestation, Independent Auditor's assertion, etc.) to Contract Manager.	SO
S1-B	Retrieves SOC 1-Type 2 documentation and adds to Repository.	CM
S1-C	SOC 1-Type 2 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 (and Subservice Organization, if applicable) Corrective Action Plans, CUEC, carve-out reports, etc.).	CM
S1-D	SOC 1-Type 2 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 (and Subservice Organization, if applicable) Corrective Action Plans, CUEC, carve-out reports, etc.).	IT
S1-E	Coordination and follow-up communications with Service Organization regarding SOC 1-Type 2 report financial/accounting findings: clarification and determination of financial risks/impacts to the Commonwealth and associated Corrective Action Plans and timeframes.	CM
S1-F	Coordination and follow-up communications with Service Organization regarding SOC 1-Type 2 IT findings clarification and determination of IT risks/impacts to the Commonwealth and associated Corrective Action Plans and timeframes.	CM
S1-G	Provide SOC 1-Type 2 Reports, associated description of systems and services (new & existing) and associated documentation (IT audit evidence, IT control deficiencies, coverage period, service auditor's test of IT controls, Service Organization's (and Subservice Organization, if applicable) Corrective Action Plans, CUEC, carve-out reports, etc.) to Auditor General's Office for their review.	OB
S1-H	Provide recommendations to Commonwealth agency consuming the service regarding the Service Organization's SOC 1-Type 2 Report findings regarding the suitability of the design and operating effectiveness of financial/accounting controls, Corrective Action Plans, and remediation or resolution timeframes.	CM
S1-I	Provide recommendations to Commonwealth agency consuming the service regarding the Service Organization's SOC 1-Type 2 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 2 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/IT, 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 2 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 2 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

B. Process Flow - SOC 1-Type 2 Report



C. RACI - SOC 1-Type 2 Report

Procedural Task ID	Service Organization (SO)	Contract Manager (CM)	OA/IT TBO	OA/IT ISO	OA/IT CTO	OA/IT CIO	Legal	OB – Comptroller Audit Bureau
S1-A	A/R	I						I
S1-B		A/R						
S1-C		A/R					C	C
S1-D		C	I	A/R	C	I	C	I
S1-E		A/R		C		C	C	C
S1-F		A/R	I	C	C	C	C	I
S1-G								A/R
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					

