# TABLE OF CONTENTS


| Chapter | | Paragraph |
|---|---|---|
| 1 | Introduction and Background | .01-.77 |
| | Introduction | .01-.06 |
| | Intended Users of a SOC 2® Report | .07-.13 |
| | Overview of a SOC 2® Examination | .14-.17 |
| | Contents of the SOC 2® Report | .18-.49 |
| | Definition of a System | .19 -.20 |
| | Boundaries of the System | .21-.23 |
| | Time Frame of Examination | .24 |
| | Difference Between Privacy and Confidentiality | .25-.26 |
| | Criteria for a SOC 2® Examination | .27-.43 |
| | The Service Organization's Service Commitments and System Requirements | .44-.49 |
| | SOC 2® Examination That Addresses Additional Subject Matters and Additional Criteria | .50-.54 |
| | SOC 3® Examination | .55-.58 |
| | Other Types of SOC Examinations: SOC Suite of Services | .59-.68 |
| | SOC 1®—SOC for Service Organizations: ICFR | .60-.62 |
| | SOC for Cybersecurity | .63-.68 |
| | Professional Standards | .69-.76 |
| | Attestation Standards | .70-.72 |
| | Code of Professional Conduct | .73 |
| | Quality in the SOC 2® Examination | .74-.76 |
| | Definitions | .77 |
| 2 | Accepting and Planning a SOC 2® Examination | .01-.172 |
| | Introduction | .01-.02 |
| | Understanding Service Organization Management's Responsibilities | .03-.29 |
| | Management Responsibilities Prior to Engaging the Service Auditor | .04-.25 |
| | Management Responsibilities During the Examination | .26-.28 |
| | Management's Responsibilities During Engagement Completion | .29 |
| | Responsibilities of the Service Auditor | .30 |
| | Engagement Acceptance and Continuance | .31-.34 |
| | Independence | .35-.38 |
| | Competence of Engagement Team Members | .39-.42 |
| | Preconditions of a SOC 2® Engagement | .43-.65 |
| | Determining Whether the Subject Matter Is Appropriate for the SOC 2® Examination | .44-.48 |
| | Determining Whether Management Is Likely to Have a Reasonable Basis for Its Assertion | .49-.56 |

| Chapter | | Paragraph |
|---|---|---|
| 2 | Accepting and Planning a SOC 2® Examination—continued | |
| | Assessing the Suitability and Availability of Criteria | .57-.58 |
| | Assessing the Appropriateness of the Service Organization's Principal Service Commitments and System Requirements Stated in the Description | .59-.65 |
| | Requesting a Written Assertion and Representations From Service Organization Management | .66-.69 |
| | Agreeing on the Terms of the Engagement | .70-.90 |
| | Accepting a Change in the Terms of the Examination | .75-.78 |
| | Additional Considerations for a Request to Extend or Modify the Period Covered by the Examination | .79-.90 |
| | Establishing an Overall Examination Strategy for and Planning the Examination | .91-.109 |
| | Planning Considerations When the Inclusive Method Is Used to Present the Services of a Subservice Organization | .96-.103 |
| | Considering Materiality During Planning | .104-.109 |
| | Performing Risk Assessment Procedures | .110-.126 |
| | Obtaining an Understanding of the Service Organization's System | .110-.119 |
| | Assessing the Risk of Material Misstatement | .120-.126 |
| | Considering Entity-Level Controls | .127-.131 |
| | Understanding the Internal Audit Function | .132-.136 |
| | Planning to Use the Work of Internal Auditors | .137-.153 |
| | Evaluating the Competence, Objectivity, and Systematic Approach Used by Internal Auditors | .139-.144 |
| | Determining the Extent to Which to Use the Work of Internal Auditors | .145-.147 |
| | Coordinating Procedures With the Internal Auditors | .148-.152 |
| | Evaluating Whether the Work of Internal Auditors Is Adequate for the Service Auditor's Purposes | .153 |
| | Planning to Use the Work of an Other Practitioner | .154-.159 |
| | Planning to Use the Work of a Service Auditor's Specialist | .160-.166 |
| | Accepting and Planning a SOC 3® Examination | .167-.172 |
| 3 | Performing the SOC 2® Examination | .01-.229 |
| | Designing Overall Responses to the Risk Assessment and Obtaining Evidence | .01-.11 |
| | Considering Materiality in Responding to the Assessed Risks and Planning Procedures | .05-.08 |
| | Defining Misstatements in This Guide | .09-.11 |
| | Obtaining and Evaluating Evidence About Whether the Description Presents the System That Was Designed and Implemented in Accordance With the Description Criteria | .12-.78 |
| | The Service Organization's Service Commitments and System Requirements | .24-.29 |




 

| Chapter | | Paragraph |
|---|---|---|
| 3 | Performing the SOC 2® Examination—continued | |
| | Disclosures About Individual Controls | .30-.32 |
| | Disclosures About System Incidents | .33-.35 |
| | Disclosures About Complementary User Entity Controls and User Entity Responsibilities | .36-.41 |
| | Disclosures Related to Subservice Organizations | .42-.51 |
| | Disclosures About Complementary Subservice Organization Controls | .52-.54 |
| | Disclosures About Significant Changes to the System During the Period Covered by a Type 2 Examination | .55-.56 |
| | Changes to the System That Occur Between the Periods Covered by a Type 2 Examination | .57-.58 |
| | Procedures to Obtain Evidence About the Description | .59-.63 |
| | Considering Whether the Description Is Misstated or Otherwise Misleading | .64-.68 |
| | Identifying and Evaluating Description Misstatements | .69-.71 |
| | Materiality Considerations When Evaluating Whether the Description Is Presented in Accordance With the Description Criteria | .72-.78 |
| | Obtaining and Evaluating Evidence About the Suitability of the Design of Controls | .79-.105 |
| | Additional Considerations for Subservice Organizations | .88-.91 |
| | Multiple Controls Are Necessary to Address an Applicable Trust Services Criterion | .92-.93 |
| | Multiple Controls to Achieve the Service Organization's Service Commitments and Service Requirements Based on the Same Applicable Trust Services Criterion | .94 |
| | Procedures to Obtain Evidence About the Suitability of Design of Controls | .95-.100 |
| | Identifying and Evaluating Deficiencies in the Suitability of Design of Controls | .101-.105 |
| | Obtaining and Evaluating Evidence About the Operating Effectiveness of Controls in a Type 2 Examination | .106-.114 |
| | Designing and Performing Tests of Controls | .110-.114 |
| | Nature of Tests of Controls | .115-.130 |
| | Evaluating the Reliability of Information Produced by the Service Organization | .121-.130 |
| | Timing of Tests of Controls | .131-.133 |
| | Extent of Tests of Controls | .134-.139 |
| | Testing Superseded Controls | .140-.141 |
| | Using Sampling to Select Items to Be Tested | .142-.146 |
| | Selecting Items to Be Tested | .145-.146 |
| | Additional Considerations Related to Risks of Vendors and Business Partners | .147-.151 |
| | Additional Considerations Related to CSOCs | .152-.155 |
| | Considering Controls That Did Not Need to Operate During the Period Covered by the Examination | .156 |

| Chapter | | Paragraph |
|---|---|---|
| 3 | Performing the SOC 2® Examination—continued | |
| | Identifying and Evaluating Deviations in the Operating Effectiveness of Controls | .157-.160 |
| | Materiality Considerations When Evaluating the Suitability of Design and Operating Effectiveness of Controls | .161-.165 |
| | Using the Work of the Internal Audit Function | .166-.177 |
| | Using the Work of a Service Auditor's Specialist | .178-.180 |
| | Revising the Risk Assessment | .181 |
| | Evaluating the Results of Procedures | .182-.189 |
| | Responding to and Communicating Known and Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, and Deficiencies in the Design or Operating Effectiveness of Controls | .190-.196 |
| | Known or Suspected Fraud or Noncompliance With Laws or Regulations | .190-.192 |
| | Communicating Incidents of Known or Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, or Internal Control Deficiencies | .193-.196 |
| | Obtaining Written Representations | .197-.212 |
| | Requested Written Representations Not Provided or Not Reliable | .209-.211 |
| | Representations From the Engaging Party When Not the Responsible Party | .212 |
| | Subsequent Events and Subsequently Discovered Facts | .213-.220 |
| | Subsequent Events Unlikely to Have an Effect on the Service Auditor's Report | .220 |
| | Documentation | .221-.225 |
| | Considering Whether Service Organization Management Should Modify Its Assertion | .226-.229 |
| 4 | Forming the Opinion and Preparing the Service Auditor's Report | .01-.119 |
| | Responsibilities of the Service Auditor | .01-.03 |
| | Forming the Service Auditor's Opinion | .04-.14 |
| | Concluding on the Sufficiency and Appropriateness of Evidence | .05-.09 |
| | Considering Uncorrected Description Misstatements and Deficiencies | .10-.12 |
| | Expressing an Opinion on Each of the Subject Matters in the SOC 2® Examination | .13-.14 |
| | Describing Tests of Controls and the Results of Tests in a Type 2 Report | .15-.30 |
| | Describing Tests of Controls and Results When Using the Internal Audit Function | .23-.27 |
| | Describing Tests of the Reliability of Information Produced by the Service Organization | .28-.30 |
| | Preparing the Service Auditor's SOC 2® Report | .31-.41 |
| | Elements of the Service Auditor's SOC 2® Report | .31-.32 |