4.2 SOC 2-Type 2 Reports

A. Procedural Tasks

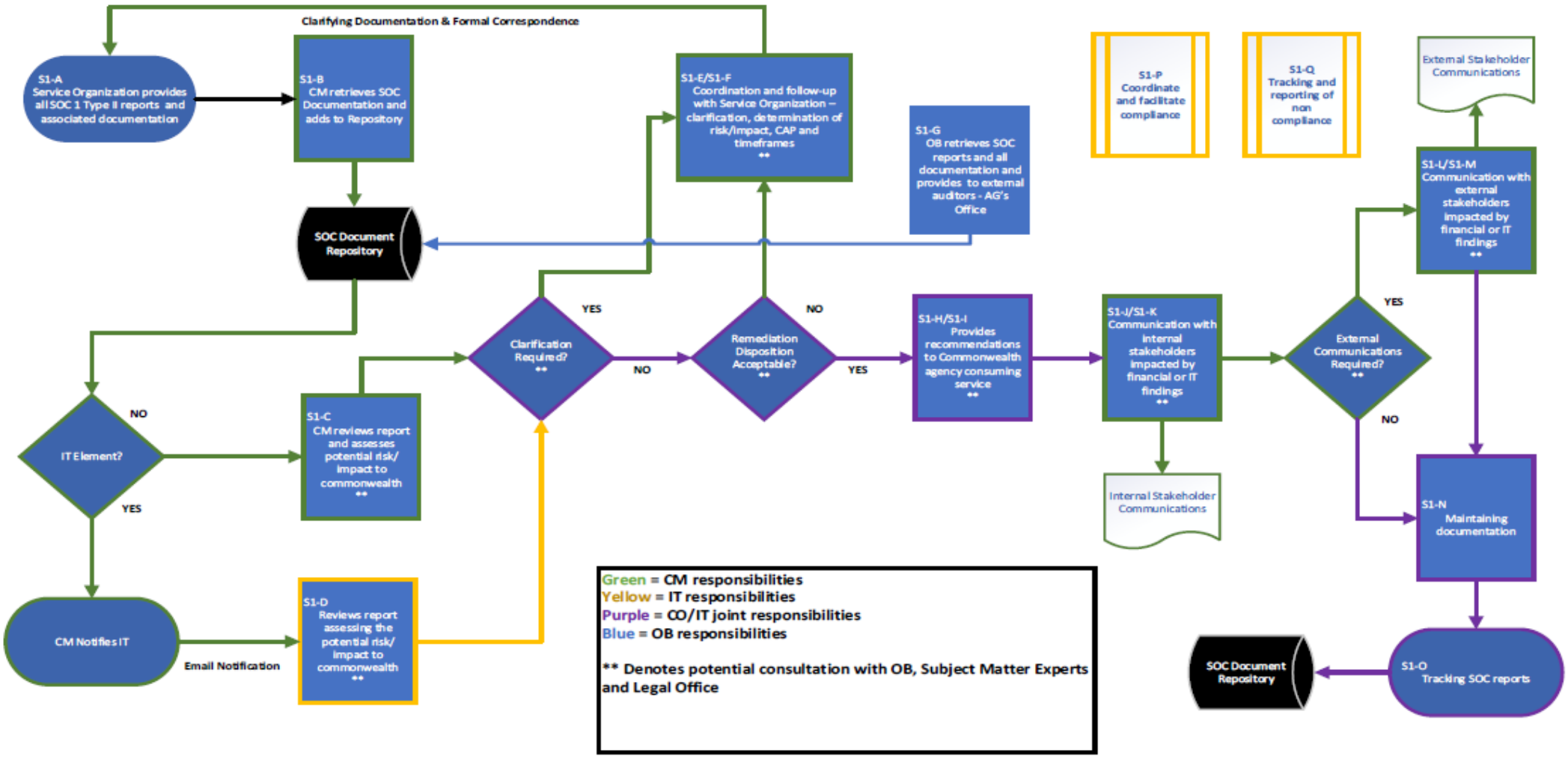
Acronyms Table

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

ID	Procedural Tasks Description	Owner
S2-A	Provides all SOC 2-Type 2 Reports and associated description of their systems and services (new & existing) and all associated documentation (cover letter, Service Organization's assertion, Independent Auditor's Report with their opinion, etc.) to Contract Manager.	SO
S2-B	Retrieves SOC 2-Type 2 documentation and adds to Repository.	CM
S2-C	SOC 2-Type 2 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 (and Subservice Organization, if applicable) Corrective Action Plans, CUEC, carve-out reports, etc.).	IT
S2-D	Coordination and follow-up communications with Service Organization regarding SOC 2-Type 2 IT findings clarification and determination of IT risks/impacts to the Commonwealth and associated Corrective Action Plans and timeframes.	CM
S2-E	Provide recommendations to Commonwealth agency consuming the service regarding Service Organization's SOC 2-Type 2 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-F	Provide SOC 2-Type 2 Reports, associated description of systems and services (new & existing) and associated documentation (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 (and Subservice Organization, if applicable) Corrective Action Plans, CUEC, carve-out reports, etc.) to Auditor General's Office for their review.	OB
S2-G	Need to know communications to key internal stakeholders impacted by SOC 2-Type 2 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/IT, etc.).	CM
S2-H	Need to know communications to key external stakeholders impacted by SOC 2-Type 2 IT findings via appropriate channels, protocols, and governance (business partners, service consumers, employees, citizens, service provider, independent auditors, etc.).	CM

ID	Procedural Tasks Description	Owner
S2-A	Provides all SOC 2-Type 2 Reports and associated description of their systems and services (new & existing) and all associated documentation (cover letter, Service Organization's assertion, Independent Auditor's Report with their opinion, etc.) to Contract Manager.	SO
S2-I	Maintaining documents and associated internal and external correspondence associated with SOC 2-Type 2 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

B. Process Flow - SOC 2-Type 2 Report



C. RACI – SOC 2-Type 2 Report

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

4.3 SOC for Cybersecurity

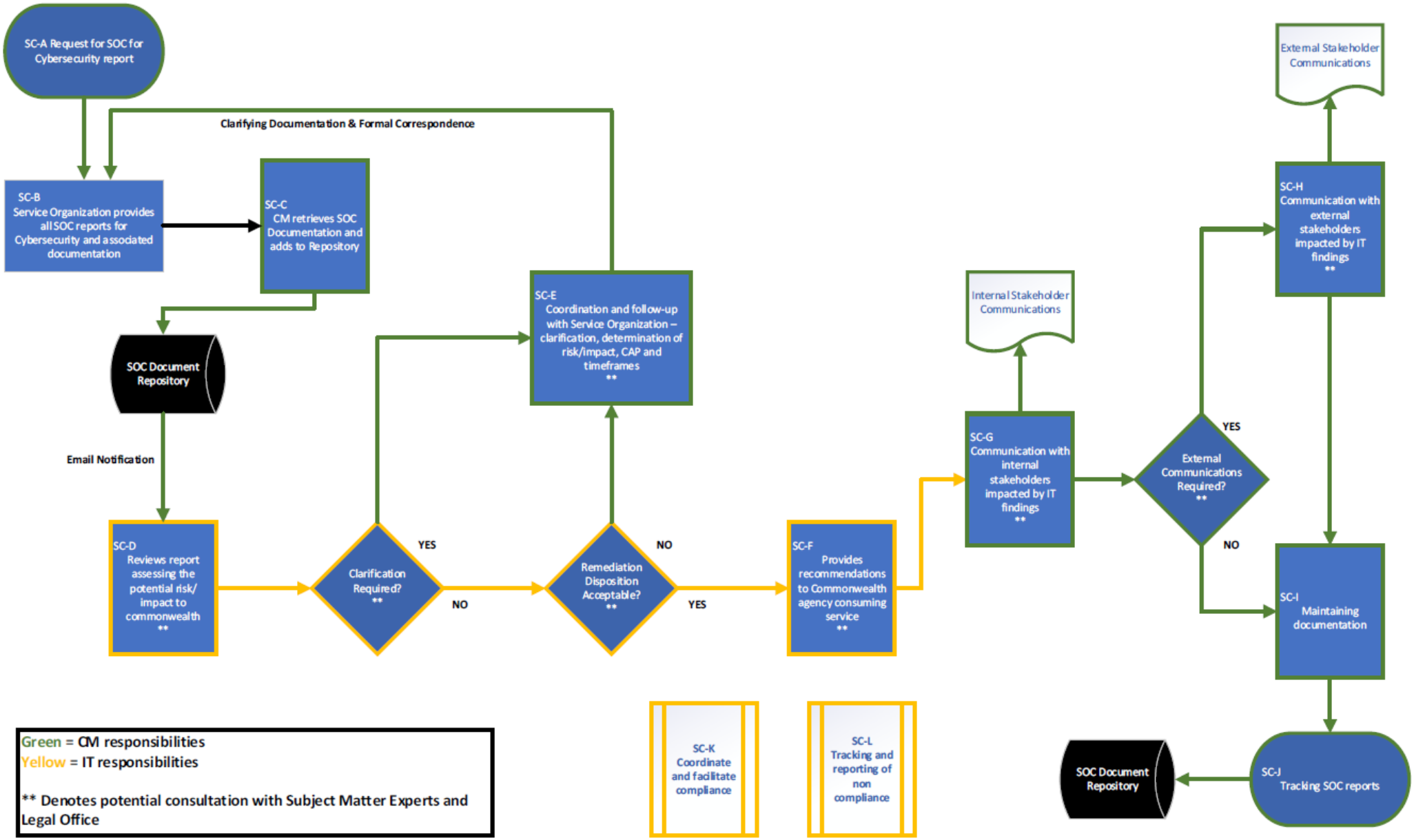
A. Procedural Tasks

Acronyms Table

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

ID	Procedural Tasks Description	Responsible
SC-A	Request for SOC for Cybersecurity report.	CM
SC-B	Provides SOC for Cybersecurity, description of Cybersecurity Risk Management Program (new & existing) and associated documentation to Contract Manager.	SO
SC-C	Retrieves SOC documentation and adds to Repository.	CM
SC-D	SOC for Cybersecurity review of Service Organization (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/IT, 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

B. Process Flow – SOC for Cybersecurity



C. RACI – SOC for Cybersecurity

Procedural Task ID	Service Organization (SO)	Contract Manager (CM)	OA/IT TBO	OA/IT ISO	OA/IT CTO	OA/IT 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					

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	Change OPD Number from BUS011B to SEC040B Changed Category from Business to Security Added Subservice Organization to definition section Added Subservice Organization to Procedural Tasks Moved OB's tasks for SOC 1 Type 2 and SOC 2 Type 2 Updated Visio documents
Revision	01/06/2022	Removed Subservice Organization from the Purpose and Procedural Tasks
Revision	07/18/2023	Replaced definitions with links to glossary Removed scope, authority, and publication version control sections consistent with other OPD documents