 

| Chapter | | Paragraph |
|---|---|---|
| 4 | Forming the Opinion and Preparing the Service Auditor's Report—continued | |
| | Requirement to Restrict the Use of the SOC 2® Report | .33-.35 |
| | Reporting When the Service Organization's Design of Controls Assumes Complementary User Entity Controls | .36-.38 |
| | Reporting When the Service Organization Carves Out the Controls at a Subservice Organization | .39-.41 |
| | Reporting When the Service Auditor Assumes Responsibility for the Work of an Other Practitioner | .42 |
| | Modifications to the Service Auditor's Report | .43-.67 |
| | Qualified Opinion | .51-.53 |
| | Adverse Opinion | .54-.55 |
| | Scope Limitation | .56-.60 |
| | Disclaimer of Opinion | .61-.67 |
| | Report Paragraphs Describing the Matter Giving Rise to the Modification | .68-.88 |
| | Illustrative Separate Paragraphs When There Are Material Misstatements in the Description | .68-.78 |
| | Illustrative Separate Paragraphs: Material Deficiencies in the Suitability of Controls | .79-.82 |
| | Illustrative Separate Paragraphs: Material Deficiencies in the Operating Effectiveness of Controls | .83-.88 |
| | Other Matters Related to the Service Auditor's Report | .89-.93 |
| | Emphasis-of-Matter Paragraphs and Other-Matter Paragraphs | .89-.90 |
| | Distribution of the Report by Management | .91-.93 |
| | Service Auditor's Recommendations for Improving Controls | .94 |
| | Other Information Not Covered by the Service Auditor's Report | .95-.104 |
| | Illustrative Type 2 Reports | .105-.106 |
| | Preparing a Type 1 Report | .107-.109 |
| | Forming the Opinion and Preparing a SOC 3® Report | .110-.119 |
| | Elements of the SOC 3® Report | .110-.115 |
| | Elements of the Service Auditor's Report | .116-.118 |
| | Illustrative SOC 3® Management Assertion and Service Auditor's Report | .119 |
| | Supplement A—2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report | |
| | Supplement B—2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy | |
| Appendix | | |
| A | Information for Service Organization Management | |
| B | Comparison of SOC 1®, SOC 2®, and SOC 3® Examinations and Related Reports | |

Appendix

C Illustrative Comparison of a SOC 2® Examination and Related Report With the Cybersecurity Risk Management Examination and Related Report

D

D-1 Illustrative Management Assertion and Service Auditor's Report for a Type 2 Examination (Carved-Out Controls of a Subservice Organization and Complementary Subservice Organization and Complementary User Entity Controls)

D-2 Illustrative Service Organization and Subservice Organization Management Assertions and Service Auditor's Report for a Type 2 Examination (Subservice Organization Presented Using the Inclusive Method and Complementary User Entity Controls)

D-3 Illustrative Service Auditor's Report for a Type 2 Examination in Which the Service Auditor Disclaims an Opinion Because of a Scope Limitation

D-4 Illustrative Type 2 Report (Including Management's Assertion, Service Auditor's Report, and the Description of the System)

E Illustrative Management Assertion and Service Auditor's Report for a Type 1 Examination

F Illustrative Management Assertion and Service Auditor's Report for a SOC 3® Examination

G

G-1 Illustrative Management Representation Letter for Type 2 Engagement

G-2 Illustrative Management Representation Letter for Type 1 Engagement

H Performing and Reporting on a SOC 2® Examination in Accordance With International Standards on Assurance Engagements (ISAEs) or in Accordance With Both the AICPA's Attestation Standards and the ISAEs

I Definitions

Index of Pronouncements and Other Technical Guidance

Subject Index